GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

COBIT® 4.1

Edizione in lingua italiana

Modello

Obiettivi di controllo

Linee guida per la gestione

Modelli di maturità

IT Governance Institute®

L'IT Governance Institute (ITGI™) (www.itgi.org) è stato fondato nel 1998 per sviluppare la cultura e gi standard internazionali per la direzione ed il controllo della funzione IT delle imprese. Un efficace governo dell'IT aiuta ad assicurare che la funzione IT contribuisca al raggiungimento degli obiettivi aziendali, ottimizzi gli investimenti aziendali nell'IT, e gestisca adeguatamente le opportunità tecnologiche ed i relativi rischi. ITGI propone ricerche originali, pubblicazioni in formato elettronico, casi di studio, per aiutare i leader delle imprese ed i consigli di amministrazione nel far fronte alle loro responsabilità per quanto riguarda l'IT Governance.

Disclaimer

ITGI (il "Proprietario") ha sviluppato e prodotto questa pubblicazione, intitolata COBIT®4.1 (il "Prodotto"), innanzitutto come una risorsa formative per i direttori della funzione IT, l'alta direzione, i responsabili intermedi della funzione IT, i professional del controllo. Il Proprietario non assicura alcun risultato dovuto all'utilizzo del Prodotto o di una sua parte. Il Prodotto non deve essere considerato come comprensivo di tutte le informazioni, procedure e test relativi ai controlli, o alternativo ad altre informazioni, procedure e test che ragionevolmente possono permettere di ottenere lo stesso risultato. Nel determinare l'applicabilità di ciascuna specifica informazione, procedura o test, i CIO, l'alta direzione, i responsabili intermedi della funzione IT, i professional del controllo devono valutare, sotto la propria responsabilità, la particolare circostanza influenzata dallo specifico sistema o dallo specifico ambito tecnologico.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

COBIT® 4.1
Printed in the United States of America

RINGRAZIAMENTI

IT Governance Institute desidera ringraziare:

Gli Esperti che hanno realizzato e rivisto questa pubblicazione

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgio
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgio
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgio
Steven De Haes, University of Antwerp Management School, Belgio
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgio
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgio
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, Sud Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, Nuova Zelanda
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguai
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Svizzera
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgio
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgio
Gary Hardy, IT Winners, Sud Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgio
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA

RINGRAZIAMENTI (SEGUITO)

Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Danimarca
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., Sud Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portogallo
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Danimarca
Jaco Sadie, Sasol, Sud Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgio
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgio
Johan Van Grieken, CISA, Deloitte, Belgio
Greet Volders, Voquals NV, Belgio
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgio
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

Il Consiglio di Amministrazione di ITGI
Everett C. Johnson, CPA, Deloitte & Touche LLP (in ritiro), USA, Presidente Internazionale
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice Presidente
William C. Boni, CISM, Motorola, USA, Vice Presidente
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice Presidente
Jean-Louis Leignel, MAGE Conseil, France, Vice Presidente
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice Presidente
Howard Nicholson, CISA, City of Salisbury, Australia, Vice Presidente
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice Presidente
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Precedente Presidente Internazionale
Robert S. Roussey, CPA, University of Southern California, USA, Precedente Presidente Internazionale
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Consigliere

Il Comitato per l'IT Governance
Tony Hayes, FCPA, Queensland Government, Australia, Presidente
Max Blecher, Virtual Alliance, Sud Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

Il Comitato strategico di COBIT

Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA, Presidente
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgio
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgio
Rafael Eduardo Fabius, CISA, República AFAP SA, Uruguai
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Svizzera
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgio
Gary Hardy, IT Winners, Sud Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgio
Robert E. Stroud, CA Inc., USA

I Consulenti di ITGI
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Presidente
Roland Bader, F. Hoffmann-La Roche AG, Svizzera
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, Francia
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Gli Enti affiliati ad ITGI e gli Sponsor

I Capitoli di ISACA
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
FIDA Inform
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

Il Gruppo di Ricerca, del Capitolo di Milano, per la traduzione in lingua italiana:
Orillo Narduzzo, CGEIT, CISA, CISM, Banca Popolare di Vicenza
Stefano Niccolini, CISA, CISM, Federazione Lombarda BCC
Leonardo Nobile, CISA, Deloitte
Alberto Piamonte, KeyMap Team
Marco Salvato, CGEIT, CISA, CISM, Generali Business Solutions
Giulio Spreafico, CGEIT, CISA, CISM, Studio Spreafico

SOMMARIO

Le appendici, ad eccezione del Glossario, si trovano nella versione originale in lingua inglese.

Ogni commento su COBIT 4.1 è benaccetto. Per inoltrare eventuali commenti utilizzare il seguente indirizzo www.isaca.org/COBITfeedback.

SINTESI PER LA DIREZIONE

Per molte imprese, l'informazione e la tecnologia che la supporta rappresentano il bene più prezioso, ma spesso il meno compreso. Le imprese di successo invece riconoscono il contributo positivo dell'Information Technology e lo utilizzano per accrescere il valore per gli stakeholder. Queste imprese, inoltre, comprendono e gestiscono i rischi associati, come la crescente esigenza di conformità alle normative e la dipendenza critica di molti processi aziendali dall'Information Technology (IT).

Il bisogno di garanzie sul valore generato dall'IT, la gestione dei rischi correlati all'IT ed i sempre maggiori requisiti relativi al controllo sulle informazioni sono finalmente compresi come elementi chiave per la gestione dell'impresa. Valore, rischio e controllo costituiscono la parte centrale dell'IT Governance.

Il governo dell'IT è responsabilità dei dirigenti e del Consiglio di Amministrazione ed è costituita da una direzione (leadership), da una struttura organizzativa e da processi che assicurano che l'IT di un'impresa sostenga e sviluppi le strategie e gli obiettivi aziendali.

Inoltre, l'IT Governance integra e istituzionalizza le best practice che assicurano che l'IT supporti gli obiettivi aziendali. Il governo dell'IT aiuta l'impresa a trarre il massimo beneficio dal proprio sistema informativo, massimizzando i benefici, cogliendo le opportunità ed acquisendo vantaggi competitivi. Tali risultati richiedono un framework per il controllo dell'IT che sia coerente e supporti sia l'Internal Control – Integrated Framework predisposto dal Committee of Sponsoring Organization of the Treadway Commission's (COSO's), cioè il quadro di riferimento per il controllo ampiamente accettato per il governo dell'impresa e la gestione del rischio, sia analoghi modelli conformi ad esso.

Le aziende devono assicurare che il proprio patrimonio informativo soddisfi i requisiti di qualità, affidabilità e sicurezza, così come avviene per tutti i loro beni. Il management, inoltre, deve ottimizzare l'uso delle risorse IT disponibili che comprendono i sistemi applicativi, le informazioni, le infrastrutture ed il personale. Per far fronte a tali responsabilità, come pure per perseguire i propri obiettivi, il management deve conoscere lo stato dell'architettura informatica della propria impresa e decidere quale livello di governo e di controllo intenda assicurare.

Il *Control Objectives for Information and related Technology* (COBIT®) fornisce le cosiddette good practice in un quadro di riferimento fatto di domini e di processi e presenta le attività in una struttura gestibile e logica. Le good practice contenute in COBIT sono condivise dagli esperti e riguardano principalmente il controllo piuttosto che gli aspetti operativi. Tali prassi possono aiutare ad ottimizzare gli investimenti nell'IT, ad assicurare l'erogazione dei servizi ed a fornire un metro di valutazione per capire quando le cose non vanno per il verso giusto.

Perché l'IT sia in grado di erogare i propri servizi con successo rispetto ai requisiti aziendali, il management deve adottare un modello per il sistema di controllo interno. Il framework di controllo proposto in COBIT risponde a tali necessità attraverso:
- l'individuazione di un collegamento con i requisiti aziendali;
- la strutturazione delle attività IT secondo un modello di processo generalmente accettato;
- l'identificazione delle principali risorse IT su cui fare leva;
- l'individuazione del livello di controllo atteso.

L'orientamento al business di COBIT si estrinseca nel collegare gli obiettivi tipici aziendali con quelli IT, nel fornire metriche e modelli di strutturazione per misurare il perseguimento di questi obiettivi, nell'identificare le responsabilità attribuite alle persone di riferimento dei processi aziendali e dei processi IT.

L'approccio per processi di COBIT è illustrato da un modello che suddivide l'IT in 4 domini e 34 processi coerente con le aree di responsabilità relative a pianificazione, realizzazione, erogazione e monitoraggio, fornendo una visione completa dell'IT. Il concetto di architettura aziendale aiuta ad identificare le risorse essenziali per il successo dei processi, cioè le applicazioni, le informazioni, l'infrastruttura ed il personale.

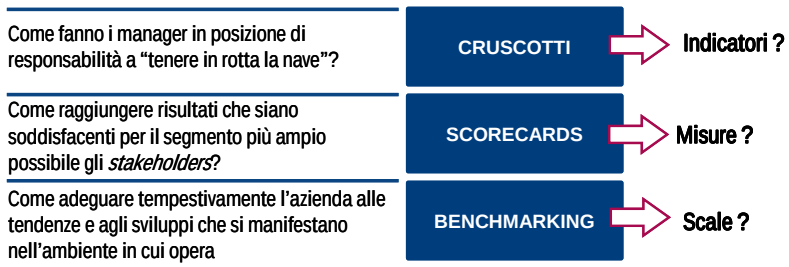
Riassumendo, al fine di fornire le informazioni di cui l'azienda ha bisogno per raggiungere i propri obiettivi, le risorse IT devono essere gestite da un insieme di processi naturalmente raggruppati.

Ma l'impresa, come tiene l'IT sotto controllo in modo che esso fornisca le informazioni di cui l'impresa stessa necessita? Come gestisce il rischio e mantiene sicure le risorse IT da cui è così dipendente? Come fa l'impresa ad assicurare che l'IT raggiunga i propri obiettivi nel mentre supporta il business?

Innanzitutto, il management ha bisogno di obiettivi di controllo che individuino gli obiettivi finali che derivano dall'implementare politiche, piani e procedure, strutture organizzative tali da garantire con ragionevole certezza che:
- gli obiettivi aziendali siano raggiunti,
- gli eventi indesiderati siano evitati o rilevati e corretti/superati.

In secondo luogo, vista la complessità delle situazioni, il management è costantemente alla ricerca di informazioni sintetiche e tempestive che gli permettano prendere velocemente ed efficacemente le difficili decisioni in materia di valore aggiunto, rischi e controlli. Ma cosa deve essere misurato, e come? Le imprese necessitano di una misura oggettiva della situazione attuale e delle aree di miglioramento, e hanno bisogno di strumenti direzionali per monitorare tale miglioramento.

Figura 1 – Informazioni per il Management



La **Figura 1** mostra alcune domande frequenti e gli strumenti informativi utilizzati dal management per avere le risposte, ma questi cruscotti hanno bisogno di indicatori, le scorecard hanno bisogno di misure, ed il benchmarking ha bisogno di una scala di confronto.

Come gestiscono l'azienda i manager responsabili? Come può l'impresa raggiungere risultati che siano soddisfacenti per la maggior parte degli stakeholder? CRUSCOTTO SCORECARDS Indicatori? BENCHMARKING Misure? Scale? brevi a sviluppi ed evoluzioni **che-Figura 1** – Informazioni per il Management Come può l'impresa adattarsi in tempi avvengono nel suo settore? Una risposta a queste richieste di determinare e monitorare l'appropriato livello di controllo e di performance per l'IT si trova nelle definizioni che COBIT fornisce per:

- il Benchmarking delle capacità e delle performance dei processi IT, espresso in termini di modelli di strutturazione, derivati dal Software Engineering Institut Ès Capability Maturity Model (CMM);
- gli obiettivi e le metriche dei processi IT per stabilire e misurare i loro risultati e le loro performance, basati sui principi della balanced business scorecard di Robert Kaplan e David Norton;
- gli obiettivi delle attività per tenere sotto controllo questi processi, basati sugli obiettivi di controllo di COBIT.

La valutazione della capacità dei processi basata sui modelli di strutturazione di COBIT è una parte cruciale dell'implementazione dell'IT Governance. Dopo aver identificato i processi ed i controlli IT critici, l'utilizzo dei modelli di strutturazione consente di identificare e riportare al management le opportunità di miglioramento della capacità di questi processi. Per portare questi processi al grado di capacità desiderato si possono poi sviluppare specifici piani di azione.

COBIT è pertanto funzionale alla definizione di un sistema di IT Governance (**Figura 2**) perché fornisce un modello per assicurare che:

- l'IT sia allineato con le strategie dell'azienda;
- l'IT consenta la gestione delle funzioni aziendali e ne massimizzi i benefici;
- le risorse IT siano usate responsabilmente;
- i rischi IT siano gestiti opportunamente.

La misurazione delle performance è essenziale per il governo dell'IT. Tale attività è supportata da COBIT ed include la definizione ed il monitoraggio di obiettivi misurabili relativi ai servizi (risultati attesi) dei processi IT e alle modalità di erogazione (capacità e performance del processo). Diverse indagini hanno identificato che la carenza di trasparenza nei costi, nel valore e nei rischi dell'IT è uno dei fattori più importanti che porta all'introduzione dell'IT Governance. Infatti, la trasparenza si raggiunge principalmente attraverso la misurazione delle performance, mentre le altre aree forniscono solo un contributo.

Figura 2 – Le Aree dell'IT Governance

L'allineamento strategico mira ad assicurare il collegamento tra i piani aziendali ed i piani dell'IT; a definire, mantenere e convalidare il valore dell'offerta dell'IT; ad allineare l'operatività dell'IT con quella aziendale.

L'erogazione del valore si riferisce alla realizzazione dell'offerta (value proposition) nel ciclo operativo, assicurando che l'IT produca i benefici promessi rispetto agli obiettivi strategici, concentrandosi sull'ottimizzazione dei costi e dimostrando il valore intrinseco dell'IT.

La gestione delle risorse è relativa all'individuazione degli investimenti migliori ed alla gestione più appropriata delle risorse IT ritenute critiche: applicazioni, informazioni, infrastrutture e risorse umane. Le principali questioni riguardano l'ottimizzazione della gestione delle conoscenze e dell'infrastruttura.

La gestione del rischio richiede consapevolezza dei rischi da parte dell'alta direzione aziendale, una chiara visione della propensione al rischio dell'impresa, la coscienza dei requisiti di conformità, la trasparenza rispetto ai rischi aziendali più significativi ed all'attribuzione responsabilità di risk management all'interno dell'organizzazione.

La misurazione delle prestazioni traccia e controlla l'implementazione della strategia, il completamento dei progetti, l'utilizzo delle risorse, la performance dei processi e l'erogazione del servizio, utilizzando, per esempio, balanced scorecard che traducono la strategia in azioni per il raggiungimento di obiettivi misurabili ben oltre la valutazione contabile convenzionale.

Le aree in cui è suddivisa l'IT Governance descrivono gli ambiti che l'alta direzione deve considerare per gestire l'IT all'interno dell'azienda. La gestione operativa utilizza dei processi per organizzare e gestire le attività IT di tutti i giorni. COBIT fornisce un modello generalizzato che rappresenta tutti i processi normalmente presenti nelle strutture IT, fornendo un modello di riferimento comune che possa essere compreso sia dai manager dell'IT sia dai manager degli altri settori aziendali. Il modello dei processi di COBIT è stato mappato sulle aree dell'IT Governance (vedi appendice II) creando un collegamento fra le informazioni per la gestione, che servono ai manager più operativi, e quelle che sono attese dall'alta direzione per il governo.

Per conseguire una governance efficace, la direzione si aspetta che i controlli vengano definiti dai manager operativi all'interno di uno schema di riferimento predefinito e valido per tutti i processi IT. Gli obiettivi di controllo dell'IT previsti da COBIT sono organizzati per processi. Pertanto il modello fornisce un chiaro legame tra i requisiti di governance, i processi ed i controlli dell'IT.

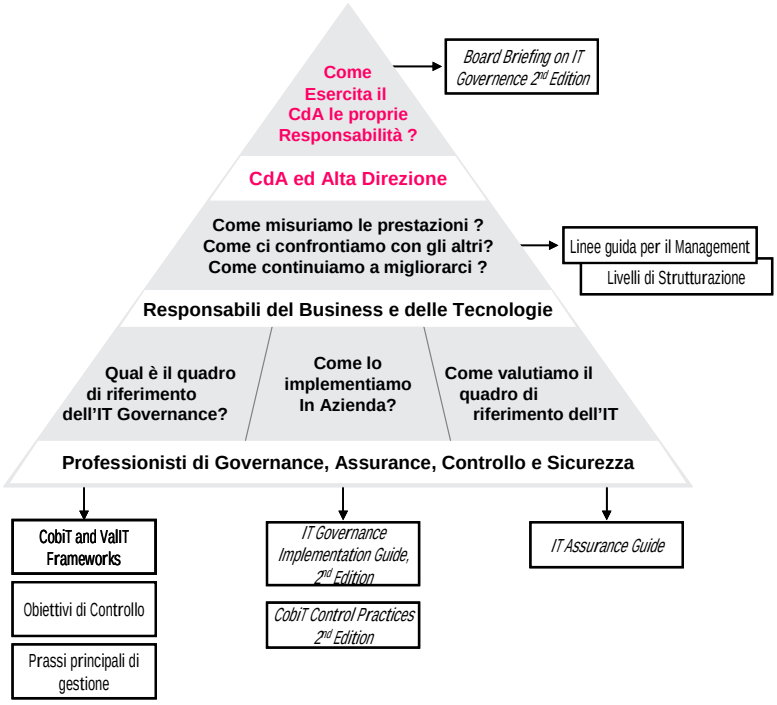
COBIT mira a definire gli aspetti necessari per conseguire un adeguato livello gestionale e di controllo dell'IT ed ha un approccio di alto profilo. COBIT è stato allineato ed armonizzato con altri più dettagliati standard e best-practice di riferimento per l'IT (vedi appendice IV) e funge da integratore di queste differenti linee guida, sintetizzando i principali obiettivi sotto un unico cappello che funge da modello e che è collegato anche con i requisiti aziendali e di governance.

COSO (e analoghi schemi di riferimento per la conformità) è generalmente accettato come il modello per il controllo interno delle imprese. COBIT è il modello per il controllo interno dell'IT generalmente accettato.

Le componenti di COBIT sono struttura- te su tre livelli (vedi **figura 3**) progetta- ti per aiutare:
- l'alta direzione e il consiglio di amministrazione,
- i manager dell'IT e degli altri settori aziendali,
- i professional che si occupano di governance, assurance, controllo e sicurezza.

In sintesi, fra le componenti di COBIT vi sono:

Figura 3 – Schema dei contenuti di COBIT



Lo schema dei prodotti basati sul framework COBIT illustra i prodotti generalmente applicabili e i ruoli principalmente coinvolti. Oltre a questi prodotti, ve ne sono altri sviluppati per specifiche esigenze (*IT Control Objectives for Sarbanes- Oxley, 2nd Edition*), per particolari ambiti quali la sicurezza (*COBIT Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), o per specifiche tipologie di imprese (COBIT Quickstart si rivolge alle piccole o medie imprese oppure alle grandi imprese che vogliono puntare direttamente sull'adozione di un modello di IT Governance pervasivo).

- Board Briefing on IT Governance, 2nd Edition – Aiuta i dirigenti a comprendere perchè è importante il governo dell'IT, quali sono le sue problematiche e quale è la loro responsabilità nel gestirlo.

- Management Guidelines, Maturity models – Aiuta ad attribuire le responsabilità, misurare le performance, confrontarsi con gli altri e superare i punti di debolezza relativi alla capacità produttiva dei processi.

- Framework – Struttura gli obiettivi di governo dell'IT e le best-practice in domini e processi IT e li collega ai requisiti aziendali.

- Control objectives – Presenta un elenco completo di requisiti di alto livello che deve essere considerato dai responsabili per controllare efficacemente ciascun processo IT.

- IT Governance Implementation Guide: Using COBIT® and Val IT™ , 2nd Edition – Fornisce un percorso generalizzato per implementare il governo dell'IT utilizzando le componenti di COBIT e di Val IT.

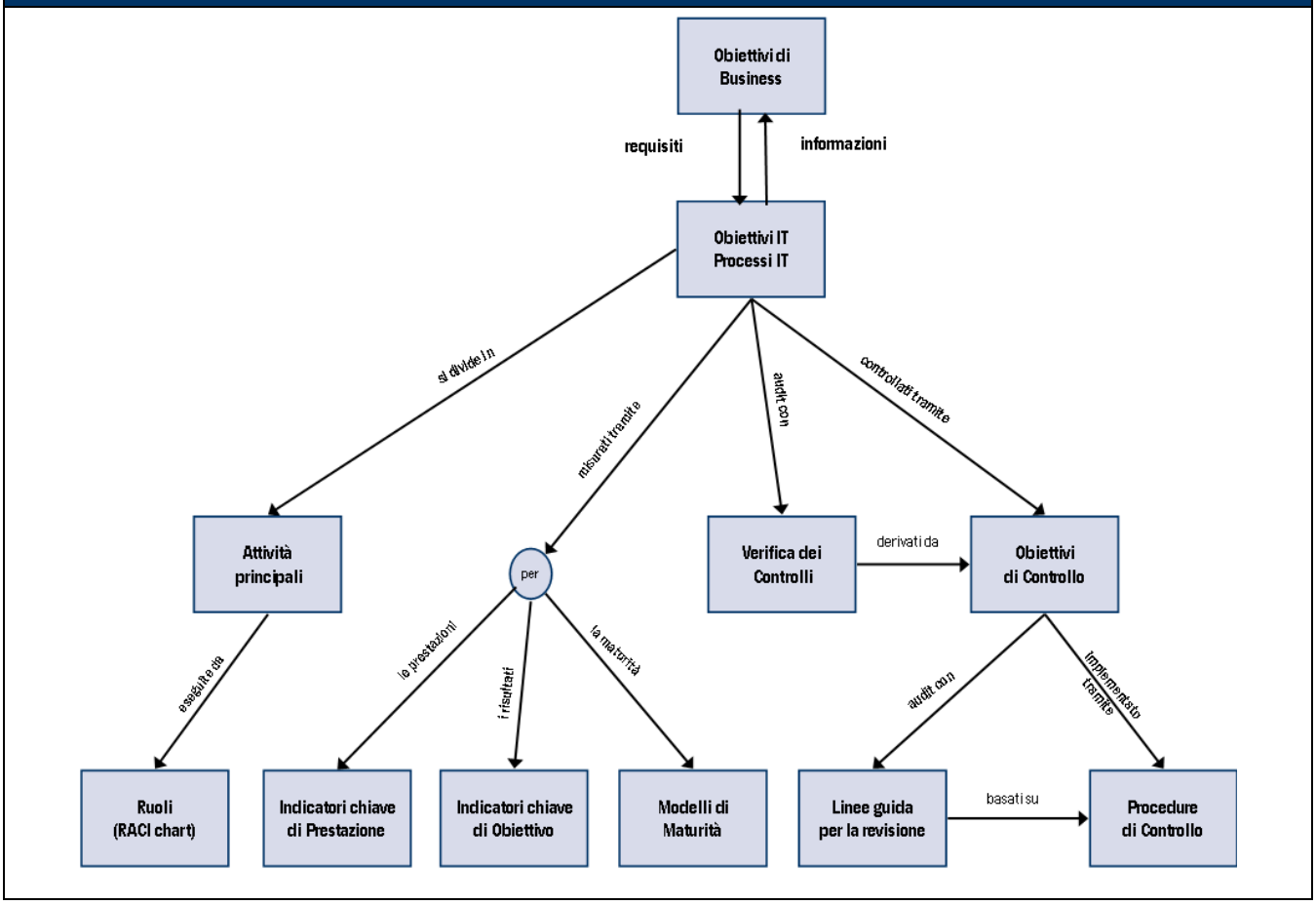
- COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition – È una guida per motivare l'introduzione dei controlli e per individuare le modalità più opportune per realizzarli

- IT Assurance Guide: Using COBIT® – Fornisce delle linee guida su come COBIT può essere usato per facilitare un'ampia gamma di attività di verifica, in particolare per gli opportuni test relativi a tutti i processi IT ed i loro obiettivi di controllo.

Le componenti di COBIT sono illustrate nella **figura 3** che evidenzia i principali utenti, le loro problematiche riguardanti l'IT Governance e le componenti che sono generalmente utilizzabili per fornire una risposta. Nella figura vi sono ulteriori componenti specifiche per particolari ambiti quali la sicurezza o le PMI.

Tutte queste componenti di COBIT, con le loro interrelazioni ed il loro supporto alle diverse funzioni aziendali per esigenze di governance, gestione, controllo e verifica, sono illustrate nella **figura 4**.

Figura 4 – Le relazioni fra le componenti di COBIT



COBIT è costituito da un modello e da un insieme di strumenti di supporto che consentono al management di colmare il divario esistente tra requisiti di controllo, le problematiche tecniche e i rischi aziendali, e di comunicare tale livello di controllo agli stakeholder. COBIT rende possibile lo sviluppo di politiche chiare e di good practice per il controllo dell'IT nelle aziende. COBIT è continuamente aggiornato ed armonizzato con gli altri standard e le e le altre linee guida. Per questa ragione, COBIT è divenuto sia l'integratore per le best-practice nell'IT sia il
quadro generale di riferimento per la governance dell'IT, che aiuta a comprendere e gestire i rischi ed i benefici dell'IT.
La struttura per processi di COBIT ed il suo approccio di alto livello orientato al business forniscono una visione completa dell'IT e delle decisioni che devono essere prese in merito.

Obiettivi di Business requisiti Obiettivi IT Processi IT Attività principali Ruoli (RACI chart) Indicatori di prestazione Misura dei risultati Livello di strutturazione (Maturity Model) informazioni Verifica dei controlli Obiettivi di Linee guida per la revisione controllo COBIT Pratiche di controllo si divide in derivate da eseguite da prestazioni risultati strutturazione audit con controllati da Implementati con monitorati con misurato da ottenuti da **Figura 4** – Le relazioni fra le componenti di COBIT I benefici derivanti dall'utilizzo di COBIT come schema di riferimento per il governo dell'IT comprendono:

- un migliore allineamento, grazie ad uno stretto collegamento con la realtà aziendale,
- una visione di cosa fa l'IT in termini comprensibili da parte del management,
- una chiara assegnazione delle proprietà e delle responsabilità, basata su un approccio orientato ai processi,
- una generale accettazione da parte di terzi e degli organi di vigilanza,
- una condivisione delle conoscenze fra tutti gli stakeholder, basata su un linguaggio comune,
- il soddisfacimento dei requisiti definiti nel modello COSO e relativi all'ambiente di controllo dell'IT.

Le pagine seguenti di questo documento forniscono una descrizione del modello di tutte le sue componenti principali organizzate nei 4 domini IT e nei 34 processi IT. Tutto questo costituisce un utile manuale di riferimento per tutte le linee guida di COBIT. Sono inoltre presenti anche diverse appendici per fornire utili riferimenti.

Informazioni aggiornate su COBIT e tutte le sue componenti, compresi gli strumenti on-line, le guide per l'implementazione, i case study, le newsletter ed il materiale didattico sono disponibili sul sito *www.isaca.org/cobit.*

IL MODELLO DI RIFERIMENTO DI COBIT

L'obiettivo di COBIT:

La ricerca, lo sviluppo, la divulgazione e la promozione di un modello di riferimento per l'IT governance che sia autorevole, aggiornato e accettato a livello internazionale, e che possa essere utilizzato dalle aziende, dalla direzione, dai professionisti IT e dagli auditors.

LA NECESSITÀ DI UN MODELLO DI CONTROLLO DI RIFERIMENTO PER L' IT GOVERNANCE

Un modello di controllo per l'IT governance definisce le ragioni per cui l'IT governance è necessaria, i suoi stakeholders e ciò che intende perseguire.

Perché

L'alta direzione comprende sempre più l'impatto significativo che l'informazione può avere sul successo dell'impresa. Il management si aspetta una maggiore comprensione del modo in cui si fa funzionare l'information technology (IT) e della possibilità che ha di essere sfruttato con successo per un vantaggio competitivo. In particolare, l'alta direzione deve sapere se l'impresa gestisce l'informazione in modo da:

- avere la probabilità di raggiungere i propri obiettivi
- essere abbastanza flessibile per imparare ed adattarsi
- gestire con criterio i rischi che incontra
- riconoscere appropriatamente le opportunità, ed agire di conseguenza

Le imprese di successo comprendono i rischi e si avvantaggiano dei benefici dell'IT e trovano il modo di :

- gestire l'allineamento della strategia IT con la strategia aziendale
- fornire ad investitori ed azionisti adeguate garanzie a conferma che l'organizzazione pone la "dovuta attenzione" riguardo la mitigazione dei rischi IT
- calare la strategia e gli obiettivi IT all'interno dell'impresa
- ottenere valore dagli investimenti IT
- fornire strutture organizzative che facilitano l'implementazione di strategie ed obiettivi
- creare relazioni costruttive e comunicazioni efficaci tra l'azienda e l'IT, e con i partner esterni
- misurare la performance dell'IT.

Le imprese non possono rispondere efficacemente a tali requisiti aziendali e di governo senza adottare ed implementare uno schema di governo e controllo per l'IT per:

- creare un collegamento con i requisiti aziendali
- dare trasparenza alla performance rispetto a questi requisiti
- organizzare le proprie attività in un modello di processo generalmente accettato
- identificare le principali risorse da attivare
- definire gli obiettivi di controllo di gestione da prendere in considerazione.

Inoltre, gli schemi di riferimento per il governo ed il controllo stanno diventando parte delle best practice dell'IT management e sono un fattore facilitante per stabilire il governo IT e conformarsi con le sempre crescenti richieste della normativa.

Le good practice dell'IT sono diventate importanti grazie ad alcuni fattori:

- i manager e gli organi direttivi dell'azienda si aspettano un maggior ritorno dagli investimenti in IT, cioè che l'IT fornisca i servizi di cui l'azienda ha bisogno per incrementare il valore per gli stakeholder
- la preoccupazione relativa all'aumento generalizzato del livello di spesa per l'IT
- l'esigenza di soddisfare le richieste della normativa per i controlli IT in aree quali la privacy e la predisposizione del bilancio (per esempio il Sarbanes-Oxley Act, Basilea II) ed in settori specifici come quelli finanziario, farmaceutico e della sanità.
- la selezione dei fornitori di servizi e la gestione dell'esternalizzazione e dell'acquisizione dei servizi
- la crescente complessità dei rischi correlati all'IT come la sicurezza delle reti
- le iniziative di IT governance che includono l'adozione di quadri di controllo di riferimento e best practice che aiutino il monitoraggio ed il miglioramento delle attività critiche di IT per incrementare il valore aziendale e ridurre i rischi
- l'esigenza di ottimizzare i costi seguendo, dove possibile, approcci standardizzati piuttosto che metodi sviluppati appositamente
- la crescente maturità e la conseguente accettazione di schemi di riferimento affermati quali COBIT, IT Infrastructure Library (ITIL), la serie ISO 27000 con gli standard relativi alla sicurezza informatica, ISO 9001:2000 *Gestione dei sistemi di qualità–Requisiti*, Capability Maturity Model® Integration (CMMI), Projects in Controlled Environments 2 (PRINCE2*), A Guide to the Project Management Body of Knowledge* (PMBOK)
- l'esigenza per le imprese di valutare le proprie prestazioni sia rispetto a standard generalmente accettati che nei confronti dei propri concorrenti (benchmarking)

Chi

Uno schema di riferimento per il governo ed il controllo deve essere in grado di soddisfare diversi stakeholder interni ed esterni, ognuno dei quali ha specifiche esigenze:

- Stakeholder interni all'impresa che hanno interesse a generare valore dagli investimenti in IT
  - chi prende le decisioni di investimento
  - chi decide i requisiti
  - chi utilizza i servizi IT
- Stakeholder interni ed esterni che forniscono i servizi IT
  - chi gestisce l'organizzazione ed i processi dell'IT
  - chi sviluppa le competenze
  - chi gestisce i servizi
- Stakeholder interni ed esterni che hanno responsabilità sui rischi/controlli
  - chi ha responsabilità in materia di sicurezza, privacy e/o rischi
  - chi svolge funzioni di verifica della conformità
  - chi richiede o fornisce servizi di assurance

Cosa

Al fine di raggiungere i requisiti sopra elencati, lo schema di riferimento per il governo ed il controllo dell'IT deve soddisfare le seguenti specifiche generali:

- offrire una prospettiva centrata sull'azienda in modo da facilitare l'allineamento tra gli obiettivi dell'azienda e dell'IT
- stabilire un orientamento dei processi per definire l'ambito e l'entità della copertura, con una struttura definita in modo da consentire di navigare con facilità tra i contenuti
- essere generalmente accettabile rimanendo coerente con le best practice e gli standard di IT ed indipendente da tecnologie specifiche
- utilizzare un linguaggio comune con termini e definizioni che siano generalmente comprensibili da tutti gli stakeholder
- aiutare a rispettare i requisiti normativi rimanendo in linea con gli standard di corporate governante generalmente accettati (es., COSO) e con i controlli IT richiesti dai supervisori e dai revisori esterni.

COME COBIT RISPONDE A QUESTE ESIGENZE

A fronte delle esigenze descritte nella sezione precedente, allo schema di riferimento del COBIT sono state attribuite fin dalla sua creazione le seguenti caratteristiche principali: è focalizzato sull'azienda, orientato ai processi, basato sui controlli e determinato dalle misurazioni.

Orientato al business

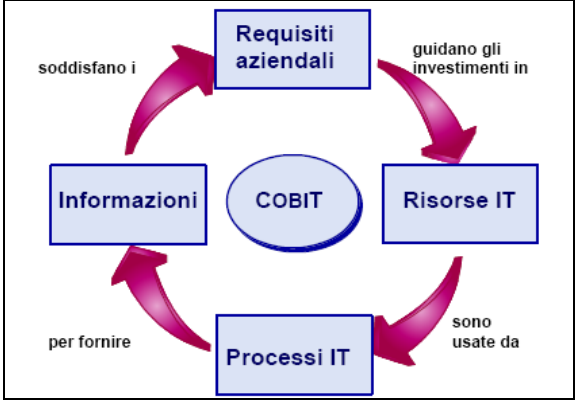
L'orientamento al business è il principale tema di COBIT, che non è stato disegnato per essere utilizzato solo da fornitori di servizi IT, utenti e revisori, ma anche, e prima ancora, per essere una guida completa per i manager ed i responsabili dei processi aziendali.

Lo schema di riferimento di COBIT è basato sul seguente Principio (**Figura 5**):

> per poter fornire le informazioni di cui l'impresa ha bisogno per raggiungere i propri obiettivi, l'azienda deve poter gestire e controllare le risorse IT utilizzando un insieme strutturato di processi per erogare i servizi informativi richiesti.

La gestione e il controllo delle informazioni sono al centro del modello di controllo COBIT e aiutano ad assicurare l'allineamento agli obiettivi aziendali.

Figura 5 - Il principio base di COBIT



I CRITERI DI VALUTAZIONE DELL INFORMAZIONI DI COBIT

Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati criteri che nella metodologia COBIT sono chiamati requisiti aziendali per le informazioni. Partendo dai requisiti più ampi di qualità, affidabilità e sicurezza, sono stati identificati sette criteri distinti, certamente sovrapponibili, definiti come segue:

- **L'efficacia** riguarda le informazioni, che debbono essere rilevanti e pertinenti rispetto ai processi aziendali e devono poter essere rese disponibili tempestivamente, senza errori, in modo coerente ed utilizzabile.
- **L'efficienza** riguarda la gestione delle informazioni attraverso l'uso ottimale delle risorse (sia dal punto di vista della maggiore produttività che della economicità)
- **La riservatezza** riguarda la protezione delle informazioni sensibili da possibili accessi non autorizzati

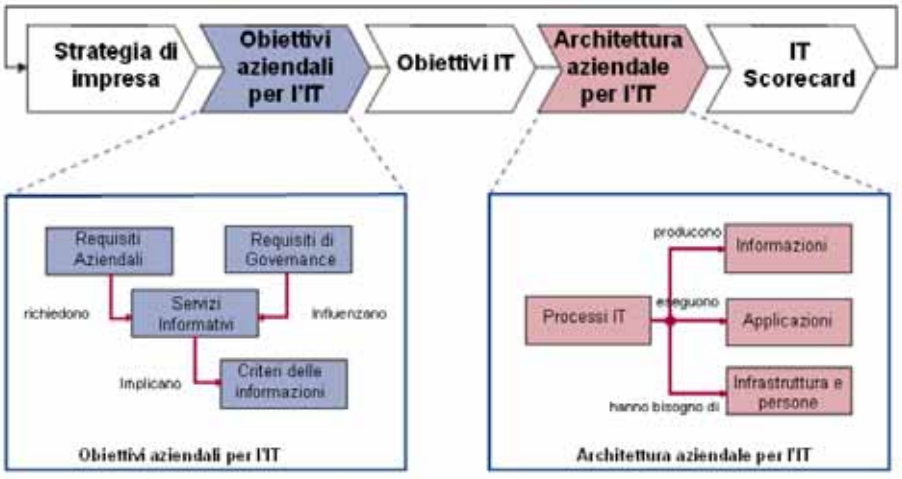
- **L'integrità** riguarda l'accuratezza e la completezza delle informazioni come pure la loro validità nel rispetto dei valori e delle aspettative aziendali
- **La disponibilità** è riferita al fatto che le informazioni devono essere disponibili quando richiesto dai processi aziendali, sia nel presente che nel futuro. Riguarda inoltre la salvaguardia delle risorse necessarie e delle relative capacità e funzionalità
- **La conformità** riguarda il rispetto di leggi, regolamenti ed accordi contrattuali cui è soggetto il processo aziendale, cioè vincoli aziendali imposti dall'esterno e politiche interne
- **L'affidabilità** riguarda la fornitura di informazioni appropriate, che permettano alla direzione di gestire l'azienda ed esercitare le proprie responsabilità come organi fiduciari e di governo.

OBIETTIVI AZIENDALI E OBIETTIVI IT

Mentre i criteri di valutazione delle informazioni forniscono un metodo generico per la definizione dei requisiti aziendali, la definizione di un insieme di obiettivi aziendali ed IT generici offre all'azienda un punto di partenza più preciso per definire i requisiti aziendali e sviluppare le metriche che consentono la misurazione di questi obiettivi. Tutte le imprese utilizzano l'IT per rendere possibili le iniziative di business, che diventano per l'IT degli obiettivi aziendali. Nell'Appendice I viene riportata una matrice degli obiettivi aziendali ed IT generici e di come essi si rapportano ai criteri di valutazione delle informazioni. Questi esempi di massima possono essere usati come guida nella determinazione di requisiti aziendali, obiettivi e metriche specifici per l'impresa.

Se l'IT fornisce con successo i propri servizi a supporto della strategia dell'impresa, l'azienda (il cliente) deve avere una chiara proprietà ed un preciso controllo dei requisiti oltre ad una chiara comprensione di cosa le debba fornire l'IT (il fornitore) e come. La **figura 6** illustra come la strategia d'impresa debba essere tradotta dall'azienda in obiettivi per consentire l'utilizzo degli strumenti predisposti dall'IT (gli obiettivi aziendali per l'IT). Questi obiettivi, a loro volta, devono portare ad una chiara definizione delle mete proprie dell'IT (gli obiettivi dell'IT) e, successivamente, definire le risorse e le capacità dell'IT (l'architettura aziendale dell'IT) che sono necessarie per svolgere con successo il proprio ruolo nella strategia dell'impresa. [1]

Figura 6 – Definizione degli obiettivi dell'IT e dell'architettura aziendale per l'IT



Dopo aver provveduto all'allineamento degli obiettivi, è necessario un monitoraggio per assicurare che i servizi erogati corrispondano alle aspettative. Ciò può essere raggiunto mediante l'utilizzo di metriche derivate dagli obiettivi e riportate in una IT Scorecard.

Tutti questi obiettivi e le relative metriche devono essere espressi in termini di business rilevanti per il cliente. Tutto ciò, combinato con un efficace allineamento dei rispettivi obiettivi e delle loro priorità, potrà sicuramente portare l'azienda a confermare che l'IT è in grado di supportare gli obiettivi dell'impresa.

L'Appendice I fornisce una visione complessiva di come degli obiettivi aziendali generici si rapportino con gli obiettivi IT, i processi IT ed i criteri di valutazione delle informazioni. Le tabelle aiutano a dimostrare l'ambito considerato in COBIT e la relazione complessiva tra COBIT e i driver aziendali. Come illustrato dalla **figura 6**, tali driver derivano dal business e dal governo dell'azienda, il primo concentrandosi più sulla funzionalità e velocità di messa in esercizio, il secondo più sull'economicità, Return on Investment (ROI) e conformità normativa.

[1] Va notato che la definizione ed implementazione di un'architettura IT aziendale crea, anche degli obiettivi IT interni che contribuiscono agli obiettivi di business ma non ne derivano direttamente.

LE RISORSE IT

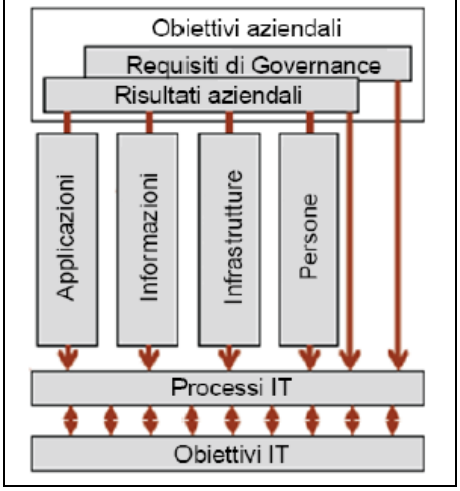
Nell'ambito di questi obiettivi, l'organizzazione IT opera con un insieme chiaramente definito di processi che, utilizzando le competenze del personale e le infrastrutture tecnologiche, gestiscono le applicazioni aziendali automatizzate sulla base delle informazioni aziendali. Queste risorse, insieme ai processi, costituiscono l'architettura aziendale dell'IT, come mostrato in **figura 6**.

Per rispondere ai requisiti aziendali per l'IT, l'impresa ha la necessità di investire nelle risorse richieste al fine di creare un'adeguata capacità tecnica (ad esempio, un sistema ERP) per supportare una possibile funzione aziendale (ad esempio, l'implementazione di un ciclo acquisti) che porti al risultato desiderato (ad esempio, l'incremento delle vendite e dei benefici economici).

Le risorse IT identificate da COBIT possono essere definite come segue:
- Applicazioni: sono costituite dai sistemi automatizzati e dalle procedure manuali che elaborano le informazioni.
- Informazioni: sono i dati in tutte le loro forme, quando sono inseriti, elaborati e prodotti dai sistemi informativi, in qualsiasi forma utilizzata dall'azienda.
- Infrastruttura: è rappresentata dalla tecnologia e dagli strumenti (hardware, sistema operativo, sistemi di gestione dei database, reti, supporti • multimediali, ecc., e l'ambiente che li ospita e li supporta) che consentono il funzionamento delle applicazioni.
- Persone: sono il personale richiesto per pianificare, organizzare, acquisire, implementare, erogare, supportare, controllare e valutare i sistemi informativi ed i servizi. Possono essere interne, esterne, o a contratto, se richiesto.

La **figura 7** sintetizza come gli obiettivi aziendali per l'IT influenzano il modo in cui le risorse IT devono essere gestite dai processi IT per raggiungere gli obiettivi dell'IT.

Figura 7 – La gestione delle IT per raggiungere gli obiettivi dell'IT



Orientato ai processi

COBIT definisce le attività IT in un modello generale di processi all'interno di quattro domini. Questi domini sono Pianificazione e Organizzazione, Acquisizione e Implementazione, Erogazione e Assistenza, e Monitoraggio e Valutazione. I domini si riferiscono alle tradizionali aree di responsabilità dell'IT di pianificazione, costruzione, esecuzione e controllo.

Lo schema di COBIT fornisce un modello di processo di riferimento ed un linguaggio comune per tutti quelli che nell'azienda controllano e gestiscono le attività IT. Incorporando un modello operativo ed un linguaggio comune per tutte le componenti aziendali coinvolte nell'IT, COBIT è uno dei passi iniziali e più importanti verso una buona governance. Inoltre fornisce uno schema per misurare e controllare le prestazioni dell'IT, comunicando con i fornitori di servizi ed integrando le best practice di gestione. Un modello di processo incoraggia la proprietà dei processi, facilitando la definizione delle responsabilità ai vari livelli.

Per governare l'IT efficacemente è importante comprendere le attività ed i rischi che devono essere gestiti all'interno dell'IT, Questi vengono normalmente ordinati nei domini di responsabilità relativi alla pianificazione, sviluppo (build), esercizio (run) e monitoraggio. All'interno del modello di controllo COBIT, questi domini, come mostrato in **figura 8** sono chiamati:
- **Pianificazione e Organizzazione (PO)—**Fornisce direzione allo sviluppo di soluzioni (AI) e allo sviluppo dei servizi (DS)
- **Acquisizione ed implementazione (AI)**—Fornisce le soluzioni e ne consente la trasformazione in servizi.
- **Erogazione e supporto (DS)**—Riceve le soluzioni e le rende utilizzabili dagli utenti finali.
- **Monitoraggio e valutazione (ME)**—Controlla tutti i processi per assicurare che siano seguite le direttive fornite.

Figura 8 – I quattro Domini correlati di CobiT

PIANIFICAZIONE E ORGANIZZAZIONE (PO)

Questo dominio si riferisce agli aspetti strategici e tattici, e riguarda l'identificazione del modo in cui l'IT può meglio contribuire al raggiungimento degli obiettivi aziendali. Inoltre la realizzazione della visione strategica ha bisogno di essere pianificata, comunicata e gestita da differenti punti di vista. Infine deve essere costituita un'appropriata organizzazione così come una valida infrastruttura tecnologica. Questo dominio riguarda le seguenti domande del management:
- La strategia dell'IT e quella aziendale sono allineate?
- L'impresa sta ottenendo il massimo dalle proprie risorse?
- All'interno della azienda tutti comprendono gli obiettivi dell'IT?
- I rischi IT sono capiti e gestiti?
- La qualità dei sistemi IT è adeguata alle esigenze aziendali?

ACQUISIZIONE ED IMPLEMENTAZIONE (AI)

Per realizzare la strategia IT, le soluzioni IT devono essere identificate, sviluppate o acquistate, come pure realizzate ed integrate nei processi aziendali. Inoltre rientrano in questo dominio le modifiche e la manutenzione delle applicazioni esistenti per assicurare che le soluzioni continuino a soddisfare gli obiettivi aziendali. Questo dominio riguarda le seguenti domande del management:
• I nuovi progetti sono in grado di garantire soluzioni che soddisfino le esigenze aziendali?
• È possibile realizzare i nuovi progetti nel rispetto dei tempi e del budget?
• I nuovi sistemi funzionano correttamente dopo l'implementazione?
• I cambiamenti verranno fatti senza impattare sulle operazioni aziendali correnti?

EROGAZIONE E SUPPORTO (DS)
In questo dominio si fa riferimento all'erogazione dei servizi richiesti, che includono l'erogazione del servizio vero e proprio, la gestione della sicurezza e della continuità, il servizio di assistenza agli utenti e la gestione dei dati e le infrastrutture operative. Questo dominio risponde alle seguenti domande del management:
• I servizi IT vengono erogati in linea con le priorità aziendali?
• I costi dell'IT sono ottimizzati?
• La forza lavoro è in grado di utilizzare i sistemi IT in modo produttivo ed in sicurezza?
• Sono adeguatamente garantite riservatezza, integrità e disponibilità?

MONITORAGGIO EVALUTAZIONE (ME)
Tutti i processi IT devono essere regolarmente valutati nel tempo sotto l'aspetto della qualità e della conformità ai requisiti di controllo. Questo dominio, che riguarda la gestione delle prestazioni, la verifica del sistema di controllo interno, la conformità ai regolamenti ed il soddisfacimento dei requisiti di governo, risponde alle seguenti domande del management:
• Le prestazioni dell'IT sono misurate al fine di individuare i problemi prima che sia troppo tardi?
• L'alta direzione assicura che i controlli interni operino in modo efficace ed efficiente?
• La performance dell'IT può essere ricollegata agli obiettivi aziendali?
• Sono attivati controlli adeguati in materia di riservatezza, integrità e disponibilità ai fini della sicurezza delle informazioni?

Attraverso questi quattro domini, COBIT identifica 34 processi IT tipicamente adottati (fare riferimento alla **figura 23** per la lista completa). Se molte aziende hanno definito formalmente le responsabilità per la pianificazione, sviluppo, esercizio e controllo dell'IT, e molte hanno gli stessi processi chiave, poche hanno la stessa struttura di processi o applicano tutti e 34 i processi COBIT. Il COBIT fornisce una lista completa di processi che possono essere utilizzati per verificare la completezza delle attività e delle responsabilità. Tuttavia, non è necessaria la completa adozione di tale lista e i processi possono essere integrati a seconda delle necessità di ciascuna azienda.

Per ciascuno dei 34 processi, viene fornito un collegamento tra obiettivi di business ed obiettivi IT. Sono fornite anche informazioni su come misurare gli obiettivi, chi sono i relativi responsabili, quali sono le attività chiave ed i principali risultati (deliverables).

Basato sui controlli

COBIT definisce obiettivi di controllo per tutti e 34 i processi, ma anche per i relativi controlli di processo e applicativi.

I PROCESSI DEVONO ESSERE CONTROLLATI

Per controllo intendiamo l'insieme delle politiche, procedure, prassi e strutture organizzative atte ad assicurare con ragionevole certezza il raggiungimento degli obiettivi aziendali e l'identificazione e correzione degli eventi indesiderati.

Gli obiettivi di controllo IT forniscono un set complete di requisiti di alto livello che devono essere considerate dalla direzione per

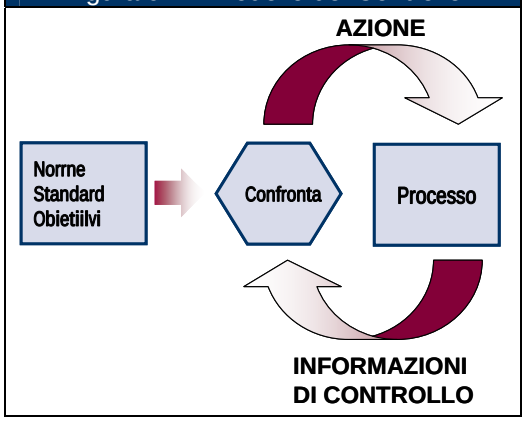
- Sono linee guida di azioni manageriali per aumentare il valore o ridurre il rischio.
- Consistono di politiche, procedure, prassi e strutture organizzative
- Sono disegnate per fornire ragionevole certezza che gli obiettivi di business saranno raggiunti e che eventi indesiderati saranno prevenuti o identificati e corretti.

l'efficace controllo di:tutti i processi IT. Essi:

La direzione aziendale deve prendere delle decisioni relativamente a questi obiettivi di controllo:
• Selezionando quelli applicabili.
• Decidendo quelli che dovranno essere implementati
• Scegliendo come implementarli (frequenza, ambito, livello di automazione ecc.)
• Accettando l'eventuale rischio di non implementare i controlli necessari.

Un'indicazione proviene dal modello di controllo standard riportato in **figura 9**, che applica i principi che sono evidenziati dalla seguente analogia: quando la temperatura di una stanza (standard) è regolata da un sistema di riscaldamento (processo), il sistema controllerà continuamente (confronto) la temperatura (informazione di controllo) e darà segno (azione) al sistema di riscaldamento di fornire più o meno calore.

Figura 9 – Il Modello del Controllo



La gestione operativa utilizza i processi per organizzare e gestire tutte le normali attività IT. COBIT fornisce un modello generale che rappresenta tutti i processi normalmente presenti nelle funzioni IT, e rappresenta un modello di riferimento comune comprensibile sia ai manager operativi dell'IT che a quelli dell'azienda. Per ottenere una governance efficace, i controlli devono essere implementati dai manager operativi all'interno di uno schema di riferimento definito e valido per tutti i processi IT. Visto che gli obiettivi di controllo IT di COBIT sono stati organizzati per relativo processo, lo schema di riferimento fornisce chiari legami tra requisiti di governo, processi e controlli dell'IT.

Ogni processo IT di COBIT ha un obiettivo di controllo di alto livello ed una serie di obiettivi di controllo di dettaglio che, nel loro insieme, costituiscono le caratteristiche di un processo ben gestito.

Gli obiettivi di controllo di dettaglio sono identificati da due lettere che fanno riferimento al dominio (PO, AI, DS e ME), dal numero del processo e dal numero dell'obiettivo di controllo. Oltre agli obiettivi di controllo di dettaglio, ogni processo di COBIT è accompagnato da requisiti di controllo generici che sono identificati dalla sigla PCn, che sta per Process Control number (numero del controllo di processo). Essi devono essere considerati congiuntamente agli obiettivi di controllo di dettaglio per avere una visione completa dei requisiti di controllo.

PC1 Scopi ed obiettivi di processo
Definisce e comunica scopi ed obiettivi specifici, misurabili, fattibili, realistici, orientati al risultato e tempestivi (SMARRT) per l'efficace esecuzione di ogni processo IT. Assicura inoltre che siano legati agli obiettivi di business e supportati da metriche adeguate.

PC2 Referente del processo
Assegna un referente ad ogni processo IT e definisce chiaramente i ruoli e responsabilità di tale referente. Ad esempio, vengono inclusi la responsabilità per il disegno del processo, la sua interazione con altri processi, la responsabilità per il risultato finale nonché la misurabilità della performance di processo e l'identificazione di opportunità di miglioramento.

PC3 Ripetibilità di processo
Definisce e stabilisce ogni processo IT in modo che sia ripetibile e produca i risultati attesi in modo coerente. Fornisce una sequenza di attività logica e ripetibile che porti ai risultati desiderati e sia sufficientemente agile da gestire eccezioni ed emergenze. Utilizza processi standard, ove possibile, e li personalizza solo quando ciò sia inevitabile.

PC4 Ruoli e responsabilità
Definisce le attività chiave e risultati finali del processo. Assegna e comunica ruoli e responsabilità non ambigue per l'efficace ed efficiente esecuzione delle attività chiave e la loro documentazione, nonché la responsabilità per il processo e relativi risultati.

PC5 Politiche, Piani e Procedure
Definisce a comunica come le politiche, i piani e le procedure che gestiscono un processo IT debbano essere documentati, revisionati, mantenuti, approvati, archiviati e utilizzati per la formazione. Assegna responsabilità per ognuna di queste attività e, ad intervalli stabiliti, il monitoraggio della loro corretta esecuzione. Assicura che le politiche, piani e procedure siano accessibili, corrette, comprese e aggiornate.

PC6 Miglioramento delle prestazioni di processo
Identifica una serie di metriche che forniscono una visione dei risultati e prestazioni di processo. Stabilisce obiettivi che si riflettono sugli obiettivi di processo e sui relativi indicatori che abilitano il raggiungimento degli obiettivi di processo. Definisce come devono essere ottenuti i dati. Confronta misurazioni rilevate con quelle attese e persegue opportune azioni sulle eventuali deviazioni. Allinea le metriche, gli obiettivi e i metodi con l'approccio complessivo al monitoraggio dell'IT.

Dei controlli efficaci riducono il rischio, aumentano la possibilità di produrre valore e migliorano l'efficienza in quanto si verificheranno meno errori e l'approccio del management sarà più coerente.

Inoltre, per ogni processo il COBIT fornisce esempi descrittivi, e quindi non rigorosi o esaustivi, di:
• Input e risultati(output) generici
• Tabelle RACI con attività e indicazioni di ruoli e responsabilità
• Obiettivi principali (le cose più importanti da fare)
• Metriche

Oltre a ciò, per comprendere quali controlli siano necessari, i responsabili di processo devono capire quali input devono ricevere dagli altri e quali devono ricevere gli altri da quel processo. COBIT fornisce un esempio generico dei principali input dei risultati di ogni processo, inclusi quelli richiesti dall'esterno. Ci sono alcuni risultati che rappresentano degli input in tutti gli altri processi, e sono contrassegnati con "ALL" nelle tabelle degli output, ma non vengono citati come input in tutti i processi: tipicamente si tratta di standard di qualità e requisiti di misurazione, il quadro di riferimento dei processi IT, ruoli e responsabilità documentati, il quadro di riferimento per il controllo dell'IT da parte dell'azienda, le politiche IT ed i ruoli e le responsabilità del personale.

La comprensione dei ruoli e delle responsabilità per ogni processo è un aspetto cruciale per un governo efficace.
COBIT fornisce una tabella RACI (acronimo di Responsible, Accountable, Consulted and Informed) per ogni processo. "Accountable" si riferisce al soggetto che fornisce direttive ed autorizza un'attività. "Responsible" si riferisce al soggetto che fa eseguire un lavoro. Gli altri due ruoli ("Consulted" e "Informed") assicurano che il processo preveda la partecipazione ed il coinvolgimento di tutti quelli che ne hanno necessità.

CONTROLLI AZIENDALI E CONTROLLI IT

Il sistema di controllo interno dell'azienda ha un triplice impatto sull'IT:

- A livello di alta direzione, si definiscono gli obiettivi aziendali, si stabiliscono le politiche e si prendono decisioni su come distribuire e gestire le risorse per mettere in pratica le strategie dell'impresa. In generale, l'approccio alla governance ed al controllo è definito dal consiglio di amministrazione e comunicato a tutta l'impresa. L'ambiente di controllo IT è guidato da questo insieme di obiettivi e politiche di alto livello.
- A livello di processo aziendale, i controlli sono applicati a specifiche attività aziendali. La maggior parte dei processi aziendali sono automatizzati ed integrati con sistemi applicativi dell'IT, il che implica che molti dei controlli effettuati a questo livello sono anch'essi automatizzati. Tali controlli sono conosciuti come controlli applicativi. Tuttavia, alcuni controlli, quali l'autorizzazione delle transazioni, la separazione dei compiti e le riconciliazioni manuali, all'interno del processo aziendale continuano ad essere effettuati manualmente. Pertanto, i controlli a livello di processo aziendale sono una combinazione di controlli manuali svolti dall'azienda, controlli aziendali e controlli applicativi automatizzati. Sono tutti responsabilità dell'azienda, che li definisce e li gestisce, anche se è necessario il supporto dell'IT per progettare e sviluppare i controlli applicativi.
- Per supportare i processi aziendali, l'IT fornisce i propri servizi, solitamente condivisi tra più processi aziendali, in quanto molti dei processi IT, sia di sviluppo che operativi, sono erogati all'intera impresa e buona parte dell'infrastruttura IT fornisce servizi comuni (per esempio le reti, i database, i sistemi operativi e le unità di memorizzazione). I controlli relativi a tutte le attività dei servizi IT sono conosciuti come controlli generali IT. L'affidabilità del funzionamento di tali controlli generali è necessaria per porre fiducia nei controlli applicativi. Per esempio, una scarsa gestione del cambiamento potrebbe mettere a rischio (accidentalmente o per azione deliberata) l'affidabilità dei controlli di integrità automatizzati.

CONTROLLI GENERALI E CONTROLLI APPLICATIVI DELL'IT

I controlli generali sono quei controlli contenuti nei processi e nei servizi IT, quali per esempio:

- Sviluppo dei sistemi
- Gestione del cambiamento
- Sicurezza
- Esercizio dei sistemi

I controlli integrati nei processi aziendali si definiscono solitamente controlli applicativi. Come esempi possiamo citare:

- Completezza
- Accuratezza
- Validità
- Autorizzazione
- Separazione dei compiti

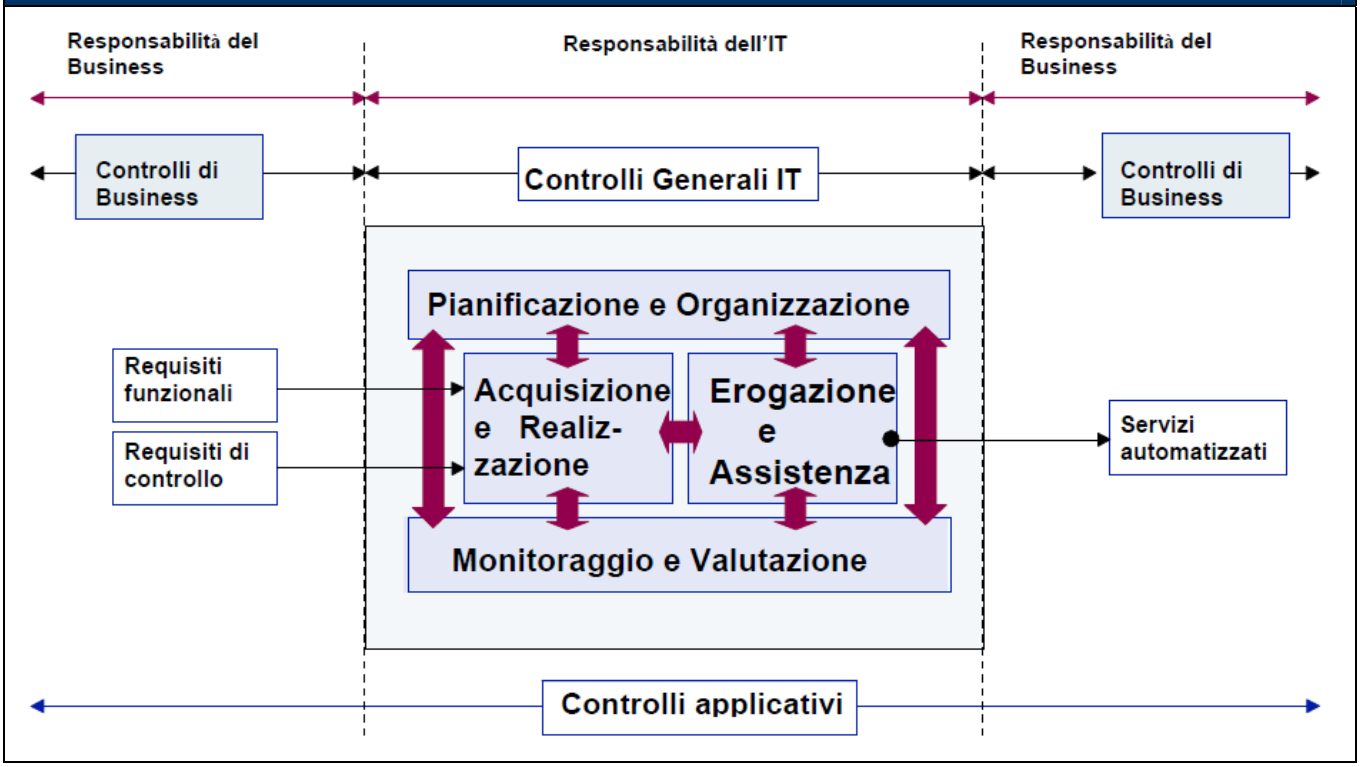
COBIT presuppone che la progettazione e l'implementazione dei controlli applicativi automatizzati siano responsabilità dell'IT, descritti nel dominio Acquisizione e Implementazione, e si basino sui requisiti aziendali definiti utilizzando i criteri di valutazione delle informazioni di COBIT, come illustrato in **figura 10**. La responsabilità per la gestione operativa ed il controllo dei controlli applicativi non è dell'IT, ma del referente del processo aziendale.

Perciò, la responsabilità dei controlli applicativi è congiunta (end-to-end) tra il business e l'IT, ma la natura della responsabilità si differenzia come di seguito descritto:

- Il business è responsabile di:
  - Definire i requisiti funzionali e di controllo
  - Utilizzare servizi automatizzati
- IT è responsabile di:
  - Automatizzare ed implementare i requisiti funzionali e di controllo stabiliti dal business
  - Stabilire i controlli atti a mantenere l'integrità dei controlli applicativi

Per questa ragione i processi IT di COBIT coprono i controlli generali IT, ma solo per quanto concerne gli aspetti attinenti allo sviluppo dei controlli applicativi; la responsabilità per l'attuazione e la definizione di tali controlli nella prassi è di competenza delle aree operative (di business).

Figura 10 - Confine fra Controlli Generali, di Business e Controlli Applicativi



La seguente lista fornisce un insieme degli obiettivi dei controlli applicativi raccomandati. Sono identificati dal codice ACn, che sta per Controllo Applicativo ed il progressivo relativo.

AC1 Autorizzazione e preparazione dei dati
Provvedere affinché i documenti con le informazioni in input siano preparati da personale qualificato seguendo procedure formalizzate, in un contesto di adeguata segregazione funzionale riferita all'origine e dall'approvazione dei documenti. Errori o omissioni devono essere ridotti da un buon design degli schemi di input. Rilevare errori e anomalie in modo tale da consentirne la registrazione e la correzione.

AC2 Raccolta ed inserimento dei dati
L'introduzione dei dati è svolta in modo puntuale da personale autorizzato e competente. La correzione e la reintroduzione di dati erroneamente introdotti dovrebbe essere svolta senza compromettere i livelli di autorizzazione originalmente assegnati alle transazioni. Laddove necessario per la tracciatura delle operazioni, conservare i documenti originari per un intervallo di tempo adeguato.

AC3 Controlli di autorizzazione, accuratezza e completezza
Assicurare l'accuratezza delle transazioni, la loro completezza e validità. Sono predisposte procedure per assicurare che i dati inseriti siano convalidati o respinti quanto più possibile vicino al punto in cui sono originati.

AC4 Validità ed integrità dell'elaborazione dei dati
Sono in atto procedure per assicurare che l'integrità e la validità dei dati attraverso l'intero ciclo di elaborazione. La rilevazione di transazioni errate non pregiudica l'elaborazione delle transazioni valide.

AC5 Revisione dei dati prodotti, riconciliazione e trattamento degli errori
Sono in atto procedure e relative responsabilità, per assicurare che sia mantenuta la sicurezza dei report prodotti, che siano consegnati ai destinatari corretti e che siano protetti durante la trasmissione. Inoltre sono predisposte procedure per identificare e trattare gli errori contenuti nell'output e per accertare che le informazioni generate in input siano effettivamente utilizzate.

AC6 Integrità ed autenticazione delle transazioni
Procedure per il controllo dell'autenticità dell'origine, dell'integrità del contenuto e dell'esatto indirizzamento assicurano la correttezza del trasferimento dei dati dalle applicazioni interne verso le funzioni di business (sia interne che esterne all'azienda). Durante la trasmissione ed il trasporto si pongono in essere adeguate misure di protezione contro accessi non autorizzati, modifiche o errori di indirizzo.

Basato sulla misurazione

Una necessità fondamentale per ogni impresa è comprendere lo stato del proprio sistema IT e decidere di quale livello di gestione e controllo abbia bisogno. Per decidere correttamente, il management dovrebbe chiedersi: Quanto lontano dobbiamo andare, i benefici giustificheranno i costi?

Non è però facile ottenere una visione oggettiva del livello della perfomance della propria impresa. Cosa deve essere misurato e come? L'impresa ha bisogno di valutare dove si trova e dove sono necessari dei miglioramenti, ed implementare strumenti di gestione per monitorare questi miglioramenti.
COBIT tratta questi argomenti fornendo:
- Modelli di maturità che consentono il confronto e l'identificazione dei necessari miglioramenti della capacità
- Obiettivi e metriche per le prestazioni dei processi IT, che dimostrano come i processi soddisfino gli obiettivi aziendali e dell'IT e siano utilizzati per misurare la performance dei processi interni basandosi sul principio della balanced scorecard
- Obiettivi delle attività per permettere una performance efficace dei processi

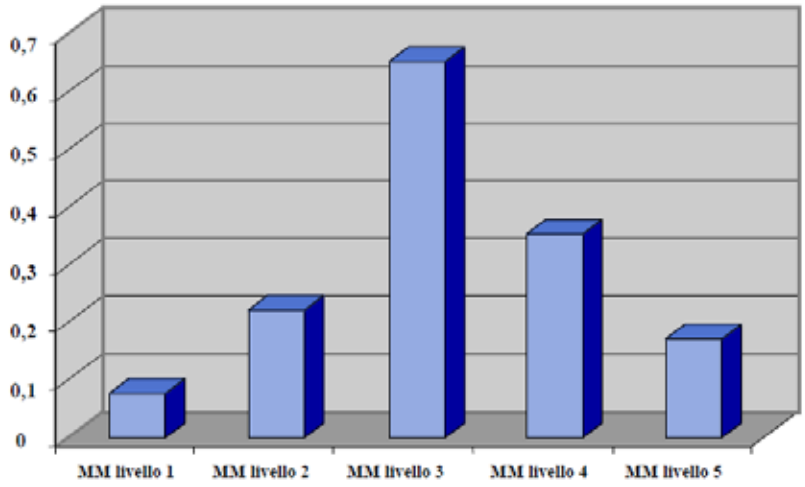
I MODELLI DI MATURITÀ
All'alta direzione delle imprese pubbliche e private è sempre più spesso richiesto di considerare la qualità della gestione dell'IT. In risposta a ciò, si richiedono lo sviluppo ed il miglioramenti dei casi aziendali ed il raggiungimento di un appropriato livello di gestione e di controllo dell'infrastruttura IT. Per quanto pochi oserebbero sostenere che ciò non è cosa buona, si devono considerare il rapporto costi-benefici e le seguenti domande:
- Cosa stanno facendo le imprese concorrenti, e come siamo posizionati rispetto a loro?
- Quale è una best practice accettabile nel nostro settore e come siamo posizionati rispetto a questa prassi?
- Sulla base di tali confronti, si può dire che stiamo facendo abbastanza?
- Come identifichiamo che cosa è necessario fare per raggiungere un adeguato livello di gestione e controllo dei nostri processi IT?

Può essere difficile dare risposte significative a queste domande. Il management di IT è costantemente alla ricerca di strumenti di confronto e autovalutazione per rispondere all'esigenza di sapere cosa fare in modo efficiente. Partendo dai processi e dagli obiettivi di controllo di alto livello di COBIT, il referente del processo dovrebbe essere in grado di sviluppare progressivamente i confronti con gli obiettivi di controllo. Ciò soddisfa tre esigenze:
1. una valutazione relativa di dove si trovi l'impresa
2. un modo per decidere efficientemente dove andare
3. uno strumento per misurare i progressi rispetto all'obiettivo

La definizione di modelli di maturità per la gestione ed il controllo dei processi IT è basata su un metodo di autovalutazione dell'organizzazione, che può valutare il proprio livello da non esistente (0) a ottimizzato (5). Questo approccio è derivato dal modello di maturità che il Software Engineering Institute (SEI) ha definito per la maturità della capacità di sviluppo del software. Nonostante sia stato seguito l'approccio SEI, l'implementazione di COBIT si è diversificata da quest'ultima che è orientata ai principi di ingegneria del software, cercando di portare l'organizzazione verso l'eccellenza in queste aree ed ad una valutazione formale dei livelli di maturità in modo da ottenere una certificazione dello sviluppo del software. In COBIT, è fornita una definizione generale di grado di maturità, che è simile al CMM ma rivista in funzione della natura dei processi di gestione IT di COBIT. Qualsiasi sia il modello, le scale non devono essere troppo granulari, in quanto ciò renderebbe il sistema difficile da utilizzare e suggerirebbe un grado di precisione non giustificabile; in generale, infatti, l'obiettivo è identificare dove sono gli aspetti critici e come attribuire le priorità per migliorarli. L'obiettivo non è di valutare il livello di aderenza agli obiettivi di controllo.

I livelli di maturità sono intesi come profili dei processi IT che un'azienda potrebbe riconoscere come descrizioni dei possibili stati presenti e futuri. Non sono stati predisposti per essere utilizzati come modelli soglia, in cui non ci si può spostare al livello superiore senza aver soddisfatto tutte le condizioni del livello precedente. Con il modello di maturità di COBIT, diversamente dall'approccio originale SEI CMM, non c'è l'intenzione di misurare i livelli con precisione o provare a certificare un preciso livello raggiunto. Una verifica secondo il modello di maturità di COBIT equivale ad identificare un profilo in cui molte condizioni rilevanti del livelli di maturità siano raggiunte, come illustrato nel disegno di **figura 11**.

Figura 11 – Possibile Livello di Maturità di un Processo IT



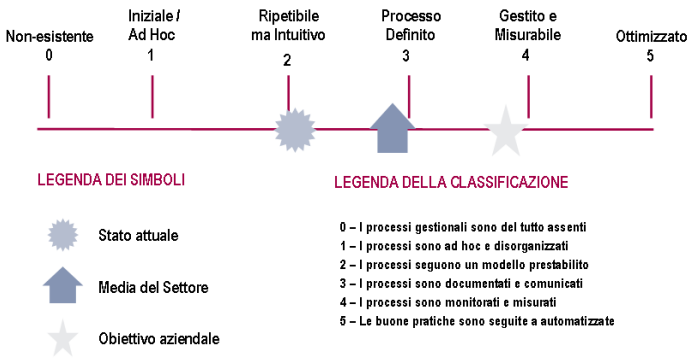
Possibili livelli di strutturazione di un processo IT: l'esempio illustra un processo che è principalmente a livello 3 ma presenta ancora delle problematiche di compliance rispetto ai requisiti dei livelli inferiori e nel contempo si sta già investendo nelle misure di performance (livello 4) e nell'ottimizzazione (livello 5).

Questo perché quando si verifica la maturità attraverso i modelli di COBIT, capita spesso che qualche attività sia operante in modo incompleto o insufficiente tra diversi livelli. Questo punto di forza può essere usato per migliorare il grado di maturità. Per esempio, alcune parti del processo possono essere ben definite mentre altre possono risultare mancanti o incomplete.

Utilizzando i modelli di maturità sviluppati per ognuno dei 34 processi di COBIT, il management può identificare:
- l'effettiva performance dell'impresa – dove si trova oggi l'impresa
- lo stato attuale del settore di attività – il confronto
- l'obiettivo dell'impresa per il proprio sviluppo – dove l'impresa vuole andare
- il percorso necessario per andare dalla situazione attuale (as-is) a quella desiderata (to-be)

Per fare in modo che i risultati siano facilmente utilizzabili negli incontri del management, in cui tali risultati saranno presentati a supporto del caso aziendale in vista di una pianificazione futura, è necessario fornire un metodo di presentazione grafica (**figura 12**).

Figura 12 – Rappresentazione grafica dei modelli di maturità



Lo sviluppo si è basato sulle descrizioni dei modelli generici di maturità indicati nella **figura 13**.

COBIT è uno schema di riferimento sviluppato per la gestione dei processi IT orientati particolarmente al controllo. Queste scale devono essere semplici da applicare e ragionevolmente facili da comprendere. Il tema della gestione dei processi IT è intrinsecamente complesso e soggettivo e, quindi, si può affrontare più facilmente attraverso valutazioni facilitate che mirino ad aumentare il livello di consapevolezza, ottengano ampio consenso e motivino il miglioramento. Queste valutazioni possono essere fatte sia rispetto alle descrizioni dei livelli di maturità nel loro insieme o con più rigore rispetto alle singole affermazioni fatte nelle varie descrizioni. In ogni caso è necessario avere esperienza nel processo aziendale sotto analisi.

Il vantaggio di un approccio basato sul modello di maturità è che è relativamente facile per il management posizionarsi sulla scala e valutare le implicazioni se è richiesto un miglioramento della performance. La scala include il valore 0 perché è possibile che non esista alcun processo. La scala da 0 a 5 è basata su una semplice scala di maturità che mostra come un processo si evolve da una capacità non esistente ad una ottimizzata.

Tuttavia, la capacità di gestione del processo non corrisponde alla prestazione del processo. La capacità richiesta, così come determinata dagli obiettivi aziendali ed IT, potrebbe non dover essere applicata allo stesso livello nell'intero ambiente IT, ma per esempio in modo non sistematico o limitatamente ad un numero ristretto di sistemi o unità. La misurazione della prestazione, come descritto nel paragrafo successivo, è essenziale nella determinazione di quale sia l'effettiva performance dell'impresa rispetto ai suoi processi IT.

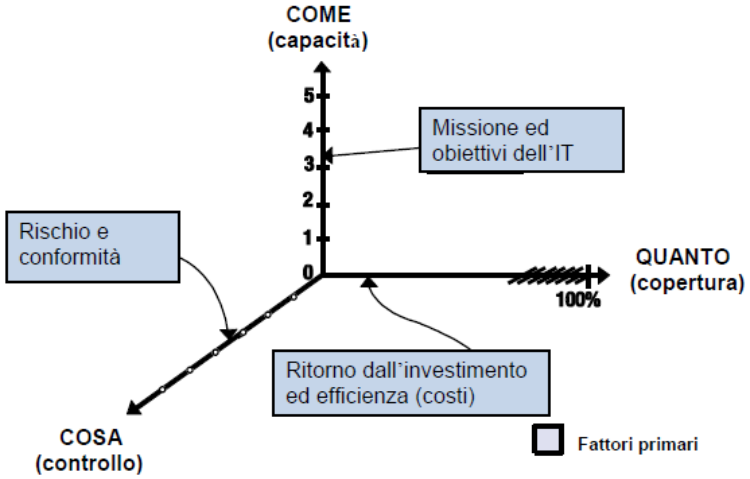
Figura 13 – Modello di maturità generale o Gradi di strutturazione generali

0 Non esistente - Assenza completa di qualsiasi processo riconoscibile. L'impresa non si è nemmeno resa conto che esiste un problema da affrontare.
1 Iniziale/*Ad hoc* - C'è evidenza che l'impresa ha riconosciuto che i problemi esistono e che devono essere affrontati. Tuttavia non esistono processi standardizzati, bensì approcci *ad hoc* che tendenzialmente vengono applicati su base individuale o caso per caso. L'approccio complessivo alla gestione non è organico.
2 Ripetibile ma Intuitivo - I processi sono stati sviluppati fino allo stadio in cui le persone che svolgono la stessa attività adottano procedure simili. Non esiste un processo formale di formazione o di comunicazione delle procedure standard, e la responsabilità è lasciata ai singoli. Si fa grande affidamento sulle conoscenze dei singoli e, conseguentemente, gli errori sono probabili.
3 Definito - Le procedure sono state standardizzate, documentate e comunicate nel corso di sessioni di formazione. È obbligatorio applicare questi processi, tuttavia è abbastanza improbabile che le deroghe siano individuate. Le procedure stesse non sono sofisticate, ma rappresentano la formalizzazione delle prassi esistenti.
4 Gestito e Misurabile - Il management misura e monitora la conformità alle procedure e adotta misure correttive nel caso in cui i processi non funzionino efficacemente. I processi sono sottoposti ad un costante miglioramento e forniscono buone prassi. L'uso dell'automazione e degli strumenti è limitato o frammentario.
5 Ottimizzato - I processi sono stati portati ad un livello di *good practice*, basandosi sui risultati di un continuo miglioramento e confrontando il grado di strutturazione con altre imprese. L'IT è utilizzato in modo integrato per automatizzare il workflow, fornire strumenti per migliorare qualità ed efficacia e rendere l'impresa più veloce nell'adattarsi ai cambiamenti.

Sebbene una capacità applicata in modo appropriato sia già in grado di ridurre i rischi, un'impresa deve comunque analizzare i controlli necessari per assicurare che il rischio sia mitigato e che si ottenga valore rimanendo in linea con la propensione al rischio e gli obiettivi dell'azienda. Tali controlli sono indicati dagli obiettivi di controllo di COBIT. L'Appendice III fornisce un modello di maturità sul controllo interno che illustra la maturità di un'impresa per quanto riguarda la creazione e la performance del controllo interno. Spesso, tale analisi viene effettuata in risposta a sollecitazioni esterne, ma idealmente dovrebbe essere istituzionalizzata, come documentato dai processi di COBIT P06 *Comunicare gli obiettivi ed indirizzi della direzione* e ME2 *Monitorare e valutare il controllo interno.*

Capacità, prestazione e controllo rappresentano gli aspetti della maturità del processo, come illustrato nella **figura 14**.

Figura 14 – Le tre dimensioni della maturità



Il modello di maturità è un modo per misurare il livello dei processi sviluppati dal management, cioè quanto siano effettivamente adeguati. Il livello di sviluppo o l'adeguatezza che dovrebbero raggiungere dipendono innanzitutto dagli obiettivi IT e dalle esigenze aziendali che essi devono supportare. Quanto di quella capacità è effettivamente impiegata dipende in larga parte dal ritorno che un'impresa vuole dai propri investimenti. Per esempio, ci potrebbero essere processi e sistemi critici che necessitano una gestione della sicurezza maggiore e più accurata rispetto a quella richiesta da quelli meno critici. D'altro lato, il grado e la sofisticazione dei controlli che devono essere applicati in un processo sono influenzati principalmente dalla propensione al rischio dell'impresa e dai requisiti di conformità applicabili.

I livelli del modello di maturità aiuteranno gli specialisti a spiegare ai manager dove esistano carenze nella gestione dei processi IT e a fissare gli obiettivi da raggiungere. Il corretto livello di maturità sarà influenzato dagli obiettivi aziendali dell'impresa, dall'ambiente operativo e dalle prassi del settore. Precisamente, il livello di maturità della gestione dipenderà dalla dipendenza dell'impresa dall'IT, dalla complessità della propria tecnologia e, soprattutto, dal valore delle proprie informazioni.

Un punto di riferimento strategico per l'impresa che intende migliorare la gestione ed il controllo dei processi IT si può trovare negli standard internazionali emergenti e nelle best practice. Le prassi che sono oggi emergenti potranno rappresentare un domani il livello atteso della performance e per questo sono utili nella pianificazione delle aziende che vogliano essere in anticipo sui tempi.

I modelli di maturità sono costruiti a partire dal modello qualitativo generico (vedi **figura 13**), cui si aggiungono in maniera crescente con l'aumentare del livello i criteri derivanti dai seguenti attributi:
- Consapevolezza e comunicazione
- Politiche, piani e procedure
- Strumenti ed automazione
- Esperienza e competenze
- Responsabilità e accountability
- Definizione e misurazione degli obiettivi

La tabella degli attributi di strutturazione mostrata in **figura 15** elenca le caratteristiche delle modalità di gestione dei processi IT e descrive come si evolvono dallo stato di "non esistente" a quello di "ottimizzato". Questi attributi possono essere utilizzati per valutazioni più complessive, per analisi delle varianze e per pianificare i miglioramenti.

In sintesi, i modelli di maturità forniscono un profilo generico degli stadi attraverso cui l'impresa evolve per la gestione ed il controllo dei processi IT, e sono:
- un insieme di requisiti e gli aspetti abilitanti ai vari livelli di strutturazione
- una scala che permette di misurare facilmente le differenze
- una scala che si presta ad un confronto pragmatico
- una base per definire la posizione attuale ("as-is") e quella desiderata ("to-be")
- un supporto per l'analisi delle varianze per determinare cosa debba essere fatto al fine di raggiungere il livello prescelto
- nel loro insieme, una visione delle modalità di gestione dell'IT nell'impresa.

I modelli di maturità di COBIT si focalizzano sulla capacità, ma non necessariamente sulla copertura o il dettaglio del controllo. Non sono numeri da raggiungere, né sono stati pensati per presentare livelli soglia ufficiali difficili da passare ai fini di una certificazione. Comunque sono stati pensati per essere sempre applicabili, ed i loro livelli forniscono descrizioni tra le quali l'impresa può riconoscere quella che più si adatta ai propri processi. Il livello giusto è determinato dal tipo di impresa, dal suo ambiente e dalla sua strategia.

Il grado di copertura, il dettaglio del controllo, e come la capacità sia utilizzata e fornita, sono decisioni soggette ad una analisi costi-benefici. La performance, o il modo di utilizzare più o meno efficacemente le capacità, dipendono da decisioni basate sul rapporto costi-benefici. Per esempio, un alto livello di gestione della sicurezza può doversi concentrare solo sui sistemi maggiormente critici.

Infine, mentre il controllo sul processo aumenta con l'aumentare del livello di maturità, l'impresa ha ancora bisogno di analizzare quale meccanismo di controllo debba applicare, sulla base di fattori di rischio e di valore. In tale analisi, un aiuto proviene dagli obiettivi generici dell'azienda e dell'IT definiti in questo schema di riferimento. I meccanismi di controllo sono guidati dagli obiettivi di controllo di COBIT e si concentrano sui contenuti del processo, mentre i modelli di maturità si concentrano principalmente sulla qualità della gestione del processo. L'Appendice III fornisce un modello di maturità generico che illustra lo stato dell'ambiente di controllo interno e l'istituzione dei controlli interni di un'azienda.

L'ambiente di controllo può risultare implementato in modo appropriato una volta che si siano presi in considerazione tutti e tre gli aspetti della maturità (capacità, performance e controllo). Il miglioramento della maturità riduce il rischio e migliora l'efficienza, in quanto porta a ridurre gli errori, avere processi più prevedibili ed utilizzare le risorse con una efficienza dei costi.

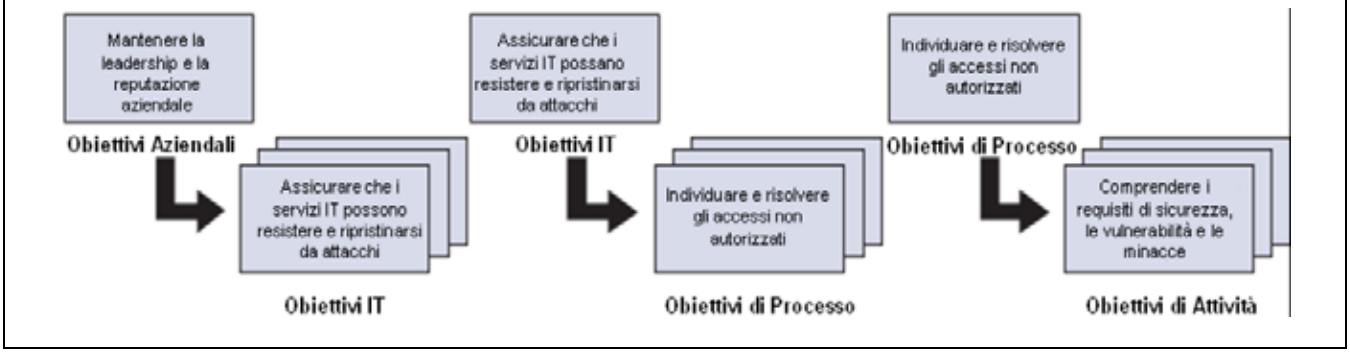
MISURAZIONE DELLE PRESTAZIONI
Obiettivi e metriche sono definiti in COBIT su tre livelli:
- obiettivi IT e metriche che definiscono cosa il business si aspetta dall'IT e come misurarlo
- obiettivi di processo e metriche che definiscono cosa deve produrre il processo IT per supportare gli obiettivi dell'IT e come misurarlo
- obiettivi delle attività e metriche in modo che sia stabilito cosa è necessario accada all'interno del processo per ottenere la performance richiesta e come misurare tutto ciò

	Consapevolezza e Comunicazione	Politiche, Piani e Procedure	Strumenti ed automazione	Esperienza e competenza	Responsabilità	Definizione e misurazione degli obiettivi
1	Si percepisce la necessità di un processo. La comunicazione dei problemi è sporadica.	Ci sono approcci *ad hoc* per i processi e le prassi. I processi e le politiche non sono definite.	Potrebbero esistere alcuni strumenti; la pratica si basa su strumenti standard da scrivania. Non c'è un approccio pianificato nell'uso degli strumenti.	Le esperienze richieste per i processi non sono identificate. Non esiste un piano per la formazione e non viene svolta attività formale di istruzione.	Non c'è definizione di responsabilità e di incarichi. Il personale si assume la responsabilità delle problematiche reattivamente sulla base di proprie iniziative.	Gli obiettivi non sono chiari e non viene effettuata alcuna misurazione
2	C'è consapevolezza della necessità di intervenire. Il management comunica le problematiche principali.	Emergono processi simili e comuni, ma sono largamente intuitivi e basati sulle conoscenze dei singoli. Alcuni aspetti dei processi sono ripetibili sulla base delle conoscenza individuali e si possono trovare sia documentazione sia informale comprensione di politiche e procedure.	Esistono approcci comuni all'utilizzo degli strumenti, ma si basano su soluzioni sviluppate da persone chiave. Potrebbero essere stati acquisti strumenti di mercato, ma probabilmente non vengono utilizzati correttamente o addirittura non utilizzati.	Requisiti minimi di esperienza sono identificate per le aree critiche. La formazione viene effettuata in risposta alle necessità, piuttosto che sulla base di un piano concordato, e viene svolta informalmente formazione sul campo.	Un individuo assume le proprie responsabilità e ne è solitamente ritenuto responsabile, anche se ciò non è stabilito formalmente. Si verifica una certa confusione riguardo la responsabilità quando si verificano dei problemi e tende ad affermarsi la cultura della "colpa".	Sono definiti alcuni obiettivi; sono stabilite alcune misure di fenomeni finanziari, ma solo l'alta direzione ne è al corrente. Un monitoraggio non affidabile copre alcune aree.
3	La necessità di intervenire è compresa. Il management è più formale e strutturato nelle proprie comunicazioni.	Cresce l'utilizzo di buone prassi. I Processi, le politiche e le procedure sono definiti e documentati per tutte le attività principali.	Viene definito un piano per l'utilizzo e la standardizzazione di strumenti per automatizzare il processo. Gli strumenti sono utilizzati per le loro finalità di base, ma potrebbero non essere allineati al piano concordato, e potrebbero non essere integrati tra loro.	I requisiti di esperienza sono definiti e documentati in ogni area. Un piano formale di formazione è stato sviluppato, ma l'attività formativa è ancora basata su iniziative personali.	Le responsabilità nella struttura dei processi sono definite ed i proprietari dei processi sono stati identificati. Il proprietario del processo è improbabile che abbia la piena autorità per esercitare la responsabilità..	Sono definiti alcuni obiettivi di efficacia ed alcune misurazioni, ma non sono stati comunicati, e c'è un chiaro legame con gli obiettivi aziendali. Sono evidenti processi di misurazione, ma non sono applicati regolarmente. L'idea dei cruscotti aziendali è adottata, come l'applicazione occasionale e intuitiva dell'analisi delle cause principali.
4	Sono compresi tutti i requisiti. Sono utilizzate tecniche mature di comunicazione e vengono impiegati strumenti standard di comunicazione.	Il processo è affidabile e completo; vengono applicate best-practice interne. Tutti gli aspetti del processo sono documentati e ripetibili. Le politiche sono state approvate e sottoscritte dal management. Sono adottati e seguiti standard per lo sviluppo e la manutenzione dei processi e delle procedure.	Gli strumenti sono sviluppati sulla base di un piano standardizzato ed alcuni sono stati integrati con altri strumenti. Gli strumenti sono usati nelle aree principali per automatizzare la gestione dei processi e monitorare attività e controlli critici.	I requisiti per le competenze sono aggiornati ciclicamente per tutte le aree, un buon livello di competenza è assicurato per tutte le aree critiche e la certificazione è incoraggiata. Tecniche di formazione mature sono applicate in conformità al piano di formazione e la condivisione della conoscenza è incoraggiata. Tutti gli esperti di domini interni sono coinvolti e l'efficacia del piano di formazione è verificata	Le responsabilità nella struttura dei processi sono accettate e funzionano in modo tale che il responsabile del processo possa far fronte completamente alle proprie responsabilità. È in essere una cultura nel sistema premiante che motiva le azioni positive.	L'efficacia e l'efficienza sono misurate e comunicate, legate agli obiettivi aziendali ed al piano strategico IT. Il cruscotto aziendale dell'IT è implementato in alcune aree nelle quali il management ha riscontrato delle eccezioni e l'analisi delle cause principali è stata standardizzata. Si rende evidente un miglioramento continuo.
5	La coscienza dei requisiti è avanzata e prospettica. Esiste una comunicazione proattiva delle problematiche basata sulle tendenze, sono utilizzate tecniche mature di comunicazione e vengono impiegati strumenti integrati di comunicazione.	Sono applicate best-practice e standard esterni. La documentazione dei processi si è evoluta in un workflow automatico. Processi, politiche e procedure sono standardizzate e integrate per consentire una gestione ed un miglioramento end-to-end.	Insiemi di strumenti standardizzati vengono utilizzati su tutta l'impresa. Gli strumenti sono pienamente integrati con gli altri strumenti per consentire un supporto completo del processo. Gli strumenti sono utilizzati per supportare il miglioramento dei processi ed individuare automaticamente le eccezioni ai controlli.	L'azienda incoraggia formalmente il continuo miglioramento della competenza, basato su obiettivi personali ed aziendali definiti chiaramente. La formazione e la istruzione supportano best practice esterne e l'uso di concetti e tecniche avanzate. La condivisione della conoscenza è parte della cultura aziendale e vengono sviluppati sistemi basati sulla conoscenza. Esperti esterni e industrie leader sono utilizzati per definire gli indirizzi.	I responsabili di processo sono autorizzati a prendere decisioni ed iniziative. L'accettazione di responsabilità è stata realizzata con un modello a cascata all'interno dell'organizzazione con un approccio importante.	È stato predisposto un sistema di misurazione integrato delle prestazioni che lega le performance IT agli obiettivi aziendali attraverso una generale applicazione del cruscotto aziendale. Le eccezioni sono registrate dal management in tutti i processi e con regolarità ed è svolta l'analisi delle cause principali. Il miglioramento continuo è uno stile di vita.

Figura 15 – Tabella degli attributi di strutturazione

Gli obiettivi sono definiti top-down in modo tale che un obiettivo aziendale determina gli obiettivi IT che lo supportano. Un obiettivo IT è conseguito da un processo o dall'interazione di più processi. Pertanto, gli obiettivi IT aiutano a definire gli obiettivi dei processi. Similmente, ogni obiettivo di processo necessita di un certo numero di attività, di conseguenza definisce gli obiettivi delle attività. La **Figura 16** fornisce degli esempi di relazione tra gli obiettivi aziendali, IT, di processo e di attività.

Figura 16 – Esempi di relazione fra gli obiettivi



I termini KGI e KPI, usati nelle precedenti versioni di COBIT, sono stati sostituiti con due tipi di metriche:
- Indicatori di risultato, precedentemente chiamati *indicatori chiave degli obiettivi* (KGI), definiscono se gli obiettivi sono stati conseguiti. Questi indicatori possono essere utilizzati solo a consuntivo dopo l'esecuzione della fase, e perciò sono chiamati "*lag indicators*" (indicatori "a posteriori" o "ex post").
- Indicatori di prestazione, precedentemente chiamati *indicatori chiave delle prestazioni* (KPI), definiscono se gli obiettivi saranno raggiunti. Questi indicatori possono essere utilizzati prima che il risultato sia ottenuto, e perciò sono chiamati "*lead indicators*" (indicatori di tendenza o "ex ante").

La **figura 17** illustra delle possibili misurazioni dei risultati e degli obiettivi degli esempi utilizzati.

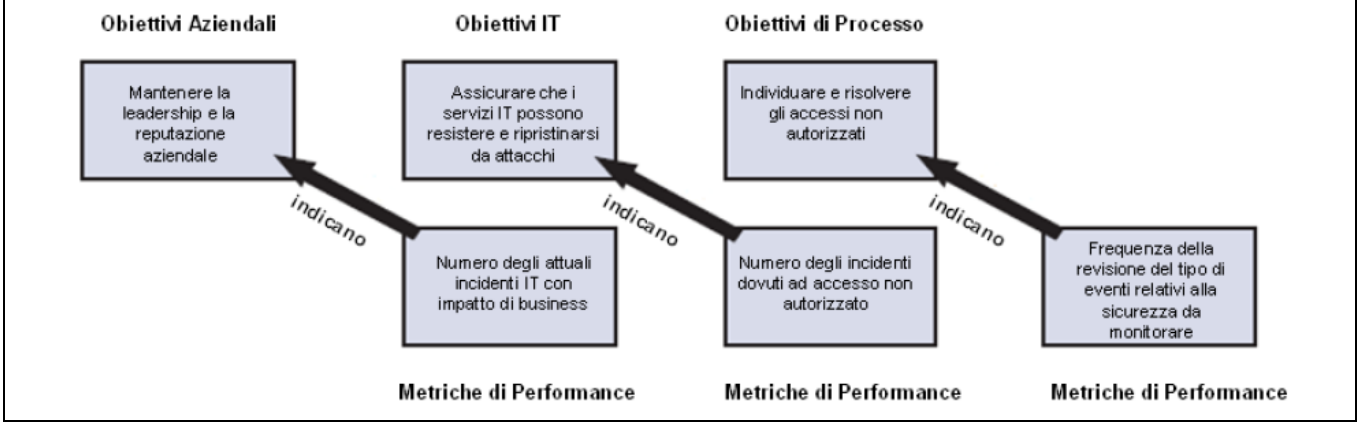
Figura 17 – Possibili misure di risultato per l'esempio di figura 16

Le misurazioni di risultato di un livello inferiore diventano indicatori di performance di un livello superiore. Come nell'esempio di **figura 16**, la misurazione di risultato che identifica la rilevazione e la risoluzione di un accesso non autorizzato, sia anche un indicatore per verificare se un servizio IT possa resistere ed essere ripristinato, in caso di attacco. Da cui, la misurazione di risultato diventa un indicatore di performance per l'obiettivo del livello superiore. La **figura 18** illustra come le misurazioni di risultato nell'esempio diventano metriche di performance.

Le misurazioni di risultato definiscono misure che dicono al management – a consuntivo – se una funzione, processo o attività IT ha raggiunto i propri obiettivi. Le misure di risultato delle funzioni IT sono solitamente espresse in termini di criteri di valutazione delle informazioni:
- disponibilità delle informazioni necessarie per supportare le esigenze aziendali
- assenza di rischi per l'integrità e la riservatezza
- efficienza dei costi di processi ed operazioni
- conferma di affidabilità, efficacia e conformità.

Gli indicatori di performance definiscono misure che determinano come il processo IT sta operando per consentire il raggiungimento degli obiettivi. Costituiscono i principali indicatori della probabilità che un obiettivo possa essere raggiunto o meno, pertanto indirizzando gli obiettivi di livello superiore. Spesso misurano la disponibilità di una adeguata capacità, esperienza e competenza, e del risultato delle sottostanti attività. Per esempio, un servizio fornito dall'IT è un obiettivo per l'IT stesso ma è un indicatore di performance e di capacità per il business. Ecco perché gli indicatori di performance sono talvolta indicati come *performance drivers,* soprattutto nelle *balanced scorecard*.

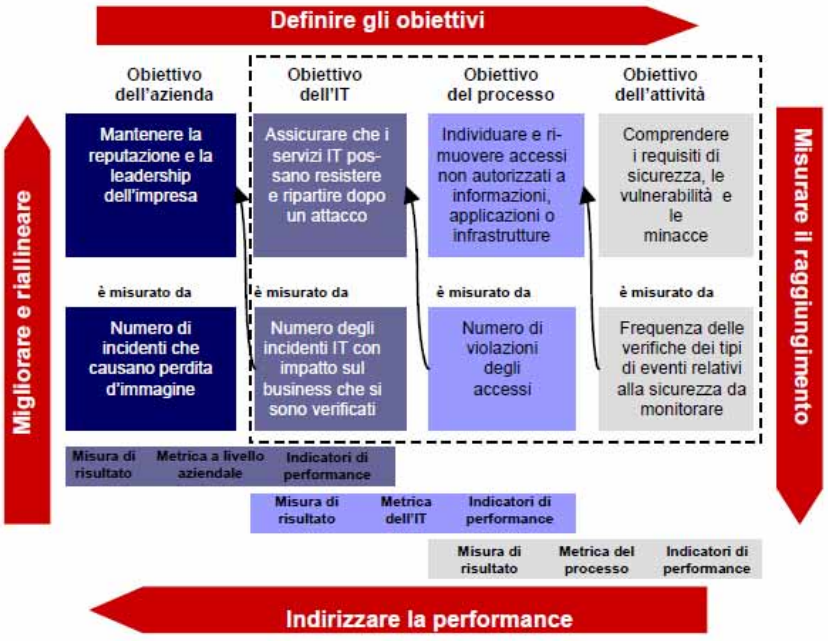
Figura 18 – Possibili Indicatori di Performance relative all'esempio in figura 16



Pertanto, le metriche fornite sono sia una misura di risultato delle funzioni IT, dei processi IT o degli obiettivi di attività che misurano, sia anche un indicatore di performance che supporta gli obiettivi di alto livello aziendali, delle funzioni IT o del processo IT.

La **figura 19** illustra la relazione tra gli obiettivi aziendali, dell'IT, dei processi e delle attività, e le varie metriche. Da sinistra in alto a destra in alto, sono illustrati gli obiettivi in cascata. Sotto l'obiettivo si trova la sua misurazione di risultato. La frecce sottili indicano che la stessa metrica è anche un indicatore di performance per l'obiettivo di livello superiore.

Figura 19 – Relazione tra Processi, Obiettivi e Metriche (DS5)

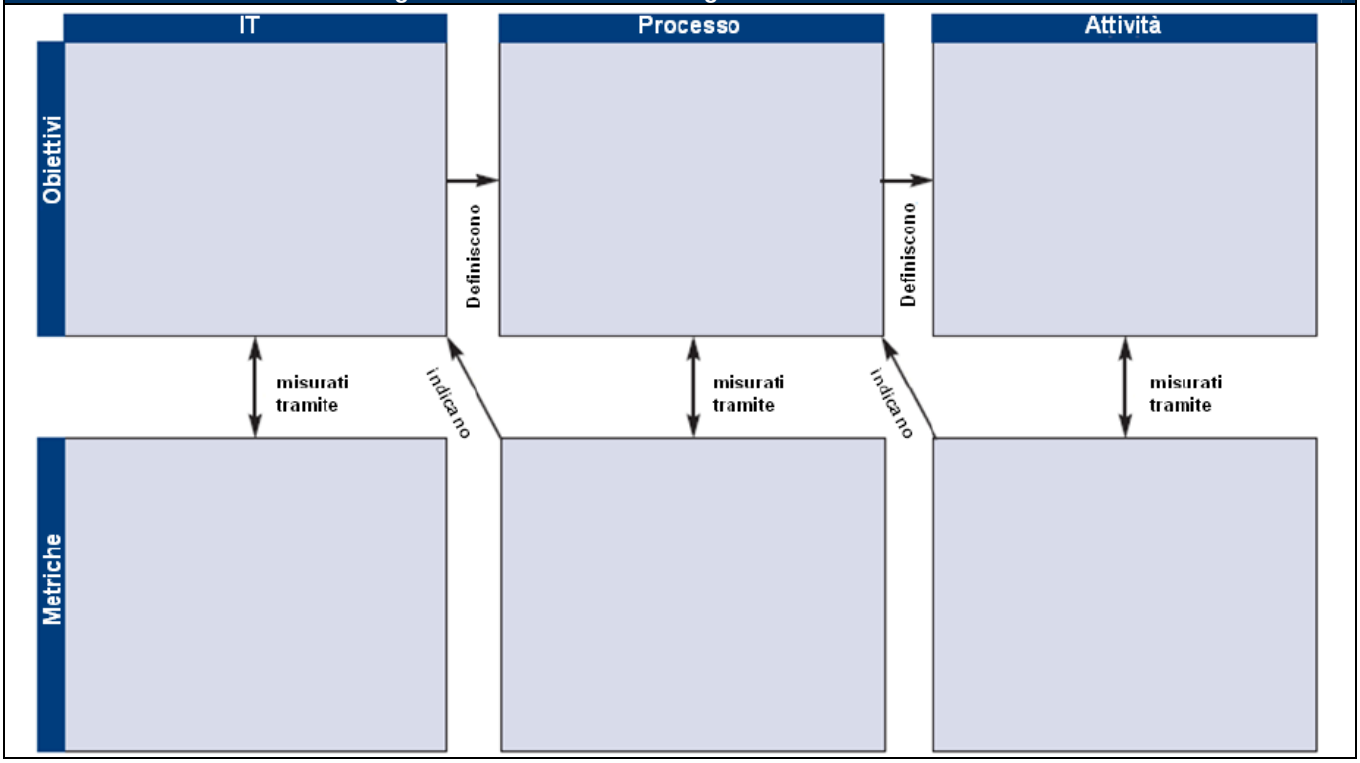


L'esempio è tratto dal processo DS5 *Garantire la sicurezza dei sistemi*. COBIT fornisce metriche solo fino ai risultati degli obiettivi IT, come delimitato dalle linee tratteggiate. Anche se sono indicatori di performance per gli obiettivi di business per l'IT, COBIT non fornisce misure di risultato per gli obiettivi di business.

Gli obiettivi IT e di business utilizzati nella sezione delle metriche ed obiettivi di COBIT, comprese le rispettive relazioni, sono riportati nell'appendice I. Per ciascun processo IT di COBIT, sono illustrati gli obiettivi e le metriche, come si può osservare nella **figura 20**.

Le metriche sono state sviluppate considerando le seguenti caratteristiche:
- Un elevato rapporto *insight-to-effort,* (cioè la concentrazione sulla performance e sul conseguimento dell'obiettivo a confronto dell'impegno per raggiungerlo)
- confrontabili internamente (per esempio, in percentuale rispetto ad una soglia o a valori nel tempo)
- confrontabili esternamente, a prescindere dalla dimensione dell'impresa o dal settore di attività
- meglio avere poche metriche buone (se ne può avere anche una sola molto buona, che può essere influenzata da fonti diverse) piuttosto che una lunga lista di metriche di qualità inferiore
- facile da misurare, e non essere confusa con gli obiettivi.

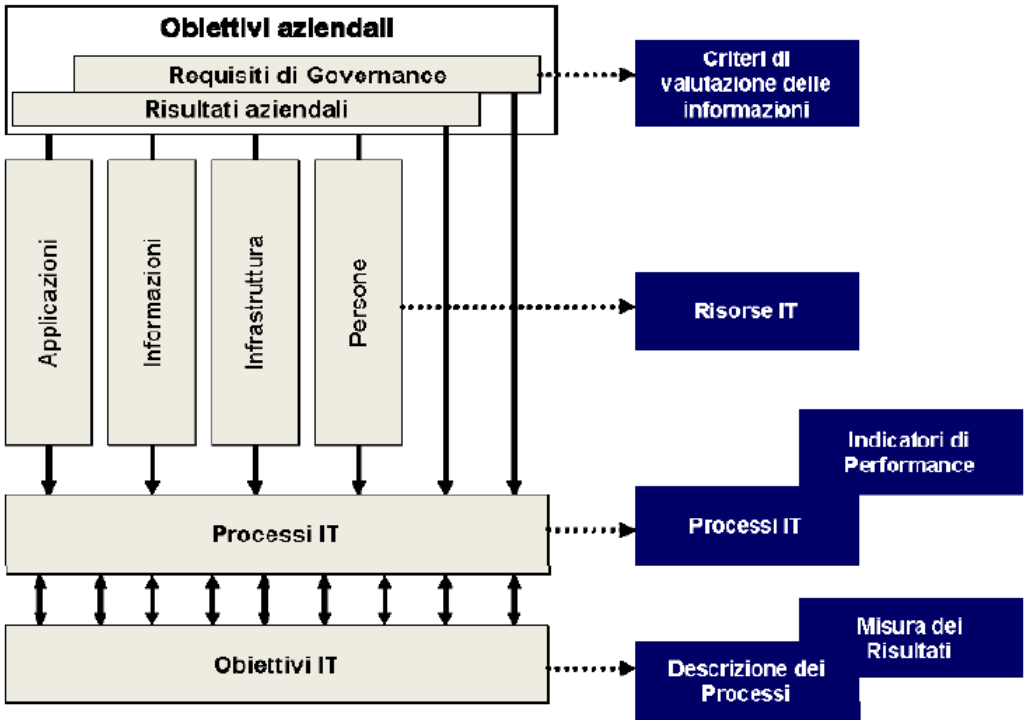
Figura 20 – Presentazione degli Obiettivi e le Metriche



IL Modello del Quadro di Riferimento di COBIT

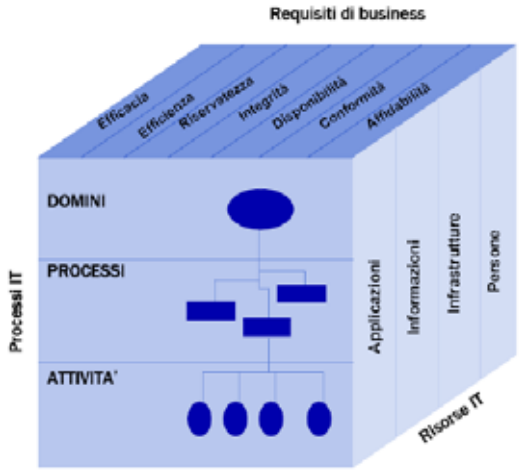
Il quadro di riferimento di COBIT, pertanto, collega i requisiti informativi e di governo dell'azienda con gli obiettivi della funzione IT. Il modello di processo di COBIT permette di gestire e controllare adeguatamente le attività IT e le risorse che le supportano, basandosi sugli obiettivi di controllo di COBIT, permette di mantenerle allineate al business e monitorate utilizzando gli obiettivi e le metriche di COBIT, come mostrato nella **figura 21**.

Figura 21 – Gestione, controllo, allineamento e monitoraggio di COBIT



In sintesi, le risorse IT sono gestite da processi IT per conseguire obiettivi IT che soddisfano requisiti aziendali. Questo è il principio base del modello di COBIT, come illustrato nel cubo di COBIT (**figura 22**).

Figura 22 – Il cubo di COBIT



Più in dettaglio, il quadro di riferimento di COBIT può essere rappresentato graficamente nel suo insieme come nella **figura 23**, con il modello di processo di COBIT strutturato in quattro domini, che raggruppano 34 processi generalizzati, e gestiscono le risorse IT per fornire all'azienda informazioni in linea con i requisiti aziendali e di governance.

L'accettabilità generale di COBIT

COBIT è basato sull'analisi e sull'armonizzazione degli standard IT e delle good practice esistenti ed è conforme ai principi di governo generalmente accettati. Si posiziona ad un alto livello, si basa sui requisiti aziendali, copre l'intera gamma delle attività dell'IT, e si concentra sugli obiettivi (*cosa*) da raggiungere piuttosto che sulle modalità (*come*) per raggiungere una governance, una gestione ed un controllo efficaci. Perciò, funge da integratore delle prassi di governance dell'IT e si rivolge all'alta direzione, alla direzione aziendale e dell'IT, ai *professional* delle aree governance, assurance/certificazione e sicurezza, così come ai *professional* dell'audit e del controllo informatico. È stato disegnato per essere complementare ad altri standard e good practice, ed essere usato assieme ad essi.

L'implementazione delle good practice deve essere coerente con il modello di riferimento per il governo ed il controllo dell'impresa, adeguata all'organizzazione, ed integrata con altri metodi e prassi in uso. Standard e good practice non sono una panacea e la loro efficacia dipende da come sono stati effettivamente implementati e mantenuti aggiornati. Risultano molto utili soprattutto quando sono applicati come espressione di un insieme di principi e come punto di partenza per predisporre procedure specifiche su misura. Per evitare che tali pratiche restino inutilizzate, il management e lo staff dovrebbero comprendere cosa fare, come farlo e perché è importante.

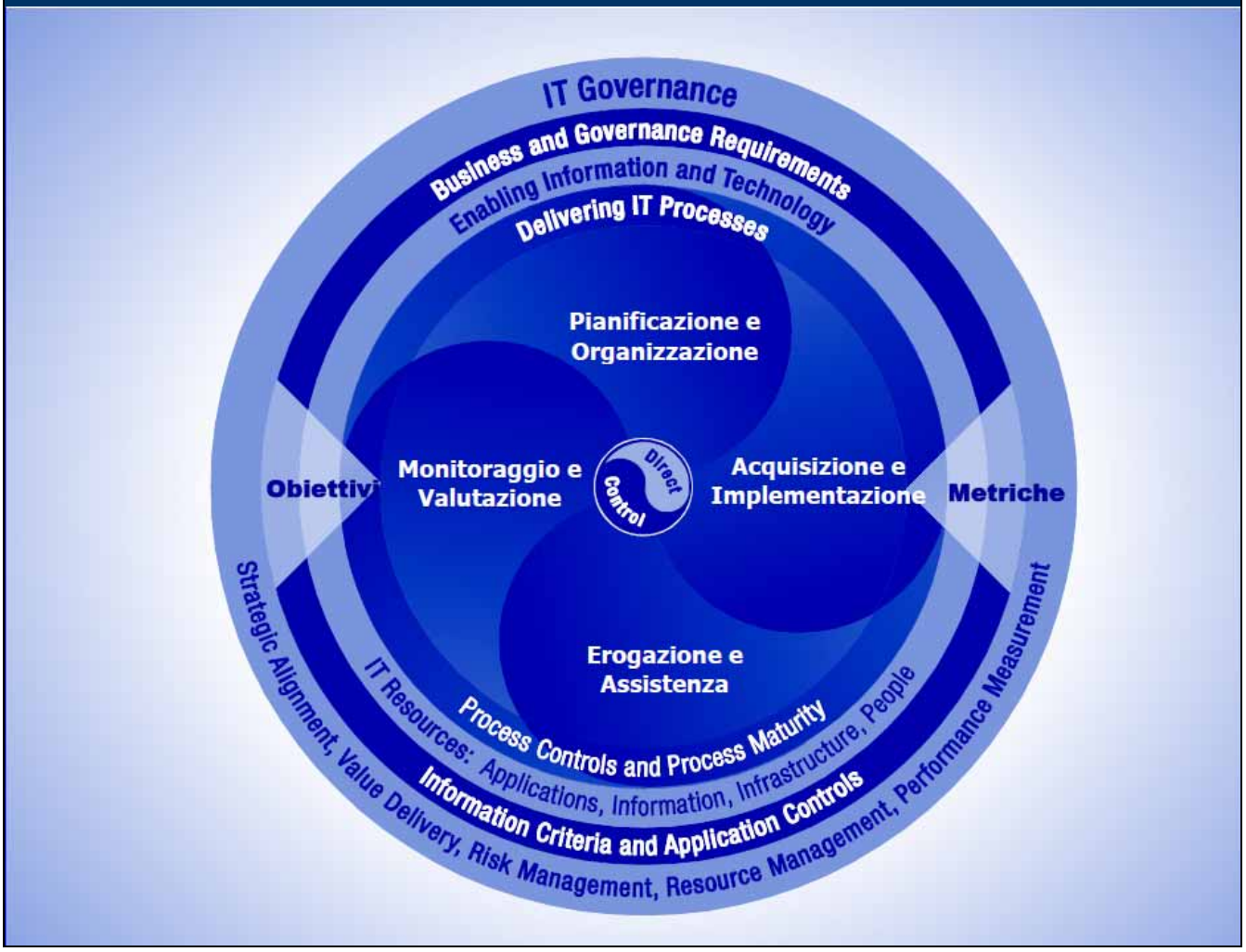
Per raggiungere l'allineamento delle good practice ai requisiti aziendali, si raccomanda di utilizzare COBIT al più alto livello, fornendo un modello di riferimento globale basato su un modello di processo IT che deve genericamente andare bene per ogni impresa. Prassi e standard specifici relativi ad aree diverse possono essere rilevati facendo riferimento a COBIT, fornendo così una serie di materiali strutturati da utilizzare come guida.

COBIT si rivolge a vari tipi di utenti:
- **Alta Direzione (executive management)** – per ottenere valore dagli investimenti in IT e bilanciare i rischi e gli investimenti in controlli in un ambiente IT spesso imprevedibile
- **Dirigenti dell'azienda (business management)** – per ottenere assicurazioni sulla gestione e sul controllo dei servizi IT forniti da strutture interne o da terze parti
- **Dirigenti dell'IT (IT management)** – per fornire i servizi IT, richiesti dall'azienda per supportare la propria strategia, in modo controllato e gestito
- **Revisori (auditors)** – per sostanziare le loro opinioni e/o fornire raccomandazioni ai dirigenti in tema di controlli interni.

COBIT è stato sviluppato ed è gestito da un istituto di ricerca indipendente senza scopo di lucro, che si avvale dell'esperienza dei membri dei capitoli ad essa affiliati, degli esperti del settore, e di specialisti in materia di controlli e sicurezza. Il suo contenuto è basato sulla continua ricerca nelle good practice dell'IT ed è continuamente tenuto aggiornato, costituendo così una risorsa oggettiva e concreta per tutti i tipi di utente.

COBIT è orientato agli obiettivi e all'ambito del governo dell'IT, assicurando che il suo schema di riferimento per i controlli sia completo, allineato con i principi di governance dell'impresa e, perciò, accettabile da parte di consigli di amministrazione, direzione, revisori e organismi di controllo. L'Appendice II riporta una mappatura di come gli obiettivi di controllo di COBIT si pongano nei confronti delle cinque aree della governance dell'IT e delle attività di controllo del COSO.

Figura 23 – Il quadro generale di riferimento di COBIT



La **figura 24** riassume come i diversi elementi dello schema di riferimento di COBIT si rapportano alle aree principali della governance dell'IT.

Figura 24 – Il quadro di riferimento di COBIT e le principali aree della Governance dell'IT

	Obiettivi	Metriche	Prassi	Modelli di maturità
Allineamento strategico	P	P		
Erogazione del valore		P	S	P
Gestione del rischio		S	P	S
Gestione delle risorse		S	P	P
Misurazione delle prestazioni	P	P		S

P = fattore primario S = fattore secondario

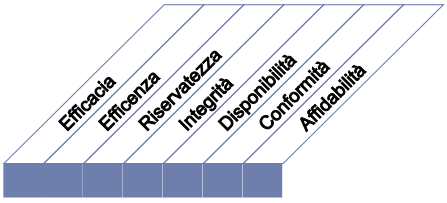
COME USARE QUESTO LIBRO

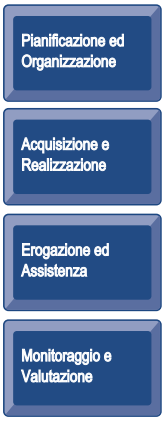
La navigazione attraverso lo schema di riferimento di COBIT

Per ognuno dei processi IT del COBIT si definisce un obiettivo di controllo di alto livello, che viene presentato insieme agli obiettivi chiave ed alle metriche in una struttura a cascata (**figura 25**).

Figura 25 – La navigazione nel modello di COBIT

Nell'ambito di ciascun processo, gli obiettivi di controllo sono presentati utilizzando descrizioni di azioni generalizzate del livello minimo di good practice di gestione tali da assicurare che il processo sia mantenuto sotto controllo.





Il controllo del processo IT

nome del Processo

che soddisfa i requisiti aziendali per l'IT di

sintesi dei principali obiettivi IT

ponendo l'attenzione su

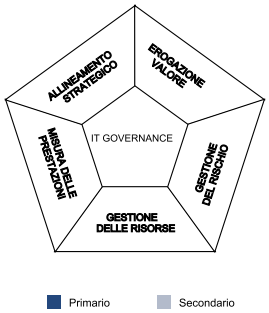
sintesi dei più importanti obiettivi del processo

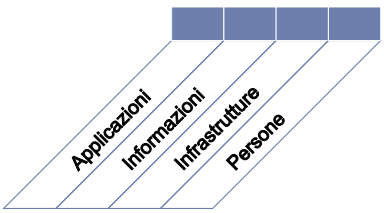
è ottenuto tramite

obiettivi delle attività

e viene misurato tramite

metriche principali





Indice dei componenti principali di COBIT

Lo schema di riferimento di COBIT è popolato dai componenti principali, indicati nel corso di questa pubblicazione e organizzati nei 34 processi IT, che forniscono un quadro completo di come controllare, gestire, e misurare ogni processo. Ogni processo è sviluppato in quattro sezioni, ciascuna di circa una pagina, come segue:

- la Sezione 1 (**Figura 25**) contiene la descrizione del processo e la sintesi degli obiettivi, la descrizione è presentata attraverso un paradigma "a cascata" . Questa pagina inoltre mostra il rapporto tra il processo e i criteri di valutazione delle informazioni, le risorse IT e le relative aree di governo dell'IT indicando con una P le relazioni principali e con una S quelle secondarie.
- la Sezione 2 contiene gli obiettivi di controllo per questo processo.
- la Sezione 3 contiene gli input e output del processo, una tabella RACI, gli obiettivi e le metriche.
- la Sezione 4 contiene il modello di strutturazione del processo.

Un altro modo di vedere il contenuto della performance del processo è:
• Gli input di processo sono quelli che il referente del processo ha bisogno di ricevere dagli altri.
• Gli obiettivi di controllo descrivono quello che il referente del processo deve fare.
• Gli output di processo sono i risultati che il referente del processo deve produrre.
• Gli obiettivi e le metriche illustrano come il processo deve essere misurato.
• La tabella RACI definisce cosa deve essere delegato ed a chi.
• Il modello di strutturazione mostra cosa deve essere fatto per migliorare il processo.

I ruoli presenti nella tabella RACI sono classificati per tutti i processi come:
• Amministratore delegato o Direttore Generale (Chief Executive Officer – CEO)
• Direttore Amministrativo (Chief Financial Officer – CFO)
• Dirigenti aziendali – Direttori utenti del servizio IT
• Direttore dell'IT (Chief Information Officer – CIO)
• Referente del processo aziendale (Business Process Owner)
• Responsabile operativo
• Responsabile architetture IT
• Responsabile dello sviluppo IT
• Responsabile amministrativo dell'IT (per le imprese di grandi dimensioni, il responsabile di funzioni quali risorse umane, budgeting e controllo interno)
• La funzione o il Responsabile della gestione dei progetti (PMO)
• Conformità, audit, rischio e sicurezza (gruppi con responsabilità di controllo che non hanno responsabilità operative nell'IT)

Alcuni processi specifici prevedono ulteriori funzioni specializzate, come il service desk o l'incident manager nel DS8.

È bene precisare che mentre il materiale è stato raccolto da centinaia di esperti, a seguito di ricerche e verifiche rigorose, gli input, gli output, le responsabilità, le metriche e gli obiettivi sono elementi puramente descrittivi e quindi per loro natura non vincolanti o esaustivi. Essi forniscono una base di conoscenze di alto livello da cui ogni azienda può trarre quelle che più le si adattano in termini di efficacia ed efficienza, in base alla strategia, agli obiettivi e alle politiche che si è data.

Utilizzatori dei componenti di COBIT

La direzione può usare il supporto di COBIT per valutare i processi IT utilizzando gli obiettivi aziendali e gli obiettivi IT dettagliati nell'appendice I, per chiarire gli obiettivi dei processi IT ed il modello di strutturazione del processo per valutare le performance attuali.

Chi definisce i processi e gli auditor possono identificare dei pratici requisiti di controllo dagli obiettivi di controllo e le responsabilità dalle attività e dalle relative tabelle RACI.

Tutti i potenziali utilizzatori possono beneficiare dei componenti di COBIT per un generico approccio alla gestione ed al governo dell'IT, unitamente ad altri standard specifici quali:
• ITIL per la gestione dei servizi (service delivery)
• CMM per lo sviluppo delle soluzioni (solution delivery)
• ISO/IEC 27002:2005 per la sicurezza delle informazioni (information security)
• PMBOK o PRINCE2 per la gestione dei progetti (project management)

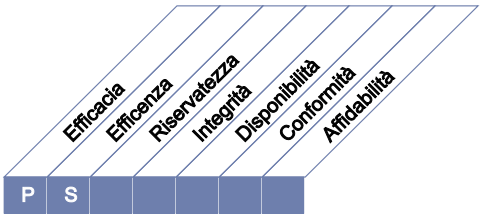
Appendici

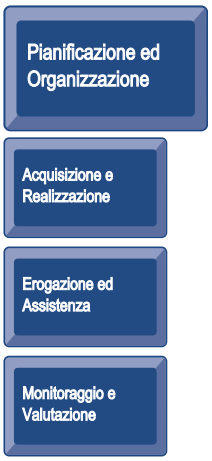
Le seguenti sezioni contenenti riferimenti aggiuntivi sono riportate alla fine del libro:
I. Tables Linking Goals and Processes (three tables)
II. Mapping IT Processes to IT Governance Focus Areas, COSO, COBIT IT Resources and COBIT Information Criteria
III. Maturity Model for Internal Control
IV. COBIT 4.1 Primary Reference Material
V. Cross-references Between COBIT® 3rd Edition© and COBIT 4.1
VI. Approach to Research and Development
VII. Glossario
VIII. COBIT and Related Products.

DESCRIZIONE DEL PROCESSO

PO1 Definire un piano strategico per l'IT

La pianificazione strategica dell'IT è necessaria per gestire tutte le risorse IT coerentemente con la strategia e le priorità aziendali. La funzione IT e tutti i soggetti aziendali interessati hanno la responsabilità di massimizzare il valore dei servizi e dei progetti. Il piano strategico permette ai principali soggetti interessati di comprendere le opportunità ed i limiti dell'IT, valutare la performance attuale, identificare i requisiti tecnici e delle risorse umane, chiarire il livello degli investimenti necessari. La strategia e le priorità aziendali devono essere riflesse nei prodotti e servizi e attuate attraverso uno o più piani tattici che definiscano sintetici obiettivi, piani e attività che siano chiari e condivisi sia dalla parte business sia da quella IT dell'azienda.





Il controllo del processo IT

Definire un piano strategico per l'IT

che soddisfa i requisiti aziendali per l'IT di

sostenere o integrare la strategia aziendale e i requisiti di governance mantenendo trasparenza per quanto riguarda costi, rischi e benefici

ponendo l'attenzione su

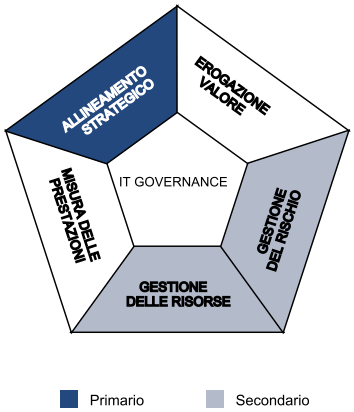
l'integrazione di business e IT nel trasformare le esigenze aziendali in offerte di servizi e lo sviluppo di strategie per fornire tali servizi in modo trasparente ed efficace.

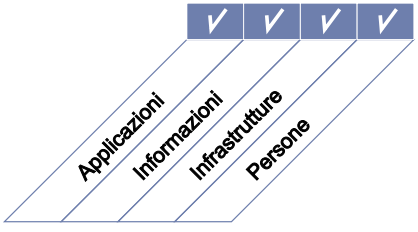
è ottenuto tramite

- il coinvolgimento del management aziendale e dell'alta direzione nell'allineamento della pianificazione strategica dell'IT rispetto alle esigenze aziendali presenti e future
- la comprensione delle attuali capacità dell'IT
- la definizione di uno schema per stabilire le priorità degli obiettivi che quantifichi i requisiti aziendali

e viene misurato tramite

- la percentuale degli obiettivi IT contenuti nel relativo piano strategico a supporto del piano strategico aziendale
- la percentuale dei progetti IT contenuti nel relativo portafoglio che si possono ricollegare direttamente ai piani tattici dell'IT
- il ritardo tra gli aggiornamenti del piano strategico di IT e quelli dei relativi piani tattici





OBIETTIVI DI CONTROLLO

PO1 Definire un piano strategico per l'IT

PO1.1 Gestione del Valore

Collaborare con l'azienda affinché il portafoglio degli investimenti dell'impresa resi possibili dall'IT contenga programmi con business case consistenti. Riconoscere che ci sono vari tipi di investimenti, per esempio obbligatori, di mantenimento o discrezionali, che differiscono per complessità e per grado di libertà nell'allocazione dei fondi. I processi IT dovrebbero fornire gli elementi dei relativi programmi in modo efficiente ed efficace ed avvisare prontamente in caso di scostamenti dal piano dovuti a costi, tempistiche o funzionalità che possono influenzare i risultati attesi. I servizi IT dovrebbero essere erogati con riferimento ad equi e sostenuti accordi sui livelli di servizio (SLA). La responsabilità di raggiungere i benefici e controllare i costi dovrebbe essere chiaramente assegnata e monitorata. Valutare i business case in modo equo, trasparente, ripetibile e comparabile, considerando anche il valore finanziario ed il rischio di non generare alcuna nuova capacità operativa o di non realizzare i benefici previsti.

PO1.2 Allineamento tra Azienda e IT

Definire processi bidirezionali di formazione e reciproco coinvolgimento nella pianificazione strategica per conseguire l'allineamento e l'integrazione fra il business e l'IT. Mediare tra gli aspetti imprescindibili dell'azienda e della tecnologia di modo che le priorità possono essere concordate da ambo le parti.

PO1.3 Valutazione della performance attuale

Valutare le performance e capacità attuali di soluzione ed erogazione del servizio per stabilire un contesto di riferimento per poter confrontare i requisiti futuri. Definire le performance in termini di contributi resi dall'IT a obiettivi aziendali, funzionalità, stabilità, complessità, costi, punti di forza e di debolezza.

PO1.4 Piano strategico

Creare un piano strategico che, in cooperazione con i principali soggetti interessati, definisca i modi in cui gli obiettivi IT contribuiranno al conseguimento degli obiettivi strategici dell'impresa anche in termini di costi e rischi. Il piano strategico dovrebbe comprendere le modalità con cui l'IT supporterà i programmi di investimento resi possibili dall'IT, i servizi IT e i beni tecnologici. Tale piano dovrebbe definire il modo in cui gli obiettivi saranno raggiunti, le misure da usare e le procedure per ottenere l'approvazione formale dei soggetti interessati. Il piano strategico dell'IT dovrebbe definire il budget di investimento e quello operativo, le fonti di finanziamento, la strategia di identificazione dei fornitori, la strategia di acquisto ed infine gli obblighi legali e normativi. Il piano strategico dovrebbe essere sufficientemente dettagliato per permettere la definizione dei relativi piani tattici.

PO1.5 Piani tattici

Creare un portafoglio di piani tattici derivanti dal piano strategico dell'IT. I piani tattici dovrebbero descrivere i programmi di investimento resi possibili dall'IT, i servizi IT e i beni tecnologici. I piani tattici dovrebbero descrivere le necessarie iniziative IT, i requisiti riguardanti le risorse, ed inoltre il modo in cui si monitoreranno e verranno gestiti l'utilizzo delle risorse ed il raggiungimento degli obiettivi. I piani tattici dovrebbero essere sufficientemente dettagliati per permettere la definizione dei piani di progetto. Gestire attivamente i piani e le iniziative IT definiti attraverso un'analisi del portafoglio dei progetti e dei servizi.

PO1.6 Gestione del portafoglio

Collaborare attivamente con l'azienda nella gestione del portafoglio dei programmi di investimento dipendenti dell'IT che sono necessari per raggiungere specifici obiettivi strategici aziendali, il che implica identificare, definire e valutare i programmi, definirne le priorità, selezionarli, avviarli, gestirli e controllarli. Questo dovrebbe comprendere il chiarimento dei risultati attesi dall'azienda, l'assicurazione che gli obiettivi del programma permettano il raggiungimento di tali risultati, la definizione di progetti all'interno del programma, l'assegnazione di risorse e fondi, la delega dell'autorità, e commissionare i progetti richiesti al momento dell'avvio del programma.

LINEE GUIDA PER LA GESTIONE

PO1 Definire un piano strategico per l'IT

Da	Inputs
PO5	Analisi costi/benefici
PO9	Analisi dei rischi
PO10	Portafoglio progetti aggiornato
DS1	Requisiti di servizio nuovi/aggiornati; portafoglio servizi aggiornati
*	Strategie e priorità di business
*	Portafoglio programmi
ME1	Analisi delle performance ai fini della pianificazione
ME4	Analisi situazione IT Governance, direzione strategica dell'impresa per l'IT

* Inputs dall'esterno di COBIT

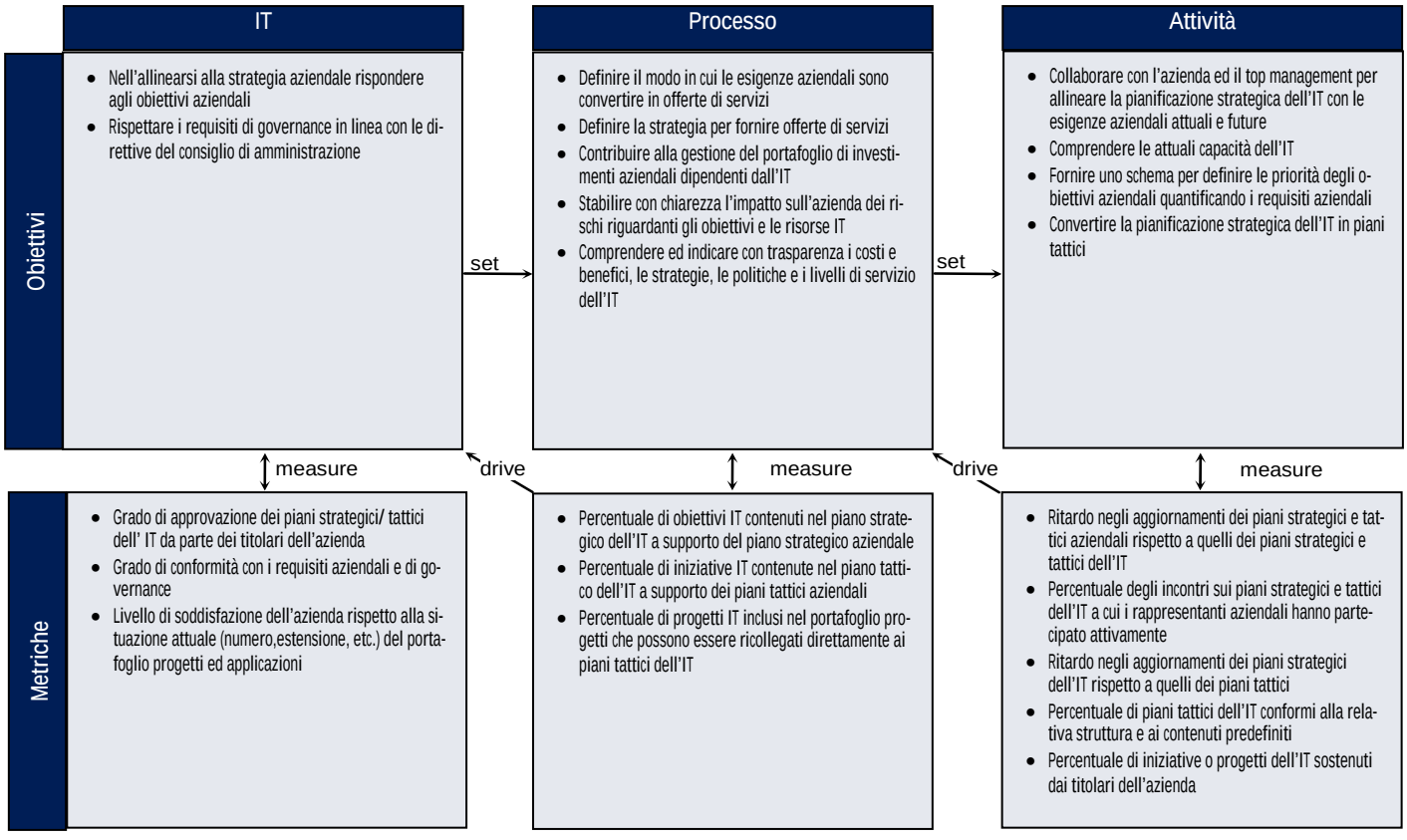
Outputs	A						
Piano strategico dell'IT	PO2..PO6	PO8	PO9	AI1	DS1		
Piano IT tattico	PO2..PO6	PO9	AI1	DS1			
Portafoglio progetti IT	PO5	PO6	PO10	AI6			
Portafoglio servizi IT	PO5	PO6	PO9	DS1			
Strategia di sviluppo IT	DS2						
Strategia per l'acquisizione IT	AI5						

RACI Chart

Attività / Ruoli	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Collegare gli obiettivi aziendali agli obiettivi dell'IT	C	I	A/R	R	C						
Identificare le dipendenze critiche e la performance attuale	C	C	R	A/R	C	C	C	C	C		C
Costruire un piano strategico per l'IT	A	C	C	R	I	C	C	C	C	I	C
Costruire piani tattici per l'IT	C	I		A	C	C	C	C	C	R	I
Analizzare i programmi e gestire i progetti e servizi in portafoglio.	C	I	I	A	R	R	C	R	C	C	I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato)

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO1 Definire un piano strategico per l'IT

Il grado di strutturazione del processo *Definire un piano strategico per l'IT* che soddisfa i requisiti aziendali per l'IT di *sostenere o integrare la strategia aziendale e i requisiti di governance mantenendo trasparenza per quanto riguarda costi, rischi e benefici* è:

0 Non esistente quando

Non esiste una pianificazione strategica dell'IT. Il Management non ha alcuna consapevolezza della necessità di una pianificazione strategica dell'IT a supporto degli obiettivi aziendali.

1 Iniziale/*Ad Hoc* quando

I responsabili IT riconoscono la necessità di una pianificazione strategica dell'IT. Tale pianificazione strategica avviene quando necessario in risposta a specifiche esigenze aziendali ed è occasionale oggetto di discussione nelle riunioni dei responsabili IT. L'allineamento tra le necessità aziendali, i software e le tecnologie di supporto avviene in modo reattivo piuttosto che in base ad una strategia globale dell'azienda. Il grado di rischio strategico viene identificato informalmente di volta in volta a livello di singolo progetto.

2 Ripetibile ma Intuitivo quando

La pianificazione strategica IT è condivisa con le Direzioni non-IT sulla base delle esigenze estemporanee. L'aggiornamento del piano IT viene effettuato quando sorge una specifica esigenza aziendale. Le decisioni strategiche sono guidate dalle esigenze indotte dai progetti, senza coerenza con un piano strategico aziendale complessivo. I rischi ed i benefici per gli utenti derivanti dalle più importanti decisioni strategiche sono dedotti intuitivamente.

3 Definito quando

Esiste un criterio per definire i tempi ed i modi della pianificazione strategica IT. La pianificazione strategica IT segue un approccio strutturato, documentato e noto a tutto lo staff. Il processo di pianificazione IT è ragionevolmente affidabile e offre buone possibilità di condurre un'opportuna pianificazione. Tuttavia, l'implementazione del processo è a discrezione dei singoli manager e non vi sono procedure di verifica. La strategia globale dell'IT comprende una definizione coerente dei rischi che l'organizzazione è disposta a correre, sia nelle vesti di innovatore che di utilizzatore di tecnologie esistenti. Le strategie IT finanziarie, tecniche e relative alle risorse umane influenzano in maniera crescente l'acquisto di nuovi prodotti e tecnologie. La pianificazione strategica dell'IT è oggetto di discussione nei management meeting aziendali.

4 Gestito e Misurabile quando

La pianificazione strategica IT è pratica normale ed ai responsabili risulta evidente qualsiasi eccezione. Tale pianificazione è una funzione definita con responsabilità a livello di senior management. I responsabili sono in grado di monitorare questo processo di pianificazione strategica, usarlo come base per prendere decisioni consapevoli e misurarne l'efficacia. La pianificazione avviene sia a breve che a lungo termine e viene estesa a tutta l'organizzazione effettuando, quando necessario, gli opportuni aggiornamenti. La strategia IT e quella aziendale sono sempre più coordinate, si occupano dei processi aziendali e delle capacità a valore aggiunto e sfruttano l'utilizzo di applicazioni e tecnologie attraverso la reingegnerizzazione dei processi aziendali. Esiste un processo ben definito per bilanciare le risorse interne ed esterne necessarie allo sviluppo e all'operatività del sistema.

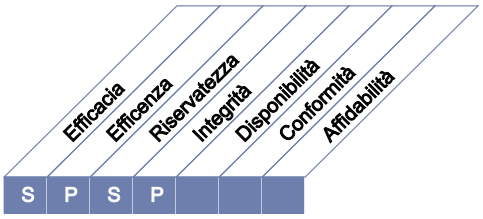
5 Ottimizzato quando

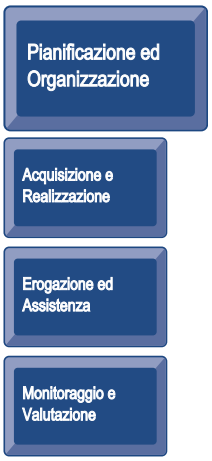
La pianificazione strategica IT è un processo attivo e documentato, è continuamente presa in considerazione nella definizione degli obiettivi aziendali e conduce ad un riconoscibile aumento del valore aziendale attraverso investimenti in IT. Le valutazioni sul rischio e sul valore aggiunto sono continuamente aggiornate nel processo di pianificazione strategica IT. Si sviluppano realistici piani IT di lungo termine che sono costantemente aggiornati in funzione dell'evoluzione delle tecnologie e del business. Il confronto (benchmark) con norme di settore chiare ed affidabili si effettua in un processo integrato nel processo di formulazione della strategia. Il piano strategico prende in considerazione anche il modo in cui i nuovi sviluppi tecnologici possono portare alla creazione di nuove competenze e potenzialità dell'azienda aumentando il vantaggio competitivo della stessa.

DESCRIZIONE DEL PROCESSO

PO2 Definire l'architettura delle informazioni

La funzione Sistemi Informativi definisce ed aggiorna regolarmente un modello delle informazioni aziendali e individua i sistemi più appropriati per ottimizzare l'uso di queste informazioni. Questo comporta lo sviluppo di un dizionario dei dati aziendali che comprende le regole di sintassi, lo schema di classificazione dei dati e i livelli di sicurezza. Questo processo migliora la qualità delle decisioni garantendo l'affidabilità e la sicurezza delle informazioni fornite e permette la razionalizzazione delle risorse dei sistemi informativi rispetto alle strategie aziendali. Tale processo è necessario anche per una chiara assegnazione di responsabilità per l'integrità e per la sicurezza dei dati e per migliorare l'efficacia ed il controllo sulla condivisione delle informazioni per gli applicativi e le entità aziendali.





Il controllo del processo IT

Definire l'architettura delle informazioni

che soddisfa i requisiti aziendali per l'IT di

essere agile nel rispondere ai requisiti, nel fornire informazioni affidabili e coerenti ed integrare perfettamente le applicazioni nei processi aziendali

ponendo l'attenzione su

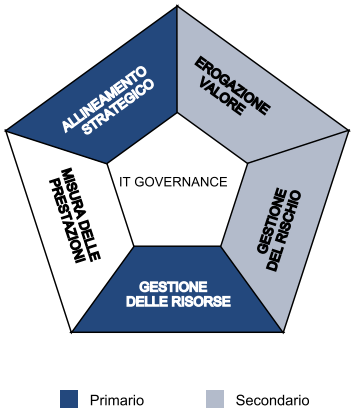
la costituzione di un modello di dati aziendali comprendente uno schema di classificazione per assicurare l'integrità e la coerenza di tutti i dati

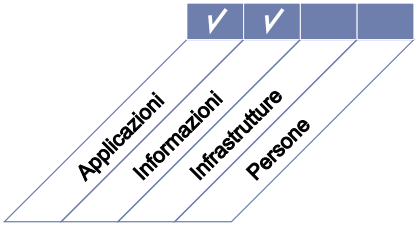
è ottenuto tramite

- l'assicurazione dell'accuratezza dell'architettura informatica e del modello dei dati
- l'assegnazione della proprietà dei dati
- la classificazione delle informazioni per mezzo di uno schema di classificazione concordato

e viene misurato tramite

- la percentuale di dati ridondanti o duplicati
- la percentuale di applicazioni non conformi con la metodologia adottata dall'impresa per la definizione dell'architettura informatica
- la frequenza delle attività di validazione dei dati





OBIETTIVI DI CONTROLLO

PO2 Definire l'architettura delle informazioni

PO2.1 Modello aziendale per l'architettura delle informazioni

Stabilire e mantenere un modello aziendale delle informazioni che renda possibile lo sviluppo degli applicativi e lo svolgimento di attività a supporto del processo decisionale, oltre ad essere in linea con i piani di IT descritti nel processo PO1. Tale modello dovrebbe facilitare i migliori creazione, utilizzo e condivisione delle informazioni a livello aziendale in modo tale da mantenerne l'integrità; tale modello si caratterizza per la sua flessibilità, funzionalità, rapporto costi benefici, tempestività, sicurezza e capacità di recupero in caso di errore.

PO2.2 Dizionario dei dati aziendali e regole di sintassi

Mantenere un dizionario aziendale dei dati che comprenda le relative regole di sintassi dei dati. Tale dizionario dovrebbe permettere la condivisione di dati tra applicativi e sistemi, promuovere una concezione comune dei dati tra l'IT e gli utenti aziendali, e prevenire la creazione di dati incompatibili.

PO2.3 Schema di classificazione dei dati

Stabilire uno schema di classificazione applicabile a tutta l'impresa, basato su criteri di criticità e sensibilità dei dati aziendali (per es. accessibile a tutti, riservato, di massima segretezza). Tale schema dovrebbe includere una dettagliata indicazione del proprietario dei dati, una definizione dei livelli di sicurezza e dei controlli di protezione appropriati, infine una breve descrizione della loro criticità e sensibilità e dei requisiti che determinano l'obbligo di conservarli o eliminarli. Tale schema dovrebbe essere usato come base per l'adozione di controlli quali la cifratura, l'archiviazione e il controllo degli accessi.

PO2.4 Gestione dell'integrità

Definire ed implementare procedure per assicurare l'integrità e la consistenza di tutti i dati archiviati in forma elettronica, come database, data-warehouse ed archivi.

Linee Guida per la Gestione

PO2 Definire l'architettura delle informazioni

Da	Inputs
PO1	Piano tattico e strategico dell'IT
AI1	Studio di fattibilità dei requisiti di business
AI7	Revisione post-attuazione
DS3	Informazioni sulle prestazioni e sulla capacità produttiva
ME1	Analisi delle prestazioni ai fini della pianificazione

Outputs	A						
Schema di classificazione dei dati	AI2						
Pianificare dei sistemi aziendali ottimizzata	PO3	AI2					
Dizionario dei dati	AI2	DS11					
Architettura delle informazioni	PO3	DS5					
Classificazioni dei dati assegnati	DS1	DS4	DS5	DS11	DS12		
Procedure e strumenti di classificazione	*						

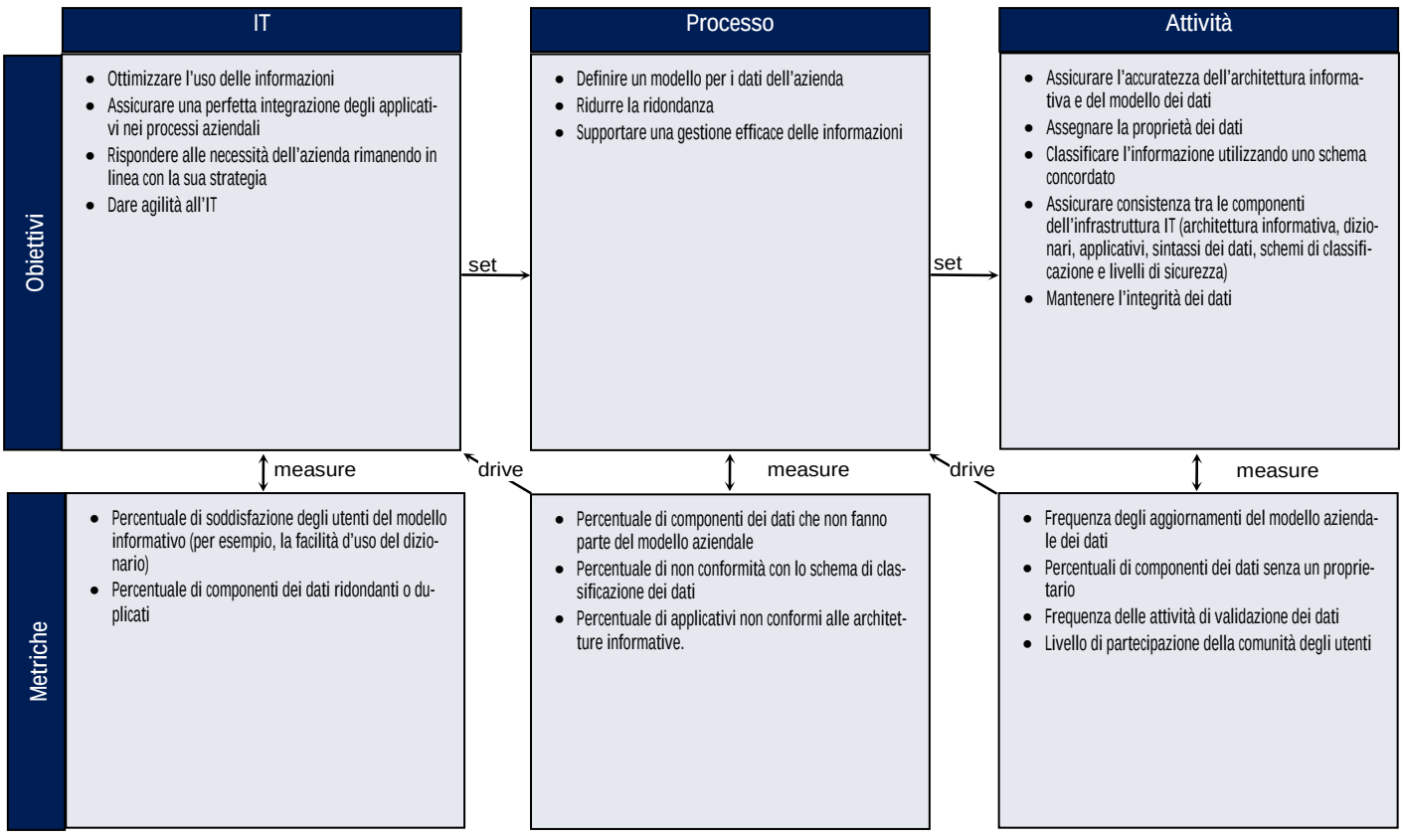
* Outputs all'esterno di COBIT

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Creare e mantenere modelli informativi a livello di azienda/organizzazione		C	I	A	C		R	C	C		C
Creare e mantenere dizionari aziendali dei dati				I	C		A/R	R			C
Definire e mantenere schemi di classificazione dei dati	I	C	A	C	C	I	C	C			R
Fornire ai proprietari dei dati procedure e strumenti per classificare i sistemi informativi	I	C	A	C	C	I	C	C			R
Utilizzare il modello informativo, il dizionario e lo schema di classificazione dei dati per pianificare l'ottimizzazione dei sistemi aziendali	C	C	I	A	C		R	C			I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO2 Definire l'architettura delle informazioni

Il grado di strutturazione del processo *Definire l'architettura delle informazioni* che soddisfa i requisiti aziendali per l'IT di *essere agile nel rispondere ai requisiti, nel fornire informazioni affidabili e coerenti ed integrare perfettamente le applicazioni nei processi aziendali* è:

0 Non esistente quando

Non esiste consapevolezza dell'importanza dell'architettura delle informazioni per l'organizzazione. Nell'azienda non esistono le conoscenze, l'esperienza e le responsabilità necessarie per sviluppare tale architettura.

1 Iniziale/*Ad Hoc* quando

I responsabili riconoscono l'esigenza di definire un'architettura delle informazioni. Alcuni elementi dell'architettura vengono sviluppati ad hoc. Le definizioni fanno riferimento a dati piuttosto che ad informazioni, e sono condizionate dalle offerte di software dei fornitori. L'esigenza di un'architettura delle informazioni viene comunicata in modo sporadico e contraddittorio.

2 Ripetibile ma Intuitivo quando

Il processo di gestione dell'architettura informativa è in fase di creazione ed individui diversi all'interno dell'organizzazione applicano già procedure simili, anche se in modo informale ed intuitivo. Il personale acquisisce le competenze per costruire un'architettura informativa attraverso esperienze pratiche e la ripetuta applicazione di tecniche. Sono le esigenze tattiche che spingono singoli componenti del personale a sviluppare parti dell'architettura informativa.

3 Definito quando

Si comprende ed accetta l'importanza dell'architettura informativa ed i responsabili della sua definizione sono chiaramente ed ufficialmente identificati. Le procedure, gli strumenti e le tecniche relative, per quanto non ancora sofisticate, sono state standardizzate e documentate e sono oggetto di attività informali di formazione. Sono stati sviluppati criteri base per l'architettura informativa, definendo anche alcuni requisiti strategici, ma il rispetto di tali criteri, standard e strumenti non è richiesto in modo coerente. Esiste una funzione di amministratore dati formalmente istituita con il compito di definire gli standard aziendali. Tale funzione sta cominciando a rendicontare sulla creazione e l'utilizzo dell'architettura informatica. Si cominciano ad utilizzare strumenti automatizzati, ma i processi e le regole in uso sono definiti dalle offerte di software per la gestione di database presentate dai venditori. Un piano di formazione formalizzato è stato sviluppato, ma la formazione ufficiale è ancora basata su iniziative di singoli individui.

4 Gestito e Misurabile quando

Lo sviluppo e l'obbligo di rispettare l'architettura informativa sono interamente supportati da metodi e tecniche formalizzate. Si stabiliscono le responsabilità per l'esecuzione del processo di sviluppo dell'architettura e si valuta il successo di tale architettura. Sono ampiamente presenti degli strumenti automatizzati di supporto, anche se non sono ancora integrati. Sono state identificate le metriche di base ed esiste un sistema di valutazione. Il processo di definizione dell'architettura informativa è pro-attivo e mira ad affrontare le future esigenze aziendali. L'organizzazione dell'amministrazione dati è coinvolta attivamente in tutti gli sforzi mirati allo sviluppo degli applicativi, al fine di garantirne la conformità. L'implementazione di un archivio automatizzato è stata completata e si stanno realizzando modelli di dati più complessi per utilizzare al meglio i contenuti informativi dei database. I sistemi informativi a disposizione dei vertici aziendali ed i sistemi di supporto alle decisioni si basano sulle informazioni disponibili.

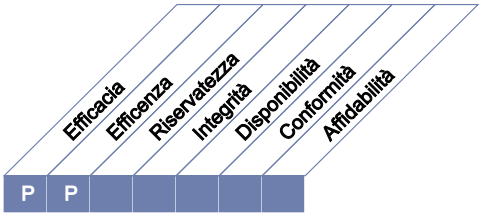
5 Ottimizzato quando

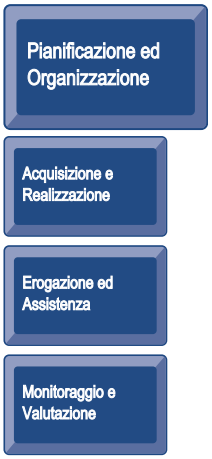
L'architettura informativa è regolarmente rispettata a tutti i livelli e si continua a porre l'accento sul suo valore per l'azienda. Il personale IT ha l'esperienza e le conoscenze necessarie per sviluppare e mantenere un'architettura informativa robusta ed adattabile, capace di riflettere tutte le esigenze aziendali. Le informazioni contenute nell'architettura informativa sono applicate in modo esteso e coerente. Nello sviluppo e mantenimento dell'architettura informativa, come pure nel continuo processo di miglioramento, si fa ampio riferimento alle good practice del settore. Si definiscono le strategie per utilizzare al meglio le informazioni tramite tecniche di data warehousing o data mining. L'architettura informatica è in continuo miglioramento e prende in considerazione anche informazioni non tradizionali relative a processi, organizzazioni e sistemi.

DESCRIZIONE DEL PROCESSO

PO3 Definire gli indirizzi tecnologici

La funzione IT definisce le linee evolutive tecnologiche per sostenere il business aziendale. Per far questo è necessario istituire un comitato che definisca l'architettura tecnologica e rediga un piano di sviluppo delle infrastrutture tecnologiche, il comitato inoltre individuerà chiare e realistiche previsioni di ciò che la tecnologia può/potrà offrire in termini di prodotti, servizi e sistemi di erogazione dei servizi. Tale piano è regolarmente aggiornato e comprendere i seguenti aspetti: architettura dei sistemi, indirizzo tecnologico, piani di acquisto, standard, strategie di migrazione e piano per le emergenze. Questi strumenti permettono una risposta tempestiva ai cambiamenti introdotti dalla concorrenza, economie di scala nell'allocazione di risorse ai sistemi informativi e negli investimenti, assieme ad una migliore integrazione operativa tra le diverse piattaforme ed applicazioni.





Il controllo del processo IT

Definire gli indirizzi tecnologici

che soddisfa i requisiti aziendali per l'IT di

avere sistemi applicativi stabili ed economici, integrati e standard, che assieme alle risorse ed alle capacità soddisfino le esigenze aziendali presenti e future

ponendo l'attenzione su

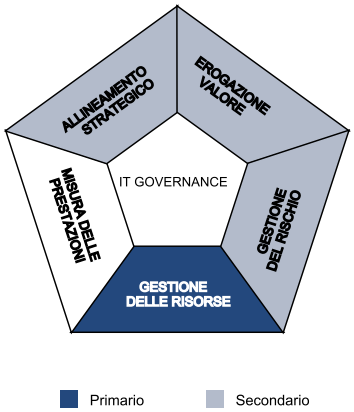
la definizione ed implementazione di un piano di infrastruttura tecnologica, di un'architettura e di standard che riconoscano e valorizzino le opportunità offerte dalla tecnologia

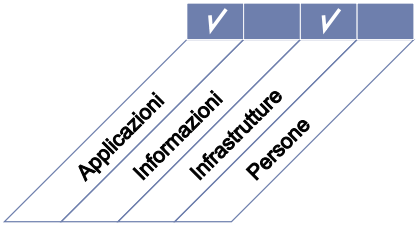
è ottenuto tramite

- l'istituzione di un forum per guidare l'architettura e verificare la conformità
- un piano di infrastruttura tecnologica definito che bilanci costi, rischi e requisiti
- la definizione degli standard di infrastruttura tecnologica basati sui requisiti dell'architettura informativa

e viene misurato tramite

- il numero ed il tipo di deviazioni dal piano di infrastruttura tecnologica
- la frequenza delle revisioni/aggiornamenti del piano di infrastruttura tecnologica
- il numero di piattaforme tecnologiche per funzione all'interno dell'impresa





OBIETTIVI DI CONTROLLO

PO3 Definire gli indirizzi tecnologici

PO3.1 Pianificazione dell'indirizzo tecnologico

Analizzare le tecnologie esistenti e pianificare l'indirizzo tecnologico più appropriato per realizzare la strategia IT e l'architettura dei sistemi aziendali. All'interno del piano, poi, identificare le tecnologie che potenzialmente possono creare opportunità per l'azienda. Il piano dovrebbe comprendere l'architettura dei sistemi, l'indirizzo tecnologico, le strategie di migrazione e gli aspetti delle emergenze che interessano le componenti dell'infrastruttura.

PO3.2 Piano per l'infrastruttura tecnologica

Creare e mantenere un piano di infrastruttura tecnologica che sia conforme ai piani strategici e tattici dell'IT. Il piano dovrebbe basarsi sull'indirizzo tecnologico e comprende aspetti relativi alla gestione delle emergenze nonché indirizzi per l'acquisto delle risorse tecnologiche. Dovrebbe prendere in considerazione i cambiamenti nella concorrenza, economie di scala per l'allocazione di risorse ai sistemi informativi e i relativi investimenti, assieme ad una migliore integrazione operativa di piattaforme ed applicativi.

PO3.3 Osservatorio sulle tendenze di mercato e sulle normative

Stabilire un processo di osservazione delle tendenze del settore in cui opera l'azienda, della tecnologia, delle infrastrutture, nonché degli aspetti relativi a leggi e regolamenti. Integrare le implicazioni di questi trend nello sviluppo del piano dell'infrastruttura tecnologica informatica.

PO3.4 Standard tecnologici

Per fornire all'impresa soluzioni tecnologiche affidabili, efficaci e sicure, istituire un forum tecnologico che formuli linee guida tecnologiche e suggerimenti sui prodotti per l'infrastruttura e linee guida sulla selezione delle tecnologie e misuri la conformità con tali standard e linee guida. Il forum dovrebbe indirizzare gli standard tecnologici e le prassi in base alla loro rilevanza per l'azienda, ai rischi e alla conformità con i requisiti esterni.

PO3.5 Il comitato per l'architettura informatica

Costituire un comitato per l'architettura informatica che formuli linee guida di natura architetturale, che eroghi consulenza sulla loro applicazione, che verifichi la conformità a tali linee guida. Questa entità dovrebbe indirizzare la progettazione dell'architettura informatica, assicurando che essa permetta l'attuazione della strategia aziendale nel rispetto dei requisiti di conformità alle normative e di continuità. Tale comitato è collegato al processo PO2 Definire l'architettura delle informazioni.

LINEE GUIDA PER LA GESTIONE

PO3 Definire gli indirizzi tecnologici

Da	Inputs
PO1	Piani strategici e tattici dell'IT
PO2	Ottimizzazione del piano dei sistemi aziendali e architettura delle informazioni
AI3	Aggiornamenti degli standard tecnologici
DS3	Informazioni sulle prestazioni e la capacità produttiva

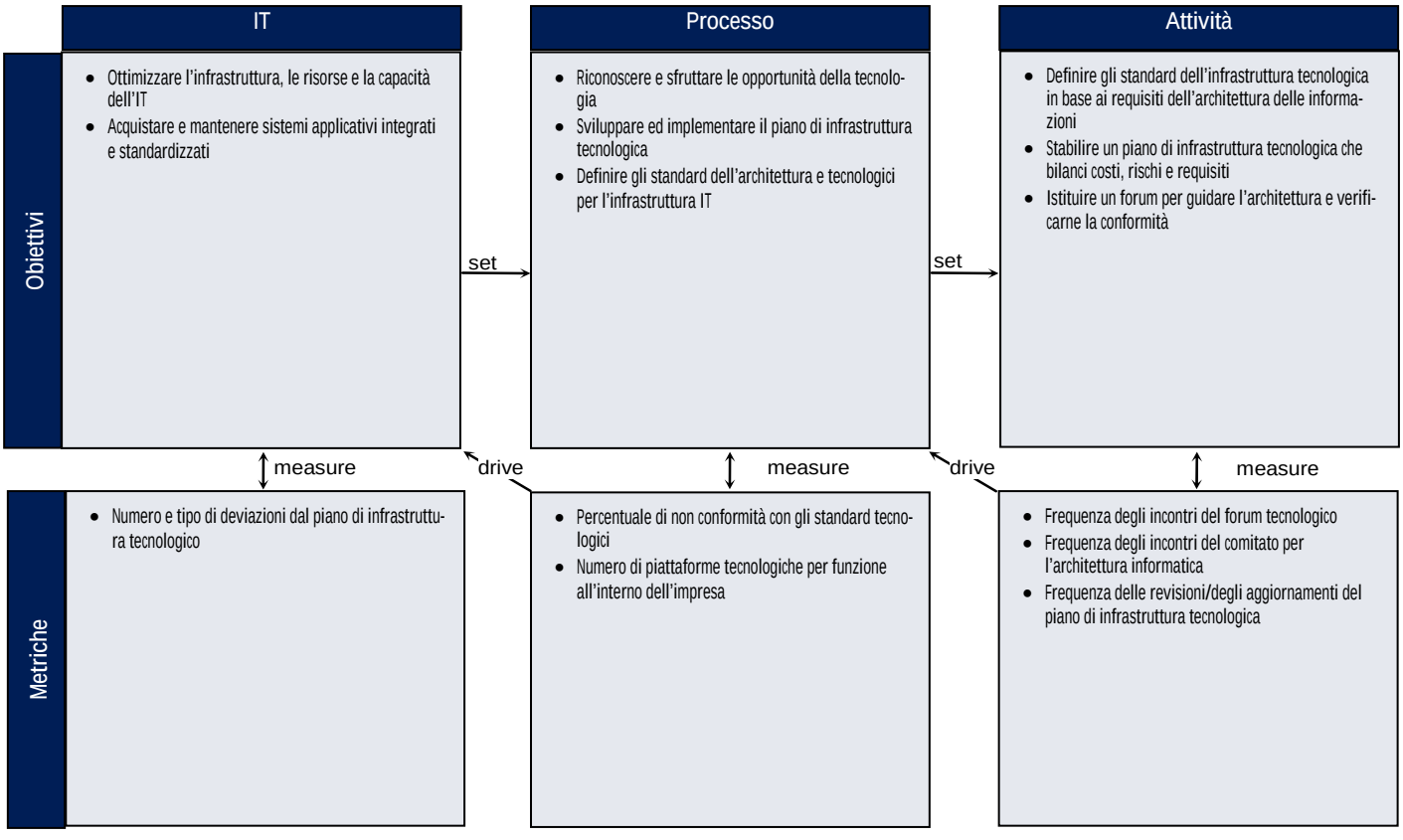
Outputs	A						
Opportunità tecnologiche	AI3						
Standard tecnologici	AI1	AI3	AI7	DS5			
Aggiornamenti regolari sulla "stato della tecnologia"	AI1	AI2	AI3				
Piano dell' infrastruttura tecnologica	AI3						
Requisiti dell'infrastruttura	PO5						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Creare e mantenere un piano di infrastruttura tecnologica		I	I	A		C	R	C	C		C
Creare e mantenere standard tecnologici				A		C	R	C	I	I	I
Pubblicare standard tecnologici		I	I	A		I	R	I	I	I	I
Monitorare l'evoluzione della tecnologia		I	I	A		C	R	C		C	C
Definire per il futuro un utilizzo strategico della nuova tecnologia.		C	C	A		C	R	C		C	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO3 Definire gli indirizzi tecnologici

Il grado di strutturazione del processo *Definire gli indirizzi tecnologici* che soddisfa i requisiti aziendali per l'IT di *avere sistemi applicativi stabili ed economici, integrati e standard, che assieme alle risorse ed alle capacità soddisfino le esigenze aziendali presenti e future* è:

0 Non esistente quando

Nell'azienda non vi è alcuna consapevolezza dell'importanza di un piano di infrastruttura tecnologica. Non esistono le conoscenze né l'esperienza per sviluppare tale piano. Non si comprende che pianificare prevedendo i cambiamenti della tecnologia è di importanza critica per una efficace allocazione delle risorse.

1 Iniziale/*Ad Hoc* quando

I responsabili aziendali riconoscono la necessità di una pianificazione dell'infrastruttura tecnologica. Lo sviluppo di componenti tecnologiche e l'impiego di tecnologie innovative sono sporadici e limitati a casi specifici. L'approccio alla pianificazione avviene in modo reattivo e si concentra su aspetti operativi. Gli indirizzi tecnologici dipendono dai piani evolutivi, frequentemente contradditori, dei fornitori di hardware, software di sistema e applicativi. Non viene data comunicazione del potenziale impatto dei cambiamenti della tecnologia in modo coerente.

2 Ripetibile ma Intuitivo quando

L'esigenza e l'importanza di una pianificazione tecnologica sono comunicate. La pianificazione avviene in modo pratico, concentrandosi sulla produzione di soluzioni tecniche a problemi tecnici, piuttosto che sull'uso della tecnologia per rispondere alle esigenze aziendali. La valutazione dei cambiamenti tecnologici è lasciata ad individui diversi che adottano processi intuitivi ma simili. Le competenze della pianificazione tecnologica sono acquisite attraverso corsi pratici di apprendimento e la ripetuta applicazione delle tecniche. Si stanno affermando tecniche comuni e standard per lo sviluppo di componenti infrastrutturali.

3 Definito quando

I responsabili aziendali sono consapevoli dell'importanza del piano di infrastruttura tecnologica. Il processo di sviluppo di tale piano è ragionevolmente valido ed allineato al piano strategico dell'IT. Esiste un piano di infrastruttura tecnologica documentato e condiviso, ma non viene adottato in maniera uniforme. Per dare una direzione all'infrastruttura tecnologica è necessario capire in quali aspetti tecnologici l'organizzazione vuole eccellere o procedere lentamente, in base ai rischi e in conformità con la strategia aziendale. I fornitori principali sono selezionati in base alla comprensione che si ha dei loro piani di sviluppo tecnologico e dei prodotti nel lungo periodo, in linea con gli indirizzi dell'azienda. La formazione e la comunicazione dei ruoli e delle responsabilità sono strutturate.

4 Gestito e Misurabile quando

Il management assicura lo sviluppo e il mantenimento per piano di infrastruttura tecnologica. Il personale IT possiede le conoscenze e l'esperienza necessarie sviluppare un piano di infrastruttura tecnologica. Il potenziale impatto dei cambiamenti tecnologici e delle nuove tecnologie è preso in considerazione. I responsabili sono in grado di identificare gli scostamenti dal piano, segnalando in anticipo i problemi. Le responsabilità per la stesura e l'aggiornamento del piano sono state assegnate. Il processo dello sviluppo del piano di infrastruttura tecnologica è sofisticato ed in grado di rispondere ai cambiamenti. Raccoglie inoltre le "good practice" interne. La gestione delle risorse umane è strategicamente allineata con gli indirizzi tecnologici, per assicurare che il personale IT sia in grado di gestire l'evoluzione tecnologica. Vi sono dei piani di migrazione definiti per l'introduzione di nuove tecnologie. Per poter avere le necessarie conoscenze ed competenze si ricorre all'outsourcing ed a partnership. Il management ha analizzato ed accettato il rischio derivante dall'utilizzo più o meno innovativo della tecnologia per sviluppare nuove opportunità aziendali o efficienze operative.

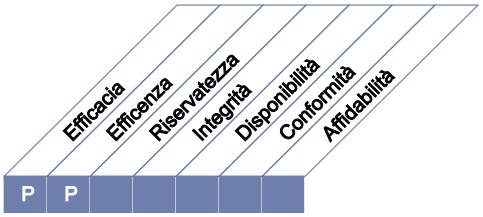
5 Ottimizzato quando

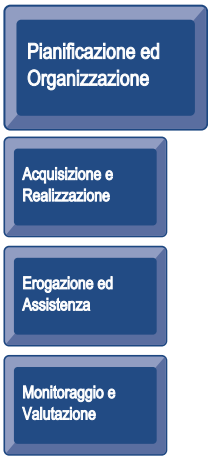
Esiste una funzione di ricerca con il compito di valutare l'evoluzione e le novità della tecnologia, nonché confrontare l'azienda con i dati di riferimento del settore. L'indirizzo del piano di infrastruttura tecnologica si basa sugli standard internazionali e di settore piuttosto che sulle proposte dei fornitori di tecnologie. Il potenziale impatto dell'evoluzione tecnologica sull'azienda è valutato ad alto livello direzionale. Novità o modifiche degli indirizzi tecnologici sono approvate formalmente a livello di alta direzione. L'entità possiede un preciso piano di infrastruttura tecnologica che riflette le esigenze aziendali, è in grado di rispondere ai cambiamenti e può essere modificato in risposta ai cambiamenti del business. Esiste e si fa applicare un continuo processo di miglioramento del piano di infrastruttura tecnologica. Nella definizione degli indirizzi tecnologici l'azienda si basa in larga misura sulle good practice del settore.

DESCRIZIONE DEL PROCESSO

PO4 Definire i processi, l'organizzazione e le relazioni dell'IT

La definizione di una struttura IT deve essere effettuata tenendo in debita considerazione i requisiti relativi a: risorse umane, competenze, funzioni, responsabilità, autorità, ruoli e compiti, controllo. Tale organizzazione deve essere inquadrata in una struttura dei processi IT che assicuri non solo trasparenza e controllo ma anche il coinvolgimento dell'alta direzione e del management non-IT dell'azienda. Un comitato strategico assicura la supervisione dell'IT ed uno o più comitati guida, a cui partecipano sia l'IT sia gli utenti dell'IT, definiscono le priorità per quanto riguarda le risorse informatiche in linea con le esigenze aziendali. Per tutte le funzioni vi sono processi, politiche amministrative e procedure; in particolar modo per il controllo, la qualità, il risk management, la sicurezza informatica, la proprietà di dati e sistemi e la separazione dei ruoli. Per poter assicurare un tempestivo supporto alle esigenze aziendali, l'IT deve essere coinvolto nei processi decisionali che lo riguardano.





Il controllo del processo IT

Definire i processi, l'organizzazione e le relazioni dell'IT

che soddisfa i requisiti aziendali per l'IT di

rispondere con prontezza alle strategie aziendali rispettando gli obblighi della governance e fornendo punti di contatto chiari e competenti

ponendo l'attenzione su

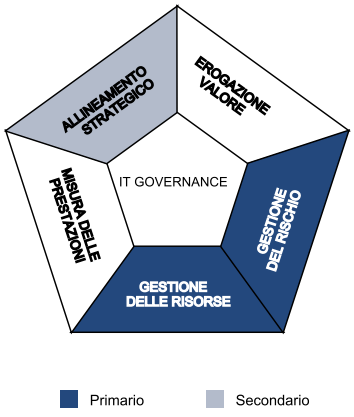
la costituzione di strutture organizzative IT trasparenti, flessibili e pronte a rispondere, oltre alla definizione ed implementazione di processi con proprietari, ruoli e responsabilità integrati nei processi aziendali e decisionali

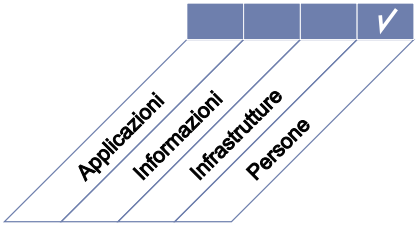
è ottenuto tramite

- la definizione di un quadro strutturale dei processi IT
- la costituzione di organi e strutture organizzative appropriati
- la definizione di ruoli e responsabilità

e viene misurato tramite

- la percentuale di ruoli a cui corrispondono posizioni e livelli di autorità ben descritti e documentati
- il numero di unità aziendali o processi non supportati dall'IT che invece dovrebbero esserlo secondo la strategia
- il numero di attività specifiche dell'IT svolte al di fuori dell'organizzazione IT che non sono approvate né soggette ai relativi standard organizzativi





OBIETTIVI DI CONTROLLO

PO4 Definire i processi, l'organizzazione e le relazioni dell'IT

PO4.1 Quadro strutturale dei processi dell'IT

Definire il quadro strutturale dei processi dell'IT al fine di dare esecuzione al relativo piano strategico. Tale quadro dovrebbe includere la struttura e le relazioni dei processi di IT (per esempio, per gestire discontinuità o sovrapposizioni tra un progetto e l'altro), la proprietà, la maturità, la valutazione della performance, la conformità, gli obiettivi di qualità e i piani per raggiungerli. Esso dovrebbe permettere inoltre di integrare i processi specifici dell'IT con la gestione del portafoglio dell'impresa, i processi aziendali e i relativi cambiamenti. Il quadro strutturale dei processi dell'IT dovrebbe andare ad integrarsi in un sistema di gestione della qualità (SGQ) e nel quadro strutturale dei controlli interni.

PO4.2 Comitato strategico per l'IT

Costituire un comitato strategico per l'IT di alto livello. Tale comitato dovrebbe assicurare che siano adeguatamente affrontati gli aspetti specifici dell'IT governante nell'ambito della corporate governance, offre consulenza sugli indirizzi strategici, verifica i principali investimenti per conto di tutto il consiglio.

PO4.3 Comitato guida (Steering Committee) per l'IT

Costituire un comitato guida (steering committee) per l'IT (o un comitato equivalente) composto dall'alta direzione, e dai manager dell'azienda e dell'IT con l'obiettivo di:
• determinare le priorità dei programmi di investimento basati sull'IT in accordo con la strategia e le priorità dell'azienda
• seguire lo stato dei progetti e risolvere i conflitti a livello di risorse
• monitorare i livelli di servizio ed i loro miglioramenti

PO4.4 Posizionamento organizzativo della funzione IT

Posizionare la funzione IT all'interno della struttura organizzativa generale secondo un modello di business dipendente dall'importanza dell'IT nell'azienda, soprattutto per la sua criticità nella strategia aziendale ed il livello di dipendenza operativa dell'azienda stessa dall'IT. La persona a cui il manager responsabile dell'IT riporterà dovrebbe dipendere dall'importanza dell'IT nell'azienda.

PO4.5 Struttura organizzativa dell'IT

Stabilire una struttura organizzativa interna ed esterna che rifletta le esigenze aziendali. Attivare inoltre un processo di revisione periodica di tale struttura con l'intenzione di rettificare le esigenze di personale e le strategie di approvvigionamento a seconda degli obiettivi aziendali e del mutare delle circostanze.

PO4.6 Definire i ruoli e le responsabilità

Definire e comunicare i ruoli e le responsabilità di tutto il personale IT e degli utenti finali al fine di delineare l'autorità, gli incarichi e le responsabilità tra il personale IT e quello utente per soddisfare le esigenze dell'azienda.

PO4.7 Responsabilità del controllo qualità dell'IT

Assegnare la responsabilità dei risultati della funzione del controllo qualità (CQ) e fornire al gruppo di CQ gli appropriati sistemi di CQ e le competenze di controllo e comunicazione opportune. Assicurare che il posizionamento all'interno della struttura, le responsabilità e le dimensioni del gruppo di CQ soddisfino le esigenze dell'azienda.

PO4.8 Responsabilità in tema di rischi, sicurezza e conformità

Attribuire la proprietà e le responsabilità dei rischi informatici all'interno dell'azienda a personale con adeguato livello gerarchico. Definire ed assegnare i ruoli critici per la gestione dei rischi dell'IT, contemplando anche le responsabilità specifiche relative a sicurezza delle informazioni, sicurezza fisica e conformità. Stabilire le responsabilità per la gestione dei rischi e della sicurezza a livello di impresa per gestire le relative problematiche. Vi potrebbe essere la necessità di assegnare anche altre responsabilità relative alla gestione della sicurezza dei sistemi per occuparsi delle relative questioni. Ricevere dal senior management indicazioni sulla disponibilità a correre rischi informatici e l'approvazione di eventuali rischi informatici residui.

PO4.9 Proprietà dei dati e dei sistemi

Dotare l'azienda di procedure e strumenti per affrontare le responsabilità riguardanti la proprietà dei dati e dei sistemi informativi. I proprietari dovrebbero decidere come classificare le informazioni ed i sistemi e come proteggerli sulla base di tale classificazione.

PO4.10 Supervisione

Attuare adeguate forme di supervisione all'interno della funzione IT per assicurare un appropriato esercizio dei ruoli e delle responsabilità, per valutare se tutto il personale ha autorità e risorse sufficienti per esercitare il proprio ruolo e le proprie responsabilità e, più in generale, per rivedere i KPI (principali indicatori di performance).

PO4.11 Separazione dei compiti (Segregation of Duties)

Attuare una divisione di ruoli e responsabilità in modo da ridurre la possibilità che un singolo individuo possa compromettere un processo critico. Assicurarsi anche del fatto che il personale svolga solo i compiti autorizzati per quanto concerne il loro lavoro e la posizione occupata.

PO4.12 Personale IT

Di regola, o in caso di importanti cambiamenti dell'azienda, o degli ambienti operativi o informatici, valutare le risorse umane necessarie al fine di assicurare alla funzione IT sufficienti risorse umane per supportare adeguatamente ed appropriatamente gli obiettivi e gli scopi aziendali.

PO4.13 Personale chiave dell' IT

Definire ed identificare le figure chiave dell'IT (ad esempio le "tavole di sostituzione") e ridurre al minimo l'eccesso di dipendenza da singoli individui che svolgono funzioni critiche.

PO4.14 Politiche e procedure per il personale a contratto

Assicurare che il personale a contratto ed i consulenti, che supportano la funzione IT, conoscano e rispettino le politiche dell'azienda per la protezione del patrimonio informativo aziendale quali quelle concordate nei requisiti contrattuali.

PO4.15 Relazioni

Stabilire e mantenere un livello ottimale di coordinamento, collegamento e comunicazione tra la funzione IT e varie altre entità o persone all'interno ed all'esterno della funzione IT, quali ad esempio il consiglio, l'alta direzione, le unità aziendali, i singoli utenti, i fornitori, i responsabili della sicurezza, i risk manager, il gruppo aziendale che si occupa di conformità, il personale in outsourcing ed il management che opera fuori sede.

Pagina intenzionalmente vuota

LINEE GUIDA PER LA GESTIONE

PO4 Definire i processi, l'organizzazione e le relazioni dell'IT

Da	Inputs
PO1	Piani tattici e strategici
PO7	Politiche e procedure per il personale IT, matrice delle competenze IT, descrizione dei compiti
PO8	Azioni per l'incremento della qualità
PO9	Azioni correttive inerenti rischi IT
ME1	Piano delle azioni correttive
ME2	Rapporto sull'efficacia dei controlli IT
ME3	Catalogo dei requisiti legali e normativi relativi alla fornitura di servizi IT
ME4	Miglioramenti della struttura dei processi

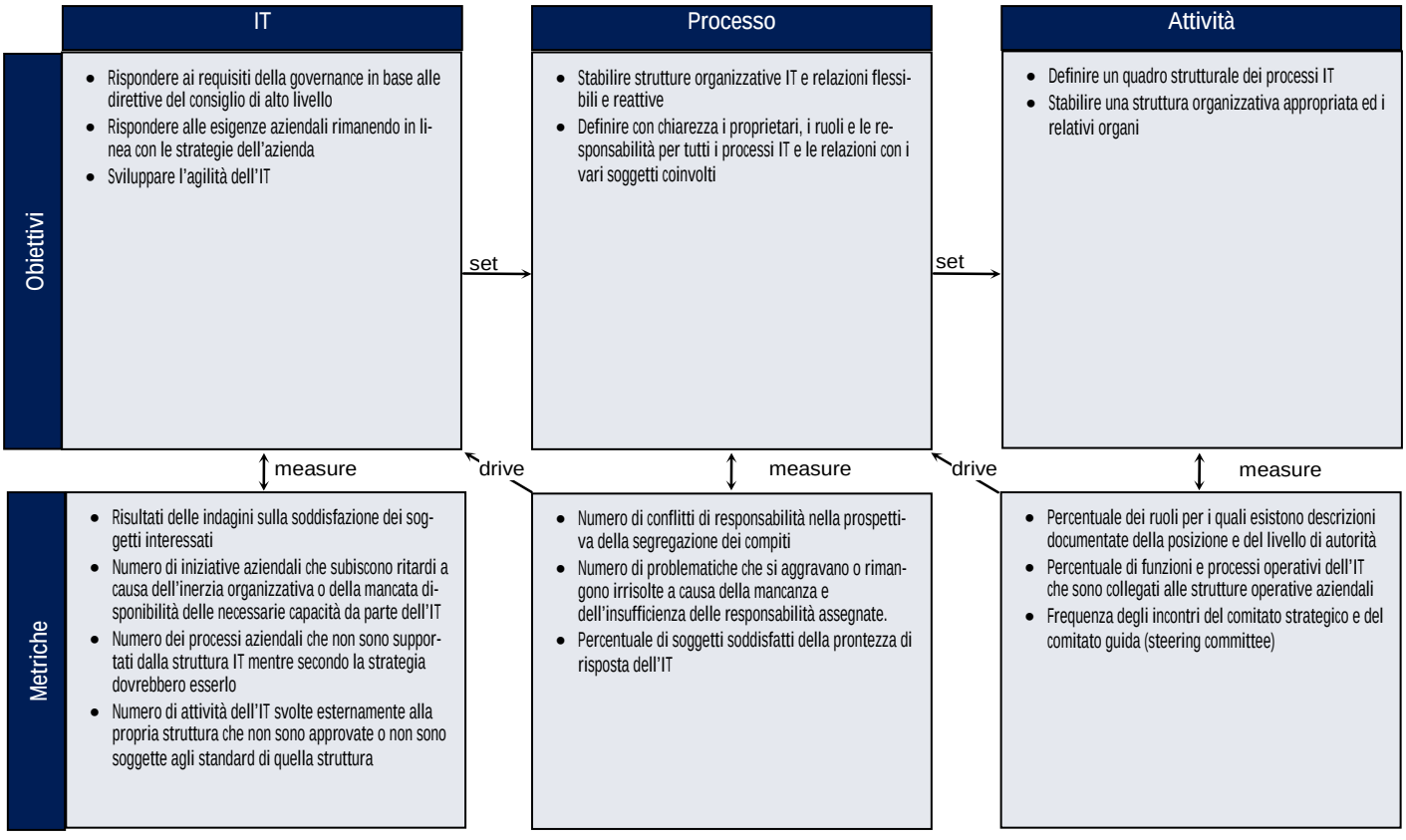
Outputs	A						
Quadro strutturale dei processi IT	ME4						
Documento descrittivo dei proprietari dei sistemi	AI7	DS6					
Organizzazione e interrelazioni IT	PO7						
Quadro strutturale dei processi IT, documento descrittivo dei ruoli e delle responsabilità	ALL						
Documento descrittivo dei ruoli e delle responsabilità	PO7						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Stabilire la struttura organizzativa dell'IT, compresi i comitati ed i collegamenti con tutti gli interessati e i fornitori	C	C	C	A		C	C	C	R	C	I
Disegnare il quadro strutturale dei processi IT	C	C	C	A		C	C	C	R	C	C
Identificare i proprietari dei processi		C	C	A	C	R	I	I	I	I	I
Identificare i proprietari dei dati		I	A	C	C	I	R	I	I	I	C
Stabilire ed implementare i ruoli e le responsabilità dell'IT, senza tralasciare la supervisione e la segregazione dei ruoli stessi.		I	I	A	I	C	C	C	R	C	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO4 Definire i processi, l'organizzazione e le relazioni dell'IT

Il grado di strutturazione del processo *Definire i processi, l'organizzazione e le relazioni dell'IT* che soddisfa i requisiti aziendali per l'IT di *rispondere con prontezza alle strategie aziendali rispettando gli obblighi della governance e fornendo punti di contatto chiari e competenti* è:

0 Non esistente quando

La struttura dell'IT non è definita in modo tale da concentrarsi efficacemente sul raggiungimento degli obiettivi aziendali.

1 Iniziale/*Ad Hoc* quando

Le attività e le funzioni dell'IT si svolgono senza sistematicità ed in risposta a situazioni contingenti. L'IT è coinvolto nei processi aziendali solo in fasi avanzate. L'IT è considerata una funzione di supporto, senza una prospettiva organizzativa d'insieme. Si comprende implicitamente l'esigenza di una struttura IT; tuttavia i ruoli e le responsabilità non sono né formalizzati né imposti come obbligo.

2 Ripetibile ma Intuitivo quando

La funzione IT è organizzata per dare risposte tattiche, e non sistematiche, alle esigenze degli utenti ed ai fornitori con cui è in rapporto. L'esigenza di una struttura organizzata e di una gestione dei fornitori è ufficialmente riconosciuta, ma le decisioni dipendono ancora dalle conoscenze e competenze di figure chiave. Si cominciano a sviluppare tecniche comuni per gestire la struttura dell'IT e i rapporti con i fornitori.

3 Definito quando

Esistono ruoli e responsabilità ben definiti per la struttura IT e gli esterni. La struttura IT viene sviluppata in linea con la relativa strategia, documentata e resa nota. L'ambiente del controllo interno è definito. I rapporti con altre entità, quali i comitati guida (steering committee), l'internal audit ed i responsabili dei fornitori, sono formalizzati. Da un punto di vista funzionale l'organizzazione IT è completa. Le funzioni pertinenti al personale IT e quelle degli utenti sono definite. Il fabbisogno minimo dell'IT in termini di personale e di livello di esperienza è definito e soddisfatto. Le relazioni con gli utenti e gli esterni sono formalmente definite. La separazione di ruoli e responsabilità è definita ed attuata.

4 Gestito e Misurabile quando

La struttura IT risponde in modo attivo ai cambiamenti e prevede tutti i ruoli necessari per rispondere alle esigenze aziendali. Nell'organizzazione delle funzioni dell'IT si sono applicate le migliori prassi interne(good practices). I responsabili IT hanno l'esperienza e le competenze necessarie per definire, realizzare e monitorare la struttura e le relazioni più importanti. Esistono parametri standard per sostenere gli obiettivi aziendali ed i fattori critici di successo (CSF) definiti dagli utenti. Per l'assegnazione di personale ai progetti e lo sviluppo professionale sono disponibili inventari delle competenze. Esiste e si impone un chiaro equilibrio tra le competenze e le risorse disponibili internamente e quelle per cui è necessario ricorrere ad organizzazioni esterne. La struttura organizzativa dell'IT riflette in maniera adeguata le esigenze aziendali in quanto i servizi che fornisce sono allineati a processi aziendali strategici piuttosto che a tecnologie isolate.

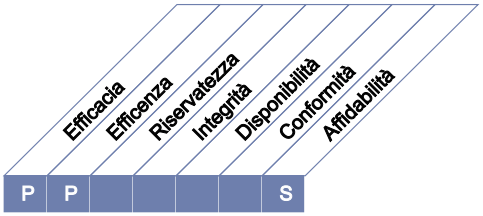
5 Ottimizzato quando

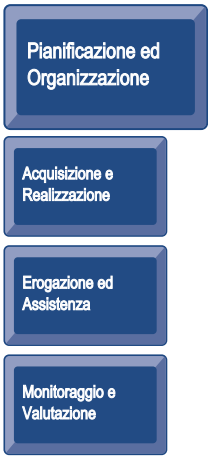
La struttura organizzativa dell'IT è flessibile ed in grado di adattarsi ai cambiamenti. Si adottano le good practice del settore. Si fa ampio ricorso alla tecnologia per monitorare la performance della struttura e dei processi di IT. Si utilizza la tecnologia per sostenere la complessità e la distribuzione geografica dell'azienda. È in atto un continuo processo di miglioramento.

DESCRIZIONE DEL PROCESSO

PO5 Gestire gli investimenti IT

Definire e mantenere un quadro di riferimento strutturato per gestire i programmi degli investimenti in IT che comprenda i seguenti aspetti: costi, benefici, definizione delle priorità nell'ambito del budget, una procedura formale per la redazione e gestione del budget. I soggetti interessati sono consultati per identificare e controllare i costi e i benefici complessivi nell'ambito dei piani strategici e tattici dell'IT e promuovere azioni correttive ove necessario. Questo processo promuove la collaborazione dei vari soggetti interessati all'IT e la funzione IT, rende possibile un uso efficace ed efficiente delle risorse IT, permette una gestione trasparente e responsabile dei costi complessivi dell'infrastruttura (TCO), dei benefici ottenuti per l'azienda, del ritorno degli investimenti per i quali l'IT è stato fattore abilitante.





Il controllo del processo IT

Gestire gli investimenti IT

che soddisfa i requisiti aziendali per l'IT di

migliorare continuamente ed in modo tangibile l'efficienza dell'IT in termini di costi ed il contributo che dà alla redditività aziendale fornendo servizi integrati e standardizzati all'altezza delle attese dell'utente finale

ponendo l'attenzione su

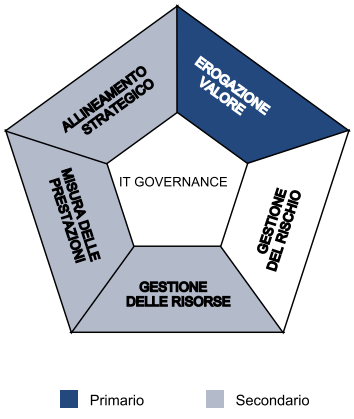
le scelte di portafoglio e di investimenti in IT efficienti ed efficaci, definendo e monitorando i budget dell'IT in base alle decisioni strategiche e di investimento della funzione IT

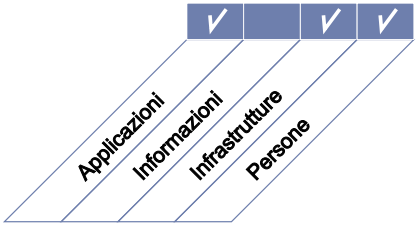
è ottenuto tramite

- la definizione dei budget di previsione ed allocando i costi
- la definizione dei criteri formali di investimento (ROI, periodo di recupero dell'investimento, percentuale del valore aggiunto netto (NPV)
- la misura e valutazione del valore aggiunto rispetto alle previsioni

e viene misurato tramite

- la percentuale di riduzione del costo unitario dei servizi IT resi
- la percentuale di deviazione del valore nel budget rispetto al totale
- la percentuale di spesa in IT espressa in fattori che aumentano il valore aggiunto (es. incremento di vendite/servizi dovuto all'aumento delle connessioni possibili)





OBIETTIVI DI CONTROLLO

PO5 Gestire gli investimenti IT

PO5.1 Quadro di riferimento per la gestione finanziaria

Definire e mantenere un quadro di riferimento per la gestione finanziaria per gestire gli investimenti e i costi dei beni informatici e dei servizi attraverso i portafogli degli investimenti abilitati dall'IT, dei business case, dei budget IT.

PO5.2 Definizione delle Priorità nell'Ambito del Budget di IT

Implementare un processo decisionale per definire le priorità nell'allocare le risorse IT alle attività operative, a quelle progettuali e a quelle di mantenimento per permettere all'IT di dare il massimo contributo ed ottimizzare il ritorno per l'impresa dei portafogli dei programmi di investimento in progetti legati all'IT e di altri beni e servizi dell'IT.

PO5.3 Processo di definizione del budget della funzione IT

Istituire un processo di formulazione del budget che rifletta le priorità definite dal portafoglio degli investimenti aziendali legati all'IT ed includa i normali costi operativi e di mantenimento dell'attuale infrastruttura. Questo processo dovrebbe sostenere lo sviluppo di un budget complessivo di IT e dei budget di singoli programmi, enfatizzando in particolar modo la componente tecnologica di quei programmi. Questo processo dovrebbe inoltre permettere di rivedere, migliorare ed approvare i budget a livello generale e di singoli programmi.

PO5.4 Gestione dei costi

Implementare un processo di gestione dei costi confrontando i costi effettivi con i budget. I costi dovrebbero essere monitorati e registrati. Si dovrebbero prontamente identificare eventuali deviazioni valutandone anche il relativo impatto sui programmi. Assieme al promotore di quei programmi, si dovrebbero poi intraprendere le opportune azioni correttive e, se necessario, aggiornare il programma di investimento proposto.

PO5.5 Gestione dei benefici

Implementare un processo di monitoraggio dei benefici derivanti dall'acquisizione e mantenimento di appropriate capacità informatiche. Il contributo informatico al business, o come componente dei programmi di investimenti abilitati dall'IT o come parte di un supporto operativo sistematico, dovrebbe essere identificato e documentato in un business case concordato da monitorare e relazionare. Tali relazioni dovrebbero essere esaminate e, nel caso vi sia l'opportunità di migliorare il contributo dell'IT, si dovrebbero definire ed intraprendere le opportune azioni. Nel caso in cui il contributo dell'IT subisca variazioni che hanno un impatto sul programma di investimento, oppure nel caso che tale programma sia influenzato dai cambiamenti di altri progetti ad esso collegati, si dovrà procedere ad aggiornare il programma di investimenti.

LINEE GUIDA PER LA GESTIONE

PO5 Gestire gli investimenti IT

Da	Inputs
PO1	Piani strategici e tattici, portafoglio progetti e servizi
PO3	Requisiti dell'infrastruttura
PO10	Portafoglio progetti IT aggiornato
AI1	Studio di fattibilità dei requisiti di business
AI7	Revisione post-implementazione
DS3	Performance & capacity plan (requisiti)
DS6	Fattori economici IT
ME4	Effetti attesi sul business degli investimenti IT

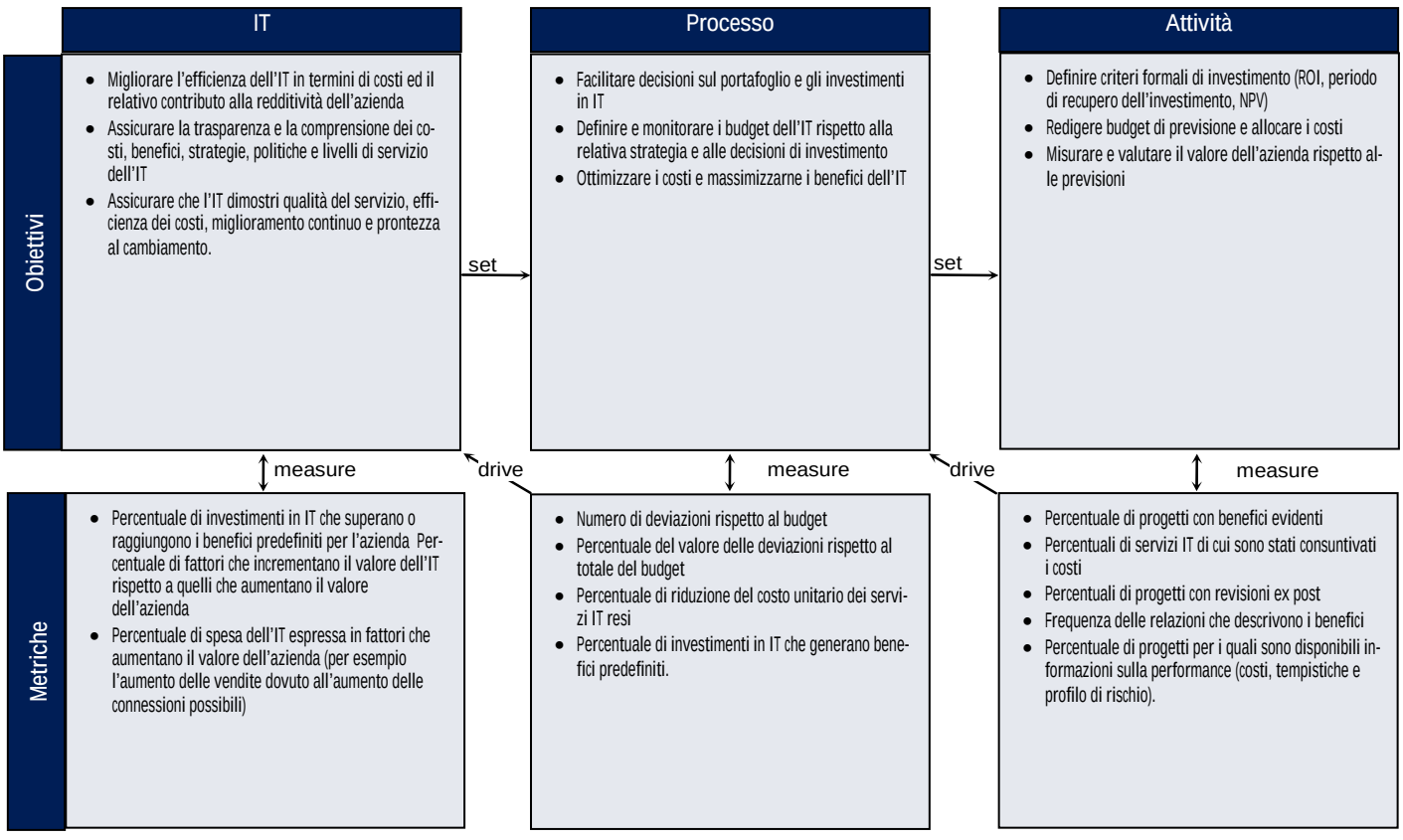
Outputs	A						
Analisi costi/benefici	PO1	AI2	DS6	ME1	ME4		
Budget IT	DS6						
Portafoglio servizi IT aggiornato	DS1						
Portafoglio progetti IT aggiornato	PO10						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Gestire il mantenimento del portafoglio programmi	A	R	R	R	C					I	I
Gestire il mantenimento del portafoglio progetti	I	C	A/R	A/R	C		C	C		C	I
Gestire il mantenimento del portafoglio servizi	I	C	A/R	A/R	C	C				C	I
Definire e mantenere il processo di preparazione del budget dell'IT	I	C	C	A		C	C	C	R	C	
Identificare, comunicare e monitorare il costo ed il valore degli investimenti in IT per l'azienda	I	C	C	A/R		C	C	C	R	C	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO5 Gestire gli investimenti IT

Il grado di strutturazione del processo *Gestire gli investimenti IT* che soddisfa i requisiti aziendali per l'IT di *migliorare continuamente ed in modo tangibile l'efficienza dell'IT in termini di costi ed il contributo che dà alla redditività aziendale fornendo servizi integrati e standardizzati all'altezza delle attese dell'utente finale* è:

0 Non esistente quando

Non c'è consapevolezza dell'importanza di scegliere e preventivare l'investimento in IT. Gli investimenti e le spese di IT non vengono né seguiti né monitorati.

1 Iniziale/*Ad Hoc* quando

L'organizzazione riconosce la necessità di gestire gli investimenti in IT, ma tale necessità non viene comunicata in modo coerente. Le responsabilità per la selezione degli investimenti in IT o lo sviluppo del budget sono attribuite ad hoc. Si verificano casi isolati in cui si attuano scelte d'investimento e si redige un budget, accompagnandoli con documentazione informale. Gli investimenti in IT sono giustificati di volta in volta. Le decisioni sul budget vengono prese in reazione ad eventi e concentrandosi su aspetti operativi.

2 Ripetibile ma Intuitivo quando

Ci si rende implicitamente conto della necessità di selezionare gli investimenti in IT e di metterli a budget. La necessità di un processo di selezione e di redazione del budget viene resa nota, ma l'osservanza di tale indicazione dipende dall'iniziativa di singoli individui all'interno dell'organizzazione. Si stanno affermando tecniche comuni per sviluppare le voci del budget di IT. Le decisioni sul budget sono prese in risposta ad esigenze tattiche.

3 Definito quando

Le politiche ed i processi di investimento e di redazione del budget sono chiaramente definiti, documentati e resi noti, e riguardano gli aspetti più rilevanti dal punto di vista tecnologico ed aziendale. Il budget di IT è in linea con i piani strategici dell'IT e dell'azienda. I processi di redazione del budget e di scelta degli investimenti in IT sono formalizzati, documentati e resi noti. Si sta sviluppando una formazione ufficiale, ma è ancora basata principalmente sull'iniziativa di singoli individui. Le scelte d'investimento in IT ed i budget vengono approvati formalmente. Il personale IT ha le competenze e le esperienze necessarie per sviluppare il budget e raccomandare gli investimenti appropriati.

4 Gestito e Misurabile quando

Le responsabilità della selezione degli investimenti e della redazione del budget sono assegnate ad una persona specifica. Gli scostamenti dal budget sono identificati e sistemati. Si eseguono analisi formali dei costi che interessano i costi diretti ed indiretti delle operazioni esistenti e gli investimenti proposti, calcolando i costi totali in un intero ciclo di vita. Il metodo usato per definire il budget è standardizzato e finalizzato a prevenire più che reagire. I piani d'investimento tengono conto del fatto che i costi operativi e di sviluppo non si riferiscono più tanto a hardware e software quanto piuttosto all'integrazione dei sistemi e alle risorse umane dell'IT. I benefici ed il ritorno degli investimenti sono calcolati sia in termini finanziari che non finanziari.

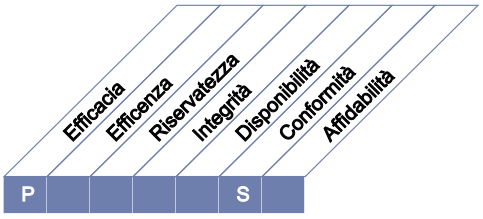
5 Ottimizzato quando

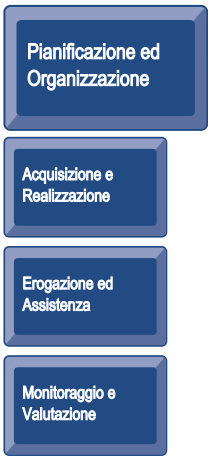
Si utilizzano le good practice del settore per comparare i costi e trovare modi per accrescere l'efficacia degli investimenti. Le scelte d'investimento ed il processo di definizione del budget si basano su analisi dell'evoluzione tecnologica. Il processo di gestione degli investimenti è soggetto ad un continuo miglioramento in base alle lezioni apprese tramite l'analisi della performance attuale. Le scelte di investimento tengono presente i trend di miglioramento del rapporto prezzo/performance. Le varie possibilità di finanziamento sono analizzate e valutate formalmente in base all'attuale struttura del capitale aziendale, utilizzando metodi formali di valutazione. Gli scostamenti sono identificati in modo preventivo. Le scelte di investimento sono fatte anche in base ad un'analisi dei costi e dei benefici di lungo periodo nel ciclo di vita completo.

ESCRIZIONE DEL PROCESSO

PO6 Comunicare gli obiettivi e gli orientamenti della Direzione

La Direzione sviluppa un quadro aziendale di riferimento per il controllo dell'IT e definisce e comunica le politiche. Viene definito un programma di comunicazione continua per articolare la missione, gli obiettivi del servizio, le politiche e le procedure, ecc., approvati e sostenuti dalla Direzione. La comunicazione sostiene il raggiungimento degli obiettivi della funzione IT ed assicura consapevolezza e comprensione dei rischi aziendali e informatici, degli obiettivi e degli orientamenti. Tale processo assicura la conformità alle leggi e ai regolamenti che riguardano l'IT.





Il controllo del processo IT

Comunicare gli obiettivi e gli orientamenti della Direzione

che soddisfa i requisiti aziendali per l'IT di

informare in modo accurato e tempestivo sui servizi IT presenti e futuri e sui rischi e sulle responsabilità ad essi associati

ponendo l'attenzione su

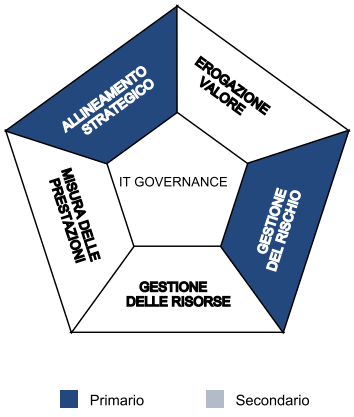
la disponibilità per gli interessati di politiche, procedure, linee guida ed altre documentazioni che siano accurate, comprensibili e approvate, e inserite nel modello di controllo dell'IT

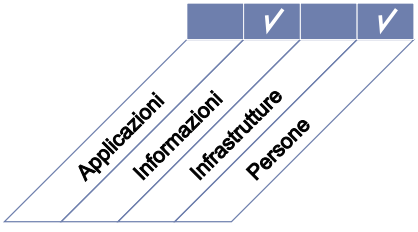
è ottenuto tramite

- la definizione di un quadro di riferimento per il controllo dell'IT
- lo sviluppo e divulgazione di politiche dell'IT
- il rispetto delle politiche dell'IT

e viene misurato tramite

- il numero di interruzioni dell'operatività aziendale causato da disservizi dell'IT
- la percentuale di persone interessate che comprendono il quadro di riferimento per il controllo dell'IT
- la percentuale di persone interessate che non rispettano le politiche





OBIETTIVI DI CONTROLLO

PO6 Comunicare gli obiettivi e gli orientamenti della Direzione

PO6.1 Le politiche IT e l'ambiente di controllo

Definire le componenti di un ambiente di controllo per l'IT che sia allineato alla filosofia di gestione ed allo stile operativo dell'impresa. Tali componenti dovrebbero comprendere le/i aspettative/requisiti relativi alla produzione di valore attraverso gli investimenti IT, la disponibilità al rischio, l'integrità, i valori etici, la competenza del personale, le responsabilità del risultato e dell'esecuzione delle attività. L'ambiente di controllo dovrebbe basarsi su una cultura che sostiene la produzione di valore mentre si gestiscono i rischi significativi, che incoraggia la cooperazione tra le varie divisioni aziendali ed il lavoro di squadra, che promuove la conformità ed il miglioramento continuo dei processi ed infine che gestisce bene le deviazioni nell'ambito dei processi (compresi i fallimenti).

PO6.2 Il rischio IT dell'impresa e il quadro di riferimento per il controllo

Sviluppare e mantenere un quadro di riferimento che definisca l'approccio generale dell'impresa verso i rischi IT ed il controllo e che sia allineato con l'ambiente di controllo e le politiche IT e con il quadro di riferimento dell'impresa per il controllo ed i rischi.

PO6.3 Gestione delle politiche IT

Sviluppare e mantenere un insieme di politiche a supporto della strategia dell'IT. Tali politiche dovrebbero comprendere gli scopi, i ruoli e le responsabilità, i processi di gestione delle eccezioni, l'approccio alla conformità ed il riferimento a procedure, standard e linee guida.

PO6.4 Divulgare le politiche, gli standard e le procedure

Divulgare e far rispettare da tutto il personale interessato le politiche IT, in modo da integrarle nell'intera operatività aziendale.

PO6.5 Comunicare gli obiettivi e gli orientamenti dell'IT

Comunicare per ottenere la consapevolezza e la comprensione del business e degli obiettivi e orientamenti dell'IT agli stakeholder e agli utenti appropriati attraverso tutta l'impresa.

LINEE GUIDA PER LA GESTIONE

PO6 Comunicare gli obiettivi e gli orientamenti della Direzione

Da	Inputs
PO1	Piano tattico e strategico per l'IT, portafoglio dei servizi e dei progetti IT
PO9	Linee guida per la gestione dei rischi IT
ME2	Analisi dell'efficacia dei controlli IT

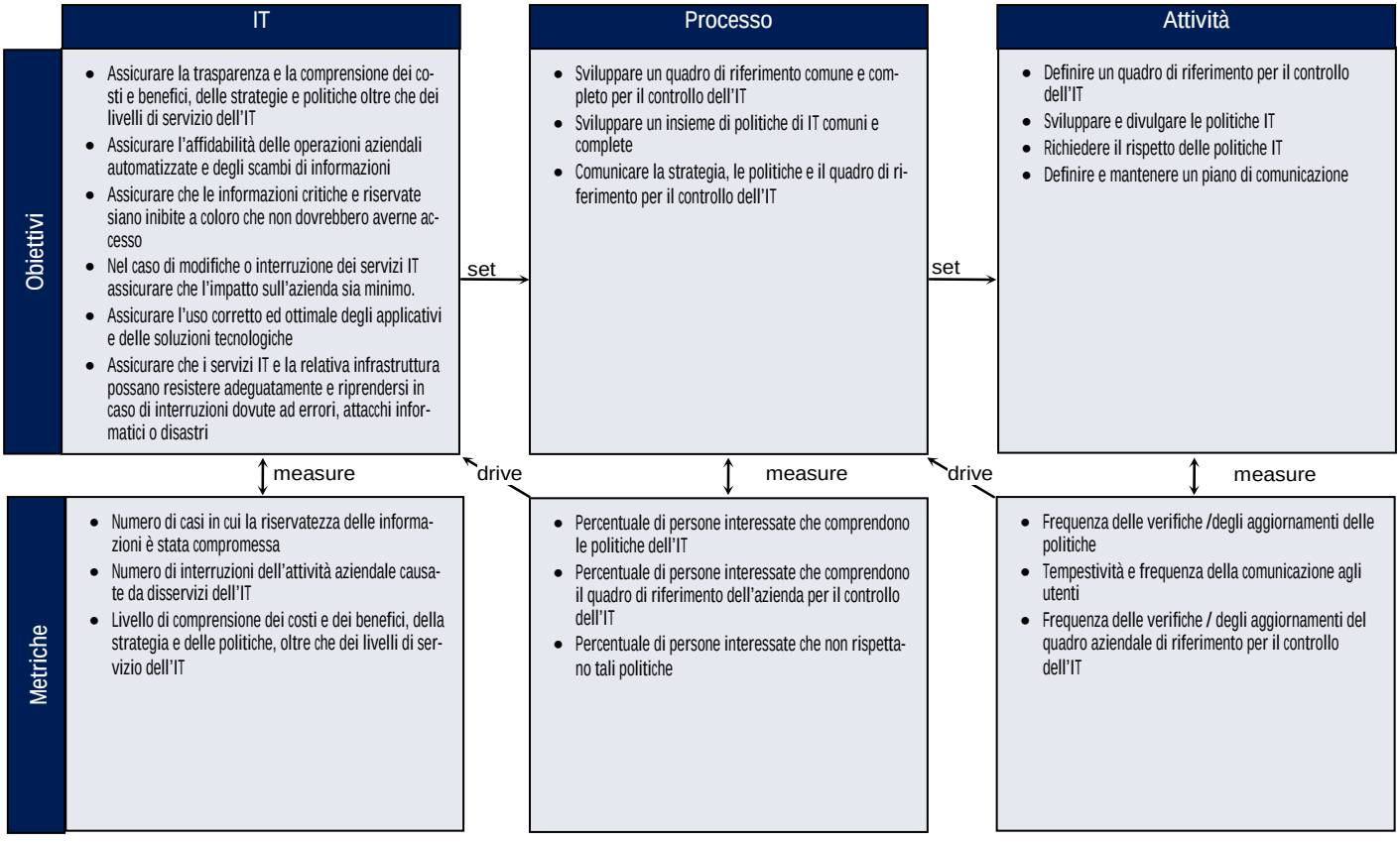
Outputs	A						
Quadro di riferimento aziendale per i controlli IT	ALL						
Politiche IT	ALL						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Stabilire ed implementare un quadro di riferimento per i controlli IT	I	C	I	A/R	I	C		C	C		C
Sviluppare e mantenere le politiche IT	I	I	I	A/R		C	C	C	R		C
Comunicare il quadro di riferimento per i controlli IT, gli obiettivi IT e la relativa direzione	I	I	I	A/R					R		C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO6 Comunicare gli obiettivi e gli orientamenti della Direzione

Il grado di strutturazione del processo *Comunicare gli obiettivi e gli orientamenti della Direzione* che soddisfa i requisiti aziendali per l'IT di *informare in modo accurato e tempestivo sui servizi IT presenti e futuri e sui rischi e sulle responsabilità ad essi associati* è:

0 Non esistente quando

I responsabili aziendali non hanno stabilito un ambiente di controllo informatico concreto. Non si percepisce l'esigenza di definire un insieme di politiche, piani e procedure e processi di conformità.

1 Iniziale/*Ad Hoc* quando

I responsabili si rispondono in modo reattivo alle esigenze dell'ambiente di controllo informatico. Le politiche, le procedure e gli standard sono sviluppati e comunicati ad hoc in risposta a problemi contingenti. I processi di sviluppo, comunicazione e conformità non hanno formalizzazione né coerenza.

2 Ripetibile ma Intuitivo quando

I responsabili hanno una percezione implicita delle esigenze e dei requisiti di un efficace ambiente di controllo informatico, tuttavia le attività aziendali sono gestite in modo alquanto informale. I responsabili hanno comunicato l'esigenza di politiche, piani e procedure, ma lo sviluppo è lasciato alla discrezione dei singoli responsabili e delle aree di business. La qualità è percepita come concetto auspicabile, ma, di fatto, le attività sono lasciate alla discrezione dei singoli responsabili. La formazione è individuale ed attivata quando necessario.

3 Definito quando

I responsabili hanno sviluppato, documentato e diffuso un ambiente completo di controllo informatico e di gestione della qualità che include un quadro di riferimento per le politiche, i piani e le procedure. Il processo di sviluppo delle politiche è strutturato, ben tenuto e noto al personale; inoltre le politiche, i piani e le procedure esistenti sono ragionevolmente validi e coprono le principali problematiche. I responsabili considerano l'importanza di un approccio consapevole alla sicurezza informatica e avviano dei programmi di formazione in tal senso. Sono disponibili corsi di formazione per sostenere l'ambiente di controllo informatico, ma non vengono attivati in modo rigoroso. Mentre esiste un quadro di riferimento per lo sviluppo generale delle politiche e delle procedure, la conformità a tali politiche e procedure non viene monitorata in modo sistematico. Esisto un quadro di riferimento per tutte le attività dello sviluppo. Le tecniche per promuovere un approccio consapevole alla questione della sicurezza sono state standardizzate e formalizzate.

4 Gestito e Misurabile quando

I responsabili accettano la responsabilità di comunicare le politiche interne di controllo e ne hanno delegato la responsabilità assegnando sufficienti risorse per mantenere l'ambiente di controllo al passo con i cambiamenti più rilevanti. È stato costituito un ambiente favorevole ed attivo per il controllo informatico, che comprende anche l'impegno per la qualità e la consapevolezza della sicurezza informatica. È stato sviluppato, mantenuto aggiornato e diffuso un insieme completo di politiche, piani e procedure che raccoglie in sé le good practice interne. È stato anche stabilito un quadro per il roll-out ed i successivi controlli di conformità.

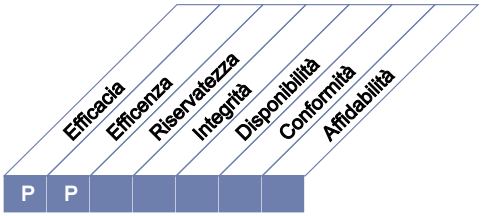
5 Ottimizzato quando

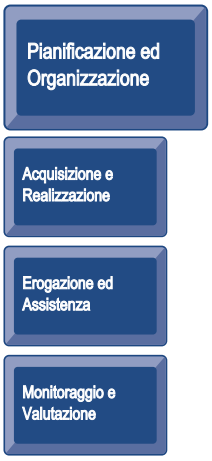
L'ambiente del controllo informatico è allineato con il quadro di riferimento e la visione strategica della gestione, ed è sottoposto a frequenti revisioni, aggiornato e migliorato continuamente. È affidato ad esperti interni ed esterni il compito di assicurare che si adottino le indicazioni delle good practice del settore in materia di controllo e di tecniche di comunicazione. Il monitoraggio, l'autovalutazione e le verifiche di conformità sono ampiamente diffusi all'interno dell'azienda. Si utilizza la tecnologia come base per conoscere con consapevolezza le politiche e per ottimizzare la comunicazione utilizzando strumenti di office automation e di formazione attraverso il computer.

DESCRIZIONE DEL PROCESSO

PO7 Gestire le risorse umane dell'IT

È acquisita e mantenuta una forza lavoro competente per creare e fornire servizi IT all'azienda. Questo risultato si ottiene applicando prassi definite e approvate per il reclutamento, la formazione, la valutazione della performance, la promozione e la conclusione del rapporto. Questo processo è critico perché le persone sono risorse importanti, inoltre sia la governance sia l'ambiente di controllo interno dipendono fortemente dalla loro motivazione e competenza.





Il controllo del processo IT

Gestire le risorse umane dell'IT

che soddisfa i requisiti aziendali per l'IT di

acquisire risorse competenti e motivate per creare e fornire servizi IT

ponendo l'attenzione su

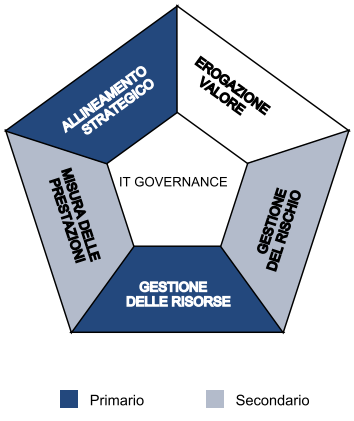
assumere e formare personale, motivarlo con percorsi di carriera chiari, assegnare ruoli corrispondenti alle rispettive competenze e stabilire un chiaro processo di verifica, creare descrizioni delle funzioni e assicurare che si comprenda il concetto di dipendenza dalle persone

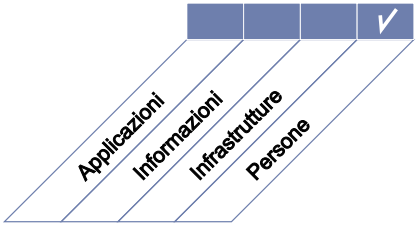
è ottenuto tramite

- la verifica della performance del personale
- l'assunzione e formazione del personale IT per supportare i piani tattici della funzione
- la mitigazione del rischio di eccessiva dipendenza dalle risorse chiave

e viene misurato tramite

- il livello di soddisfazione degli stakeholder per quanto riguarda l'esperienza e le competenze del personale IT
- l'avvicendamento delle risorse IT
- la percentuale delle risorse IT dotate delle opportune certificazioni a seconda delle esigenze del lavoro.





OBIETTIVI DI CONTROLLO

PO7 Gestire le risorse umane dell'IT

PO7.1 Assunzione e ritenzione del personale

Mantenere i processi di assunzione del personale IT in linea con le policy e le procedure aziendali (es. assunzione, ambiente di lavoro positivo, orientamento). Il management attiva questi processi per assicurare all'azienda che il personale IT sia adeguatamente utilizzato e possegga le competenze necessarie per raggiungere gli obiettivi aziendali.

PO7.2 Competenze del personale

Verificare regolarmente che il personale abbia le competenze per svolgere il proprio ruolo in base alla propria istruzione, formazione ed esperienza. Definire i requisiti in termini di competenze principali informatiche e verificare che questi siano rispettati, ove necessario, attraverso adeguati programmi di accreditamento e certificazione.

PO7.3 Assegnazione dei ruoli

Definire, monitorare e controllare i ruoli, le responsabilità e gli schemi di compensazione del personale, oltre a definire la necessità di aderire alle policy e procedure, al codice etico e alla professional practice. Il livello di controllo dovrebbe essere in linea con la delicatezza della posizione occupata e l'entità delle responsabilità assegnate.

PO7.4 Formazione del personale

Fornire al personale un adeguato orientamento in fase di assunzione e formazione continua per mantenere conoscenze, competenze, abilità, consapevolezza dei controlli interni e della sicurezza al livello richiesto per il raggiungimento degli obiettivi aziendali.

PO7.5 Dipendenza dai singoli individui

Ridurre al minimo l'esposizione al rischio di dipendenza eccessiva dal personale più importante attraverso un'opportuna documentazione e condivisione delle conoscenze, piani di sostituzione e backup del personale.

PO7.6 Procedure di autorizzazione del personale

Includere controlli sulle precedenti esperienze del personale in fase di reclutamento. L'entità e la frequenza di tali controlli dovrebbero dipendere dalla delicatezza e criticità della funzione e dovrebbero essere adottati sia per i dipendenti, sia per il personale a contratto sia per i fornitori.

PO7.7 Valutazione della performance del personale

Richiedere che siano fatte prontamente e regolarmente valutazioni in base ai singoli obiettivi derivanti dagli obiettivi aziendali di lungo periodo, gli standard definiti e le specifiche responsabilità del lavoro. La performance e la condotta del dipendente, se opportuno, dovranno essere oggetto di attività di coaching.

PO7.8 Cambiamento di mansioni e risoluzione del rapporto

In caso di variazioni delle funzioni, o specialmente nel caso di risoluzione del rapporto, adottare opportune azioni. Dovrebbe essere organizzati il trasferimento delle conoscenze, la rassegnazione delle responsabilità e la rimozione dei diritti di accesso, in modo da minimizzare i rischi e garantire la continuità della funzione.

Linee Guida per la Gestione

PO7 Gestire le risorse umane dell'IT

Da	Inputs
PO4	Organizzazione e interrelazioni IT, documentazione dei ruoli e delle responsabilità
AI1	Studio di fattibilità dei requisiti di business

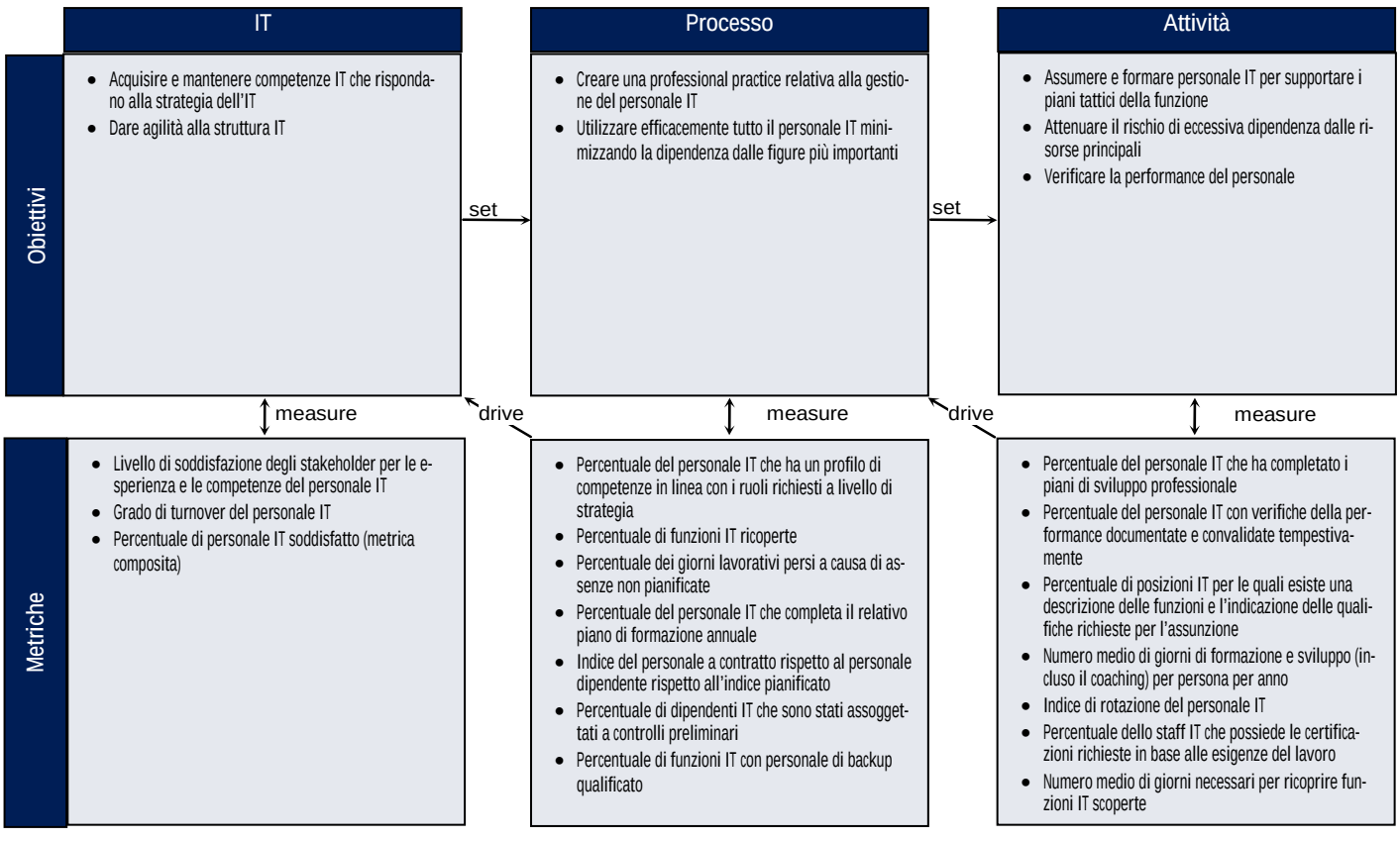
Outputs	A						
Politiche e procedure per il personale IT	PO4						
Matrice conoscenze IT	PO4	PO10					
Descrizione dei compiti	PO4						
Conoscenze ed esperienze individuali, inclusi corsi frequentati da ciascuno	DS7						
Requisiti per corsi specifici	DS7						
Ruoli e responsabilità	ALL						

RACI Chart

Attività \ Ruoli	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Identificare competenze IT, descrizioni delle posizioni, livelli di retribuzione e parametri della performance personale		C		A		C	C	C	R	C	
Dare attuazione alle policy e procedure delle Risorse Umane (recruiting, assunzione, verifica delle esperienze pregresse, compensi, formazione, valutazioni, promozioni e licenziamenti)				A		R	R	R	R	R	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO7 Gestire le risorse umane dell'IT

Il grado di strutturazione del processo *Gestire le risorse umane dell'IT* che soddisfa i requisiti aziendali per l'IT di *acquisire risorse competenti e motivate per creare e fornire servizi IT* è:

0 Non esistente quando

Non esiste consapevolezza dell'importanza che riveste per l'azienda il fatto di mantenere la gestione delle risorse umane IT in linea con il processo di pianificazione tecnologica. Non vi è nessuno, singolo o gruppo, ufficialmente responsabile della gestione del personale IT.

1 Iniziale/*Ad Hoc* quando

La direzione riconosce l'esigenza di una gestione del personale IT. Il processo di gestione di tali risorse è informale, risponde a situazioni di necessità e si concentra sugli aspetti operativi dell'assunzione e della gestione. Ci si comincia a rendere conto dell'influenza che i rapidi cambiamenti del business e tecnologici, nonché la crescente complessità delle soluzioni, hanno sulla necessità di nuove specializzazioni e livelli di competenza.

2 Ripetibile ma Intuitivo quando

L'assunzione e la gestione del personale IT avvengono in modo tattico, sulla base di specifiche esigenze di progetto, piuttosto che a seguito di un indirizzo tecnologico e della consapevolezza della necessità di mantenere un equilibrio tra disponibilità di personale specializzato all'interno e all'esterno dell'azienda. Il nuovo personale riceve formazione in modo informale e solo a seguito di specifiche richieste.

3 Definito quando

Esiste, ed è documentato, un chiaro processo di gestione delle risorse umane dell'IT. Esiste anche il relativo piano. L'assunzione e la gestione del personale IT si basano su un approccio strategico. In risposta alle esigenze del personale IT esiste un piano di formazione ufficiale. Esiste un programma di rotazione dei ruoli per garantire lo sviluppo delle competenze tecniche e gestionali del personale.

4 Gestito e Misurabile quando

La responsabilità dello sviluppo e dell'aggiornamento del piano di gestione del personale IT è stata assegnata ad un determinato individuo o gruppo con l'esperienza e le competenze necessarie. Il processo di sviluppo e aggiornamento del piano si adatta ai cambiamenti. L'azienda ha misure standard che le permettono di identificare gli scostamenti dal piano di gestione delle risorse umane IT, ponendo particolare attenzione alla gestione della crescita e del turnover del personale. Gli stipendi e la performance sono verificati e confrontati con le good practice di altre organizzazioni IT e del settore. La gestione delle risorse umane IT è condotta in modo attivo e propositivo, tenendo conto dello sviluppo dei percorsi di carriera.

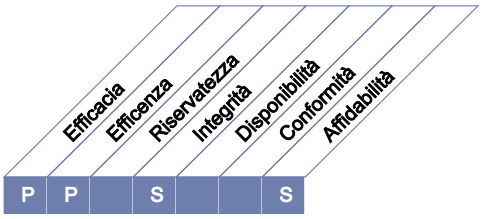
5 Ottimizzato quando

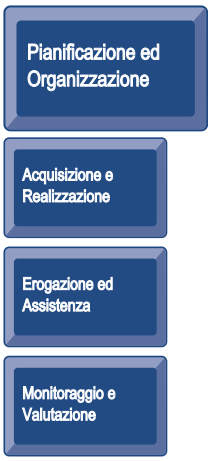
Il piano di gestione del personale IT è continuamente aggiornato per rispondere ai mutamenti del business. La gestione del personale IT si integra con l'indirizzo strategico aziendale e si adatta ad esso. Gli elementi gestiti dalla funzione Risorse Umane dell'IT, quali retribuzione, performance review, partecipazione a forum di settore, trasferimento di conoscenze, formazione e guida, sono allineati con le good practice del settore. Per qualsiasi nuovo standard o prodotto tecnologico, si svolgono programmi di formazione prima che ne sia introdotto l'utilizzo in azienda.

DESCRIZIONE DEL PROCESSO

PO8 Gestire la qualità

Si sviluppa e mantiene un sistema di gestione della qualità (SGQ) che consideri e documenti i processi di sviluppo e di acquisizione e i relativi standard. Questo risultato è ottenibile con la pianificazione, realizzazione e manutenzione di un SGQ, con la definizione di chiari requisiti, procedure e politiche per la qualità. I requisiti di qualità sono definiti e comunicati utilizzando indicatori quantitativi con valori di soglia raggiungibili. Un processo di miglioramento continuo è conseguito attraverso sistematici monitoraggi, analisi, interventi per gestire gli scostamenti, report per comunicare i risultati ai soggetti interessati. La gestione della qualità è essenziale per assicurare che l'IT sia portatore di valore per l'azienda, sia fattore di miglioramento continuo e di trasparenza per gli stakeholder.





Il controllo del processo IT

Gestire la qualità

che soddisfa i requisiti aziendali per l'IT di

assicurare il miglioramento continuo e misurabile della qualità dei servizi erogati dall'IT

ponendo l'attenzione su

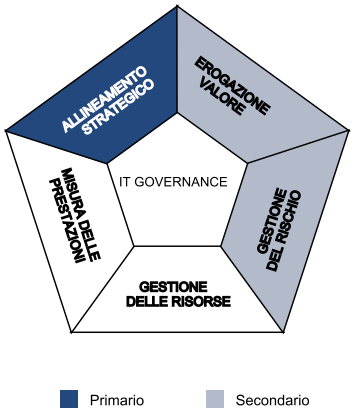
la definizione di un sistema di gestione della qualità (SGQ), il costante monitoraggio della performance rispetto agli obiettivi predefiniti e l'implementazione di un programma di miglioramento continuo dei servizi IT.

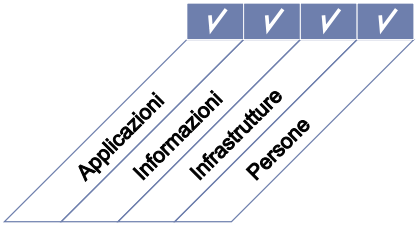
è ottenuto tramite

- la definizione di standard di qualità e relative pratiche
- il monitoraggio e la verifica della performance interna ed esterna rispetto agli standard di qualità fissati e alle relative pratiche
- il miglioramento continuo del Sistema di Gestione della Qualità

e viene misurato tramite

- la percentuale di stakeholder soddisfatti della qualità dell'IT (ponderata per importanza)
- la percentuale di processi sottoposti a verifica periodica del Controllo Qualità che risultano in linea con gli obiettivi di qualità di medio e lungo termine
- la percentuale di processi sottoposti alle verifiche del Controllo Qualità (CQ)





OBIETTIVI DI CONTROLLO

PO8 Gestire la qualità

PO8.1 Il Sistema di Gestione della Qualità (SGQ/QMS)

Definire e mantenere un Sistema di Gestione della Qualità con un approccio standard, formale e sistematico in linea con le necessità aziendali. L'SGQ dovrebbe definire i requisiti e criteri di qualità: i principali processi dell'IT, la sequenza e l'interazione degli stessi, e le politiche, i metodi e i criteri per definire, identificare, correggere e prevenire i casi di non conformità. L'SGQ dovrebbe definire la struttura organizzativa per la gestione della qualità, indicando ruoli, compiti e responsabilità. Tutte le aree principali dovrebbero sviluppare piani di qualità propri in base a criteri e politiche e registrarne i dati. Monitorare e valutare l'efficacia e l'accettazione dell'SGQ e migliorarlo, ove necessario.

PO8.2 Standard e prassi per la gestione della qualità dell'IT

Identificare e mantenere gli standard, le procedure e pratiche per i principali processi IT al fine di guidare l'organizzazione a rispondere alle finalità del SGQ. Utilizzare come riferimento le good practice del settore quando si stanno migliorando e personalizzando le pratiche per la gestione della qualità dell'azienda.

PO8.3 Standard di sviluppo ed acquisizione

Adottare e mantenere standard di sviluppo ed acquisto per tutto il ciclo di vita del prodotto finale e prevedere approvazioni formali a conclusione delle fasi principali secondo criteri di approvazione formale. Gli aspetti da considerare comprendono: gli standard per la codifica dei software, la definizione di una nomenclatura convenzionale, i formati dei file, gli standard di progettazione dei dizionari degli schemi e dei dati, gli standard dell'interfaccia utente, l'interoperatività, l'efficienza della performance del sistema, la scalabilità, gli standard di sviluppo e verifica, la convalida in base ai requisiti, i piani di verifica, ed infine, i test di unità, regressione ed integrazione.

PO8.4 Centralità del cliente

Assicurare che la gestione della qualità si concentri sui clienti determinandone i requisiti ed allineandoli agli standard e le pratiche dell'IT. Definire i ruoli e le responsabilità per la risoluzione dei conflitti tra il consumatore/utente e la struttura dell'IT.

PO8.5 Miglioramento continuo

Mantenere e comunicare regolarmente un piano generale per gestione della qualità che promuova il miglioramento continuo.

PO8.6 Valutazione, monitoraggio e verifica della qualità

Definire, pianificare ed implementare attività di valutazione per monitorare che l'SGQ venga costantemente adottato e se ne percepisca il valore aggiunto. Le valutazioni, il monitoraggio e la registrazione delle informazioni dovrebbero servire al proprietario del processo per adottare le opportune misure correttive e preventive.

LINEE GUIDA PER LA GESTIONE

PO8 Gestire la qualità

Da	Inputs
PO1	Piano strategico IT
PO10	Piano dettagliato dei progetti
ME1	Piano delle azioni correttive

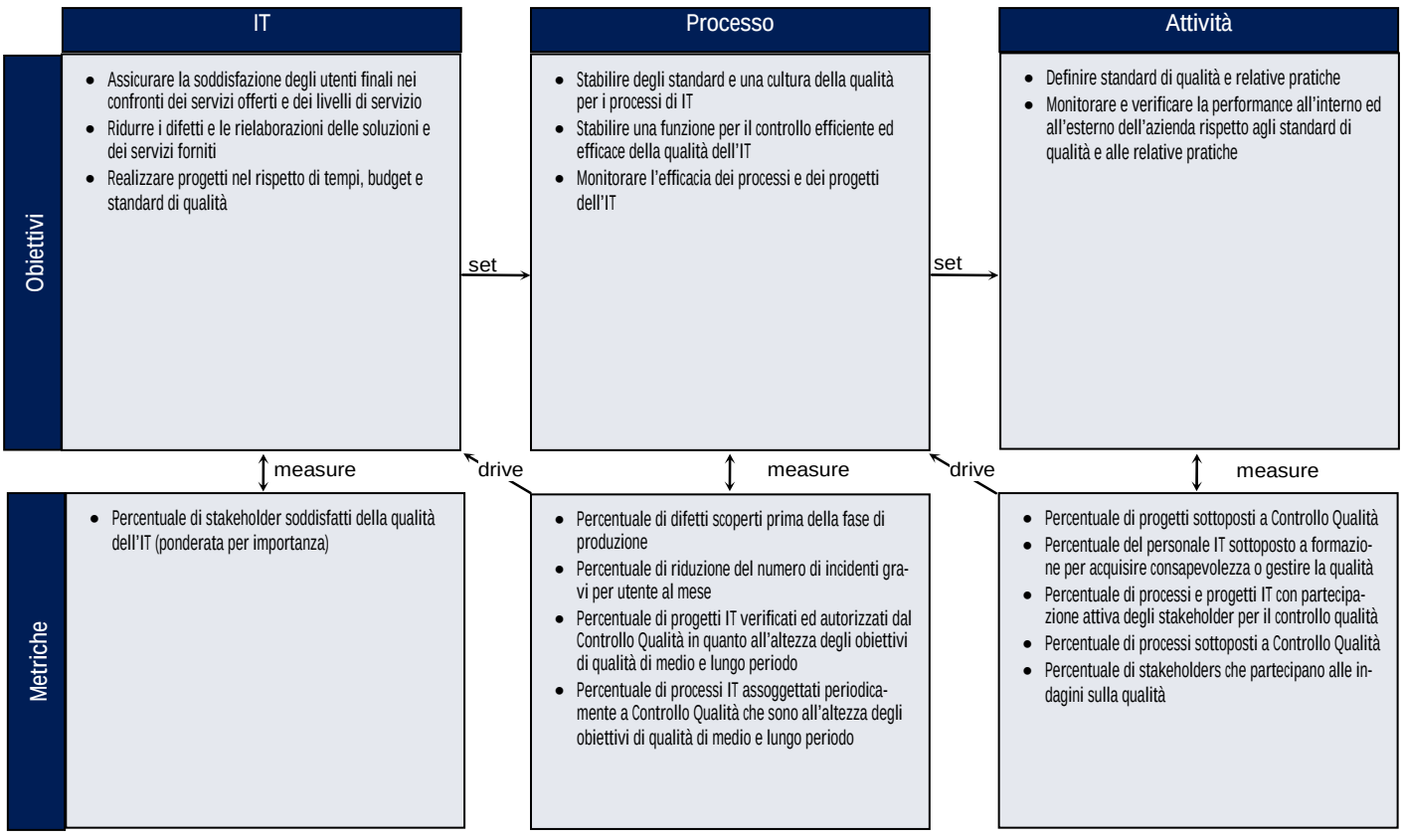
Outputs	A						
Linee guida per le acquisizioni	AI1	AI2	AI3	AI5	DS2		
Standard per lo sviluppo	PO10	AI1	AI2	AI3	AI7		
Standard di qualità e requisiti di misurazione	ALL						
Interventi per il miglioramento della qualità	PO4	AI6					

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire un sistema di gestione della qualità	C		C	A/R	I	I	I	I	I	I	C
Stabilire e mantenere il sistema di gestione della qualità	I	I	I	A/R	I	C	C	C	C	C	C
Definire standard di qualità e comunicarli all'interno dell'azienda		I		A/R	I	C	C	C	C	C	C
Definire il piano di gestione della qualità e gestirlo nell'ottica di un miglioramento continuo				A/R	I	C	C	C	C	C	C
Valutare, monitorare e verificare il rispetto degli obiettivi di qualità di lungo periodo				A/R	I	C	C	C	C	C	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO8 Gestire la qualità

Il grado di strutturazione del processo *Gestire la qualità* che soddisfa i requisiti aziendali per l'IT di *assicurare il miglioramento continuo e misurabile della qualità dei servizi erogati dall'IT* è:

0 Non esistente quando

L'azienda non ha processi per la pianificazione di un SGQ né alcuna metodologia applicabile all'intero ciclo di sviluppo. L'alta direzione ed il personale IT non riconoscono la necessità di un programma per la gestione della qualità. I progetti e le attività non sono mai assoggettati a verifiche della qualità.

1 Iniziale/*Ad Hoc* quando

La direzione è consapevole della necessità di un Sistema di Gestione della Qualità. Se ne esiste uno, ciò dipende dall'iniziativa di singoli individui. La direzione dà giudizi informali sulla qualità.

2 Ripetibile ma Intuitivo quando

Si sta creando un programma per definire e monitorare le attività del SGQ all'interno dell'IT. Tali attività si concentrano su progetti e processi dell'IT e non su progetti aziendali in senso ampio.

3 Definito quando

La direzione ha comunicato un processo definito per l'SGQ che coinvolge i responsabili dell'IT e degli utenti finali. Sta nascendo un programma di formazione sulla qualità da proporre a tutti i livelli aziendali. Le aspettative minime sulla qualità sono definite e condivise a livello di progetti e di struttura IT. Si stanno sviluppando strumenti e pratiche di gestione della qualità. Si pianificano, e talvolta si svolgono, indagini sul livello di qualità percepito.

4 Gestito e Misurabile quando

Al SGQ si fa riferimento in tutti i processi, compresi quelli dipendenti da esterni. Per le metriche della qualità si è definita una base di conoscenze standard. Per giudicare le iniziative del SGQ si adottano metodi di analisi costi/benefici. Si stanno cominciando a fare confronti nell'ambito del proprio settore economico e della concorrenza. È stato istituito un programma di istruzione e formazione sulla qualità da presentare a tutti i livelli aziendali. Si stanno standardizzando gli strumenti e le pratiche e si effettuano periodicamente analisi per ricercare le cause primarie delle non conformità. Si eseguono regolarmente indagini sul livello di qualità percepito. Esiste un programma standard ben strutturato per la valutazione della qualità. I responsabili IT stanno creando una base di conoscenze per le metriche della qualità.

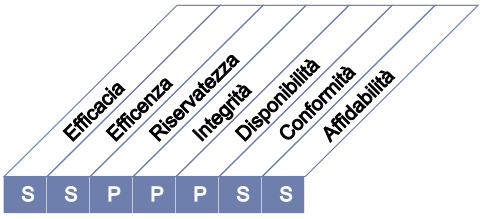
5 Ottimizzato quando

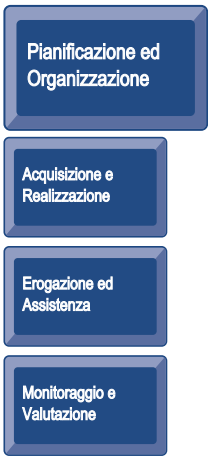
Il SGQ è integrato ed applicato in tutte le attività dell'IT. I processi del SGQ sono flessibili ed adattabili ai cambiamenti dell'ambiente IT. La base di conoscenze per i parametri della qualità è potenziata dalle good practice esterne. Si eseguono regolarmente confronti con gli standard esterni. Lo svolgimento di verifiche sul livello di qualità percepito è un processo continuo e dà luogo a root cause analysis e azioni di miglioramento. Si svolgono controlli formali sul livello del processo di gestione della qualità.

DESCRIZIONE DEL PROCESSO

PO9 Valutare e gestire i rischi informatici

Creare e mantenere un quadro di riferimento per la gestione dei rischi. Tale quadro di riferimento documenta il livello conosciuto e condiviso dei rischi informatici aziendali, le strategie per contenerli ed i rischi residui accettati. Sono identificati, analizzati e valutati tutti gli impatti sugli obiettivi aziendali che potrebbero essere determinati da eventi imprevisti. Sono adottate strategie di contenimento dei rischi per ridurre il rischio residuo ad un livello accettato. Il risultato della valutazione dei rischi è comprensibile per gli stakeholder ed è espresso in termini finanziari, per permettere agli stessi stakeholder di allineare il rischio ad un accettabile livello di tolleranza.





Il controllo del processo IT

Valutare e gestire i rischi informatici

che soddisfa i requisiti aziendali per l'IT di

analizzare e comunicare i rischi informatici ed il loro potenziale impatto sui processi e gli obiettivi dell'azienda

ponendo l'attenzione su

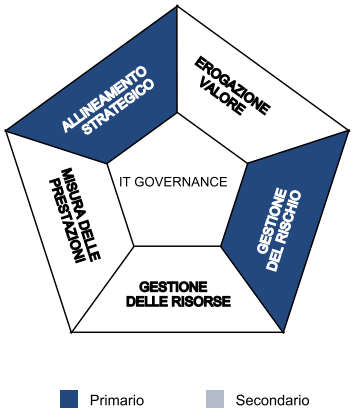
lo sviluppo di un quadro di riferimento per la gestione dei rischi, che si integri con i modelli di gestione dei rischi aziendali e di quelli operativi, la valutazione e l'attenuazione dei rischi e la comunicazione del rischio residuo

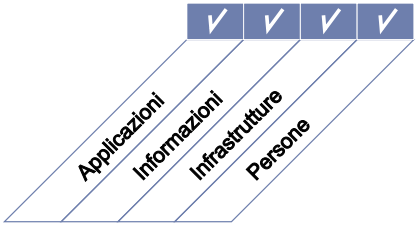
è ottenuto tramite

- l'assicurazione che la gestione del rischio è pienamente integrata nei processi gestionali, internamente ed esternamente, ed applicata con sistematicità
- lo svolgimento di valutazioni dei rischi
- la raccomandazione e comunicazione di piani di azioni correttive

e viene misurato tramite

- la percentuale di obiettivi critici dell'IT presi in considerazione nella valutazione dei rischi
- la percentuale di rischi critici dell'IT identificati per i quali sono stati sviluppati dei piani d'azione
- la percentuale di piani d'azione per la gestione dei rischi dei quali è stata approvata l'attuazione





OBIETTIVI DI CONTROLLO

PO9 Valutare e gestire i rischi informatici

PO9.1 Il quadro di riferimento per la gestione del rischio informatico

Definire un quadro di riferimento per la gestione del rischio informatico che sia allineato con quello dell'organizzazione (dell'impresa).

PO9.2 Definizione del contesto di Rischio

Definire il contesto di applicazione del modello di valutazione dei rischi al fine di assicurare risultati appropriati. Ciò implica che dovrebbe essere determinato anche il contesto interno ed esterno per ciascuna valutazione del rischio, le finalità della valutazione ed i criteri adottati per la valutazione dei rischi.

PO9.3 Identificazione degli eventi

Identificare tutti gli eventi (una importante e realistica minaccia che si concretizza in una significativa vulnerabilità che si può verificare) che potenzialmente hanno un impatto sulle finalità e sull'operatività aziendali, compresi gli aspetti legati al business o alla normativa, gli aspetti legali, tecnologici, i partner commerciali, il personale e gli aspetti operativi. Determinare la natura dell'impatto e registrarne le informazioni relative. Registrare e conservare i rischi rilevanti in un registro dei rischi.

PO9.4 Valutazione dei rischi

Valutare periodicamente la probabilità e l'impatto di tutti i rischi identificati utilizzando metodi qualitativi e quantitativi. La probabilità e l'impatto associati al rischio intrinseco e a quello residuo dovrebbero essere determinati separatamente, utilizzando delle categorie ed un modello dei rischi.

PO9.5 Risposta ai rischi

Sviluppare e mantenere un processo di pronta capacità di risposta ai rischi per assicurare che controlli efficaci e convenienti mitighino l'esposizione al rischio in modo sistematico. Il processo di risposta al rischio dovrebbe identificare strategie per evitare, ridurre, condividere o accettare il rischio, stabilire le responsabilità associate, considerare i livelli di tolleranza dei rischi.

PO9.6 Mantenimento e monitoraggio di un piano d'azione per la gestione dei rischi

Una volta definite le priorità, pianificare le attività di controllo dei rischi a tutti i livelli per implementare le risposte ai rischi ritenute necessarie, oltre ad identificare i costi, i benefici ed i responsabili esecutivi. Ottenere l'approvazione delle azioni suggerite e l'accettazione dei rischi residui, assicurare che le azioni approvate siano assegnate al/ai proprietario/ri dei processi soggetti a quel rischio. Monitorare l'esecuzione dei piani e riferire qualsiasi deviazione alla Direzione.

LINEE GUIDA PER LA GESTIONE

PO9 Valutare e gestire i rischi informatici

Da	Inputs
PO1	Piano IT tattico e strategico, portafoglio servizi IT
PO10	Piano per la gestione dei rischi di progetto
DS2	Rischi connessi ai fornitori
DS4	Risultati del test di contingency
DS5	Rischi e vulnerabilità di sicurezza
ME1	Storico dei rischi con relative tendenze ed accadimenti
ME4	Propensione aziendale verso i rischi IT

Outputs	A						
Analisi dei rischi	PO1	DS4	DS5	DS12	ME4		
Rapporti inerenti i rischi	ME4						
Linee guida per la gestione dei rischi IT	PO6						
Piano delle azioni correttive dei rischi IT	PO4	AI6					

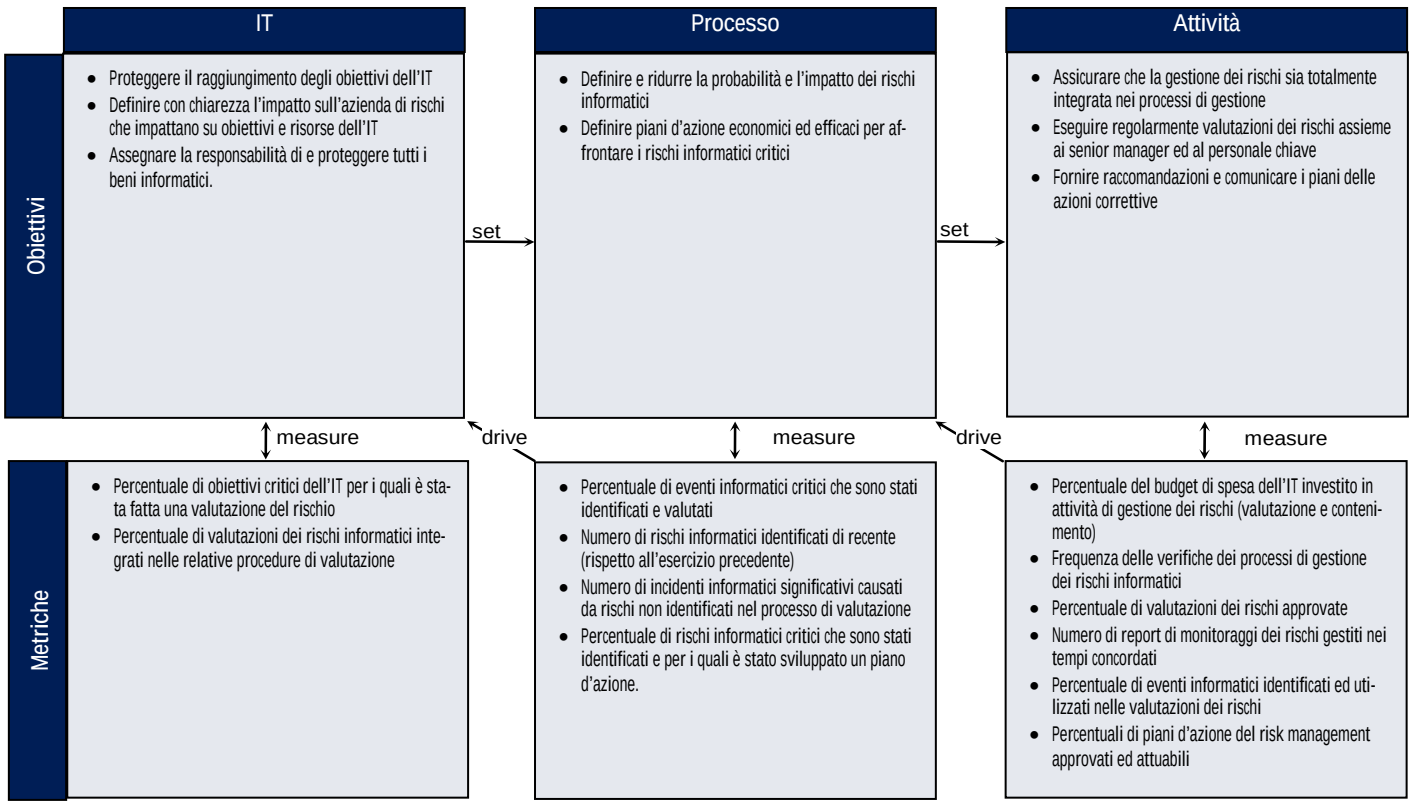
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Determinare l'allineamento del gestione dei rischi (o risk management) (es., valutare il rischio)	A	R/A	C	C	R/A	I					I
Comprendere i relativi obiettivi strategici dell'azienda		C	C	R/A	C	C					I
Comprendere i relativi obiettivi dei processi aziendali				C	C	R/A					I
Identificare gli obiettivi interni all'IT e definire l'ambiente del rischio					R/A		C	C	C		I
Identificare gli eventi associati agli obiettivi [alcuni eventi hanno un impatto sull'azienda (azienda = A); altri hanno un impatto sull'IT (IT=A, azienda =C)]	I			A/C	A	R	R	R	R		C
Valutare i rischi derivanti da eventi				A/C	A	R	R	R	R		C
Valutare le risposte al rischio	I	I	A	A/C	A	R	R	R	R		C
Definire le priorità e pianificare le attività di controllo	C	C	A	A	R	R	C	C	C		C
Approvare ed assicurare la disponibilità dei fondi per sovvenzionare i piani d'azione per la gestione dei rischi		A	A		R	I	I	I	I		I
Mantenere e monitorare un piano di azione per la gestione dei rischi	A	C	I	R	R	C	C	C	C	C	R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO9 Valutare e gestire i rischi informatici

Il grado di strutturazione del processo *Valutare e gestire i rischi informatici* che soddisfa i requisiti aziendali per l'IT di *analizzare e comunicare i rischi informatici ed il loro potenziale impatto sui processi e gli obiettivi dell'azienda* è:

0 Non esistente quando

L'organizzazione non effettua analisi dei rischi relativi ai processi e alle decisioni aziendali. L'azienda non considera gli effetti associati alle vulnerabilità della sicurezza e alle incertezze dei progetti di sviluppo. La gestione dei rischi non è considerata rilevante né per l'acquisto di soluzioni IT né per l'erogazione dei servizi informatici.

1 Iniziale/*Ad Hoc* quando

I rischi informatici sono gestiti caso per caso. Vengono svolte valutazioni informali dei rischi di progetto secondo modalità dipendenti da ciascun progetto. Talvolta le attività di analisi del rischio sono identificate in un project plan ma sono raramente assegnate a responsabili specifici. I rischi informatici specifici, quali la sicurezza, la disponibilità e l'integrità delle informazioni sono presi in considerazione occasionalmente a livello di singolo progetto. I rischi informatici che influenzano la normale operatività sono raramente oggetto di discussione nei management meeting. Anche quando i rischi sono oggetto di osservazione, non vi è sistematicità poi nelle iniziative per ridurli. Si sta cominciando a comprendere l'importanza dei rischi informatici e la necessità di identificarli.

2 Ripetibile ma Intuitivo quando

L'approccio alla valutazione dei rischi esiste, ma è ancora immaturo e viene applicato a discrezione dei project manager. Il risk management è solitamente ad alto livello e si applica solo ai progetti principali o in risposta a situazioni problematiche. Quando si identificano dei rischi, si cominciano ad implementare processi per attenuarli.

3 Definito quando

Una politica generale di gestione dei rischi aziendali definisce quando e come condurre le valutazioni degli stessi. Tali valutazioni seguono un processo definito e documentato. È disponibile una formazione sul risk management per tutto il personale. È lasciata alla discrezione del singolo individuo la decisione di seguire il processo di valutazione dei rischi e ricevere formazione. La metodologia della valutazione dei rischi è solida e convincente, ed assicura l'identificazione dei principali rischi aziendali. Una volta che i rischi sono identificati, solitamente si istituisce un processo per attenuare quelli principali. Le descrizioni delle posizioni professionali indicano anche le responsabilità per la gestione dei rischi.

4 Gestito e Misurabile quando

La valutazione e la gestione dei rischi sono procedure standard. Le eccezioni al processo di gestione dei rischi vengono riferite al management dell'IT, che solitamente ha responsabilità di alto livello. La valutazione e la conseguente gestione dei rischi si svolgono sia a livello di singolo progetto che normalmente anche in riferimento al complesso delle attività dell'IT. La direzione è informata dei cambiamenti del business e dell'ambiente IT che potrebbero avere effetti rilevanti sugli scenari dei rischi informatici. Il management è in grado di monitorare i rischi e ha informazioni per decidere quale livello di esposizione è disposto ad accettare. Per tutti i rischi identificati viene nominato un proprietario; il senior management e la direzione IT stabiliscono i livelli di rischio che l'organizzazione potrà tollerare. La direzione IT sviluppa criteri standard per valutare i rischi e definire i relativi indici di ritorno. Il management prevede a budget un progetto di gestione operativa per ripetere regolarmente la valutazione dei rischi. Si stabilisce una banca dati per la gestione dei rischi e si comincia ad automatizzare parte dei processi di gestione. Il management IT prende in considerazione strategie per ridurre i rischi.

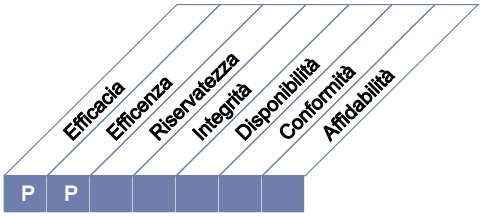
5 Ottimizzato quando

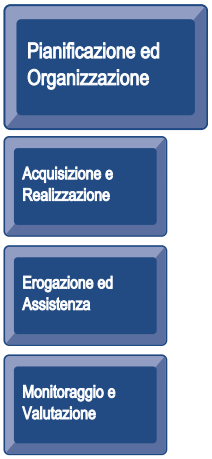
Il risk management si sta sviluppando verso un processo strutturato a livello aziendale, ben gestito e che viene applicato. In tutta l'organizzazione si applicano "good practice". La raccolta e l'analisi dei dati del risk management, nonché la relativa reportistica, sono fortemente automatizzate. Le linee guida sono definite dai leader del settore e l'organizzazione IT partecipa a gruppi fra "pari" per scambiare esperienze. Le attività di gestione dei rischi sono ben integrate in tutte le attività aziendali e dell'IT, sono ben accette e coinvolgono ampiamente gli utenti dei servizi IT. Se si prendono importanti decisioni di investimento o operative per l'IT senza tenere in considerazione il piano di gestione dei rischi, Il risk management si sta sviluppando verso un processo strutturato a livello aziendale, ben gestito e che viene applicato. In tutta l'organizzazione si applicano "good practice". La raccolta e l'analisi dei dati del risk management, nonchè la relativa reportistica, sono fortemente automatizzate. Le linee guida sono definite dai leader del settore e l'organizzazione IT partecipa a gruppi fra "pari" per scambiare esperienze. Le attività di gestione dei rischi sono ben integrate in tutte le attività aziendali e dell'IT, sono ben accette e coinvolgono ampiamente gli utenti dei servizi IT. Se si prendono importanti decisioni di investimento o operative per l'IT senza tenere in considerazione il piano di gestione dei rischi, la direzione identifica il fatto e interviene. La direzione valuta continuamente le strategie per il contenimento dei rischi. la direzione identifica il fatto e interviene. La direzione valuta continuamente le strategie per il contenimento dei rischi.

DESCRIZIONE DEL PROCESSO

PO10 Gestire i progetti

Viene stabilito un quadro generale di riferimento per la gestione delle iniziative e di tutti progetti dell'IT, al fine di assicurare una corretta definizione delle priorità e un adeguato coordinamento di tutti i progetti. Per assicurare la gestione dei rischi di progetto e la produzione di valore per l'azienda tale quadro generale comprende: il master plan, i criteri per l'allocazione delle risorse, la definizione dei risultati, l'approvazione degli utenti, un approccio all'erogazione del servizio per fasi, il controllo qualità, il piano di prove documentato, il test e la verifica successivi all'installazione. Tale approccio riduce i rischi derivanti da costi inattesi o da interruzione di progetti, migliora le comunicazioni ed coinvolgimento con i settori non-IT e con gli utenti finali, assicura la validità e la qualità dei prodotti realizzati dai progetti, massimizza il contributo di questi prodotti ai programmi di investimento che fanno leva sull'IT.





Il controllo del processo IT

Gestire i progetti

che soddisfa i requisiti aziendali per l'IT di

assicurare la produzione dei risultati dei progetti nel rispetto dei tempi, del budget e della qualità concordati

ponendo l'attenzione su

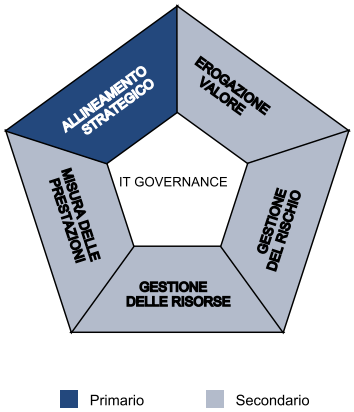
un chiaro approccio per la gestione dei programmi e dei progetti applicato ai progetti dell'IT e che permetta la partecipazione degli stakeholder e il monitoraggio dei rischi e dello stato di avanzamento dei progetti

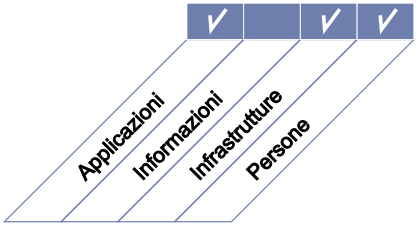
è ottenuto tramite

- la definizione ed il rispetto dell'approccio e dei quadri di riferimento per i programmi e per i progetti
- l'emanazione di linee guida per la gestione dei progetti
- la definizione di un piano di progetto per ciascuno dei progetti inseriti nel portafoglio

e viene misurato tramite

- la percentuale di progetti che soddisfano le attese degli stakeholder (rispetto dei tempi e del budget e soddisfacimento dei requisiti – ponderati per importanza)
- la percentuale di progetti sottoposti a verifiche successivamente all'implementazione
- la percentuale di progetti conformi agli standard e alle pratiche di project management





OBIETTIVI DI CONTROLLO

PO10 Gestire i progetti

PO10.1 Quadro di riferimento per la gestione dei programmi

Gestire il programma dei progetti, relativamente al portafoglio dei programmi di investimento legati all'IT, attraverso l'identificazione, la definizione, la valutazione, la determinazione delle priorità, la selezione, l'attivazione, la gestione ed il controllo dei progetti. Assicurare che i progetti supportino gli obiettivi del programma. Coordinare le attività e le relazioni di dipendenza tra progetti multipli, gestire il contributo di tutti i progetti inseriti nel programma rispetto ai risultati attesi, fornire le risorse necessarie e risolvere i conflitti.

PO10.2 Quadro di riferimento per la gestione dei progetti

Definire e gestire un quadro di riferimento per la gestione dei progetti che definisca l'ambito ed i limiti della gestione dei progetti, come pure le metodologie da adottare ed utilizzare per ciascuno dei progetti attivati. Il quadro generale e le metodologie dovrebbero essere integrati con i processi aziendali di gestione dei programmi.

PO10.3 Approccio alla gestione dei progetti

Stabilire un approccio alla gestione dei progetti proporzionato alla dimensione e complessità dei singoli progetti, oltre che ai relativi obblighi normativi. La struttura di governance di progetto può comprendere i ruoli, le attività e le responsabilità degli sponsor del programma e dei progetti, il comitato guida, la funzione di supporto alla gestione, il responsabile del progetto, ed i meccanismi attraverso cui questi dimostrano di aver ottemperato a tali responsabilità (per esempio, attraverso verifiche delle singole fasi del lavoro e relazioni). Assicurarsi che tutti i progetti informatici abbiano degli sponsor con adeguato titolo per essere di riferimento per la realizzazione del progetto nell'ambito del programma strategico generale.

PO10.4 Impegno degli stakeholder

Ottenere l'impegno e la partecipazione degli stakeholder interessati nella definizione ed esecuzione del progetto nell'ambito del programma generale degli investimenti legati all'IT.

PO10.5 Dichiarazione dell'oggetto del progetto

Definire e documentare il progetto per confermare e sviluppare tra gli stakeholder una visione comune della natura e dell'oggetto del progetto e dei suoi rapporti con gli altri progetti nell'ambito del programma generale degli investimenti legati all'IT.

PO10.6 Fase di attivazione di progetto

Approvare l'attivazione di ciascuno dei principali progetti e comunicarlo a tutti gli stakeholder. Basare l'approvazione della fase di avvio sulle decisioni di governo del programma. L'approvazione delle fasi successive dovrebbe basarsi sulla verifica e l'accettazione dei risultati della fase precedente, sull'approvazione di un business case aggiornato alla successiva importante verifica del programma. Nel caso di sovrapposizione di due fasi del progetto, gli sponsor del programma e del progetto dovrebbero definire il punto in cui dare l'autorizzazione a procedere.

PO10.7 Piano di progetto integrato

Definire ed approvare un piano di progetto ufficiale ed integrato (comprendente le risorse dell'azienda e dei sistemi informativi) al fine di guidare l'esecuzione ed il controllo del progetto per tutta la durata del progetto stesso. Nell'ambito di un programma si dovrebbero comprendere e documentare le attività del progetto e le relazioni di dipendenza con gli altri progetti. Il piano dovrebbe essere mantenuto per tutta la durata del progetto. Assieme alle sue eventuali modifiche, poi, tale piano dovrebbe essere approvato secondo il quadro di riferimento per la gestione dei programmi e dei progetti.

PO10.8 Risorse di progetto

Definire le responsabilità, le relazioni, i livelli di autorità ed i parametri della performance dei partecipanti al gruppo di lavoro e specificare i criteri per l'acquisizione e assegnazione di personale competente e/o collaboratori esterni al progetto. L'acquisto dei prodotti e servizi necessari per ciascun progetto dovrebbe essere pianificato e gestito per poter raggiungere gli obiettivi del progetto utilizzando le modalità di acquisto definite dall'azienda.

PO10.9 Gestione dei rischi di progetto

Eliminare o minimizzare i rischi specifici associati ai singoli progetti attraverso un processo sistematico di pianificazione, identificazione, analisi, risposta, monitoraggio e controllo delle aree e degli eventi che rappresentano cause potenziali di variazioni impreviste. I rischi affrontati nel processo di gestione del progetto e i risultati del progetto dovrebbero essere definiti e registrati a livello centrale.

PO10.10 Piano per la qualità di progetto

Preparare un piano per gestire la qualità del progetto descrivendo il sistema di qualità del progetto e le modalità di implementazione. Tale piano dovrebbe essere ufficialmente verificato ed approvato da tutte le parti interessate, ed essere poi incluso nel piano integrato di progetto.

PO10.11 Controllo delle variazioni di progetto

Creare un sistema di controllo per gestire le modifiche di ciascun progetto, cosicché sia possibile verificare in modo appropriato tutte le modifiche degli aspetti definiti inizialmente per il progetto (costi, tempistiche, oggetto e qualità), approvarle ed includerle nel piano integrato di progetto secondo il quadro di riferimento per la governance dei programmi e dei progetti.

PO10.12 Pianificazione di progetto per i metodi di validazione

Identificare le necessarie attività di valutazione per convalidare sistemi nuovi o modificati nel corso della pianificazione del progetto, ed includerle nel piano integrato di progetto. Tali attività dovrebbero assicurare la garanzia che i controlli interni e le procedure di sicurezza soddisfino i requisiti definiti.

PO10.13 Misura, report e monitoraggio della performance di progetto

Misurare la performance di progetto secondo criteri chiave di performance di progetto relativamente all'oggetto, la tempistica, la qualità, i costi ed i rischi. Identificare eventuali deviazioni rispetto al piano. Valutare l'impatto delle deviazioni sul progetto e sul programma in generale, riferire i risultati agli stakeholder principali. Raccomandare, implementare e monitorare eventuali azioni correttive, se necessario, in linea con il quadro di riferimento per la governance dei programmi e dei progetti.

PO10.14 Chiusura del progetto

A conclusione di ciascun progetto, richiedere che gli stakeholder accertino se il progetto ha realizzato i risultati e i benefici desiderati. Identificare e comunicare eventuali azioni ancora da svolgere per raggiungere i risultati pianificati per il progetto e i benefici del programma, ed identificare e documentare quanto appreso al fine di poterle utilizzare in futuri progetti e programmi.

Pagina intenzionalmente vuota

LINEE GUIDA PER LA GESTIONE

PO10 Gestire i progetti

Da	Inputs
PO1	Portafoglio progetti IT
PO5	Portafoglio progetti IT aggiornato
PO7	Matrice competenze IT
PO8	Standard per lo sviluppo
AI7	Revisione post-implementazione

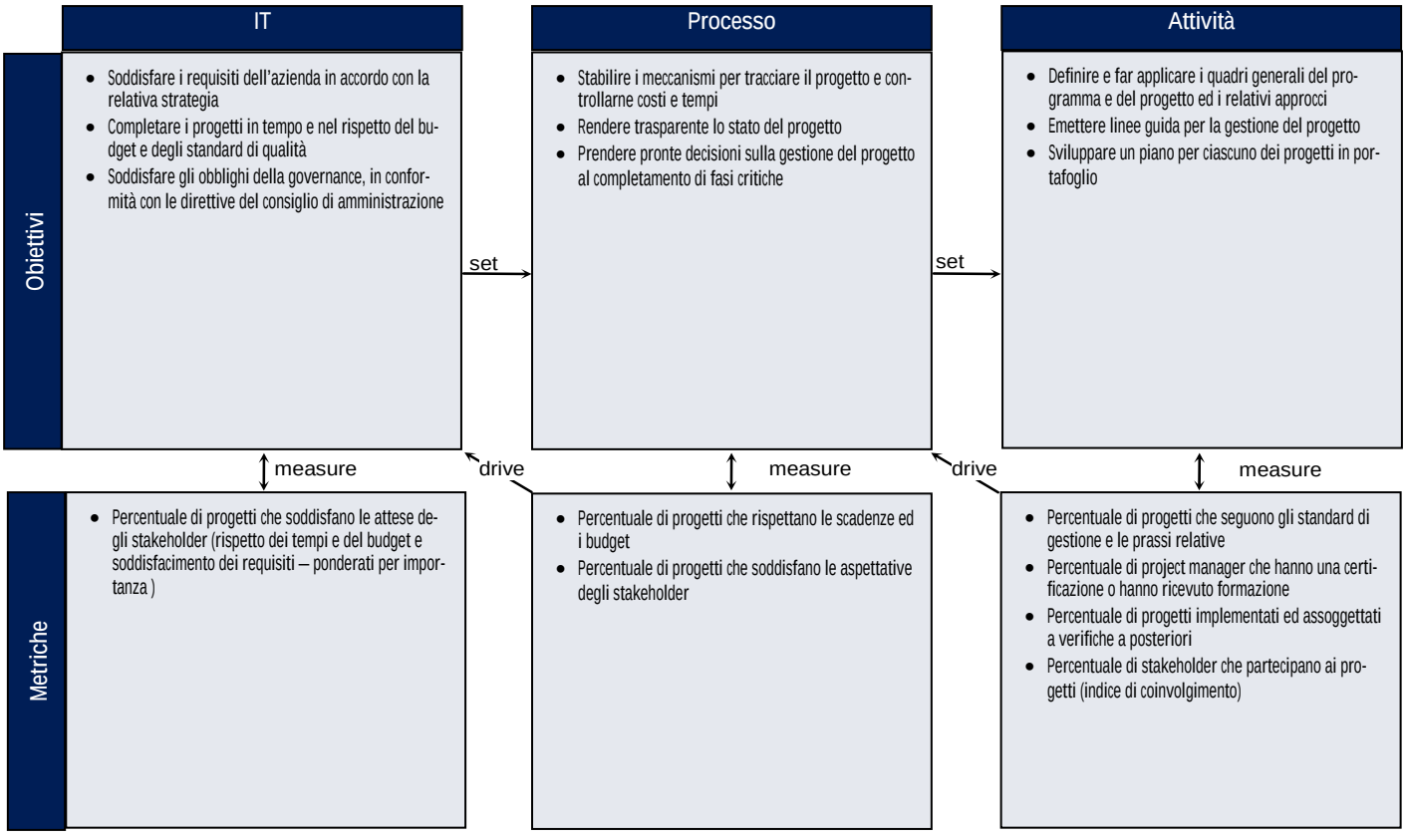
Outputs	A						
Analisi della performance dei progetti	ME1						
Piano per la gestione dei rischi dei progetti	PO9						
Linee guida per la gestione dei progetti	AI1..AI7						
Piani dettagliati dei progetti	PO8	AI1..AI7	DS6				
Portafoglio progetti IT aggiornato	PO1	PO5					

RACI Chart

Attività / Ruoli	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire un quadro generale per la gestione del programma e del portafoglio di investimenti in IT	C	C	A	R						C	C
Definire e gestire un quadro generale per la gestione dei progetti IT	I	I	I	A/R	I	C	C	C	C	R	C
Definire e gestire un sistema per monitorare, valutare e gestire i progetti IT	I	I	I	R		C	C	C	C	A/R	C
Creare carte del progetto, tempistiche, piani per la gestione della qualità, budget, e piani di gestione dei rischi e delle comunicazioni.			C	C	C	C	C	C	C	A/R	C
Assicurare la partecipazione e l'impegno degli interessati ai progetti	I		A	R	C						C
Assicurare il controllo efficace dei progetti e delle relative modifiche			C	C		C	C	C		A/R	C
Definire e realizzare metodi di convalida e verifica dei progetti			I	C				I		A/R	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

PO10 Gestire i progetti

Il grado di strutturazione del processo *Gestire i progetti* che soddisfa i requisiti aziendali per l'IT di *assicurare la produzione dei risultati dei progetti nel rispetto dei tempi, del budget e della qualità concordati* è:

0 Non esistente quando

Non si utilizzano tecniche di project management e l'organizzazione non considera gli impatti sull'azienda derivanti da una cattiva gestione dei progetti e dal fallimento dei progetti di sviluppo.

1 Iniziale/*Ad Hoc* quando

L'uso di tecniche ed approcci di project management all'interno dell'IT è lasciato alle decisioni dei singoli manager IT. In generale, il management non si impegna a gestire il progetto ed a farne da referente. Le decisioni critiche sulla gestione dei progetti sono prese senza ricevere l'opinione dei responsabili degli utenti o dei clienti. Il coinvolgimento di clienti ed utenti nella definizione dei progetti è basso o assente. All'interno dell'IT non c'è una chiara organizzazione di project management ed i relativi ruoli e responsabilità non sono definiti. I progetti, le tempistiche ed i milestones sono poco, o per nulla, definiti. Il tempo e le spese dello staff dedicato ai progetti non sono tenuti sotto controllo né confrontati con i budget.

2 Ripetibile ma Intuitivo quando

Il senior management ottiene e comunica la consapevolezza della necessità della gestione dei progetti IT. L'azienda sta sviluppando ed utilizzando le tecniche ed i metodi appresi da un progetto all'altro. Per i progetti di IT si definiscono in via informale gli obiettivi aziendali e tecnici. Gli stakeholder sono poco coinvolti nella gestione dei progetti. Sono state sviluppate delle linee guida iniziali per molti aspetti del project management, ma la loro applicazione è lasciata alla discrezione dei singoli project manager.

3 Definito quando

Il processo e la metodologia di gestione dei progetti di IT sono stati definiti e comunicati. La definizione dei progetti di IT comprende appropriati obiettivi aziendali e tecnici. I senior manager dell'IT e dell'azienda cominciano ad essere coinvolti intensamente nella gestione dei progetti IT. All'interno dell'IT si crea un ufficio di project management, definendone i ruoli e le responsabilità iniziali. Si monitorano i progetti IT, se ne definiscono ed aggiornano le milestones, le tempistiche, i budget e le valutazioni della performance. È disponibile una formazione specifica per la gestione dei progetti, ma è principalmente il risultato di iniziative personali dello staff. Si sono definite sia procedure a garanzia della qualità sia attività di post implementazione dei sistemi, ma i manager dell'IT non le applicano in modo estensivo. I progetti cominciano ad essere gestiti nell'ambito di portafogli.

4 Gestito e Misurabile quando

La direzione richiede che a completamento dei progetti sia esplicitato quanto appreso e siano rivisti i parametri standard di misurazione dei progetti. La gestione dei progetti è misurata e valutata a livello di tutta l'organizzazione e non soltanto all'interno della funzione IT. I miglioramenti nei processi di gestione dei progetti sono formalizzati e comunicati, ed i partecipanti ai gruppi di progetto ricevono formazione appropriata. La direzione IT implementa una struttura organizzativa che prevedere ruoli, responsabilità e parametri della performance documentati all'interno dei progetti. Sono stabiliti i criteri per la valutazione del successo di ogni milestone. Valore e rischio sono misurati e gestiti prima, durante e dopo il completamento del progetto. I progetti sono sempre più gestiti in vista di obiettivi aziendali, piuttosto che solamente per fini specifici della funzione IT. Gli stakeholder ed il senior management che sponsorizza i vari progetti supportano ampiamente ed attivamente i progetti. Esistono piani di formazione in project management per il personale del relativo ufficio e per tutta la funzione IT.

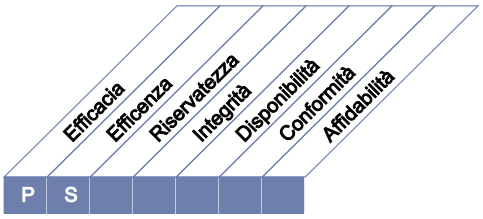
5 Ottimizzato quando

L'azienda adotta e fa applicare una metodologia per la gestione dell'intero ciclo di vita dei programmi e dei progetti integrandola nel complesso della cultura aziendale. È stata avviata un'attività sistematica volta ad identificare ed istituzionalizzare le best practice del project management. È stata definita ed implementata una strategia per i progetti operativi e di sviluppo relativi alla gestione dei fornitori. Un ufficio integrato di project management è responsabile dei progetti e dei programmi dall'inizio fino alla fase successiva all'implementazione. Una pianificazione dei programmi e progetti a livello aziendale assicura che gli utenti e le risorse IT siano utilizzate al meglio per sostenere le iniziative strategiche.

DESCRIZIONE DEL PROCESSO

AI1 Identificare soluzioni automatizzate

L'esigenza di disporre di una nuova applicazione o funzione richiede che, prima dell'acquisizione o della realizzazione, venga effettuata un'analisi, per garantire che i requisiti aziendali siano soddisfatti, adottando un approccio efficace ed efficiente. Questo processo comprende le seguenti fasi: definizione dei fabbisogni informativi, valutazione di soluzioni alternative, verifica della fattibilità tecnologica ed economica, analisi dei rischi, analisi costi-benefici, analisi e scelta tra le opzioni di realizzazione interna o acquisto di un pacchetto. L'esecuzione di queste fasi consente alle imprese di minimizzare i costi di acquisizione e di realizzazione delle soluzioni e nel contempo assicurano che queste soluzioni mettano l'azienda in condizione di perseguire i propri obiettivi.



Il controllo del processo IT

Identificare soluzioni automatizzate

che soddisfa i requisiti aziendali per l'IT di

tradurre i requisiti funzionali e di controllo dell'azienda in un efficace ed efficiente progetto di soluzioni automatizzate

ponendo l'attenzione su

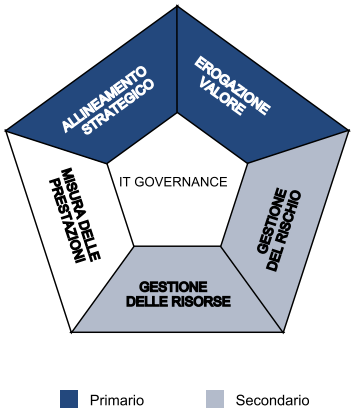
l'identificazione di soluzioni tecniche fattibili ed economicamente adeguate

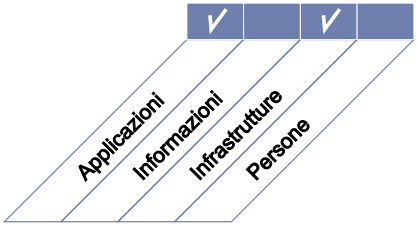
è ottenuto tramite

- la definizione dei fabbisogni funzionali e tecnici
- l'avvio di studi di fattibilità come definito negli standard di sviluppo
- l'approvazione, o non approvazione, dei risultati della definizione dei fabbisogni informativi e dell'analisi di fattibilità

e viene misurato tramite

- il numero di progetti per i quali i benefici attesi non sono raggiunti a causa di assunzioni errate effettuate durante l'analisi di fattibilità
- la percentuale degli studi di fattibilità che sono sottoscritti dal referente del processo aziendale
- la percentuale degli utenti soddisfatti dalle funzionalità rilasciate





OBIETTIVI DI CONTROLLO

AI1 Identificare soluzioni automatizzate

AI1.1 Definizione e manutenzione dei requisiti funzionali e tecnici

Identificare, definire le priorità, specificare e condividere i requisiti funzionali e tecnici di tutte le iniziative richieste per conseguire i risultati attesi previsti nel programma di investimenti resi possibili dall'IT.

AI1.2 Analisi dei rischi

Identificare, documentare ed analizzare i rischi associati ai fabbisogni aziendali e al progetto di soluzione intesi come parte del processo aziendale di sviluppo dei requisiti.

AI1.3 Studio di fattibilità e formulazione di opzioni alternative d'intervento

Sviluppare uno studio di fattibilità che esamini la possibilità di realizzare quanto richiesto. Il management aziendale, con il supporto della funzione IT, deve valutare la fattibilità e le alternative per raccomandare una soluzione allo sponsor aziendale.

AI1.4 Requisiti, determinazione della fattibilità ed approvazione

Lo sponsor aziendale deve approvare e sottoscrivere i requisiti funzionali e tecnici e lo studio di fattibilità in momenti chiave prestabiliti nel processo di selezione delle soluzioni automatizzate. Lo sponsor aziendale ha la titolarità della decisione finale conformemente a quanto previsto nel processo di selezione ed acquisizione delle soluzioni automatizzate.

LINEE GUIDA PER LA GESTIONE

AI1 Identificare soluzioni automatizzate

Da	Inputs
PO1	Piani IT strategici e tattici
PO3	Aggiornamenti periodici sullo "stato della tecnologia"; standard tecnologici
PO8	Standard di acquisizione e sviluppo
PO10	Linee guida per la gestione dei progetti e piani dettagliati di progetto
AI6	Descrizione del processo di modifica
DS1	SLA
DS3	(Requisiti di) prestazioni e pianificazione della capacità elaborativa

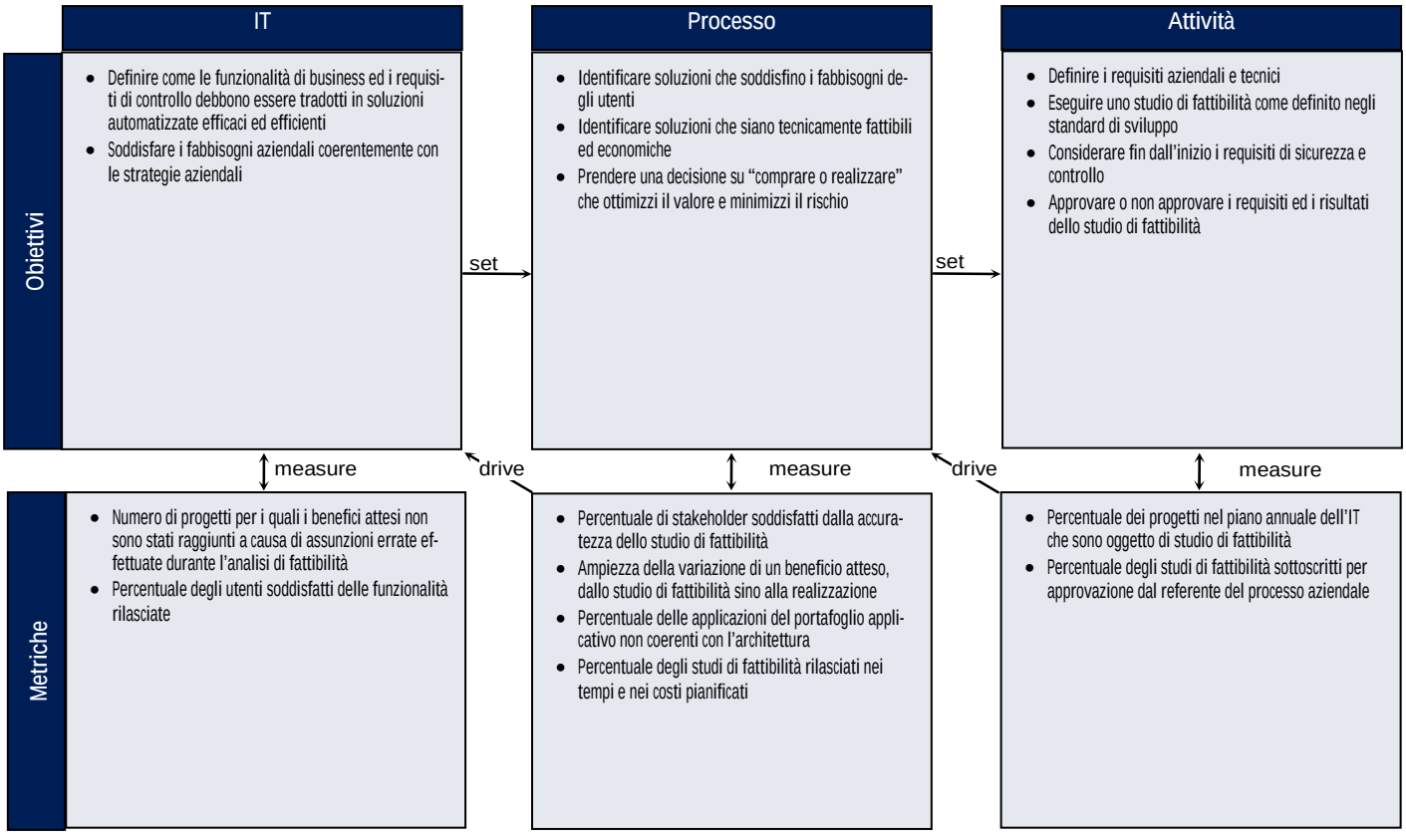
Outputs	A						
Requisiti aziendali e studio di fattibilità	PO2	PO5	PO7	AI2	AI3	AI4	AI5

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire i requisiti funzionali e tecnici			C	C	R	C	R	R		A/R	I
Definire processi per mantenere l'integrità e l'aggiornamento dei requisiti				C		C		C		A/R	C
Identificare, documentare ed analizzare il rischio dei processi aziendali			A/R	R	R	R	C	R		R	C
Condurre uno studio di fattibilità e una valutazione dell'impatto rispetto all'implementazione dei requisiti di business proposti			A/R	R	R	C	C	C		R	C
Stimare i benefici di natura tecnica delle soluzioni proposte		I	R	A/R	R	I	I	I		R	
Stimare i benefici delle soluzioni proposte sul business			A/R	R		C	C	C	I	R	
Sviluppare un processo di approvazione dei requisiti			C	A		C	C	C		R	C
Approvare e sottoscrivere le soluzioni proposte		C	A/R	R	R	C	C	C	I	R	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI1 Identificare soluzioni automatizzate

Il grado di strutturazione del processo *Identificare soluzioni automatizzate* che soddisfa i requisiti aziendali per l'IT di *tradurre i requisiti funzionali e di controllo dell'azienda in un efficace ed efficiente progetto di soluzioni automatizzate* è:

0 Non esistente quando

L'azienda non richiede l'identificazione dei requisiti funzionali ed operativi per lo sviluppo, la realizzazione o la modifica di soluzioni relative a sistemi, servizi, infrastruttura, software e dati. L'azienda non ha consapevolezza della disponibilità di soluzioni tecnologiche potenzialmente rilevanti per il suo business.

1 Iniziale/*Ad Hoc* quando

Esiste la consapevolezza della necessità di definire i requisiti e di identificare le soluzioni tecnologiche. I gruppi si incontrano per discutere le esigenze in maniera informale e i requisiti sono documentati solo occasionalmente. Le soluzioni sono identificate dai singoli addetti in base a conoscenze limitate del mercato, oppure su sollecitazione di offerte del venditore. La ricerca o l'analisi delle tecnologie disponibili è poco strutturata.

2 Ripetibile ma Intuitivo quando

Esistono differenti approcci intuitivi per identificare le soluzioni IT in azienda. Le soluzioni sono identificate in modo informale sulla base dell'esperienza e delle conoscenze della funzione IT. Il successo di ciascun progetto dipende dalle competenze di poche persone chiave. La qualità della documentazione e il processo decisionale variano in modo considerevole. Per definire i fabbisogni e identificare le soluzioni tecnologiche sono usati approcci non strutturati.

3 Definito quando

Esiste un approccio chiaro e strutturato per determinare le soluzioni IT. L'approccio per individuare le soluzioni IT richiede di considerare e valutare delle alternative relativamente ai requisiti aziendali, alle richieste utente, alle opportunità tecnologiche, alla fattibilità economica, alla stima del rischio e ad altri fattori. Il processo per determinare le soluzioni IT è applicato in alcuni progetti ed è basato su alcuni fattori come le decisioni prese dal personale coinvolto, il tempo dedicato dalla Direzione, la dimensione e la priorità della richiesta aziendale originale. Sono usati approcci strutturati per definire i requisiti e identificare le soluzioni IT.

4 Gestito e Misurabile quando

Esiste una metodologia consolidata per l'identificazione e la valutazione delle soluzioni IT ed è usata per la maggior parte dei progetti. La documentazione di progetto è di buona qualità e ciascuna fase è soggetta ad approvazione. I requisiti sono ben articolati ed in conformità con le strutture predefinite. Sono valutate soluzioni alternative, comprensive dell'analisi di costi e benefici. La metodologia è chiara, definita, comprensibile a tutti e misurabile. Esiste un'interfaccia chiaramente definita tra la funzione IT e l'azienda per l'identificazione e la valutazione delle soluzioni IT.

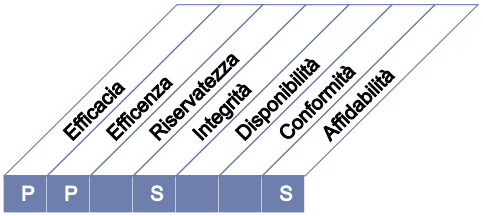
5 Ottimizzato quando

La metodologia per l'identificazione e la valutazione delle soluzioni IT è soggetta a continui miglioramenti. La metodologia di acquisizione e realizzazione ha la flessibilità per poter gestire un ampio spettro di progetti, da quelli di grandi dimensioni sino ai piccoli progetti. La metodologia è supportata da fonti di conoscenza interne ed esterne contenenti il materiale di riferimento relativo alle soluzioni tecniche. La metodologia stessa produce documentazione secondo una struttura predefinita che rende efficienti sia la produzione sia la manutenzione. L'organizzazione è spesso capace di identificare nuove opportunità nell'uso delle tecnologie per acquisire vantaggi competitivi, influenzare la reingegnerizzazione dei processi aziendali e migliorare l'efficienza complessiva. La direzione rileva ed interviene se le soluzioni IT sono approvate senza considerare alternative relativamente alla tecnologia o ai requisiti funzionali.

DESCRIZIONE DEL PROCESSO

AI2 Acquisire e manutenere il software applicativo

Le applicazioni devono essere rese disponibili come previsto dai requisiti di business. Questo processo comprende la progettazione delle applicazioni, un'adeguata considerazione dei controlli applicativi e dei requisiti di sicurezza, lo sviluppo e configurazione delle soluzioni nel rispetto degli standard. Questo approccio consente alle organizzazioni di supportare in modo appropriato l'operatività aziendale attraverso applicazioni informatiche adatte.



Il controllo del processo IT

Acquisire e manutenere il software applicativo

che soddisfa i requisiti aziendali per l'IT di

rendere disponibili le applicazioni secondo i requisiti di business, nei tempi previsti ed a costi ragionevoli

ponendo l'attenzione su

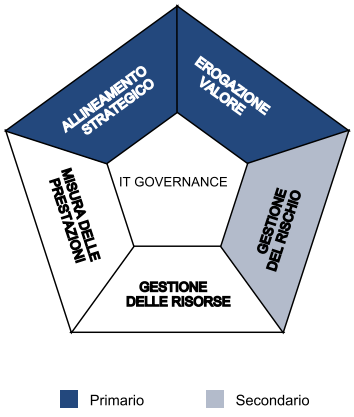
la garanzia che vi sia un processo di sviluppo tempestivo ed economicamente adeguato

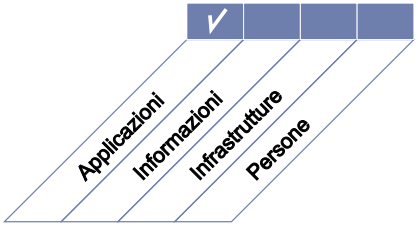
è ottenuto tramite

- la traduzione dei requisiti aziendali in specifiche di progetto
- il rispetto degli standard di sviluppo per tutte le modifiche
- la separazione delle attività di sviluppo, di test e di produzione

e viene misurato tramite

- il numero di problemi in produzione, per ogni applicazione, che causano indisponibilità percepibili
- la percentuale di utenti soddisfatti dalle funzionalità rilasciate





OBIETTIVI DI CONTROLLO

AI2 Acquisire e manutenere il software applicativo

AI2.1 Progettazione di alto livello

Tradurre i requisiti aziendali in specifiche di progettazione di alto livello per lo sviluppo del software, considerando gli indirizzi tecnologici dell'azienda e l'architettura informativa; ottenere l'approvazione delle specifiche di progettazione ad alto livello per garantire che queste soddisfino i requisiti. Durante lo sviluppo o la manutenzione, effettuare una nuova valutazione ogniqualvolta si verifichino delle incongruenze logiche o tecniche rilevanti.

AI2.2 Progettazione di dettaglio

Effettuare la progettazione di dettaglio e definire i requisiti tecnici per il software applicativo. Definire i criteri di accettazione dei requisiti. Ottenere l'approvazione dei requisiti per garantire che corrispondano alla progettazione di alto livello. Durante lo sviluppo o la manutenzione, effettuare una nuova valutazione ogniqualvolta si verifichino delle incongruenze logiche o tecniche rilevanti.

AI2.3 Controllo e verificabilità delle applicazioni

Tradurre i controlli funzionali, ove appropriato, in controlli applicativi automatizzati in modo tale che l'elaborazione sia accurata, completa, tempestiva, autorizzata e verificabile.

AI2.4 Sicurezza applicativa e disponibilità delle applicazioni

Considerare la sicurezza delle applicazioni e i requisiti di disponibilità in risposta ai rischi identificati, coerentemente con la classificazione dei dati, l'architettura della sicurezza delle informazioni ed il profilo di rischio aziendale.

AI2.5 Configurazione ed implementazione del software applicativo acquisito

Configurare e implementare il software applicativo acquisito al fine di soddisfare gli obiettivi aziendali.

AI2.6 Aggiornamenti significativi ai sistemi esistenti

Nel caso vi siano cambiamenti rilevanti ai sistemi esistenti che comportano una modifica significativa nel progetto e/o nelle funzionalità del sistema, seguire un processo di sviluppo analogo a quello dello sviluppo dei nuovi sistemi.

AI2.7 Sviluppo di software applicativo

Garantire che le funzionalità automatizzate siano sviluppate coerentemente con le specifiche di progettazione, secondo gli standard di sviluppo, di documentazione, dei requisiti di qualità e di approvazione. Garantire che siano identificati e risolti tutti gli aspetti legali e contrattuali relativi allo sviluppo di software applicativo realizzato da terze parti.

AI2.8 Garanzia di qualità del software

Sviluppare, assegnare risorse ed eseguire un piano di verifica della qualità del software per ottenere la qualità specificata nella definizione dei requisiti e nelle politiche e procedure di qualità aziendali.

AI2.9 Gestione dei requisiti applicativi

Tracciare lo stato dei singoli requisiti (inclusi tutti i requisiti rifiutati) durante la progettazione, lo sviluppo e l'implementazione, e approvare le modifiche ai requisiti attraverso un processo di gestione delle modifiche predefinito.

AI2.10 Manutenzione del software applicativo

Sviluppare una strategia e pianificare la manutenzione delle applicazioni software.

Linee Guida per la Gestione

AI2 Acquisire e manutenere il software applicativo

Da	Inputs
PO2	Dizionario dati; schema della classificazione dei dati, piano dei sistemi aziendali ottimizzato
PO3	Aggiornamenti regolari sullo "stato dell'arte tecnologico"
PO5	Relazioni sui costi / benefici
PO8	Standard di acquisizione e sviluppo
PO10	Linee guida per la gestione dei progetti, piani di progetto dettagliati
AI1	Studio di fattibilità dei requisiti aziendali
AI6	Descrizione del processo di modifica

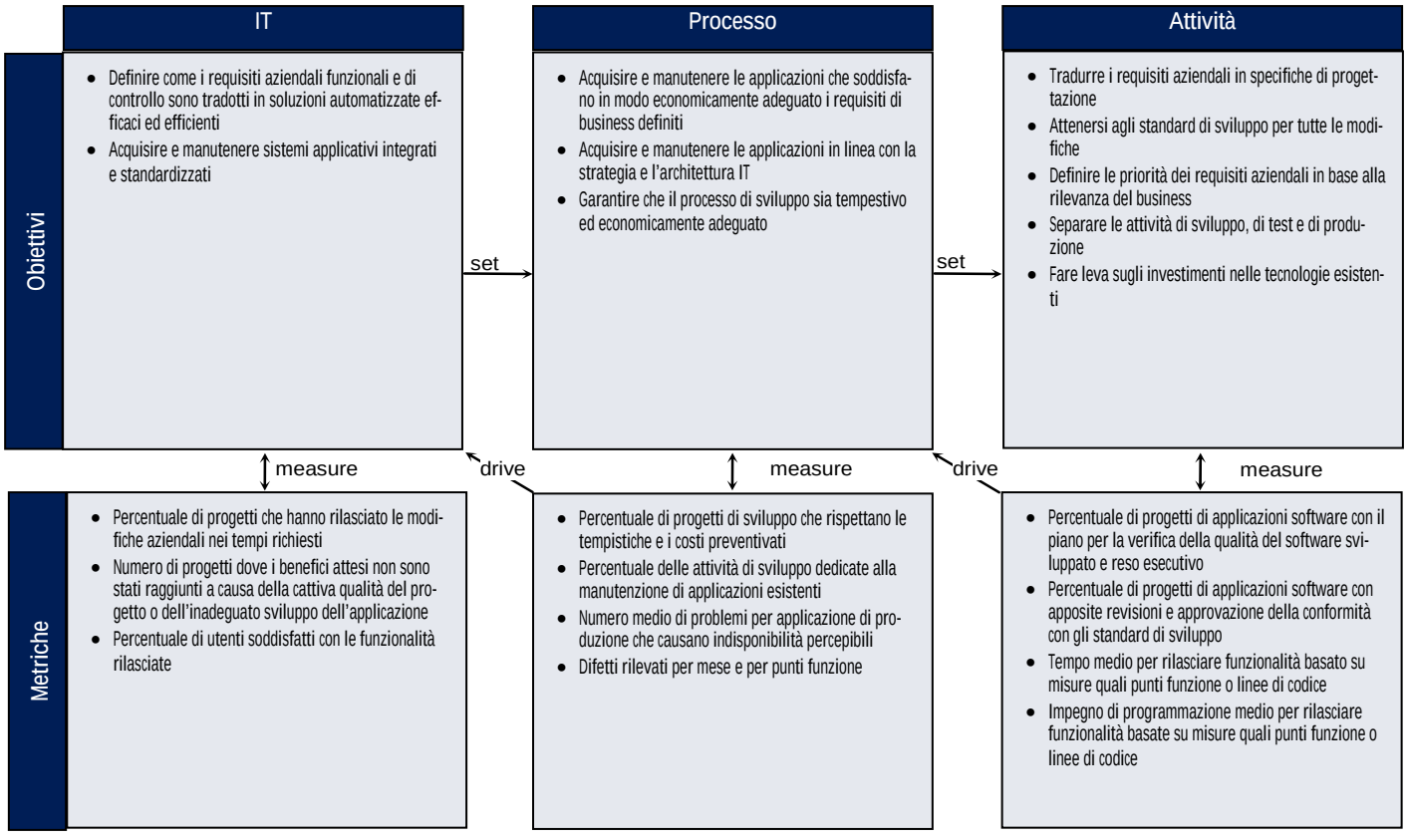
Outputs	A						
Specifiche dei controlli di sicurezza dell'applicazione	DS5						
Conoscenza dell'applicazione e del pacchetto software	AI4						
Decisioni di approvvigionamento	AI5						
Livelli di servizio (SLA) pianificati inizialmente	DS1						
Specifiche relative a disponibilità, continuità e ripristino	DS3	DS4					

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Tradurre i requisiti aziendali in specifiche di progetto ad alto livello.					C		C	A/R		R	C
Preparare il progetto dettagliato e i requisiti tecnici del software applicativo.				I	C	C	C	A/R		R	C
Specificare i controlli applicativi all'interno del progetto.					R	C		A/R		R	R
Personalizzare e implementare le funzionalità automatizzate acquisite.					C	C		A/R		R	C
Sviluppare metodologie formalizzate e processi per gestire il processo di sviluppo applicativo.				C		C	C	A	C	R	C
Creare un piano per l'assicurazione di qualità del progetto.					I		C	R		A/R	C
Tracciare e gestire i requisiti applicativi.								R		A/R	
Sviluppare un piano per la manutenzione delle applicazioni software				C		C		A/R		C	

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI2 Acquisire e manutenere il software applicativo

Il grado di strutturazione del processo *Acquisire e manutenere il software applicativo* che soddisfa i requisiti aziendali per l'IT di *rendere disponibili le applicazioni secondo i requisiti di business, nei tempi previsti ed a costi ragionevoli* è:

0 Non esistente quando

Non esiste alcun processo per progettare e raccogliere i requisiti delle applicazioni. Di norma, le applicazioni sono ottenute basandosi sulle offerte proposte dal venditore, sulla conoscenza di una marca o sulla familiarità del personale IT con prodotti specifici, con scarsa o nessuna considerazione per i requisiti reali.

1 Iniziale/*Ad Hoc* quando

Esiste la consapevolezza che è necessario un processo per l'acquisizione e la manutenzione del software applicativo. Gli approcci per acquisire e manutenere il software applicativo cambiano da progetto a progetto. È probabile che siano acquisite indipendentemente una varietà di singole soluzioni per particolari bisogni di business causando inefficienze nella manutenzione e nel supporto. Nella progettazione o nell'acquisizione di software applicativo viene data scarsa considerazione alla sicurezza e alla disponibilità dell'applicazione.

2 Ripetibile ma Intuitivo quando

Esistono differenti processi, ancorché simili tra loro, per l'acquisizione e la manutenzione degli applicativi basati sulle specifiche competenze all'interno della funzione IT. Il grado di successo nell'acquisto, sviluppo e manutenzione di applicazioni dipende principalmente dalle competenze interne e dai livelli di professionalità nell'ambito IT. La manutenzione è generalmente uno degli aspetti più problematici ed è particolarmente difficoltosa qualora l'organizzazione perde la competenza interna sull'applicativo specifico. Nella progettazione o nell'acquisizione di software applicativo viene data scarsa considerazione alla sicurezza e alla disponibilità dell'applicazione.

3 Definito quando

Esiste un processo chiaro, definito e condiviso per l'acquisizione e la manutenzione del software applicativo; questo processo è allineato con le strategie aziendali e IT. Viene fatto uno sforzo per applicare in modo consistente i processi documentati in diverse applicazioni e progetti. Le metodologie sono generalmente rigide e difficoltose da applicare in tutti i casi perciò è probabile che alcuni passi siano omessi. Le attività di manutenzione sono pianificate, programmate e coordinate.

4 Gestito e Misurabile quando

Esiste una metodologia formale e ben compresa che include un processo di progettazione e definizione delle specifiche, criteri per l'acquisizione, un processo di test e la documentazione dei requisiti. Esistono dei meccanismi documentati e condivisi per garantire che tutti i passi siano eseguiti e che le eccezioni siano autorizzate. Le prassi e le procedure sono evolute per essere adeguate all'organizzazione, usate da tutto lo staff e applicabili alla maggior parte dei requisiti applicativi.

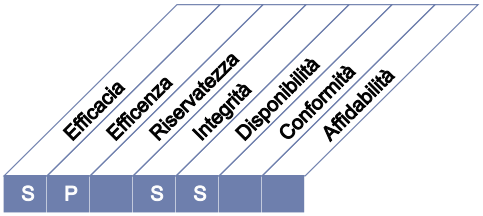
5 Ottimizzato quando

Le prassi per l'acquisizione e la manutenzione del software applicativo sono allineate con il processo definito. L'approccio è basato su componenti, con applicazioni predefinite e standardizzate, che soddisfano le necessità del business. L'approccio è comune a tutta l'azienda. La metodologia di acquisizione e manutenzione è molto evoluta e consente sviluppi rapidi permettendo alta reattività e flessibilità nel rispondere alle variazioni dei requisiti aziendali. La metodologia di acquisizione ed implementazione del software applicativo è soggetta a continui miglioramenti ed è supportata da una base di conoscenza interna ed esterna, contenente materiali di riferimento e le good practice. La metodologia prevede la creazione di documentazione secondo una struttura predefinita che rende la produzione e la manutenzione efficienti.

DESCRIZIONE DEL PROCESSO

AI3 Acquisire e manutenere l'infrastruttura tecnologica

Le aziende hanno dei processi per gestire l'acquisizione, l'implementazione e l'aggiornamento dell'infrastruttura tecnologica. Questo richiede un approccio basato su dei piani per l'acquisizione, la manutenzione e la protezione dell'infrastruttura coerente con le strategie tecnologiche concordate, oltre alla disponibilità di ambienti di sviluppo e test. Questo approccio garantisce che ci sia un supporto tecnologico continuo per le applicazioni aziendali.



Il controllo del processo IT

Acquisire e manutenere l'infrastruttura tecnologica

che soddisfa i requisiti aziendali per l'IT di

acquisizione e manutenzione di un'infrastruttura IT integrata e standardizzata

ponendo l'attenzione su

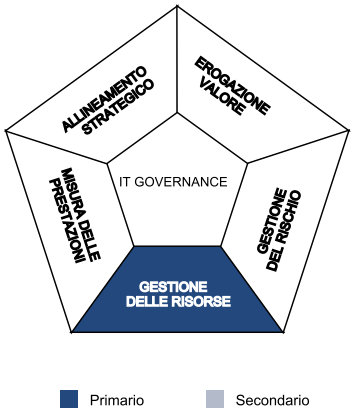
la predisposizione di piattaforme appropriate per le applicazioni aziendali coerentemente con l'architettura IT e gli standard tecnologici definiti

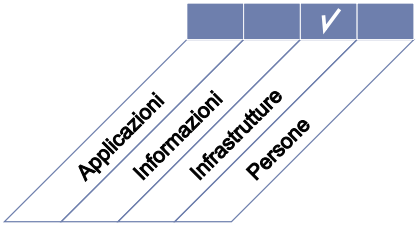
è ottenuto tramite

- la produzione di un piano di acquisizione di risorse tecnologiche che sia allineato con il piano per l'infrastruttura tecnologica
- la pianificazione della manutenzione dell'infrastruttura
- l'implementazione di controlli interni, di misure di sicurezza e di quelle per rendere verificabile l'infrastruttura

e viene misurato tramite

- la percentuale delle piattaforme che non sono allineate con l'architettura IT e gli standard tecnologici definiti
- il numero di processi aziendali critici basati su infrastrutture obsolete (o che lo stanno diventando a breve)
- il numero di componenti dell'infrastruttura che non sono più supportati (o che non lo saranno nell'immediato futuro)





OBIETTIVI DI CONTROLLO

AI3 Acquisire e manutenere l'infrastruttura tecnologica

AI3.1 Piano per l'acquisizione dell'infrastruttura tecnologica

Produrre un piano per l'acquisizione, l'implementazione e la manutenzione dell'infrastruttura tecnologica che soddisfi i requisiti aziendali funzionali e tecnici e sia coerente con gli indirizzi tecnologici dell'organizzazione.

AI3.2 Protezione e disponibilità delle risorse di infrastruttura

Implementare i controlli interni, le misure di sicurezza e di verifica durante la configurazione, l'integrazione e la manutenzione dell'hardware e del software di infrastruttura, per proteggere le risorse e garantirne la disponibilità e l'integrità. Le responsabilità per l'uso di componenti critiche dell'infrastruttura dovrebbero essere chiaramente definite e comprese da quanti sviluppano e integrano i componenti dell'architettura. Il loro uso dovrebbe essere monitorato e valutato.

AI3.3 Manutenzione delle infrastrutture

Sviluppare una strategia e un piano per la manutenzione delle infrastrutture e garantire che le modifiche siano controllate coerentemente con le procedure aziendali di gestione delle modifiche. Prevedere verifiche periodiche rispetto ai fabbisogni aziendali, alle strategie di gestione delle patch e degli aggiornamenti, ai rischi, alla valutazione delle vulnerabilità e ai requisiti di sicurezza.

AI3.4 Attendibilità dell'ambiente di test

Installare ambienti di sviluppo e test per supportare efficacemente ed efficientemente i test di fattibilità e di integrazione di componenti dell'infrastruttura.

Linee Guida per la Gestione

AI3 Acquisire e manutenere l'infrastruttura tecnologica

Da	Inputs
PO3	Piano dell'infrastruttura tecnologica, degli standard e delle opportunità; aggiornamenti regolari dello "stato dell'arte della tecnologia"
PO8	Standard di acquisizione e sviluppo
PO10	Linee guida per la gestione dei progetti e piani di progetto dettagliati
AI1	Studio di fattibilità rispetto ai requisiti aziendali
AI6	Descrizione del processo di gestione delle modifiche
DS3	Requisiti di performance e capacity plan

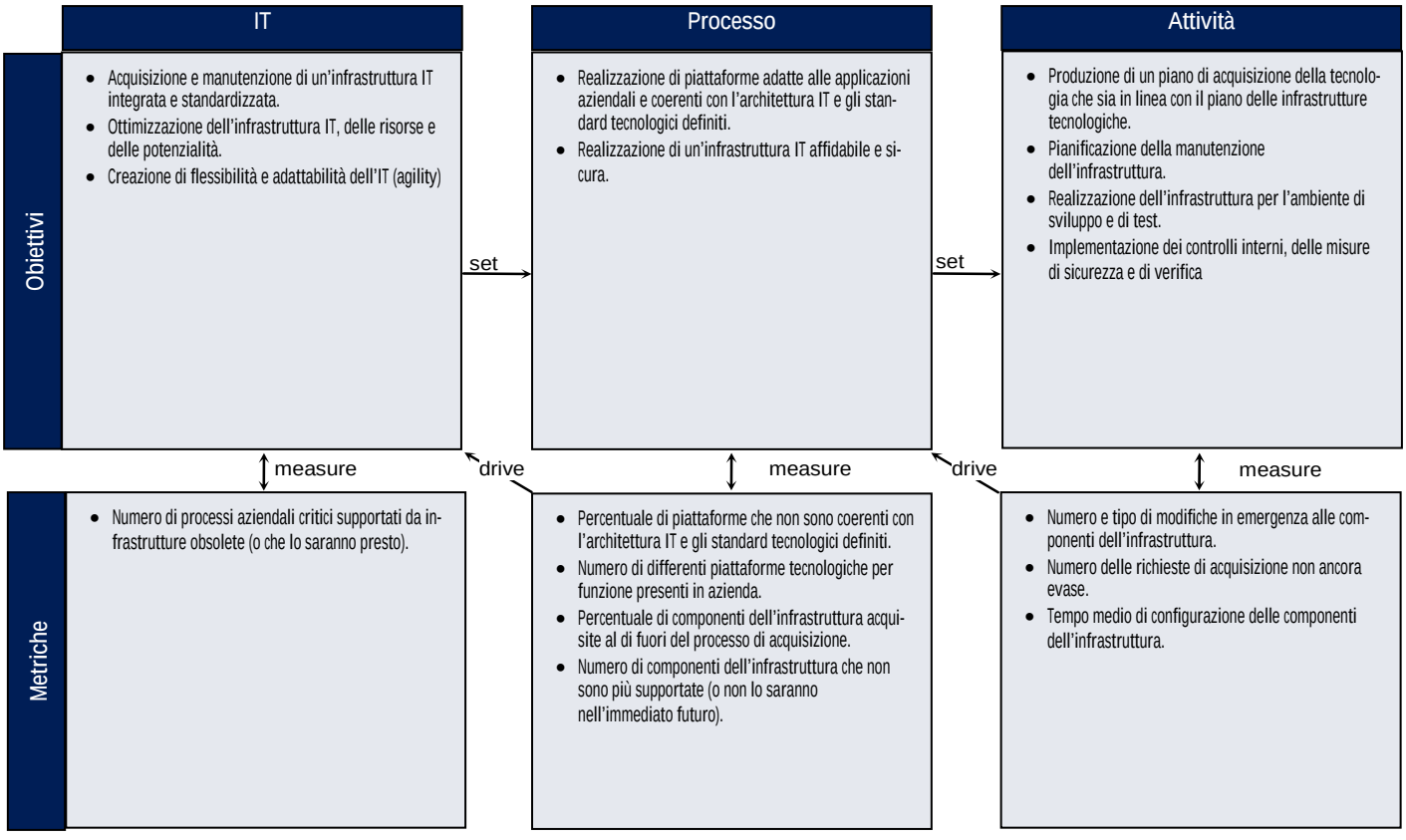
Outputs	A						
Decisioni di approvvigionamento	AI5						
Sistemi configurati da testare/installare	AI7						
Requisiti dell'ambiente fisico	DS12						
Aggiornamenti degli standard tecnologici	PO3						
Requisiti di monitoraggio del sistema	DS3						
Conoscenza dell'infrastruttura	AI4						
OLA pianificati inizialmente	DS1						

RACI Chart

Attività \ Ruoli	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire il processo/la procedura di acquisizione.		C		A		C	C	C	R		I
Negoziare l'acquisizione e acquisire l'infrastruttura necessaria dai venditori prescelti		C/I		A	I	R	C	C	R		I
Definire la strategia e il piano di manutenzione dell'infrastruttura				A		R	R	R	C		
Configurare i componenti dell'architettura				A		R	C				I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI3 Acquisire e manutenere l'infrastruttura tecnologica

Il grado di strutturazione del processo *Acquisire e manutenere l'infrastruttura tecnologica* che soddisfa i requisiti aziendali per l'IT di *acquisizione e manutenzione di un'infrastruttura IT integrata e standardizzata* è:

0 Non esistente quando

la gestione dell'infrastruttura tecnologica non è considerata sufficientemente importante per essere affrontata in modo specifico.

1 Iniziale/*Ad Hoc* quando

ci sono modifiche fatte all'infrastruttura per ogni nuova applicazione, senza un piano complessivo. Sebbene ci sia una consapevolezza che l'infrastruttura IT è importante, non esiste un approccio generale consolidato. L'attività di manutenzione risponde alle necessità del breve termine. L'ambiente di produzione coincide con l'ambiente di test.

2 Ripetibile ma Intuitivo quando

c'è coerenza tra gli approcci tattici all'acquisizione e alla manutenzione dell'infrastruttura IT. L'acquisizione e la manutenzione dell'infrastruttura IT non sono basate su una strategia definita e non considerano le necessità delle applicazioni aziendali che devono essere supportate. C'è consapevolezza che l'infrastruttura IT è importante e deve essere supportata da alcune procedure formali. Alcune manutenzioni sono programmate, ma non è tutto completamente programmato e coordinato. Per alcuni ambiti esiste un ambiente di test separato.

3 Definito quando

esiste un processo chiaro, definito e generalmente accettato per l'acquisizione e la manutenzione dell'infrastruttura IT. Il processo è funzionale alla gestione delle necessità delle applicazioni critiche per l'azienda ed è allineato con le strategie aziendali ed IT ma non è applicato in modo continuativo. La manutenzione è pianificata, programmata e coordinata. Ci sono ambienti separati per il test e la produzione.

4 Gestito e Misurabile quando

il processo di acquisizione e manutenzione dell'infrastruttura tecnologica si è sviluppato al punto da essere efficacemente impiegato nella maggior parte delle situazioni, da essere applicato in modo significativo ed essere focalizzato sulla riusabilità. L'infrastruttura IT supporta in modo adeguato le applicazioni aziendali. Il processo è ben organizzato e proattivo. Il costo e la durata del ciclo per raggiungere il livello atteso di scalabilità, flessibilità e integrazione sono parzialmente ottimizzati.

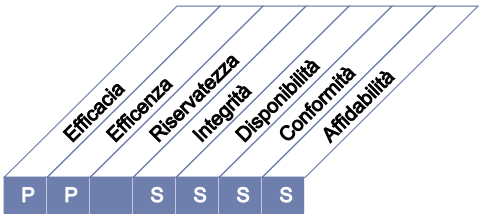
5 Ottimizzato quando

il processo di acquisizione e manutenzione dell'infrastruttura tecnologica è proattivo, è strettamente allineato con le applicazioni aziendali critiche e con l'architettura tecnologica. Sono applicate buone prassi operative relativamente alle soluzioni tecnologiche e l'organizzazione è consapevole degli sviluppi più recenti delle piattaforme e degli strumenti gestionali. La razionalizzazione e la standardizzazione delle componenti infrastrutturali e l'uso di automatismi permettono una riduzione dei costi. Un alto livello di consapevolezza tecnica può consentire l'identificazione di modalità ottimali per migliorare proattivamente le prestazioni, compresa la valutazione delle alternative di outsourcing. L'infrastruttura IT è vista come un fattore chiave abilitante per stimolare l'uso dell'IT.

DESCRIZIONE DEL PROCESSO

AI4 Permettere il funzionamento e l'uso dei sistemi IT

È resa disponibile la conoscenza sui nuovi sistemi. Questo processo richiede la produzione di documentazione e di manuali per gli utenti e per il personale tecnico, la fornitura della formazione per assicurare l'utilizzo ed il funzionamento appropriato delle applicazioni e delle infrastrutture.



Il controllo del processo IT

Permettere il funzionamento e l'uso dei sistemi IT

che soddisfa i requisiti aziendali per l'IT di

assicurare la soddisfazione degli utenti finali con i servizi offerti e i livelli di servizio erogati e con l'integrazione senza soluzioni di continuità di applicazioni e soluzioni tecnologiche nei processi aziendali

ponendo l'attenzione su

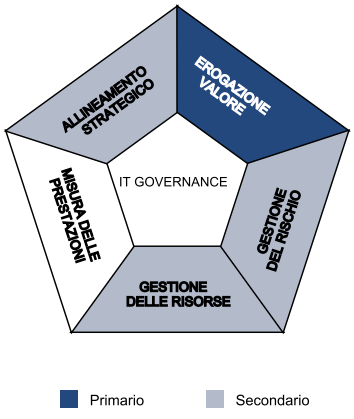
la fornitura di efficaci manuali utente e operativi e dei supporti per la formazione per trasferire le conoscenze necessarie per utilizzare e far funzionare i sistemi con successo

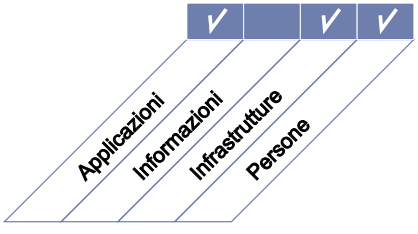
è ottenuto tramite

- lo sviluppo e disponibilità di documentazione per il trasferimento della conoscenza
- la comunicazione agli e la formazione degli utenti, dei responsabili dei servizi, del personale di supporto e operativo
- la produzione dei supporti per la formazione

e viene misurato tramite

- Il numero di applicazioni dove le procedure IT sono integrate nei processi aziendali senza soluzioni di continuità
- la percentuale di referenti di processi aziendali soddisfatti della formazione applicativa e dei materiali di supporto
- il numero di applicazioni con adeguato supporto formativo per gli utenti e per il personale operativo





OBIETTIVI DI CONTROLLO

AI4 Permettere il funzionamento e l'uso dei sistemi IT

AI4.1 Pianificazione delle soluzioni operative

Sviluppare un piano per identificare e documentare tutti gli aspetti tecnici, operativi e di utilizzo dei sistemi in modo che tutti gli interessati, che gestiscono operativamente o utilizzano o mantengono i sistemi informatici, possano assumere le proprie responsabilità.

AI4.2 Trasferimento di conoscenza al management aziendale

Trasferire la conoscenza sui sistemi al management aziendale per consentir loro di prendere possesso di sistemi e dati ed inoltre di assumere coscientemente le responsabilità sui servizi erogati, sulla qualità, sui controlli interni e sui processi di amministrazione dell'applicazione.

AI4.3 Trasferimento di conoscenza agli utenti finali

Trasferire conoscenze e competenze per consentire agli utenti finali di usare efficacemente ed efficientemente il sistema applicativo per supportare i processi aziendali.

AI4.4 Trasferimento di conoscenza allo staff operativo e di supporto

Trasferire conoscenza e competenze per consentire al personale operativo e di supporto tecnico di rilasciare, supportare e manutenere il sistema applicativo e l'infrastruttura associata efficacemente ed efficientemente.

LINEE GUIDA PER LA GESTIONE

AI4 Permettere il funzionamento e l'uso dei sistemi IT

Da	Inputs
PO10	Linee guida per la gestione dei progetti e piani di progetto dettagliati
AI1	Studio di fattibilità delle soluzioni per i requisiti aziendali
AI2	Conoscenza del software applicativo e dei package
AI3	Conoscenza dell'infrastruttura
AI7	Errori conosciuti e accettati
DS7	Aggiornamenti richiesti alla documentazione

Outputs	A						
Manuali utente, operativi, tecnici, per il supporto e per gli amministratori	AI7	DS4	DS8	DS9	DS11	DS13	
Requisiti di trasferimento della conoscenza per l'implementazione delle soluzioni	DS7						
Materiali per la formazione	DS7						

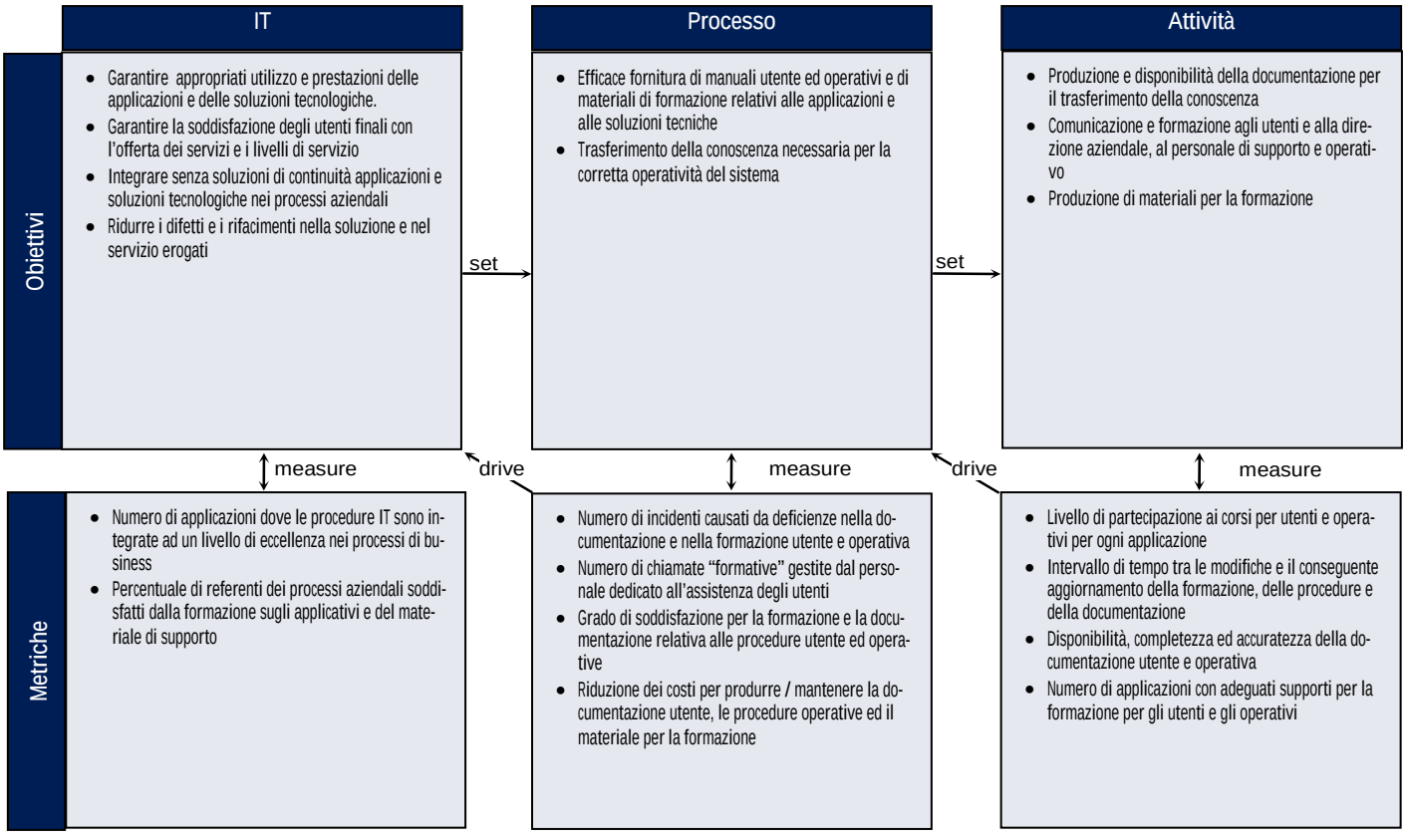
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Squadre installazioni	Ufficio formazione
Sviluppare una strategia per rendere operativa la soluzione				A	A	R		R			I	R	C
Sviluppare una metodologia per il trasferimento delle conoscenze				C	A							C	R
Sviluppare i manuali delle procedure per gli utenti finali					A/R			R			C	C	
Sviluppare la documentazione tecnica di supporto per l'operatività e lo staff di supporto						A/R		C			C		
Sviluppare ed erogare la formazione					A	A		R					R
Valutare i risultati della formazione e migliorare la documentazione come richiesto					A	A						R	R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI4 Permettere il funzionamento e l'uso dei sistemi IT

Il grado di strutturazione del processo *Permettere il funzionamento e l'uso dei sistemi IT* che soddisfa i requisiti aziendali per l'IT di *assicurare la soddisfazione degli utenti finali con i servizi offerti e i livelli di servizio erogati e con l'integrazione senza soluzioni di continuità di applicazioni e soluzioni tecnologiche nei processi aziendali* è:

0 Non esistente quando

Non c'è un processo relativo alla produzione di documentazione utente, di manuali operativi e materiale di formazione. I soli supporti esistenti sono quelli forniti con i prodotti acquistati.

1 Iniziale/*Ad Hoc* quando

C'è la consapevolezza che il processo di documentazione è necessario. La documentazione è prodotta occasionalmente e distribuita saltuariamente a gruppi limitati. Gran parte della documentazione e molte procedure sono obsolete. I materiali di formazione tendono a seguire schemi una tantum con qualità variabile. Praticamente non esiste integrazione di procedure tra diversi sistemi e unità aziendali. Non ci sono indicazioni dalle unità aziendali per la progettazione delle attività di formazione.

2 Ripetibile ma Intuitivo quando

Sono usati approcci simili per produrre procedure e documentazioni ma tali attività non sono basate su un approccio strutturato o su un modello comune. Non c'è un approccio uniforme per lo sviluppo di procedure utente e operative. I supporti per la formazione sono prodotti da singole persone o dai gruppi di progetto e la qualità dipende dalle persone coinvolte. Le procedure e la qualità dei supporti utente possono variare in modo considerevole, con poca consistenza ed integrazione nell'ambito dell'organizzazione. Sono forniti o facilitati i programmi di formazione per l'azienda e gli utenti, ma non c'è un piano complessivo per l'erogazione della formazione.

3 Definito quando

C'è un modello chiaramente definito, accettato e condiviso per la documentazione utente, i manuali operativi e i supporti di formazione. Le procedure sono memorizzate e mantenute in una biblioteca formalmente gestita e sono accessibili a chiunque ne abbia la necessità. Le correzioni alla documentazione e alle procedure sono effettuate solo su segnalazione. Le procedure sono disponibili offline e possono essere accedute e mantenute in caso di disastro. Esiste un processo che specifica gli aggiornamenti delle procedure e del materiale di formazione che devono essere esplicitamente rilasciati in caso di modifica di un sistema. Malgrado l'esistenza di approcci definiti i contenuti attuali variano perché non c'è un controllo che obblighi al rispetto degli standard. Gli utenti sono coinvolti in modo informale in questo processo. Gli strumenti automatici sono sempre più utilizzati nella generazione e nella distribuzione delle procedure. La formazione delle risorse è pianificata e programmata.

4 Gestito e Misurabile quando

C'e una struttura definita per la manutenzione delle procedure e dei materiali per la formazione ed è sponsorizzata dalla Direzione IT. L'approccio utilizzato per manutenere le procedure e i manuali di formazione copre tutti i sistemi e tutte le unità aziendali in modo tale che i processi possano essere inquadrati secondo una prospettiva aziendale (e non solo tecnica). Le procedure ed il materiale per la formazione sono integrati ed includono le interdipendenze e le interfacce. Esistono dei controlli per garantire l'aderenza agli standard e che le procedure siano sviluppate e mantenute per tutti i processi. I feed-back aziendali e degli utenti, relativi alla documentazione e alla formazione, sono raccolti e valutati come parte di un processo continuo di miglioramento. La documentazione e il materiale per la formazione sono generalmente ad un buon livello di affidabilità e disponibilità. È in fase di implementazione un nuovo processo per l'utilizzo di procedure automatiche di documentazione e gestione. Lo sviluppo di procedure automatiche è costantemente integrato con lo sviluppo dei sistemi applicativi facilitando la consistenza dei contenuti e l'accesso degli utenti. La formazione delle risorse impegnate nel business e degli utenti risponde alle necessità aziendali. La Direzione IT sta definendo delle metriche per monitorare lo sviluppo ed il rilascio di documentazione, materiale e programmi di formazione.

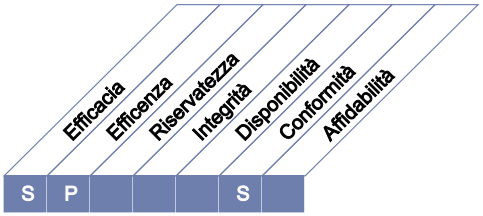
5 Ottimizzato quando

Il processo per la gestione della documentazione utente ed operativa è costantemente migliorato attraverso l'adozione di nuovi strumenti o metodi. I supporti delle procedure e della formazione sono trattati come una base di conoscenza costantemente in evoluzione che è mantenuta elettronicamente utilizzando innovativi sistemi di gestione della conoscenza, workflow e tecnologie per la distribuzione delle informazioni, rendendoli accessibili e facili da manutenere. I supporti documentali e formativi sono aggiornati per rispecchiare i cambiamenti organizzativi, operativi e del software. Lo sviluppo di supporti documentali e formativi e l'erogazione dei programmi di formazione sono completamente integrati con l'attività dell' azienda e con le definizioni dei processi aziendali, supportando in tal modo l'organizzazione nel suo complesso piuttosto che solo le procedure nell'ambito IT.

DESCRIZIONE DEL PROCESSO

AI5 Approvvigionamento delle risorse IT

Le risorse IT, comprendendo con questa accezione le persone, l'hardware, il software e i servizi, devono essere acquisite. Questo richiede la definizione e l'applicazione di procedure di approvvigionamento, la selezione dei venditori, la definizione di accordi contrattuali e l'acquisizione vera e propria. Operare in questo modo garantisce che l'organizzazione abbia a disposizione tutte le risorse IT richieste nel momento opportuno e con costi appropriati.



Il controllo del processo IT

Approvvigionamento delle risorse IT

che soddisfa i requisiti aziendali per l'IT di

migliorare l'efficienza dei costi IT e il suo contributo alla profittabilità aziendale

ponendo l'attenzione su

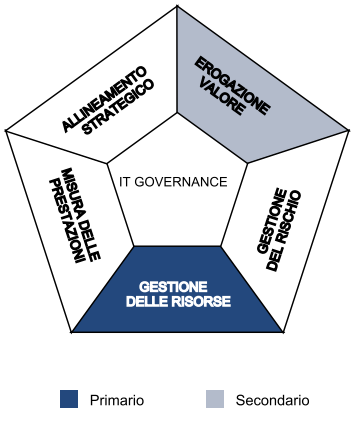
l'acquisizione e il mantenimento di competenze IT che soddisfino le strategie di rilascio, un'infrastruttura IT integrata e standardizzata e la riduzione dei rischi di approvvigionamento IT

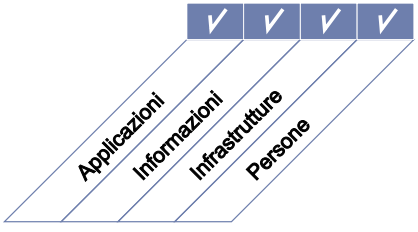
è ottenuto tramite

- l'ottenimento di pareri professionali su questioni legali e contrattuali
- la definizione di standard e procedure di approvvigionamento
- l'approvvigionamento dell'hardware opportuno, del software e dei servizi richiesti coerentemente con le procedure definite

e viene misurato tramite

- Il numero di controversie relative ai contratti di approvvigionamento
- l'ammontare risparmiato a seguito della riduzione dei costi di acquisto
- la percentuale di stakeholder chiave soddisfatti dei fornitori identificati





OBIETTIVI DI CONTROLLO

AI5 Approvvigionamento delle risorse IT

AI5.1 Controllo dell'approvvigionamento

Sviluppare e agire in conformità a un insieme di procedure e standard che siano coerenti con il processo aziendale di approvvigionamento e con la strategia di acquisizione per garantire che l'acquisizione di infrastrutture, facilities, hardware, software e servizi IT soddisfi i requisiti aziendali.

AI5.2 Gestione del contratto di fornitura

Definire una procedura con cui istituire, modificare e chiudere i contratti con tutti i fornitori. La procedura dovrebbe coprire almeno gli aspetti legali, finanziari, organizzativi, di documentazione, prestazione, sicurezza, proprietà intellettuale e le responsabilità di chiusura ivi inclusi quelli per la gestione dei contenziosi (comprese le penali). Tutti i contratti e le loro modifiche dovrebbero essere rivisti da consulenti legali.

AI5.3 Selezione dei fornitori

Selezionare i fornitori secondo una prassi equa e formale per garantire la scelta attuabile più appropriata sulla base di specifici requisiti. I requisiti dovrebbero essere ottimizzati sfruttando le indicazioni dei potenziali fornitori.

AI5.4 Acquisizione delle risorse informatiche

Garantire che gli interessi dell'azienda siano salvaguardati in tutti gli accordi contrattuali di acquisizione, compresi i diritti e gli obblighi di tutte le parti coinvolte nelle clausole contrattuali per l'acquisizione di software, risorse per lo sviluppo, infrastrutture e servizi.

LINEE GUIDA PER LA GESTIONE

AI5 Approvvigionamento delle risorse IT

Da	Inputs
PO1	Strategia degli approvvigionamenti IT
PO8	Standard di approvvigionamento
PO10	Linee guida per la gestione dei progetti e piani di progetto dettagliati
AI1	Studio di fattibilità dei requisiti aziendali
AI2,AI3	Decisioni di approvvigionamento
DS2	Catalogo dei fornitori

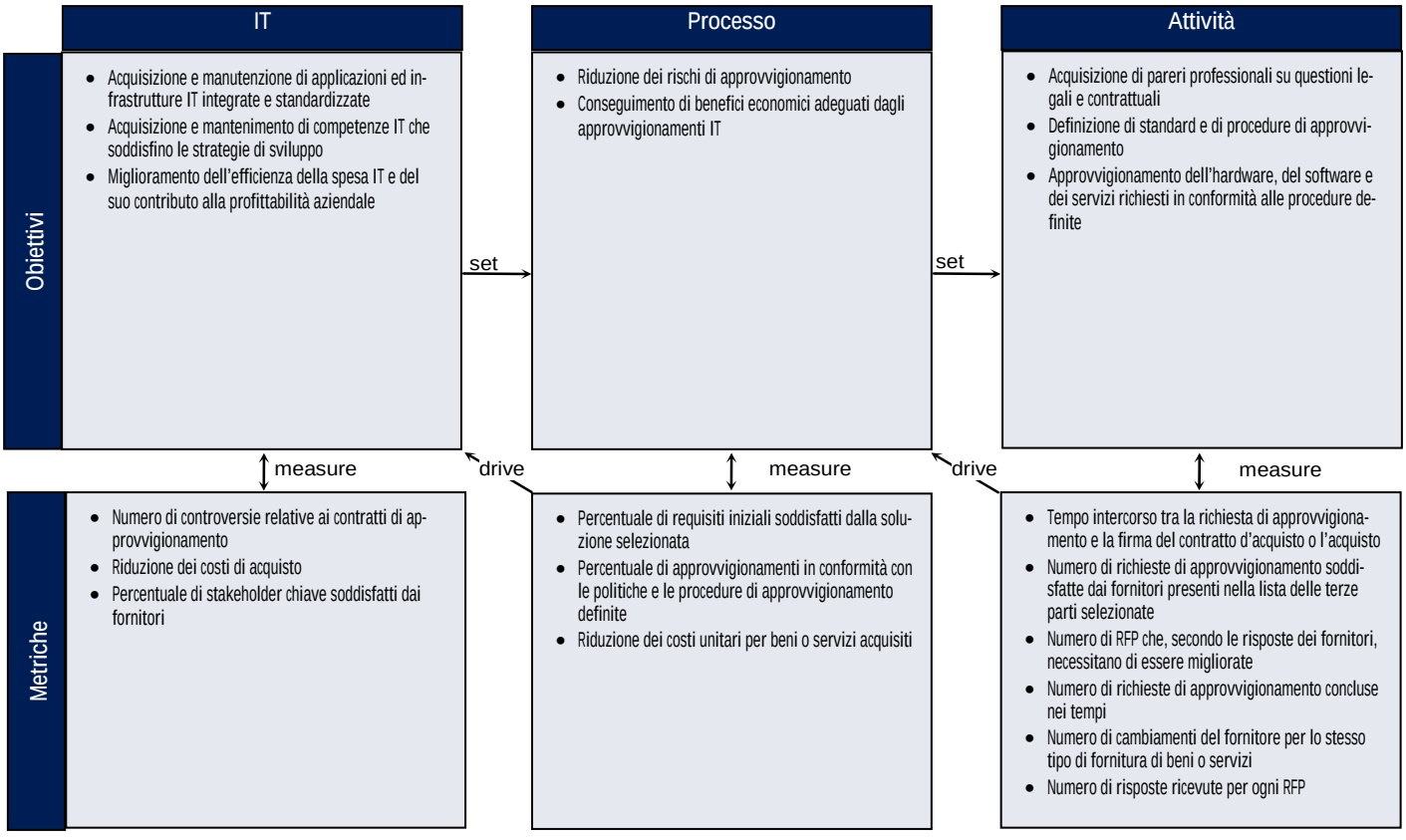
Outputs	A						
Requisiti per la gestione delle relazioni con terze parti	DS2						
Articoli procurati	AI7						
Intese contrattuali	DS2						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Sviluppare politiche di approvvigionamento IT allineate con le politiche di approvvigionamento a livello aziendale [corporate].	I	C		A		I	I	I	R		C
Definire e manutenere una lista di fornitori accreditati.									A/R		
Valutare e selezionare i fornitori attraverso un processo di sollecito delle proposte [request for proposal] (RFP)	C	C		A		R		R	R	R	C
Sviluppare contratti che proteggano gli interessi dell'azienda.	R	C		A		R		R	R		C
Approvvigionarsi in conformità con le procedure esistenti.				A		R		R	R		C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI5 Approvvigionamento delle risorse IT

Il grado di strutturazione del processo *Approvvigionamento delle risorse IT* che soddisfa i requisiti aziendali per l'IT di *migliorare l'efficienza dei costi IT e il suo contributo alla profittabilità aziendale* è:

0 Non esistente quando

Non è definito un processo per l'approvvigionamento di risorse IT. L'azienda non percepisce il bisogno di politiche e procedure di acquisizione chiare per garantire che tutte le risorse IT siano disponibili nel momento opportuno e in modo economicamente conveniente.

1 Iniziale/*Ad Hoc* quando

L'azienda ha riconosciuto la necessità di avere politiche e procedure documentate che correlino le acquisizioni IT al processo di approvvigionamento globale aziendale. I contratti per l'acquisizione delle risorse IT sono sviluppati e gestiti dai gestori di progetto e da altre risorse che utilizzando la propria esperienza professionale anziché come risultato dell'applicazione di procedure e politiche formali. C'è solo una relazione ad hoc tra gli acquisti aziendali e i processi di gestione dei contratti e l'IT. I contratti per l'acquisizione di risorse sono gestiti alla conclusione dei progetti anziché su base continuativa.

2 Ripetibile ma Intuitivo quando

C'è una consapevolezza aziendale della necessità di avere politiche e procedure per l'acquisizione di risorse IT. Politiche e procedure sono parzialmente integrate con il processo di approvvigionamento globale aziendale. I processi di approvvigionamento sono utilizzati principalmente per progetti grandi e di maggior visibilità. Le responsabilità e la competenza dell'approvvigionamento e della gestione dei contratti IT sono determinate dall'esperienza del gestore del singolo contratto. È riconosciuta l'importanza della gestione del fornitore e della gestione della relazione ma le stesse sono lasciate ad iniziative individuali. I processi di gestione dei contratti sono utilizzati maggiormente in progetti rilevanti o di maggior visibilità.

3 Definito quando

La direzione ha istituito politiche e procedure per l'acquisizione di risorse IT. Le politiche e procedure sono guidate dal processo di approvvigionamento globale aziendale. L'acquisizione di risorse IT è in larga misura integrata con i sistemi globali di approvvigionamento aziendale. Esistono gli standard IT per l'acquisizione di risorse IT. I fornitori delle risorse IT, dal punto di vista della gestione del contratto, sono integrati nei meccanismi di gestione dei progetti dell'azienda. La direzione IT comunica la necessità di gestire in modo appropriato acquisti e contratti a tutta la funzione IT.

4 Gestito e Misurabile quando

Gli acquisti IT sono completamente integrati con i sistemi di approvvigionamento globali aziendali. Gli standard IT per l'acquisizione di risorse IT sono usati per tutti gli approvvigionamenti. Le misure relative alla gestione del contratto e dell'approvvigionamento sono considerate rilevanti ai fini dei "casi di business" relativi all'acquisizione di risorse IT. Sono disponibili dei report che supportano il raggiungimento degli obiettivi aziendali. La direzione dovrebbe essere normalmente a conoscenza delle eccezioni alle politiche e alle procedure per le acquisizioni IT. È sviluppata una gestione strategica delle relazioni. La direzione IT impone l'applicazione del processo di gestione dell'acquisizione e del contratto per tutte le acquisizioni verificando gli indici di prestazione.

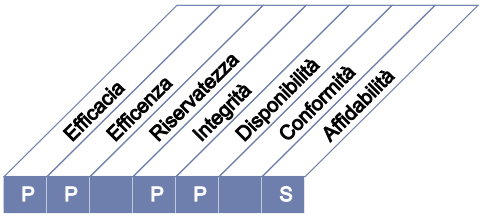
5 Ottimizzato quando

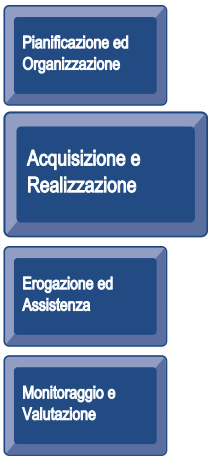
La direzione ha istituito e previsto risorse per tutte le fasi del processo di acquisizione IT. La direzione impone la conformità alle politiche e alle procedure per l'acquisizione IT. Le misure relative alla gestione del contratto e dell' approvvigionamento sono considerate rilevanti ai fini dei "casi di business" relativi all'acquisizione di risorse IT. Nel tempo sono stabilite buone relazioni con la maggior parte dei fornitori e dei partner e la qualità delle relazioni è misurata e controllata. Le relazioni sono gestite in modo strategico. Gli standard, le politiche e le procedure IT per l'acquisizione delle risorse IT sono gestite in modo strategico e consentono la misurazione del processo. La direzione IT comunica a tutta la funzione IT l'importanza strategica della gestione sia dell'appropriata acquisizione sia del contratto.

DESCRIZIONE DEL PROCESSO

AI6 Gestire le modifiche

Tutte le modifiche, inclusa la manutenzione di emergenza e le patch, riguardanti l'infrastruttura e le applicazioni in ambiente di produzione devono essere gestite formalmente in modo controllato. Le modifiche (incluse quelle relative a procedure, processi, parametri di sistema e di servizio) devono essere registrate, valutate e autorizzate prima dell'implementazione e riviste confrontandole con i risultati attesi a seguito dell'implementazione. Questi controlli riducono i rischi di un impatto negativo sulla stabilità o sull'integrità dell'ambiente di produzione.





Il controllo del processo IT

Gestire le modifiche

che soddisfa i requisiti aziendali per l'IT di

soddisfare i requisiti aziendali coerentemente con le strategie aziendali, nel contempo di ridurre i difetti e le rielaborazioni del sistema esistente e del servizio fornito

ponendo l'attenzione su

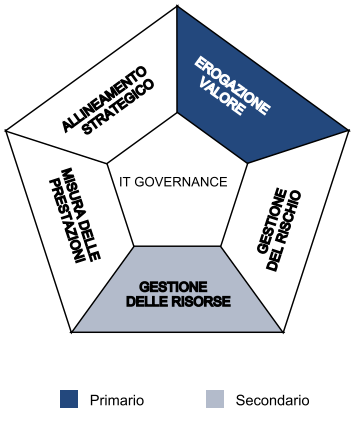
il controllo della valutazione dell'impatto, dell'autorizzazione e della realizzazione di tutte le modifiche all'infrastruttura IT, alle applicazioni e alle soluzioni tecniche; la riduzione al minimo degli errori dovuti a specifiche incomplete; il blocco dell'implementazione di modifiche non autorizzate

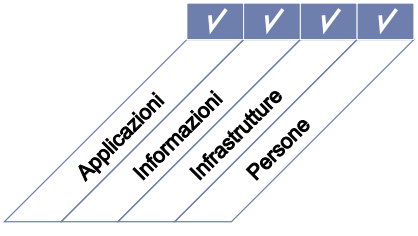
è ottenuto tramite

- la definizione e la comunicazione di procedure da seguire per apportare modifiche, comprese quelle effettuate in stato di emergenza
- la valutazione delle modifiche nel merito, la definizione delle priorità e l'autorizzazione.
- la registrazione dello status delle modifiche e produzione delle opportune informative.

e viene misurato tramite

- il numero di interruzioni o errori nei dati causati da specifiche imprecise o da valutazioni d'impatto incomplete
- il volume di rielaborazioni nell'ambito applicativo o sistemistico causate da specifiche di modifica inadeguate
- la percentuale delle modifiche che si conformano al processo formale di gestione delle modiche





OBIETTIVI DI CONTROLLO

AI6 Gestire le modifiche

AI6.1 Standard e procedure per la gestione delle modifiche

Attivare procedure formali di gestione delle modifiche per trattare in modo standardizzato tutte le richieste (incluse quelle di manutenzione e le patch) di variazione di: applicazioni, procedure, processi, parametri di sistema e di servizio e delle piattaforme sottostanti.

AI6.2 Valutazione dell'impatto, definizione delle priorità e autorizzazione

Assicurarsi che tutte le richieste di modifica siano valutate secondo una prassi strutturata e considerino gli impatti sui sistemi che supportano l'operatività e sulle loro funzionalità. Assicurarsi che le modifiche siano classificate secondo categorie predefinite, che sia assegnata la priorità, e che siano autorizzate.

AI6.3 Modifiche in stato di emergenza

Stabilire un processo per definire, proporre, testare, documentare, valutare e autorizzare le modifiche in stato di emergenza che non seguono il processo di gestione delle modifiche predefinito.

AI6.4 Registrazioni e informative sullo status della modifica

Stabilire un sistema di registrazioni e di informative per documentare le richieste non accolte, e comunicare lo stato delle modifiche approvate, di quelle in corso di realizzazione, di quelle completate. Assicurarsi che le modifiche approvate siano realizzate secondo quanto pianificato.

AI6.5 Chiusura delle modifiche e documentazione

Ogni qualvolta sono implementate delle modifiche al sistema, aggiornare opportunamente i sistemi collegati e la documentazione utente e le procedure.

LINEE GUIDA PER LA GESTIONE

AI6 Gestire le modifiche

Da	Inputs
PO1	Portafoglio dei progetti IT
PO8	Azioni per migliorare la qualità
PO9	Piani d'azione per attenuare i rischi connessi all'IT
PO10	Linee guida per la gestione dei progetti e piano di progetto dettagliato
DS3	Modifiche richieste
DS5	Modifiche di sicurezza richieste
DS8	Richieste di servizio / richieste di modifica
DS9, DS10	Richieste di modifica (dove e come applicare la correzione)
DS10	Registrazioni dei problemi

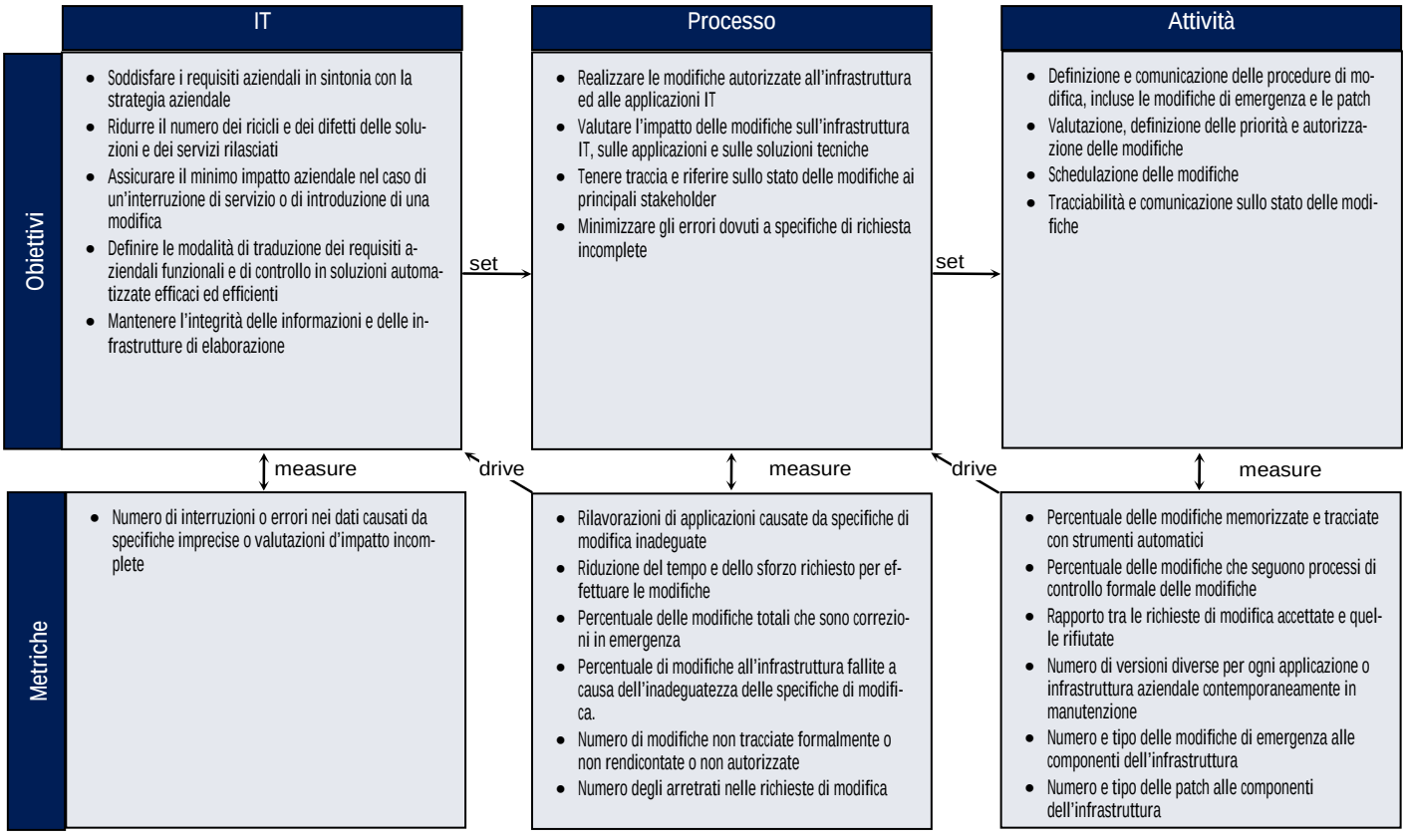
Outputs	A						
Descrizione del processo di modifica	AI1…AI3						
Rendicontazioni dello stato della modifica	ME1						
Autorizzazione della modifica	AI7	DS8	DS10				

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Sviluppo e implementazione di un processo per memorizzare, valutare e definire le priorità per le richieste di modifica in modo coerente.				A	I	R	C	R	C	C	C
Valutare l'impatto e definire le priorità per le modifiche basandosi sui bisogni aziendali.				I	R	A/R	C	R	C	R	C
Garantire che ogni modifica, in emergenza o critica, segua il processo approvato.				I	I	A/R	I	R			C
Autorizzare le modifiche.				I	C	A/R		R			
Gestire e divulgare le informazioni rilevanti relative alle modifiche.				A	I	R	C	R	I	R	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI6 Gestire le modifiche

Il grado di strutturazione del processo *Gestire le modifiche* che soddisfa i requisiti aziendali per l'IT di *soddisfare i requisiti aziendali coerentemente con le strategie aziendali, nel contempo di ridurre i difetti e le rielaborazioni del sistema esistente e del servizio fornito* è:

0 Non esistente quando

Non esiste alcun processo definito per la gestione delle modifiche, che possono essere effettuate potenzialmente senza controllo. Non esiste la consapevolezza che le modifiche possono essere distruttive sia per le operazioni IT sia per quelle aziendali e non esiste alcuna consapevolezza dei benefici di un'opportuna gestione delle modifiche.

1 Iniziale/*Ad Hoc* quando

Si riconosce che le modifiche dovrebbero essere gestite e controllate. Le prassi variano ed è probabile che modifiche non autorizzate siano realizzate. La documentazione delle modifiche è scadente o inesistente e la documentazione della configurazione è incompleta e inaffidabile. È probabile che si verifichino errori e/o interruzioni nell'erogazione dei servizi in ambiente di produzione causati da una gestione insoddisfacente delle modifiche.

2 Ripetibile ma Intuitivo quando

Esiste un processo informale per la gestione delle modifiche e la maggior parte delle modifiche seguono questo approccio; tuttavia è destrutturato, rudimentale e incline alla generazione di errori. L'accuratezza della documentazione della configurazione è insoddisfacente e la pianificazione e la valutazione dell'impatto prima di porre in essere una modifica sono limitate.

3 Definito quando

Esiste un processo formale definito per la gestione delle modifiche, che include la classificazione, la definizione delle priorità, le procedure di emergenza, l'autorizzazione delle modifiche e la gestione delle versioni, e la conformità inizia ad essere considerata. Sono utilizzate delle soluzioni temporanee alternative [workarounds] e i processi sono spesso non applicati. È probabile che avvengano errori e che occasionalmente si attivino modifiche non autorizzate. L'analisi dell'impatto delle modifiche IT sull'operatività aziendale sta acquisendo un miglior livello di formalizzazione, al fine di supportare i rilasci pianificati a nuove applicazioni e tecnologie.

4 Gestito e Misurabile quando

Il processo di gestione delle modifiche è ben sviluppato e applicato in modo costante per tutte le modifiche; la Direzione si attende solo sporadiche eccezioni. Il processo è efficiente e efficace, ma dipende da un numero considerevole di procedure e controlli manuali per garantire che la qualità desiderata sia raggiunta. Tutte le modifiche sono soggette alla pianificazione e alla valutazione completa degli impatti per minimizzare la probabilità di accadimento di problemi dopo il passaggio in produzione. È attivato un processo per l'approvazione delle modifiche. La documentazione sulla gestione delle modifiche è aggiornata e corretta, e mantiene traccia delle variazioni in maniera formale. La documentazione della configurazione è in generale accurata. La pianificazione della gestione delle modifiche IT e l'implementazione diventano sempre più integrate con le modifiche dei processi aziendali, per garantire che i requisiti della formazione, dei cambiamenti organizzativi e l'aspetto della continuità operativa siano adeguatamente indirizzati. Esiste un coordinamento crescente tra la gestione delle modifiche IT e la riprogettazione dei processi aziendali. Esiste un processo costante/coerente per monitorare la qualità e i risultati del processo di gestione delle modifiche.

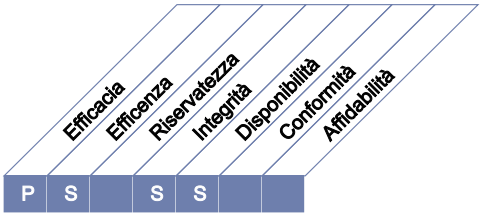
5 Ottimizzato quando

Il processo di gestione delle modifiche è regolarmente rivisto ed aggiornato perché sia allineato con le migliori prassi. Il processo di revisione rispecchia le evidenze del monitoraggio. Le informazioni sulla configurazione sono gestite in modo automatico e informatizzato e consentono il controllo delle versioni. La tracciatura delle modifiche è evoluta e comprende strumenti per rilevare la presenza di software non autorizzato o senza licenza. La gestione delle modifiche IT è integrata con la gestione dei cambiamenti aziendali per garantire che l'IT faciliti l'aumento della produttività e la creazione di nuove opportunità di business per l'organizzazione.

DESCRIZIONE DEL PROCESSO

AI7 Installare e certificare le soluzioni e le modifiche

È necessario che i nuovi sistemi siano resi operativi quando lo sviluppo è completato. Questo richiede un test appropriato in un ambiente dedicato con dei dati di test significativi, la definizione del rilascio e delle istruzioni per la migrazione, la pianificazione dei rilasci e dell'effettivo passaggio in produzione, la revisione post implementazione. Questo garantisce che i sistemi applicativi siano allineati con le aspettative e i risultati concordati.



Il controllo del processo IT

Installare e certificare le soluzioni e le modifiche

che soddisfa i requisiti aziendali per l'IT di

avere sistemi nuovi o modificati funzionanti in ambiente di produzione senza problemi rilevanti dopo l'installazione

ponendo l'attenzione su

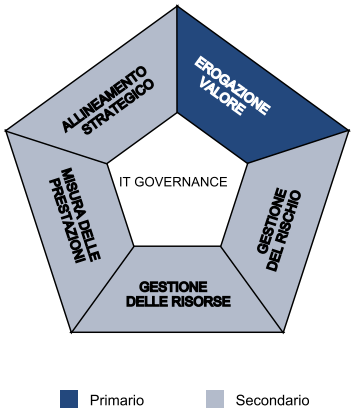
il test delle applicazioni e delle soluzioni infrastrutturali per verificare se corrispondono allo esigenze prefissate e se sono prive di errori, e la pianificazione dei rilasci in produzione

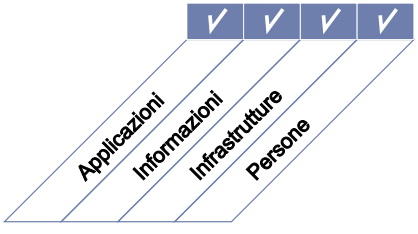
è ottenuto tramite

- la definizione di una metodologia di test
- la pianificazione dei rilasci
- la valutazione ed approvazione dei risultati dei test da parte dei responsabili delle funzioni aziendali destinatarie dei sistemi rilasciati
- la verifica post implementazione dei sistemi rilasciati

e viene misurato tramite

- la durata dei fermi delle applicazioni o numero di correzioni dei dati causati da test inadeguati
- la percentuale dei sistemi i cui benefici misurati attraverso il processo di post implementazione sono in linea con i benefici attesi
- la percentuale di progetti con piani di test documentati ed approvati





OBIETTIVI DI CONTROLLO

AI7 Installare e certificare le soluzioni e le modifiche

AI7.1 Formazione

Formare il personale dei dipartimenti utente interessati e la funzione IT che gestisce le attività operative coerentemente con il piano di formazione e implementazione e la documentazione relativa. Le attività di formazione devono essere parte di ogni progetto di sviluppo, di realizzazione o modifica dei sistemi informativi.

AI7.2 Pianificazione dei test

Definire un piano dei test basato sugli standard dell'impresa e che definisca ruoli e responsabilità, criteri per la considerazione dei casi e per la determinazione del superamento del test. Assicurarsi che il piano sia approvato dalle parti rilevanti.

AI7.3 Piano di implementazione

Stabilire un piano di implementazione, di rilascio e di ripristino delle versioni. Ottenere l'approvazione del piano dalle controparti rilevanti.

AI7.4 Ambiente di test

Realizzare un ambiente di test sicuro e rappresentativo dell'ambiente operativo atteso relativamente a sicurezza, controlli interni, prassi operative, qualità dei dati, requisiti per il trattamento dei dati personali, e carichi di lavoro.

AI7.5 Conversione del sistema e dei dati

Pianificare la conversione dei dati e la migrazione dell'infrastruttura come parte dei metodi di sviluppo aziendali, comprese le registrazioni per l'audit, i rilasci ed i ripristini.

AI7.6 Test delle modifiche

Testare le modifiche indipendentemente secondo il piano di test definito e prima della migrazione nell'ambiente di produzione. Assicurarsi che il piano consideri gli aspetti di sicurezza e le performance.

AI7.7 Test di accettazione finale

Assicurarsi che i referenti dei processi aziendali e gli stakeholder informatici valutino i risultati del processo di test come determinato dal piano di test. Correggere gli errori importanti identificati nel processo di test, dopo aver completato l'insieme di test identificati nel piano e i test di regressione eventualmente necessari.

AI7.8 Passaggio in produzione

Dopo il test, controllare il comportamento del nuovo sistema in produzione, portandolo a regime secondo quanto pianificato. Ottenere l'approvazione degli stakeholder chiave, quali gli utenti, i referenti dei sistemi, i responsabili operativi. Se appropriato, mantenere operativo il precedente sistema in parallelo e per un certo periodo, e confrontare il comportamento dei due sistemi e i loro risultati.

AI7.9 Verifica post-implementazione

Stabilire delle procedure in linea con gli standard aziendali di gestione delle modifiche che richiedano una verifica post-implementazione come stabilito nel piano di realizzazione.

Linee Guida per la Gestione

AI7 Installare e certificare le soluzioni e le modifiche

Da	Inputs
PO3	Standard tecnologici
PO4	Responsabili dei sistemi individuati
PO8	Standard di sviluppo
PO10	Linee guida per la gestione dei progetti e piano di progetto dettagliato
AI3	Configurazione del sistema da testare / installare
AI4	Manuali utente, operativi, di supporto, tecnici e amministrativi
AI5	Elementi approvvigionati
AI6	Autorizzazione della modifica

Outputs	A						
Elementi della configurazione rilasciata	DS8	DS9					
Errori noti ed accettati	AI4						
Piano di passaggio in produzione	DS13						
Piano di rilascio e di distribuzione del software	DS13						
Risultato della verifica post-implementazione	PO2	PO5	PO10				
Monitoraggio dei controlli interni	ME2						

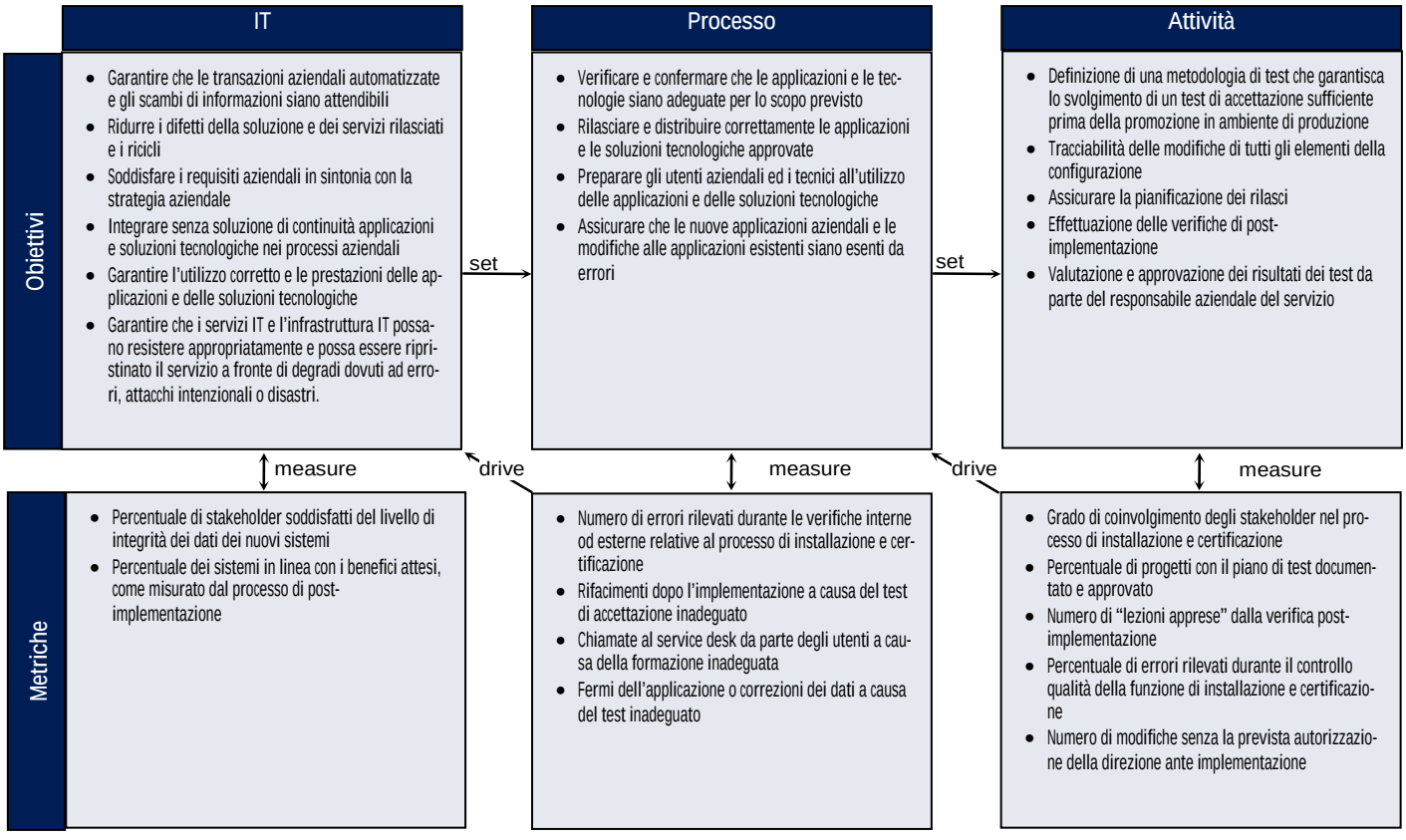
RACI Chart

Ruoli / Attività

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Realizzare e verificare i piani di implementazione			C	A	I	C	C	R		C	C
Definire e verificare la strategia di test (compresi i criteri di selezione e completamento) e una metodologia di pianificazione dei test dell'ambiente operativo.			C	A	C	C	C	R		C	C
Realizzare e manutenere un repository dei requisiti aziendali e tecnici e dei casi di test per i sistemi validati				A				R			
Realizzare la conversione del sistema e i test di integrazione nell'ambiente di test			I	I	R	C	C	A/R		I	C
Costituire l'ambiente di test ed eseguire i test finali di accettazione.			I	I	R	A	C	A/R		I	C
Raccomandare il passaggio in produzione basandosi sui criteri di certificazione concordati			I	R	A	R	C	R		I	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

AI7 Installare e certificare le soluzioni e le modifiche

Il grado di strutturazione del processo *Installare e certificare le soluzioni e le modifiche* che soddisfa i requisiti aziendali per l'IT di *avere sistemi nuovi o modificati funzionanti in ambiente di produzione senza problemi rilevanti dopo l'installazione* è:

0 Non esistente quando

Mancano completamente i processi formali di installazione e certificazione; né la Direzione né il personale IT riconoscono la necessità di verificare se le soluzioni sono adeguate per lo scopo prefissato.

1 Iniziale/*Ad Hoc* quando

Esiste la consapevolezza della necessità di verificare e confermare che le soluzioni realizzate concorrono a perseguire gli obiettivi definiti. I test sono eseguiti per alcuni progetti, ma l'iniziativa è lasciata ai singoli gruppi di progetto e gli approcci adottati sono differenti. La certificazione e la conclusione formale (firma, data, …) del test sono rare o inesistenti.

2 Ripetibile ma Intuitivo quando

Esiste un certo grado di coerenza tra gli approcci di test e di certificazione, ma solitamente non sono basati su una metodologia. Normalmente l'approccio alla fase di test viene definito dai singoli gruppi di sviluppo; generalmente non sono svolti test di integrazione. Esiste un processo informale di approvazione.

3 Definito quando

Esiste una metodologia formale relativa all'installazione, migrazione, conversione e accettazione. I processi IT di installazione e certificazione sono integrati nel ciclo di vita dei sistemi e sono parzialmente automatizzati. La formazione, il test e il passaggio in produzione nonché la certificazione possono differire dal processo definito a seguito di decisioni individuali. La qualità dei sistemi promossi in ambiente di produzione è di basso livello, i nuovi sistemi spesso generano un numero significativo di problemi nella fase di post implementazione.

4 Gestito e Misurabile quando

Le procedure sono formalizzate e sviluppate in modo da essere ben organizzate e attuabili con ambienti di test e procedure di certificazione definiti. In pratica tutti i maggiori cambiamenti ai sistemi seguono questo approccio formalizzato. La valutazione della soddisfazione dei requisiti utente è standardizzata e misurabile, prodotta con metriche che possono essere effettivamente esaminate ed analizzate dalla Direzione. La qualità dei sistemi promossi in ambiente di produzione è soddisfacente per la Direzione e con un livello di problemi di post implementazione ragionevole. L'automatizzazione del processo è ad hoc e dipendente dal progetto. La Direzione può ritenersi soddisfatta del livello di efficienza attuale malgrado l'assenza della valutazione di post implementazione. Il sistema di test riflette adeguatamente l'ambiente di produzione. I test di stress per i nuovi sistemi e i test di regressione per quelli esistenti sono effettuati solo per i progetti principali.

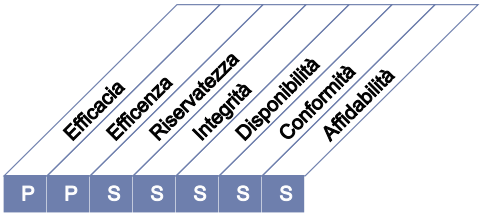
5 Ottimizzato quando

I processi di installazione e di certificazione sono stati perfezionati a livello delle migliori prassi, a seguito di continui miglioramenti e affinamenti. I processi IT di installazione e certificazione sono pienamente integrati nel ciclo di vita dei sistemi ed automatizzati quando opportuno; facilitano la formazione, il test e il passaggio in produzione per i nuovi sistemi con la maggiore efficienza possibile. Gli ambienti di test ben sviluppati, il registro dei problemi e i processi di risoluzione degli errori garantiscono un efficiente ed efficace passaggio nell'ambiente di produzione. La certificazione avviene di norma senza rifacimenti ed i problemi di post implementazione sono in genere limitati a correzioni di secondaria importanza. Le verifiche di post implementazione sono standardizzate, le "lezioni apprese" sono considerate nella verifica del processo in modo da garantire un continuo miglioramento della sua qualità. I test di stress per i nuovi sistemi e quelli di regressione per i sistemi modificati sono eseguiti sistematicamente.

DESCRIZIONE DEL PROCESSO

DS1 Definire e gestire i livelli di servizio

Una comunicazione efficace tra la Direzione IT ed i clienti interni relativamente ai servizi richiesti è resa possibile attraverso un accordo sui servizi IT e sui livelli di servizio e una loro definizione ben documentata. Questo processo comprende anche il monitoraggio e il reporting tempestivo agli stakeholder sul raggiungimento dei livelli di servizio. Questo processo facilita l'allineamento tra i servizi IT ed i relativi requisiti aziendali.



Il controllo del processo IT

Definire e gestire i livelli di servizio

che soddisfa i requisiti aziendali per l'IT di

assicurare l'allineamento fra i servizi chiave IT e la strategia aziendale

ponendo l'attenzione su

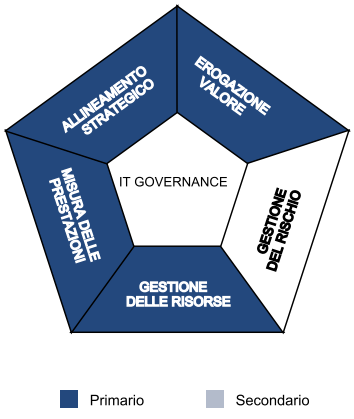
l'identificazione dei requisiti dei servizi, la definizione di accordi sui livelli di servizio e il monitoraggio del perseguimento di questi livelli

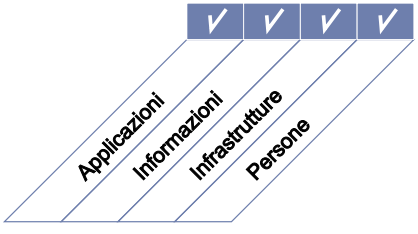
è ottenuto tramite

- la formalizzazione degli accordi interni ed esterni, in linea con i requisiti e la capacità di erogazione
- la produzione di relazioni sui livelli di servizio raggiunti (report e livelli conseguiti)
- l'identificazione e la comunicazione alla pianificazione strategica dei nuovi requisiti dei servizi e degli aggiornamenti

e viene misurato tramite

- la percentuale di stakeholder soddisfatti che i servizi erogati abbiano raggiunto i livelli concordati
- il numero di servizi erogati non in catalogo
- il numero di riunioni formali di revisione degli SLA svolte con le altre componenti aziendali nell'arco dell'anno





OBIETTIVI DI CONTROLLO

DS1 Definire e gestire i livelli di servizio

DS1.1 Modello per la gestione dei livelli di servizio

Definire un modello di riferimento che stabilisca un processo formalizzato di gestione dei livelli di servizio fra i clienti ed i fornitori del servizio. Questo modello di riferimento dovrebbe mantenere un allineamento continuo con le priorità e i requisiti aziendali e dovrebbe facilitare la comprensione comune del servizio fra il cliente ed i fornitori. Il modello di riferimento dovrebbe comprendere i processi per la definizione dei requisiti dei servizi e dei servizi stessi, degli accordi sui livelli di servizio (SLA), degli accordi sui livelli operativi (OLA) e delle fonti di finanziamento. Questi attributi dovrebbero essere organizzati in un catalogo dei servizi. Il modello di riferimento dovrebbe definire la struttura organizzativa per la gestione dei livelli di servizio identificando i ruoli, le attività e le responsabilità dei clienti e dei fornitori, sia interni sia esterni.

DS1.2 Definizione dei servizi

Definire i servizi IT basandosi sulle caratteristiche e sui requisiti dei servizi aziendali. Assicurarsi che questi siano organizzati e mantenuti centralmente mediante la realizzazione di un catalogo del portfolio dei servizi.

DS1.3 Accordi sui livelli di servizio

Definire e concordare gli accordi sui livelli di servizio (SLA) per tutti i servizi IT critici basandosi sui requisiti posti dal cliente e sulle potenzialità dell'IT. Gli accordi dovrebbero comprendere: il mandato dei clienti, i requisiti di supporto ai servizi, le metriche qualitative e quantitative per misurare i servizi sottoscritti dagli stakeholder, le condizioni finanziarie e commerciali qualora applicabili, i ruoli e le responsabilità compresa la supervisione degli SLA. Elementi da considerare sono la disponibilità, l'affidabilità, le prestazioni, la capacità di crescita, i livelli di assistenza, il piano di continuità, la sicurezza e i limiti relativamente a nuove richieste.

DS1.4 Accordi sui livelli operativi

Definire i livelli operativi in modo tale da spiegare come i servizi saranno tecnicamente erogati per supportare gli SLA in modo ottimale. Gli OLA dovrebbero descrivere i processi tecnici in termini comprensibili per il fornitore e ciascuno di essi potrebbe supportare diversi SLA.

DS1.5 Monitoraggio e reporting dei livelli di servizio conseguiti

Monitorare sistematicamente i criteri seguiti per la definizione dei livelli di prestazione dei servizi. I report, riguardanti il raggiungimento dei livelli di servizio, dovrebbero essere forniti in un formato comprensibile per gli stakeholder. I controlli statistici dovrebbero essere attivati e analizzati per identificare andamenti positivi e/o negativi di ciascun servizio o dei servizi nel loro complesso.

DS1.6 Revisione degli accordi sui livelli di servizio e dei contratti

Revisionare regolarmente gli accordi sui livelli di servizio e i relativi contratti con i fornitori di servizi, sia interni sia esterni, per assicurarsi che siano efficaci, aggiornati e che i cambiamenti nei requisiti siano stati presi adeguatamente in considerazione.

LINEE GUIDA PER LA GESTIONE

DS1 Definire e gestire i livelli di servizio

Da	Inputs
PO1	Piano strategico per l'IT, piano tattico per l'IT, portafoglio dei servizi IT
PO2	Classificazioni dei dati definite
PO5	Portafoglio dei servizi IT aggiornato
AI2	Pianificazione iniziale degli SLA
AI3	Pianificazione iniziale degli OLA
DS4	Requisiti per i servizi di disaster recovery, inclusi i ruoli e le responsabilità
ME1	Requisiti di performance in input alla pianificazione IT

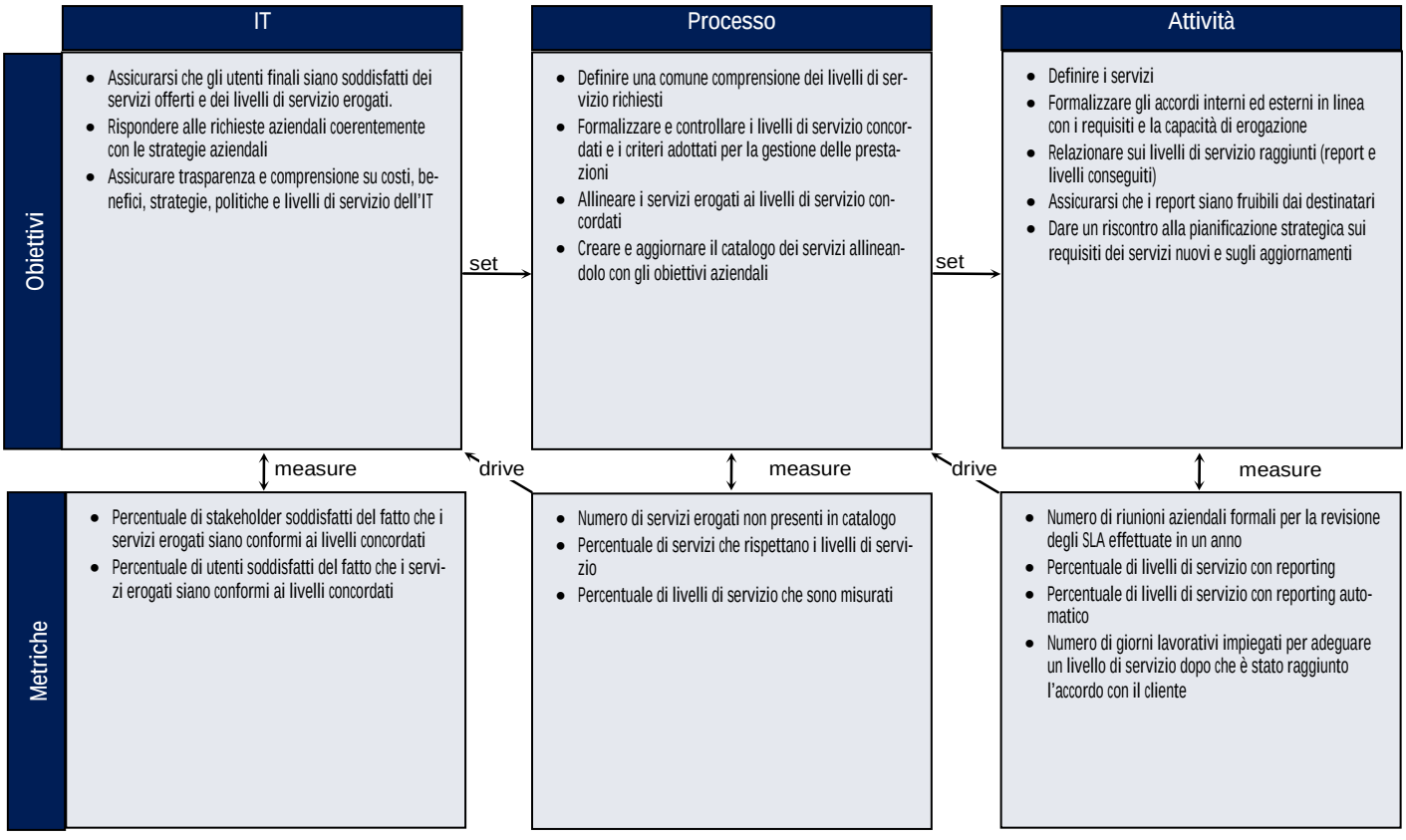
Outputs	A						
Relazione sulla revisione dei contratti	DS2						
Relazione sulle prestazioni dei processi	ME1						
Requisiti nuovi o aggiornati dei servizi	PO1						
SLA	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLA	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Portafoglio dei servizi IT aggiornato	PO1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Service Manager
Creare un modello di riferimento per definire i servizi IT			C	A	C	C	I	C	C	I	C	R
Realizzare il catalogo dei servizi IT			I	A	C	C	I	C	C	I	I	R
Definire accordi sui livelli di servizio (SLA) per i servizi IT critici		I	I	C	C	R	I	R	R	C	C	A/R
Definire accordi sui livelli operativi (OLA) per soddisfare gli SLA				I	C	R	I	R	R	C	C	A/R
Monitorare e rendicontare end-to-end le prestazioni sui livelli di servizio				I	I	R		I	I		I	A/R
Riesaminare gli SLA e i relativi contratti con i fornitori		I		I	C	R		R	R		C	A/R
Riesaminare ed aggiornare il catalogo dei servizi IT			I	A	C	C	I	C	C	I	I	R
Creare un piano di miglioramento dei servizi			I	A	I	R	I	R	C	C	I	R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS1 Definire e gestire i livelli di servizio

Il grado di strutturazione del processo *Definire e gestire i livelli di servizio* che soddisfa i requisiti aziendali per l'IT di *assicurare l'allineamento fra i servizi chiave IT e la strategia aziendale* è:

0 Non esistente quando

La Direzione non ha riconosciuto la necessità di un processo per la definizione dei livelli di servizio. Non sono state assegnate le responsabilità e le attività per il monitoraggio dei livelli di servizio.

1 Iniziale/*Ad Hoc* quando

Esiste la consapevolezza della necessità di gestire i livelli di servizio, ma il processo è informale e di natura reattiva. Non sono assegnate le responsabilità e i compiti per la definizione e la gestione dei servizi. Se esistono delle misure delle prestazioni, esse sono solamente qualitative con obiettivi vagamente definiti. I report sono informali, sporadici e approssimativi.

2 Ripetibile ma Intuitivo quando

Esistono dei livelli di servizio concordati, ma sono informali e non vengono rivisti. I rapporti sui livelli di servizio sono incompleti e potrebbero essere poco significativi o ambigui per i clienti. I rapporti sui livelli di servizio dipendono dalle capacità e dall'iniziativa di singoli responsabili. È stato designato un coordinatore dei livelli di servizio, con responsabilità definite ma senza sufficiente autorità. Se esiste il processo di conformità dei livelli di servizio concordati, è attivato su base volontaria e non obbligatoriamente.

3 Definito quando

Le responsabilità sono ben definite ma con autorità discrezionale. È attivo un processo di sviluppo degli accordi sui livelli di servizio con punti di controllo per la valutazione dei livelli di servizio e della soddisfazione dell'utente. Servizi e livelli di servizio sono definiti, documentati e concordati utilizzando un processo standard. Sono identificate le carenze dei livelli di servizio ma le procedure su come superarle sono informali. C'è un chiaro collegamento fra il raggiungimento dei livelli di servizio attesi e i finanziamenti forniti. I livelli di servizio sono concordati ma potrebbero non essere coerenti con le esigenze aziendali.

4 Gestito e Misurabile quando

I livelli di servizio sono identificati sempre più nella fase di definizione dei requisiti di sistema e sono compresi nella fase di progettazione dell'ambiente operativo e applicativo. La soddisfazione dell'utente viene misurata e valutata sistematicamente. La misura delle prestazioni considera le esigenze dell'utente piuttosto che solamente gli obiettivi IT. Le misure per valutare i livelli di servizio stanno diventando standardizzate e riflettono le norme industriali. I criteri per definire i livelli di servizio sono basati sulle criticità aziendali e includono disponibilità, affidabilità, prestazioni, crescita di potenzialità, supporto all'utente, pianificazione della continuità e considerazioni sulla sicurezza. Quando non vengono raggiunti i livelli di servizio viene eseguita sistematicamente l'analisi delle cause. Il sistema di reportistica sul monitoraggio dei livelli di servizio diventa sempre più automatizzato. Sono definiti e compresi chiaramente i rischi finanziari e operativi associati al non raggiungimento dei livelli di servizio concordati. Un formale sistema di misurazione è istituito e aggiornato.

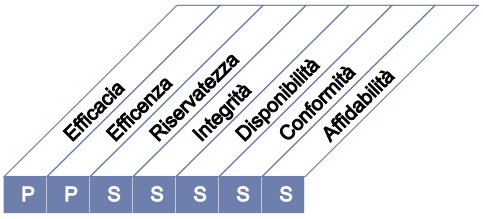
5 Ottimizzato quando

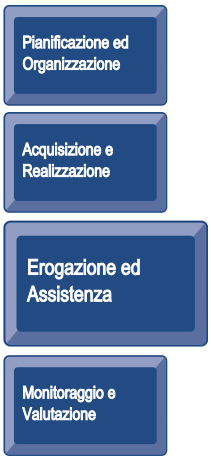
I livelli di servizio vengono di continuo rivisti per assicurare l'allineamento degli obiettivi IT a quelli aziendali, mentre si trae vantaggio dall'innovazione tecnologica includendo il rapporto costi-benefici. Tutti i processi di gestione dei livelli di servizio sono soggetti a continui miglioramenti. I livelli di soddisfazione della clientela sono continuamente monitorati e gestiti. I livelli di servizio attesi riflettono gli specifici obiettivi strategici delle unità aziendali e sono valutati sulla base di criteri industriali. La Direzione IT ha le risorse e la responsabilità necessarie per raggiungere gli obiettivi relativi ai livelli di servizio e la retribuzione è strutturata in modo da prevedere degli incentivi per il raggiungimento di questi obiettivi. L'alta Direzione controlla le metriche di performance quale parte di un processo di miglioramento continuo.

DESCRIZIONE DEL PROCESSO

DS2 Gestire i servizi di terze parti

La necessità di assicurare che i servizi forniti da terze parti (fornitori, rivenditori, partner) siano conformi ai requisiti aziendali comporta l'istituzione di un efficace processo di gestione delle terze parti. Questo processo è attuato sia attraverso l'inserimento negli accordi con le terze parti di una chiara definizione dei ruoli, delle responsabilità e delle aspettative, sia attraverso la revisione ed il monitoraggio di tali accordi per garantirne l'efficacia e la conformità. Un'efficace gestione dei servizi di terze parti minimizza i rischi aziendali associati a mancate o parziali prestazioni dei fornitori.





Il controllo del processo IT

Gestire i servizi di terze parti

che soddisfa i requisiti aziendali per l'IT di

fornire servizi acquisiti da terze parti soddisfacenti, mantenendosi trasparenti rispetto a benefici, costi e rischi

ponendo l'attenzione su

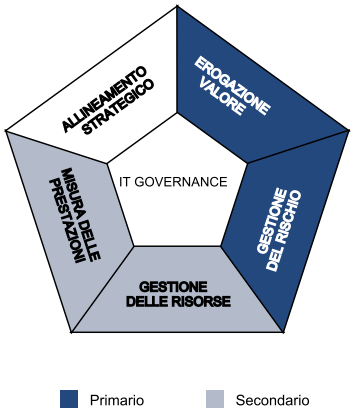
stabilire relazioni e responsabilità bilaterali con qualificate terze parti fornitrici di servizi e monitorare i servizi erogati per verificare ed assicurare il rispetto degli accordi

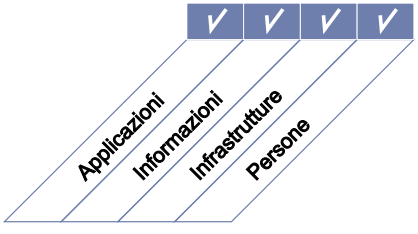
è ottenuto tramite

- l'identificazione e la classificazione dei fornitori di servizi
- l'identificazione e la mitigazione del rischio relativo ai fornitori
- il controllo e la misura delle prestazioni dei fornitori

e viene misurato tramite

- il numero degli utenti insoddisfatti dei servizi contrattualizzati
- la percentuale dei principali fornitori conformi ai requisiti ed ai livelli di servizio chiaramente definiti
- la percentuale dei principali fornitori sottoposti a monitoraggio





OBIETTIVI DI CONTROLLO

DS2 Gestire i servizi di terze parti

DS2.1 Identificazione delle relazioni con tutti i fornitori

Individuare tutti i fornitori di servizi e classificarli in funzione del tipo di fornitura, importanza e criticità. Mantenere aggiornata la documentazione formale delle caratteristiche tecniche ed organizzative contenenti: ruoli e responsabilità, finalità, erogazioni attese e credenziali dei rappresentanti di questi fornitori.

DS2.2 Gestione delle relazioni con i fornitori

Formalizzare il processo di gestione del rapporto intrattenuto con ciascun fornitore. Il responsabile del rapporto con il fornitore dovrebbe relazionare sui problemi esistenti con i clienti e con il fornitore e assicurare la qualità della relazione basata sulla fiducia reciproca e sulla trasparenza (ad esempio attraverso accordi sui livelli di servizio)

DS2.3 Gestione del rischio relativo ai fornitori

Individuare e mitigare il rischio relativo alla capacità dei fornitori di continuare ad erogare il servizio con: efficacia, sicurezza, efficienza e continuità. Assicurare che i contratti siano in linea con gli standard di mercato e conformi ai requisiti previsti da leggi e norme. La gestione dei rischi dovrebbe inoltre considerare: gli accordi di non divulgazione (NDA- Non Disclosure Agreement), le clausole di garanzia (ad esempio sui sorgenti), la continuità dei fornitori critici, la conformità ai requisiti di sicurezza, la disponibilità di fornitori alternativi, le penali ed i premi, ecc.

DS2.4 Monitoraggio delle prestazioni dei fornitori

Stabilire un processo di monitoraggio dei servizi erogati per assicurare che i fornitori siano conformi agli attuali requisiti aziendali e continuino ad essere aderenti ai contratti ed ai livelli di servizio contrattualizzati e che le prestazioni siano competitive rispetto a fornitori alternativi ed alle condizioni di mercato.

LINEE GUIDA PER LA GESTIONE

DS2 Gestire i servizi di terze parti

Da	Inputs
PO1	Strategia di fornitura IT
P08	Standard di acquisizione
AI5	Accordi contrattuali, requisiti di gestione delle relazioni con terze parti
DS1	SLA, resoconto sulla revisione dei contratti
DS4	Requisiti per i servizi di Disater Recovery, compresi i ruoli e le responsabilità

Outputs	A						
Relazione sulle prestazioni dei processi	ME1						
Catalogo dei fornitori	AI5						
Rischi relativi ai fornitori	PO9						

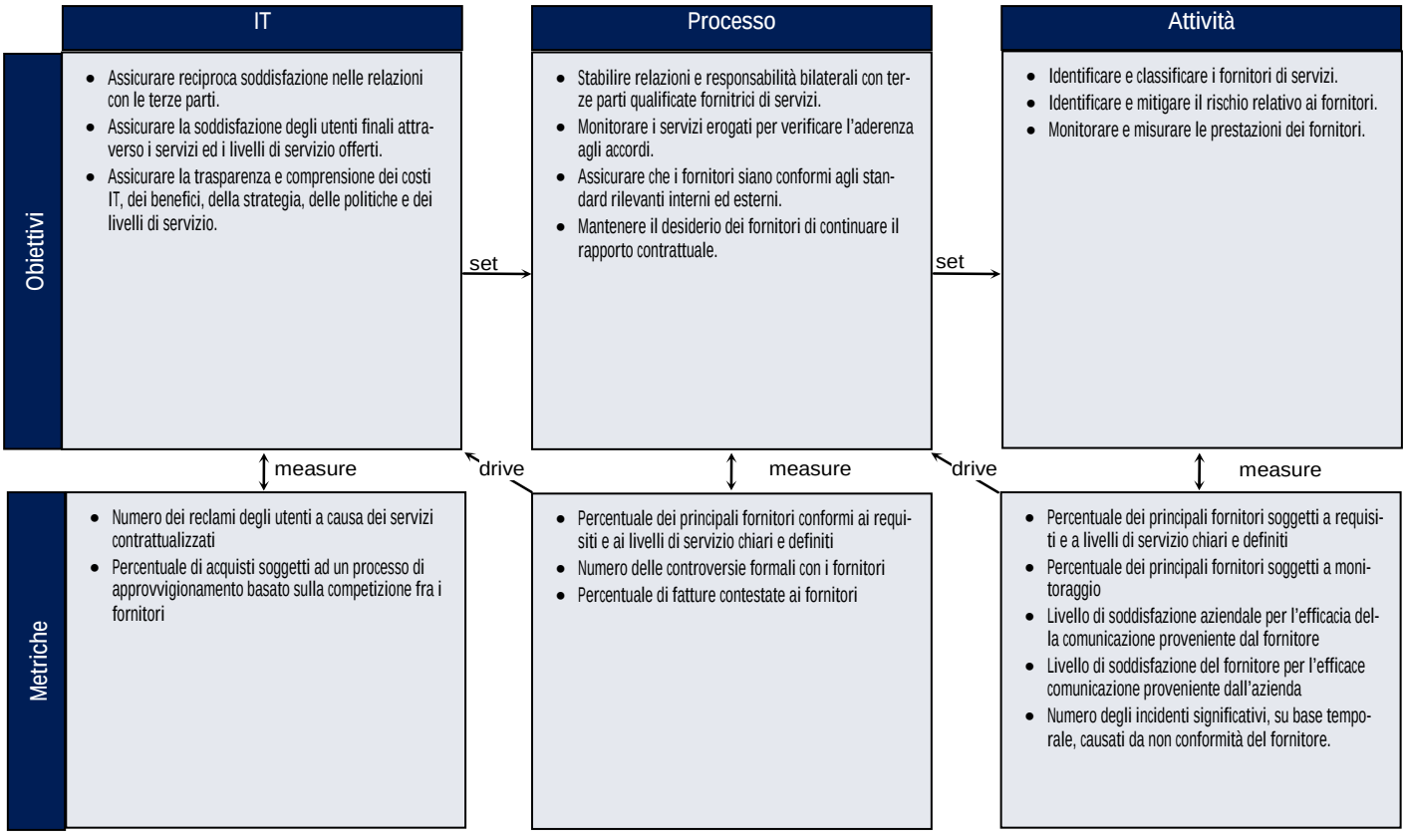
RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Identificare e classificare le caratteristiche dei servizi di terze parti				I	C	R	C	R	A/R	C	C
Definire e documentare il processo di gestione dei fornitori		C		A	I	R	I	R	R	C	C
Definire politiche e procedure per la selezione e valutazione dei fornitori		C		A	C	C		C	R	C	C
Identificare, valutare e mitigare i rischi relativi ai fornitori		I		A		R		R	R	C	C
Monitorare i servizi erogati dai fornitori				R	A	R		R	R	C	C
Valutare gli obiettivi a lungo termine del rapporto di fornitura tenendo in considerazione le esigenze di tutti gli stakeholder	C	C	C	A/R	C	C	C	C	R	C	C

Ruoli

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS2 Gestire i servizi di terze parti

Il grado di strutturazione del processo *Gestire i servizi di terze parti* che soddisfa i requisiti aziendali per l'IT di *fornire servizi acquisiti da terze parti soddisfacenti, mantenendosi trasparenti rispetto a benefici, costi e rischi* è:

0 Non esistente quando

Le responsabilità non sono definite. Non ci sono politiche e procedure formali relative ai contratti con le terze parti. I servizi di terze parti non sono né approvati né rivisti dalla Direzione. Non ci sono attività di misurazione e reporting provenienti dalle terze parti. In assenza di obblighi contrattuali di rendicontazione, la Direzione non è informata sulla qualità del servizio fornito.

1 Iniziale/*Ad Hoc* quando

La Direzione è consapevole della necessità di disporre di procedure e politiche documentate per la gestione dei servizi di terze parti, inclusi i contratti firmati. Non ci sono condizioni contrattuali standard da usare con i fornitori di servizi. La misurazione del servizio fornito è informale e su base spontanea. Le procedure dipendono dall'esperienza del singolo e dal fornitore (ad esempio: a richiesta).

2 Ripetibile ma Intuitivo quando

Il processo di supervisione dei servizi forniti da terze parti, dei rischi associati e dei servizi erogati è informale. Viene firmato un contratto pro forma con indicati i termini e le condizioni standard del fornitore (ad esempio la descrizione dei servizi che devono essere forniti). Sono disponibili dei resoconti sui servizi forniti ma non supportano gli obiettivi aziendali.

3 Definito quando

Esistono delle procedure ben documentate per gestire i servizi di terze parti, con chiari processi che assicurano idonee analisi e trattative con i venditori. Quando un accordo per la fornitura di un servizio viene concluso, la relazione con la terza parte è puramente contrattuale. Nel contratto viene spiegata in dettaglio la natura del servizio che deve essere fornito e comprende i requisiti operativi, legali e di controllo. È assegnata la responsabilità di supervisione dell'erogazione del servizio fornito da terze parti. Le condizioni contrattuali sono basate su modelli standardizzati. Il rischio aziendale associato al servizio fornito dalla terza parte è valutato e sono redatte delle relazioni periodiche.

4 Gestito e Misurabile quando

Sono stati stabiliti dei criteri formali e standardizzati che definiscono i termini di incarico, ambito, servizi da erogare o beni da fornire, convenzioni, tempificazione, costi, accordi di fatturazione, responsabilità. Sono assegnate le responsabilità per la gestione sia del contratto sia del fornitore. Sono sistematicamente verificati l'idoneità del venditore, i rischi attinenti e le sue potenzialità operative. I requisiti dei servizi sono definiti e collegati agli obiettivi aziendali. È previsto un processo di revisione delle prestazioni del servizio rispetto ai termini contrattuali, fornendo un contributo alla valutazione attuale e futura dei servizi di terze parti. Un modello di contabilità analitica (attribuzione dei costi ai servizi) è usato nel processo di acquisizione. Tutte le parti interessate sono consapevoli delle aspettative di servizio, di costo, di tempificazione e di controllo. Gli obiettivi e le metriche per la supervisione dei fornitori di servizi sono stati concordati.

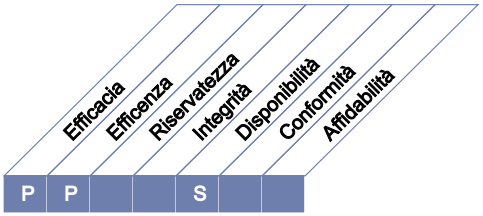
5 Ottimizzato quando

I contratti firmati con terze parti vengono rivisti sistematicamente con scadenze predefinite. La responsabilità per la gestione dei fornitori e della qualità dei servizi forniti è assegnata. Le evidenze di conformità ai contratti in termini operativi, legali e di controllo sono monitorate e vengono imposte eventuali azioni correttive. La terza parte è soggetta ad una periodica revisione indipendente, che fornisce dei feedback sulle prestazioni utilizzati per migliorare i servizi erogati. Le misurazioni variano in risposta ai cambiamenti delle condizioni aziendali. Le misure sono di supporto per la rilevazione tempestiva di eventuali problemi relativi a servizi di terze parti. Il rendiconto finale (predefinito e complessivo rispetto ai servizi forniti) sui livelli di servizio conseguiti è collegato alla remunerazione del fornitore. La direzione, sulla base delle misure ottenute, corregge il processo di selezione dei fornitori e il monitoraggio dei servizi di terze parti.

DESCRIZIONE DEL PROCESSO

DS3 Gestire le prestazioni e la capacità produttiva

La necessità di gestire le prestazioni e la capacità produttiva delle risorse IT richiede un processo di revisione periodica delle prestazioni e della capacità produttiva delle risorse IT. Questo processo include la previsione delle necessità future basata sui requisiti relativi al carico di lavoro, alla memorizzazione e alle emergenza. Questo processo fornisce la garanzia che le risorse informative supportano i requisiti di business e sono continuamente disponibili.



Il controllo del processo IT

Gestire le prestazioni e la capacità produttiva

che soddisfa i requisiti aziendali per l'IT di

ottimizzare le prestazioni delle infrastrutture, delle risorse e della capacità produttiva dell'IT per soddisfare le esigenze aziendali

ponendo l'attenzione su

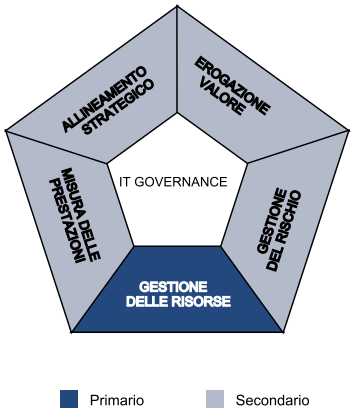
il raggiungimento dei tempi di risposta concordati negli SLA, la minimizzazione dei tempi di fermo e il miglioramento continuo delle prestazioni e della capacità produttiva dell'IT attraverso monitoraggi e misurazioni

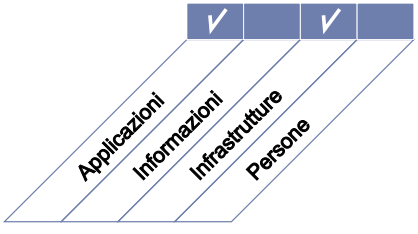
è ottenuto tramite

- la pianificazione e la fornitura della necessaria capacità e disponibilità dei sistemi
- il controllo e la rendicontazione delle prestazioni dei sistemi
- la modellazione e la previsione delle prestazioni dei sistemi

e viene misurato tramite

- il numero di ore perse a causa di una insufficiente pianificazione della capacità produttiva
- la percentuale di picchi dove l'utilizzo eccede l'obiettivo prefissato
- la percentuale di tempi di risposta non conformi agli SLA.





OBIETTIVI DI CONTROLLO

DS3 Gestire le prestazioni e la capacità produttiva

DS3.1 Pianificazione delle prestazioni e della capacità produttiva

Definire un processo di pianificazione per il riesame delle prestazioni e della capacità produttiva delle risorse IT, per assicurare che siano disponibili prestazioni e capacità produttive ad un costo giustificabile, per far fronte ai carichi di lavoro concordati come determinato dagli accordi sui livelli di servizio. La pianificazione della capacità produttiva e delle prestazioni dovrebbe utilizzare appropriate tecniche di modellizzazione per produrre un modello delle performance attuali e previste, della capacità produttiva e del throughput delle risorse IT..

DS3.2 Capacità produttiva e prestazioni attuali

Valutare le attuali capacità produttive e le prestazioni delle risorse IT per determinare se esistono una capacità produttiva e prestazioni sufficienti rispetto ai livelli di servizio concordati.

DS3.3 Capacità produttiva e prestazioni future

Effettuare ad intervalli regolari previsioni sulle prestazioni e sulla capacità produttiva delle risorse IT, per minimizzare il rischio di non fornitura del servizio a causa di una insufficiente capacità produttiva o prestazioni ridotte, e per identificare anche la capacità produttiva in eccesso per un possibile reimpiego. Identificare i trend dei carichi di lavoro e determinare le relative previsioni per contribuire alla pianificazione delle prestazioni e della capacità produttiva.

DS3.4 Disponibilità delle risorse IT

Fornire la capacità produttiva e le performance richieste, prendendo in considerazione aspetti come il normale carico, le emergenze, le esigenze di memorizzazione e il ciclo di vita delle risorse IT. Dovrebbero essere definite delle linee guida per l'assegnazione delle priorità alle attività, la gestione della tolleranza ai guasti e le modalità di allocazione delle risorse. La Direzione dovrebbe assicurare che i piani di emergenza forniscano una adeguata soluzione per la disponibilità, la capacità produttiva e le prestazioni di ciascuna risorsa IT.

DS3.5 Monitoraggio e rapporti

Monitorare continuamente le prestazioni e la capacità produttiva delle risorse IT. I dati raccolti hanno due finalità:
- Mantenere e mettere a punto le prestazioni attuali dell'IT e fornire soluzioni per problematiche come la capacità di resistenza o ripresa (resilienza), le emergenze, i carichi di lavoro attuali e previsti, i trend delle esigenze di memorizzazione e l'acquisizione pianificata delle risorse.
- Rendicontare la disponibilità dei servizi erogati all'azienda come richiesto dagli SLA.

Allegare a tutte le eccezioni documentate le raccomandazioni sulle azioni correttive.

Linee Guida per la Gestione

DS3 Gestire le prestazioni e la capacità produttiva

Da	Inputs
AI2	Specifiche sulla disponibilità, sulla continuità e sul ripristino
AI3	Requisiti di monitoraggio dei sistemi
DS1	SLA

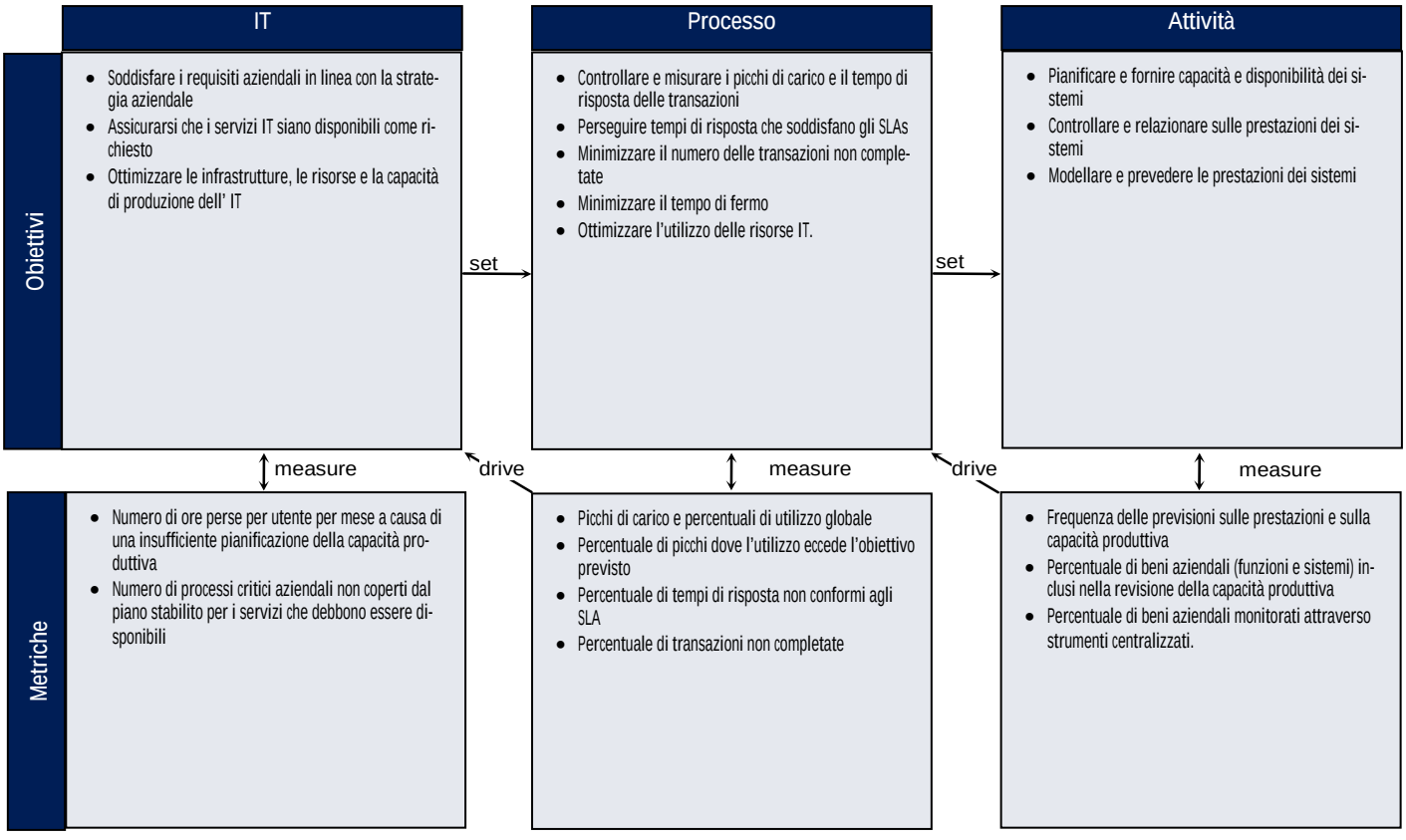
Outputs	A						
Informazioni sulla capacità produttiva e sulle prestazioni	PO2	PO3					
Piani sulle prestazioni e sulla capacità produttiva (requisiti)	PO5	AI1	AI3	ME1			
Cambiamenti richiesti	AI6						
Relazioni sulle prestazione dei processi	ME1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Stabilire un processo pianificato per la revisione delle prestazioni e della capacità produttiva delle risorse IT				A		R	C	C	C	C	
Revisionare le prestazioni e le capacità produttive attuali delle risorse IT				C	I	A/R		C	C	C	
Condurre una previsione sulle prestazioni e sulle capacità produttive delle risorse IT				C	C	A/R	C	C	C	C	
Condurre un'analisi delle differenze (gap analisys) per identificare il divario delle risorse IT				C	I	A/R		R	C	C	I
Condurre la pianificazione delle emergenze per le potenziali risorse IT non disponibili				C	I	A/R		C	C	I	C
Costante monitoraggio e resoconto sulla disponibilità, prestazioni e capacità produttiva delle risorse IT				I	I	A/R		I	I	I	I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS3 Gestire le prestazioni e la capacità produttiva

Il grado di strutturazione del processo *Gestire le prestazioni e la capacità produttiva* che soddisfa i requisiti aziendali per l'IT di *ottimizzare le prestazioni delle infrastrutture, delle risorse e della capacità produttiva dell'IT per soddisfare le esigenze aziendali* è:

0 Non esistente quando

La Direzione non ha rilevato che i processi chiave aziendali possano richiedere prestazioni di alto livello all'IT o che l'azienda globalmente necessiti di servizi IT che potrebbero superare la capacità produttiva. Non esiste un processo di pianificazione della capacità produttiva.

1 Iniziale/*Ad Hoc* quando

Gli utenti ricorrono ad elaborazioni alternative a causa dei vincoli sulle prestazioni o sulla potenza di elaborazione. Da parte dei titolari dei processi aziendali c'è poca sensibilità alle esigenze di pianificazione della capacità produttiva e delle prestazioni . Le azioni intraprese per la gestione delle prestazioni e della potenza di elaborazione sono tipicamente reattive. Il processo di pianificazione della capacità produttiva e delle prestazioni è informale. La comprensione delle capacità produttive e delle prestazioni delle risorse IT attuali e future è limitata.

2 Ripetibile ma Intuitivo quando

La Direzione aziendale e IT è consapevole dell'impatto della non gestione delle prestazioni e della capacità produttiva. Le prestazioni necessarie sono generalmente soddisfatte basandosi su sistemi individuali di valutazione e sulle conoscenze dei team di progetto e di assistenza. Possono essere utilizzati singoli strumenti per identificare i problemi legati alle prestazioni e alla potenza elaborativa, ma la consistenza dei risultati dipende dall'esperienza di dipendenti chiave. Non è prevista una valutazione globale delle prestazioni dell'IT né considerazioni relative alle peggiori situazioni o con picchi di carico. È probabile che si manifestino problemi di disponibilità in maniera casuale ed inattesa e che sia richiesto un tempo considerevole per la relativa diagnosi e soluzione. Tutte le misure sulle performance IT sono basate principalmente sulle necessità dell'IT e non sulle necessità dei clienti.

3 Definito quando

Le richieste di prestazioni e capacità produttiva sono definite attraverso il ciclo di vita dei sistemi. Sono definiti i requisiti del servizio e le metriche da utilizzare per misurare le prestazioni operative. Le prestazioni e le capacità produttive future sono modellate attraverso un processo definito. Si possono produrre report che forniscono statistiche sulle prestazioni. I problemi relativi alle prestazioni ed alla capacità produttiva sono ancora probabili e viene impiegato del tempo per correggerli. Nonostante i livelli di servizio siano resi pubblici, gli utenti e i clienti sono talvolta scettici sulle potenzialità del servizio.

4 Gestito e Misurabile quando

Sono disponibili strumenti e processi atti a misurare l'utilizzo dei sistemi, le prestazioni e la capacità produttiva ed i risultati sono confrontati con gli obiettivi definiti. Sono disponibili informazioni aggiornate che forniscono statistiche standardizzate sulle prestazioni segnalando casi quali insufficienti prestazioni o capacità produttive. Prestazioni insufficienti e problemi sulla capacità produttiva sono affrontati in accordo con standard e procedure definite. Vengono usati strumenti automatizzati per sorvegliare risorse specifiche come spazio su disco, rete, server e gateways di rete. Le statistiche sulle prestazioni e capacità produttive sono documentate utilizzando il linguaggio usato nei processi aziendali affinché gli utenti e i clienti possano comprendere i livelli di servizio IT. Gli utenti sono generalmente soddisfatti delle attuali capacità di servizio e ma possono richiedere livelli di disponibilità nuovi e migliorati. Le metriche per misurare le prestazioni e la capacità produttiva dell'IT sono concordati ma possono essere applicati in modo sporadico ed inconsistente.

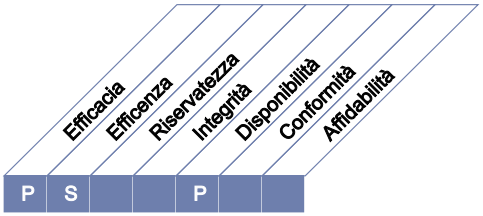
5 Ottimizzato quando

I piani relativi alle prestazioni ed alla potenza sono allineati con le previsioni aziendali. L'infrastruttura IT e le richieste aziendali sono soggette a regolare revisione per assicurare il raggiungimento dell'ottimizzazione della capacità produttiva al più basso costo possibile. Gli strumenti per controllare le risorse IT critiche sono stati standardizzati per tutte le piattaforme e sono collegati ad un unico sistema aziendale di gestione dei problemi. Gli strumenti di monitoraggio rilevano e possono correggere automaticamente i problemi relativi alle prestazioni ed alla capacità produttiva. Gli andamenti vengono rilevati per segnalare problemi di prestazioni incombenti, causati dall'aumento dei volumi del business, permettendo la pianificazione ed evitando incidenti inattesi. Le metriche per misurare le prestazioni e la capacità produttiva IT sono state allineate con le metriche e con gli indicatori di performance di tutti i processi aziendali critici e sono misurate sistematicamente. La Direzione corregge la pianificazione delle prestazioni e della capacità produttiva sulla base dell'analisi di queste misure.

DESCRIZIONE DEL PROCESSO

DS4 Assicurare la continuità del servizio

La necessità di assicurare la continuità dei servizi IT richiede lo sviluppo, la manutenzione ed il test del piano di continuità IT, l'utilizzo di sistemi di archiviazione dei dati per il ripristino del sistema collocati a sufficiente distanza dal sito e l'addestramento periodico al piano di continuità. Un efficace processo di continuità del servizio minimizza la probabilità e l'impatto di una grave interruzione del servizio IT per processi e funzioni aziendali chiave.



Il controllo del processo IT

Assicurare la continuità del servizio

che soddisfa i requisiti aziendali per l'IT di

assicurare il minimo impatto sull'azienda in caso di interruzione del servizio IT

ponendo l'attenzione su

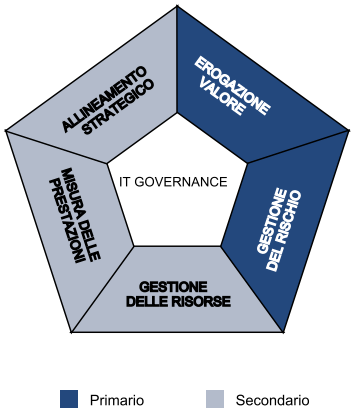
costruire la capacità di ripresa (resilienza) all'interno della soluzione automatica e sviluppare, aggiornare e testare il piano di continuità IT.

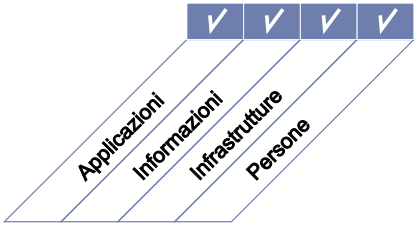
è ottenuto tramite

- lo sviluppo, la manutenzione ed il miglioramento del piano di emergenza IT
- l'addestramento ed il test del piano di emergenza IT
- la conservazione di copie del piano di emergenza e dei dati in un'ubicazione remota

e viene misurato tramite

- Il numero di ore perse dagli utenti per mese a causa di una interruzione non pianificata
- Il numero di processi aziendali critici dipendenti dall'IT non coperti dal piano di continuità IT.





OBIETTIVI DI CONTROLLO

DS4 Assicurare la continuità del servizio

DS4.1 Modello di riferimento della continuità IT

Sviluppare un modello di riferimento per la continuità IT che supporti la gestione della continuità aziendale attraverso un processo coerente. L'obiettivo del modello di riferimento è di aiutare a determinare le richieste di capacità di ripresa delle infrastrutture e guidare lo sviluppo di un piano di Disaster Recovery e un piano di emergenza IT. Il modello di riferimento dovrebbe indirizzare la struttura organizzativa nella gestione della continuità operativa, includendo ruoli, compiti e responsabilità dei fornitori di servizi interni ed esterni, del loro management e dei loro clienti e il processo di pianificazione che crea le regole e le strutture coinvolte nella documentazione, nel test del Disaster Recovery e del piano di emergenza IT. Il piano dovrebbe anche indirizzare aspetti come l'identificazione delle risorse critiche, il controllo ed i rapporti sulla disponibilità delle risorse critiche, i processi alternativi e i principi di salvataggio e ripristino.

DS4.2 Piano di continuità IT

Sviluppare il piano di continuità IT basandosi sulla struttura di riferimento e finalizzandolo alla riduzione dell'impatto o della grave interruzione dei processi e delle funzioni aziendali chiave. I piani dovrebbero essere basati sulla comprensione e valutazione del rischio di potenziali impatti sul business e indirizzare i requisiti sulla capacità di ripresa, sui processi alternativi e sulla capacità di ripristino di tutti i servizi IT critici. I piani dovrebbero trattare i seguenti argomenti: linee guida per l'utilizzo, ruoli e responsabilità, procedure, processi di comunicazione e approccio al test.

DS4.3 Risorse critiche IT

Concentrare l'attenzione sugli elementi più critici del piano di continuità per costruire capacità di ripresa (resilienza) e stabilire delle priorità per le situazioni di ripristino. Evitare di disperdere l'impegno nel ripristino di elementi poco rilevanti e assicurare risposte e ripristini in linea con le priorità aziendali, assicurare allo stesso tempo che i costi siano mantenuti ad un livello accettabile e conformi a regolamenti e requisiti contrattuali. Considerare i fabbisogni di resilienza, di risposta e di ripristino per differenti livelli, p. e. da 1 a 4 ore, da 4 a 24, più di 24 ore e per periodi nei quali vengono svolte operazioni aziendali critiche.

DS4.4 Aggiornamento del piano di continuità IT

Incoraggiare la Direzione IT a definire ed eseguire procedure di controllo dei cambiamenti per assicurare che il piano di continuità IT sia mantenuto aggiornato e rifletta continuamente i requisiti aziendali in essere. Comunicare i cambiamenti nelle procedure e nelle responsabilità in modo chiaro e in maniera tempestiva.

DS4.5 Verifica del piano di continuità IT

Verificare regolarmente il piano di continuità IT per assicurare che i sistemi IT possano essere effettivamente ripristinati, i difetti siano riscontrati e il piano rimanga efficace. Questo richiede un'attenta preparazione, documentazione e relazione sui risultati dei test e, in base ai risultati, l'implementazione di un piano di azione. Comprendere nei test di ripristino le situazioni relative a singole applicazioni, a scenari di test integrato, a test end-to-end, a test integrati con i fornitori.

DS4.6 Addestramento sul piano di continuità IT

Fornire a tutte la parti interessate regolari sessioni di addestramento relativamente alle procedure, ai ruoli e alle responsabilità in caso di incidente o disastro. Verificare e migliorare l'addestramento in accordo con i risultati dei test di emergenza.

DS4.7 Distribuzione del piano di continuità IT

Verificare se esiste e se è operante una strategia di distribuzione del piano per assicurare che il piano sia distribuito in modo appropriato e sicuro, e che sia disponibile alle parti interessate debitamente autorizzate quando e dove necessario. Dovrebbe essere posta attenzione nel rendere i piani accessibili, qualunque sia lo scenario di disastro.

DS4.8 Recupero e ripristino dei servizi IT

Pianificare le azioni che devono essere intraprese nel periodo in cui i servizi IT devono essere recuperati e ripristinati. Questo potrebbe includere l'attivazione di siti alternativi (backup sites), l'attivazione di processi alternativi, la comunicazione di procedure di ripristino alla clientela ed al personale interessato, ecc. Assicurare che l'azienda sia consapevole dei tempi di ripristino e degli investimenti tecnologici necessari per supportare le esigenze di recupero e ripristino aziendali.

DS4.9 Conservazione dei supporti di backup in ubicazione remota

Conservare in un'ubicazione remota tutti i supporti critici di backup, la documentazione e le altre risorse IT necessarie per il ripristino IT e per l'attuazione del piano di continuità aziendale. Determinare il contenuto dei supporti di backup necessari, in collaborazione con i proprietari dei processi aziendali e con il personale IT. La Direzione del servizio di archiviazione remota dovrebbe conformarsi alla politica di classificazione dei dati ed alle pratiche aziendali di archiviazione dei media. La Direzione IT dovrebbe assicurare che le attrezzature dell'ubicazione remota siano periodicamente analizzate, almeno annualmente, sia per quanto riguarda il contenuto che le misure di sicurezza e protezione ambientale. Assicurare la compatibilità dell'hardware e del software per ripristinare i dati archiviati e verificare e aggiornare periodicamente i dati archiviati.

DS4.10 Revisione Post-Ripristino

Determinare se la Direzione IT ha previsto procedure per valutare l'adeguatezza del piano, in riferimento al ripristino della funzione IT a seguito di un disastro, e l'aggiornamento del piano coerentemente alle esigenze emerse nell'attività di ripristino.

LINEE GUIDA PER LA GESTIONE

DS4 Assicurare la continuità del servizio

Da	Inputs
PO2	Classificazione assegnata ai dati
PO9	Valutazione dei rischi
AI2	Specifiche di disponibilità, continuità e ripristino
AI4	Manuali utenti, operativi, di supporto, tecnici e amministrativi
DS1	SLA e OLA

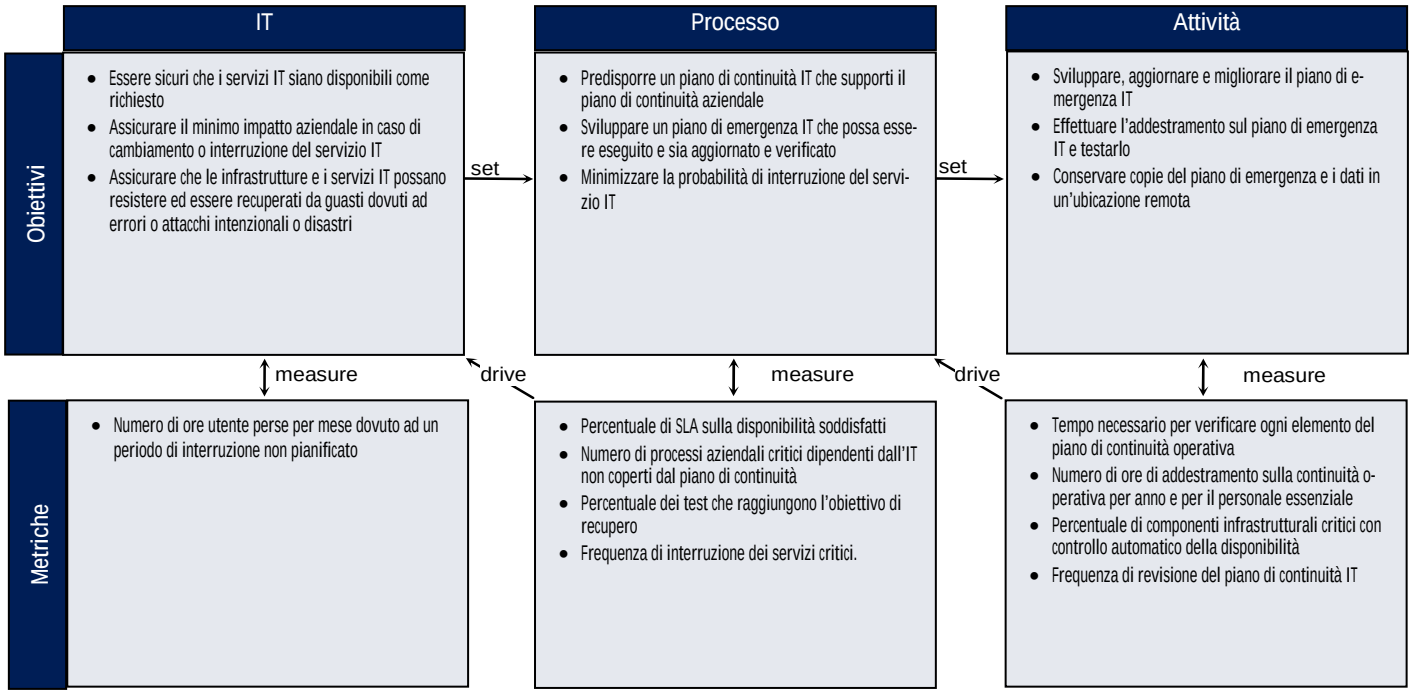
Outputs	A						
Risultati dei test di emergenza	PO9						
Elementi critici di configurazione IT	DS9						
Supporti di memorizzazione e piano di protezione	DS11	DS13					
Soglie di dichiarazione di incidente/disastro	DS8						
Requisiti del servizi in caso di disastro, compresi ruoli e responsabilità	DS1	DS2					
Relazioni sulle performance dei processi	ME1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Sviluppare un modello di riferimento per la continuità IT		C	C	A	C	R	R	R	C	C	R
Condurre un'analisi sugli impatti aziendali e la valutazione dei rischi		C	C	C	C	A/R	C	C	C	C	C
Sviluppare e aggiornare un piano di continuità IT	I	C	C	C	I	A/R		C	C	C	C
Identificare e classificare le risorse IT sulla base degli obiettivi di ripristino				C		A/R		C	I	C	I
Definire ed eseguire una procedura di controllo dei cambiamenti per assicurare che il piano di continuità sia aggiornato				I		A/R		R	R	R	I
Testare regolarmente il piano di continuità IT				I	I	A/R		C	C	I	I
Sviluppare un piano di azione come conseguenza dei risultati delle verifiche				C	I	A/R	C	R	R	R	I
Pianificare e condurre l'addestramento sul piano di continuità IT				I	R	A/R		C	R	I	I
Pianificare il recupero ed il ripristino dei servizi IT		I	I	C	C	A/R	C	R	R	R	C
Pianificare e implementare la conservazione e la protezione dei supporti di back up				I		A/R		C	C	I	I
Prevedere procedure per condurre revisioni post ripristino				C	I	A/R		C	C		C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS4 Assicurare la continuità del servizio

Il grado di strutturazione del processo *Assicurare la continuità del servizio* che soddisfa i requisiti aziendali per l'IT di *assicurare il minimo impatto sull'azienda in caso di interruzione del servizio IT* è:

0 Non esistente quando

Non c'è comprensione del rischio, delle vulnerabilità e delle minacce all'operatività dell'IT o dell'impatto aziendale derivante dalla perdita dei servizi IT. La continuità del servizio non è considerata degna di attenzione da parte della Direzione.

1 Iniziale/*Ad Hoc* quando

Le responsabilità per la continuità del servizio sono informali, e l'autorità per assumere tale responsabilità è limitata. La Direzione sta iniziando a prendere consapevolezza dei rischi correlati e della necessità della continuità del servizio. L'attenzione della Direzione nei confronti dei servizi di continuità è focalizzata sulle risorse infrastrutturali piuttosto che sui servizi IT. Gli utenti stanno escogitando soluzioni alternative in risposta all'interruzione dei servizi. La risposta dell'IT ai grandi disastri è reattiva e impreparata. Le interruzioni pianificate vanno incontro alle esigenze dell'IT ma non considerano i requisiti aziendali.

2 Ripetibile ma Intuitivo quando

La responsabilità di assicurare la continuità del servizio è stata assegnata. L'approccio per assicurare la continuità dei servizi è frammentario. Il reporting sulla disponibilità del sistema è sporadica, potrebbe essere incompleta e non tenere conto dell'impatto sul business. Non ci sono documenti sul piano di continuità, sebbene ci sia l'impegno alla disponibilità continua del servizio e ne siano noti i principiali fondamenti. Esiste un inventario dei sistemi e dei componenti critici, ma potrebbe non essere affidabile. Stanno emergendo pratiche per la continuità del servizio, ma il successo si basa sull'iniziativa dei singoli.

3 Definito quando

La responsabilità per la gestione della continuità di servizio è univoca. La responsabilità per la pianificazione e la verifica della continuità di servizio è chiaramente definita e assegnata. Il piano di continuità operativa IT è documentato ed è basato sulle criticità del sistema e sull'impatto aziendale. C'è un resoconto periodico sui test per la continuità del servizio. È lasciata al singolo l'iniziativa di seguire gli standard e addestrarsi per gestire i principali incidenti o disastri. La Direzione comunica costantemente le esigenze da pianificare per la continuità del servizio. Vengono utilizzati componenti ad alta affidabilità e si provvede a ridondare adeguatamente i sistemi. Viene mantenuto aggiornato l'inventario dei sistemi e delle componenti critiche.

4 Gestito e Misurabile quando

Le responsabilità e gli standard per la continuità del servizio sono sponsorizzati. È assegnata la responsabilità per la manutenzione del piano di continuità. Le attività di manutenzione tengono conto dei risultati dei test sulla continuità di servizio, le "buone pratiche" interne ed i cambiamenti all'ambiente IT e aziendali. Vengono raccolti ed analizzati i dati strutturati sulla continuità, si realizzano report e si agisce di conseguenza. Un addestramento formale è obbligatorio per il processo relativo alla continuità di servizio. Le linee guida sulla ridondanza dei sistemi sono costantemente sviluppate. Pratiche di disponibilità e pianificazione della continuità del servizio si influenzano vicendevolmente. Gli incidenti connessi alla sicurezza sono classificati e il percorso di escalation dei problemi è ben conosciuto da tutti gli attori coinvolti. Gli obiettivi e le metriche per la continuità del servizio sono stati sviluppati e concordati ma potrebbero essere misurati in modo non coerente.

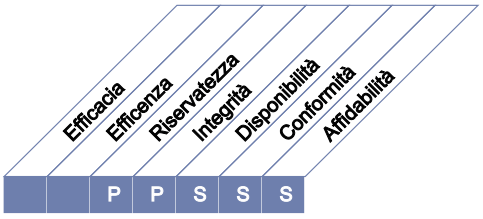
5 Ottimizzato quando

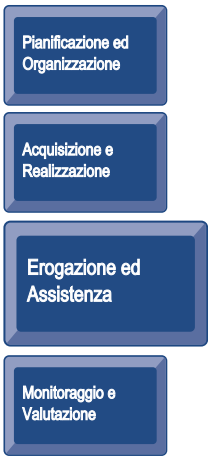
I processi integrati di continuità del servizio tengono conto di valutazioni comparative e delle linee guida esterne. Il piano di continuità IT è integrato con il piano di continuità aziendale e continuamente aggiornato. Requisiti per assicurare la continuità del servizio sono assicurati dai venditori e dai principali fornitori. Vengono effettuati dei test globali sulla continuità di servizio IT ed i risultati sono utilizzati per il processo di manutenzione del piano. La raccolta e l'analisi dei dati viene utilizzata per il continuo miglioramento del processo. È presente un completo allineamento tra le pratiche sulla disponibilità e la pianificazione della continuità di servizio. La Direzione assicura che i disastri o i principali incidenti non accadano a causa di un singolo punto di debolezza (single point of failure). Le pratiche di escalation sono comprese e applicate. Gli obiettivi e le metriche sulla continuità di servizio raggiunti sono misurati in modo sistematico. La Direzione da indicazioni per la ripianificazione della continuità di servizio sulla base delle misure effettuate.

DESCRIZIONE DEL PROCESSO

DS5 Garantire la sicurezza dei sistemi

La necessità di mantenere l'integrità delle informazioni e la protezione delle risorse IT richiede un processo di gestione della sicurezza. Questo processo comprende la definizione e l'aggiornamento dei ruoli e delle responsabilità sulla sicurezza IT, delle politiche, degli standard e delle procedure. La gestione della sicurezza comprende anche il monitoraggio della sicurezza, lo svolgimento di test periodici e l'implementazione delle azioni correttive a fronte di punti di debolezza o incidenti di sicurezza identificati. Una gestione efficace della sicurezza protegge tutte le risorse IT al fine di minimizzare gli impatti aziendali derivanti da vulnerabilità e da incidenti.





Il controllo del processo IT

Garantire la sicurezza dei sistemi

che soddisfa i requisiti aziendali per l'IT di

salvaguardare l'integrità delle informazioni e dei processi infrastrutturali, minimizzare l'impatto derivante da vulnerabilità e da incidenti

ponendo l'attenzione su

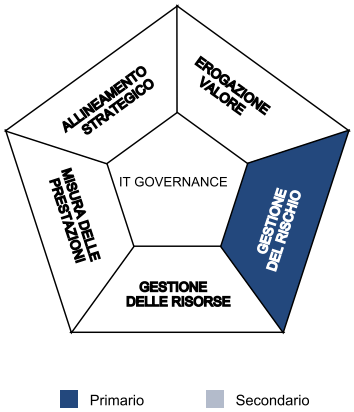
la definizione di politiche, di piani e di procedure di sicurezza informatica ed il monitoraggio, la rilevazione, il relazionare e sistemare le vulnerabilità e gli incidenti di sicurezza

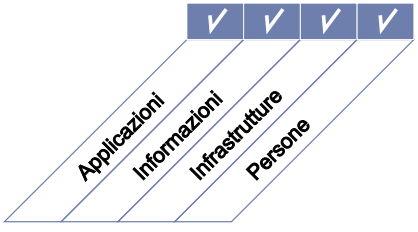
è ottenuto tramite

- la comprensione dei requisiti di sicurezza, delle vulnerabilità e delle minacce
- la gestione delle identità degli utenti e delle autorizzazioni in modalità standardizzata
- il test regolare delle funzionalità di sicurezza

e viene misurato tramite

- il numero di incidenti che hanno compromesso la reputazione dell'azienda presso il pubblico
- il numero di sistemi per i quali non sono soddisfatti i requisiti di sicurezza
- il numero di violazioni relative alla segregazione delle funzioni





OBIETTIVI DI CONTROLLO

DS5 Garantire la sicurezza dei sistemi

DS5.1 Gestione della sicurezza IT

Gestire la sicurezza IT al più alto livello aziendale appropriato, così che la gestione degli interventi di sicurezza sia in linea con i fabbisogni aziendali

DS5.2 Piano di sicurezza IT

Tradurre le esigenze aziendali di business, di rischio e di conformità in un piano generale di sicurezza IT, tenendo in considerazione l'infrastruttura IT e la cultura della sicurezza. Assicurarsi che il piano sia realizzato attraverso politiche e procedure di sicurezza insieme ad appropriati investimenti in servizi, personale, software e hardware. Comunicare le politiche e le procedure di sicurezza agli stakeholder ed agli utenti.

DS5.3 Gestione delle Identità

Assicurare che tutti gli utenti (interni, esterni o temporanei) e le loro attività sui sistemi IT (applicazioni aziendali, sistemi operativi, sviluppo e manutenzione) siano identificati in modo univoco. Abilitare le identità degli utenti attraverso meccanismi di autenticazione. Assicurare che i diritti di accesso ai sistemi ed ai dati siano in linea con le necessità aziendali, definite e documentate, e le esigenze di lavoro siano coerenti all'identità degli utenti. Assicurarsi che i diritti di accesso siano richiesti dalla Direzione Utente, approvati dal proprietario del sistema e implementati dalla persona responsabile della sicurezza. Mantenere gli identificativi utente e i diritti di accesso in modo centralizzato. Sviluppare tecniche operative e procedure economicamente giustificate e mantenerle aggiornate per definire l'identificazione degli utenti, l'implementazione dell'autenticazione e l'applicazione dei diritti di accesso.

DS5.4 Gestione degli identificativi degli utenti.

Stabilire delle regole per la richiesta, la definizione, il rilascio, la sospensione, la modifica e la revoca degli identificativi utente ed i relativi privilegi attraverso un insieme di procedure per la gestione degli identificativi utente, compresa una procedura di approvazione e concessione dei privilegi di accesso basata sul proprietario dei dati o dei sistemi. Queste procedure dovrebbero essere applicata per tutti gli utenti, inclusi gli amministratori (utenti privilegiati), utenti interni ed esterni, sia per i casi normali sia di emergenza. Diritti e obblighi relativi agli accessi alle informazioni e ai sistemi aziendali dovrebbero essere stabiliti contrattualmente per tutti i tipi di utente. Eseguire una sistematica revisione di tutti gli identificativi ed i relativi privilegi.

DS5.5 Verifica, sorveglianza e monitoraggio della sicurezza

Testare e controllare in modo proattivo l'implementazione della sicurezza IT. La sicurezza IT dovrebbe essere valutata periodicamente per assicurare il mantenimento del livello della sicurezza delle informazioni approvato per l'azienda. Esiste una funzione di registrazione e monitoraggio che consente una rapida prevenzione e/o rilevazione, e conseguentemente una pronta rendicontazione di attività non usuali e/o anomale che potrebbero richiedere un intervento.

DS5.6 Definizione degli incidenti di sicurezza

Definire chiaramente e comunicare le caratteristiche dei potenziali incidenti sulla sicurezza così che possano essere classificati in modo appropriato e trattati nel processo di gestione dei problemi e degli incidenti.

DS5.7 Protezione della tecnologia sulla sicurezza

Rendere la tecnologia connessa alla sicurezza resistente alle manomissioni e non divulgare inutilmente la documentazione relativa alla sicurezza.

DS5.8 Gestione delle chiavi crittografiche

Verificare che siano definite e messe in atto politiche e procedure per organizzare la generazione, modifica, revoca, distruzione, distribuzione, certificazione, memorizzazione, immissione, uso e archiviazione delle chiavi crittografiche per assicurarne la protezione da modifiche e divulgazioni non autorizzate.

DS5.9 Prevenzione, rilevazione e correzione del software malevolo

Mettere in atto misure preventive, di rilevazione e correzione (specialmente l'aggiornamento delle patch di sicurezza e il controllo dei virus) per tutta l'organizzazione allo scopo di proteggere i sistemi informativi e le tecnologie da malware (ad esempio virus, worms, spyware, spam).

DS5.10 Sicurezza della Rete

Utilizzare le tecniche di sicurezza e le relative procedure di gestione (e.g. firewalls, dispositivi di sicurezza, segmentazione della rete e rilevazione delle intrusioni) per autorizzare l'accesso ed il controllo del flusso di informazioni da e per la rete.

DS5.11 Scambio di dati sensibili

Effettuare le transazioni con dati sensibili solo su percorsi affidabili o ambienti controllati per assicurare l'autenticità del contenuto, la traccia di chi ha avviato e chi ha ricevuto la transazione, ed il non ripudio da parte del mittente

LINEE GUIDA PER LA GESTIONE

DS5 Garantire la sicurezza dei sistemi

Da	Inputs
PO2	Architettura delle informazioni; classificazione assegnata ai dati
PO3	Standard tecnologici
PO9	Valutazione dei rischi
AI2	Specifiche su controlli di sicurezza alle applicazioni
DS1	OLA

Outputs	A							
Definizione degli incidenti di sicurezza	DS8							
Requisiti di formazione specifica sulla consapevolezza della sicurezza	DS7							
Relazione sulle prestazioni dei processi	ME1							
Cambiamenti richiesti sulla sicurezza	AI6							
Minacce e vulnerabilità alla sicurezza	PO9							
Piani e politiche di sicurezza IT	DS11							

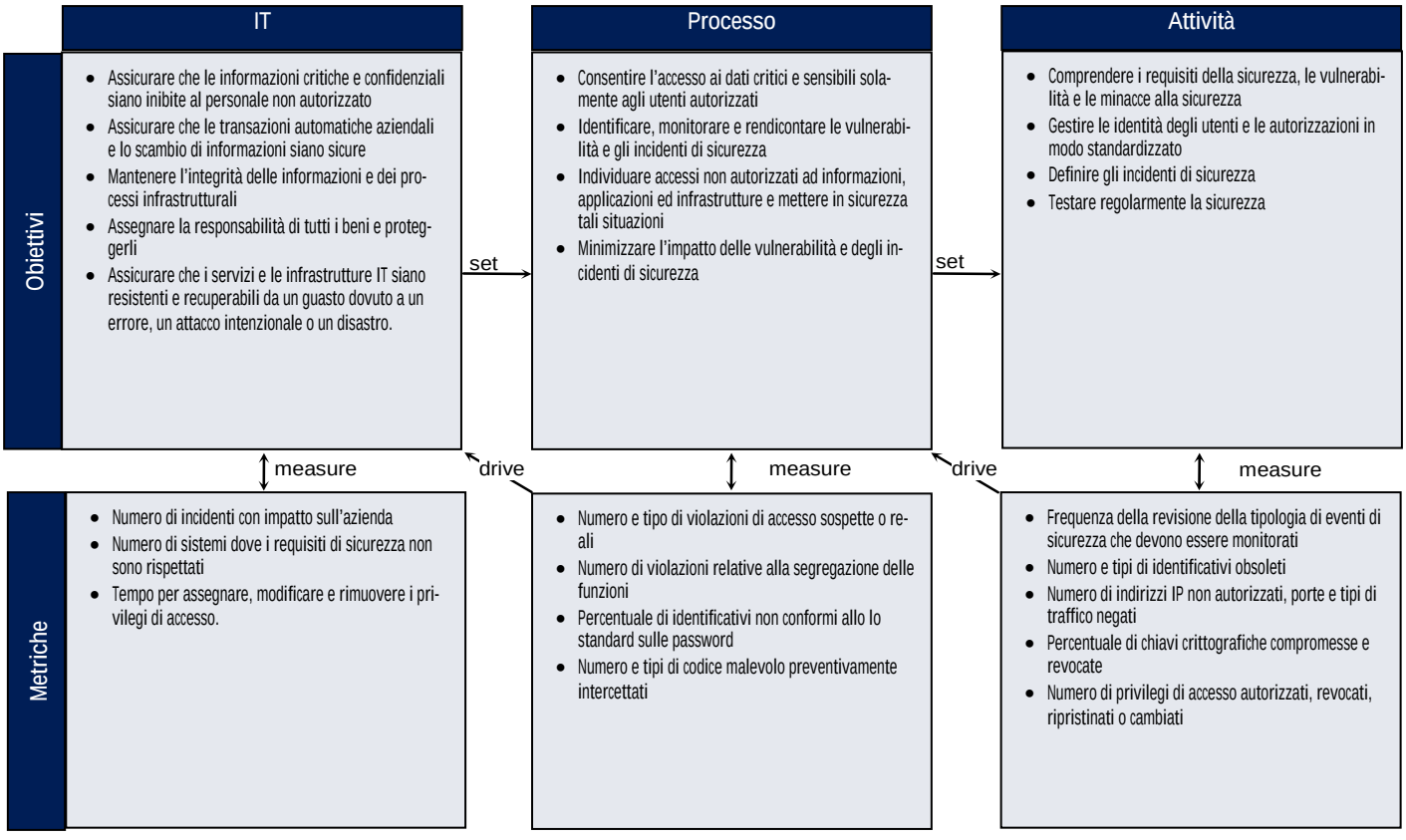
RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire e aggiornare un piano di sicurezza IT	I	C	C	A	C	C	C	C	I	I	R
Definire, stabilire e rendere operativo un processo di gestione degli identificativi (account)			I	A	C	R	R	I			C
Monitorare i potenziali e reali incidenti sulla sicurezza				A	I	R	C	C			R
Periodicamente revisionare e convalidare i diritti di accesso e i privilegi degli utenti				I	A	C					R
Definire e aggiornare una procedura per gestire e salvaguardare le chiavi crittografiche				A		R			I		C
Implementare e aggiornare le tecniche e i controlli procedurali per proteggere il flusso di informazioni attraverso la rete				A	C	C	R	R			C
Condurre una regolare valutazione delle vulnerabilità		I		A	I	C	C	C			R

Ruoli

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS5 Garantire la sicurezza dei sistemi

Il grado di strutturazione del processo *Garantire la sicurezza dei sistemi* che soddisfa i requisiti aziendali per l'IT di *salvaguardare l'integrità delle informazioni e dei processi infrastrutturali, minimizzare l'impatto derivante da vulnerabilità e da incidenti* è:

0 Non esistente quando

L'azienda non ravvisa la necessità di sicurezza IT. Non sono assegnate le responsabilità per garantire la sicurezza. Non sono implementate misure di supporto alla gestione della sicurezza IT. Non sono previsti report per la sicurezza IT e non ci sono processi di risposta alle falle sulla sicurezza dell'IT. C'è una completa carenza del processo di amministrazione della sicurezza.

1 Iniziale/*Ad Hoc* quando

L'organizzazione riconosce la necessità della sicurezza IT. La consapevolezza della sicurezza dipende principalmente dal singolo. La sicurezza IT è indirizzata su base reattiva. La sicurezza IT non viene misurata. Le falle alla sicurezza IT rilevate scatenano la ricerca di un singolo 'colpevole', perché le responsabilità non sono chiare. Le risposte alle falle sulla sicurezza IT sono imprevedibili.

2 Ripetibile ma Intuitivo quando

Le responsabilità per la sicurezza IT sono assegnate a un coordinatore senza autorità direttiva ed il coordinamento è limitato. La consapevolezza sulla necessità di sicurezza è limitata e frammentaria. Tuttavia le informazioni rilevanti sulla sicurezza IT sono prodotte dai sistemi ma non vengono analizzate. I servizi di terze parti potrebbero non verso tener conto delle necessità di sicurezza dell'organizzazione. Si stanno sviluppando alcune politiche di sicurezza ma le competenze e gli strumenti sono inadeguati. I report sulla sicurezza IT risultano incompleti, fuorvianti o non pertinenti. La formazione per la sicurezza è disponibile, ma viene erogata soprattutto su iniziativa individuale. La sicurezza IT è vista principalmente come responsabilità in ambito IT mentre l'azienda non la vede nell'ambito delle proprie, più ampie, responsabilità.

3 Definito quando

Esiste una consapevolezza della sicurezza che viene promossa dalla Direzione. Le procedure per la sicurezza IT sono definite e allineate con le politiche di sicurezza IT. Le responsabilità per la sicurezza IT sono assegnate e comprese, ma non sono applicate in modo coerente. Un piano per la sicurezza IT e le soluzioni di sicurezza esistono e si basano su una analisi del rischio. Il reporting sulla sicurezza non è chiaramente focalizzato sull'azienda. Vengono realizzate prove di intrusione ad hoc (es. test di intrusione). La formazione sulla sicurezza è disponibile per l'IT e l'azienda ma è programmata e gestita solo in modo informale.

4 Gestito e Misurabile quando

Le responsabilità per la sicurezza IT sono chiaramente assegnate, gestite e applicate. L'analisi del rischio e degli impatti vengono eseguite in modo appropriato. Le politiche e le prassi di sicurezza sono complete con specifici principi di base. È obbligatoria l'adozione di metodi promuovere che promuovano la consapevolezza della sicurezza. L'identificazione, l'autenticazione e l'autorizzazione dell'utente sono standardizzate. La certificazione della sicurezza è perseguita dallo staff che è responsabile del controllo e della gestione della sicurezza. I test sulla sicurezza sono portati a termine usando processi standard e formalizzati, orientati al miglioramento del livello di sicurezza. I processi della sicurezza IT sono coordinati con la funzione di sicurezza globale dell'organizzazione. Il reporting sulla sicurezza IT è collegato agli obiettivi aziendali. La formazione sulla sicurezza IT è condotta sia in ambito aziendale che IT. La formazione della sicurezza IT è pianificata e gestita in modo tale da rispondere alle necessità aziendali e ai profili definiti a rischio per la sicurezza. Gli obiettivi e le metriche per la gestione della sicurezza sono stati definiti ma non ancora misurati.

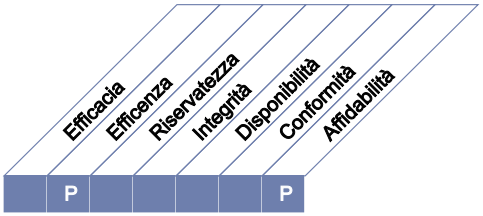
5 Ottimizzato quando

La sicurezza IT è responsabilità congiunta della Direzione aziendale e di quella IT ed è integrata con gli obiettivi di gestione della sicurezza aziendale. I requisiti della sicurezza IT sono chiaramente definiti, ottimizzati e inclusi in un piano approvato di sicurezza. Gli utenti e i clienti sono sempre più responsabilizzati nella definizione dei requisiti di sicurezza e le funzioni di sicurezza sono integrate con le applicazioni durante le fasi di progettazione. Gli incidenti di sicurezza sono prontamente affrontati con procedure formalizzate di risposta agli incidenti, supportate da strumenti automatici. Accertamenti periodici della sicurezza sono condotti per valutare l'efficacia del piano di sicurezza implementato. Le informazioni sulle minacce e sulle vulnerabilità vengono sistematicamente raccolte e analizzate. Adeguati controlli per mitigare i rischi sono prontamente comunicati e implementati. Test di sicurezza, analisi delle cause degli incidenti relativi alla sicurezza e una proattiva identificazione del rischio sono usati nel processo di miglioramento continuo. I processi e le tecnologie relative alla sicurezza sono integrati nell'organizzazione in modo esteso. Le metriche per la gestione della sicurezza sono raccolte e comunicate. All'interno di un processo di miglioramento continuo, la Direzione usa tali misure per correggere il piano di sicurezza.

DESCRIZIONE DEL PROCESSO

DS6 Identificare ed attribuire i costi

La necessità di un giusto ed equo sistema di attribuzione dei costi IT ai costi aziendali richiede un'accurata misurazione dei costi IT e accordi con gli utenti aziendali sulla giusta allocazione. Questo processo comprende la costruzione e l'utilizzo di un sistema per identificare, allocare e rendicontare i costi IT agli utilizzatori dei servizi. Un equo sistema di allocazione consente all'azienda di prendere decisioni più fondate relativamente all'utilizzo dei sistemi IT.



Il controllo del processo IT

Identificare ed attribuire i costi

che soddisfa i requisiti aziendali per l'IT di

assicurare la trasparenza e la comprensione dei costi IT ed il miglioramento dell'efficienza attraverso un uso consapevole dei servizi IT.

ponendo l'attenzione su

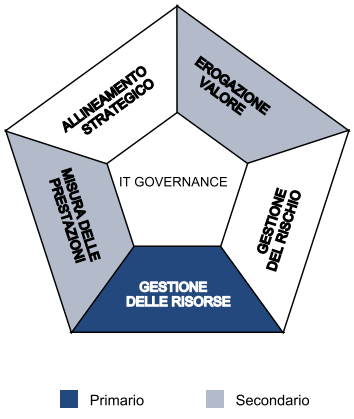
la completa ed accurata identificazione dei costi IT, un equo sistema di allocazione concordato con gli utenti aziendali, ed un sistema per un tempestivo resoconto dell'utilizzo dell'IT e dell'allocazione dei costi.

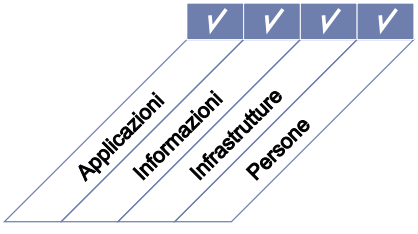
è ottenuto tramite

- l'allineamento della rilevazione dei costi alla qualità e quantità dei servizi forniti
- la costruzione e la condivisione di un modello dei costi completo
- l'implementazione della rilevazione dei costi secondo la politica concordata

e viene misurato tramite

- la percentuale degli addebiti di servizi IT accettate/pagate dalla Direzione aziendale.
- la percentuale delle variazioni fra budget, previsioni e costi reali.
- la percentuale di costi generali IT allocati secondo il modello dei costi concordato





OBIETTIVI DI CONTROLLO

DS6 Identificare ed attribuire i costi

DS6.1 Definizione dei servizi

Identificare tutti i costi IT e mapparli sui servizi IT per supportare un modello di costi trasparente. I servizi IT dovrebbero essere collegati ai processi aziendali così che l'azienda possa identificare i livelli di addebito associati ai servizi.

DS6.2 Contabilizzazione IT

Rilevare e allocare i costi attuali secondo il modello dei costi dell'impresa. Variazioni fra costi previsti e reali dovrebbero essere analizzati e riportati in conformità con i sistemi di misurazione finanziaria dell'impresa.

DS6.3 Modello dei costi e delle tariffe

Stabilire ed utilizzare un modello dei costi, basato sulla definizione dei servizi, che supporti il calcolo del tasso di ricarico per ciascun servizio. Il modello dei costi IT dovrebbe assicurare che l'addebito dei servizi sia identificabile, misurabile e prevedibile da parte degli utenti al fine di promuovere un corretto uso delle risorse.

DS6.4 Aggiornamento del modello dei costi

Rivedere e confrontare periodicamente l'adeguatezza del modello dei costi/ricarichi per mantenerne validità ed adeguatezza in un'ottica di sviluppo dell'azienda e delle attività IT.

LINEE GUIDA PER LA GESTIONE

DS6 Identificare ed attribuire i costi

Da	Inputs
PO4	Dettaglio degli owner dei sistemi
PO5	Resoconto costi/benefici, budget IT
PO10	Piani di progetto dettagliati
DS1	SLA e OLA

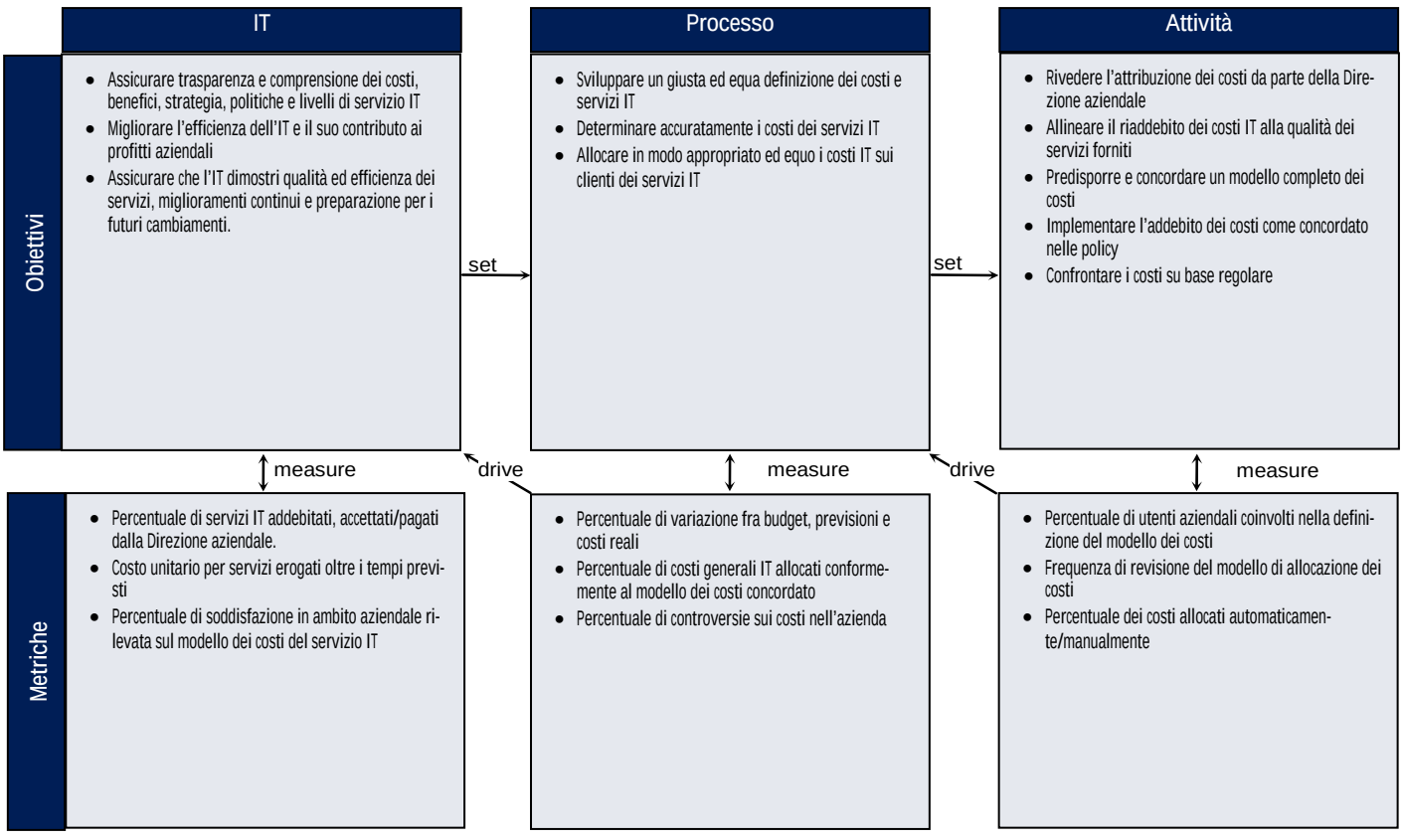
Outputs	A						
Componenti finanziarie dell'IT	PO5						
Rapporto sulle prestazioni dei processi	ME1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Mappare le infrastrutture IT con i servizi forniti /processi aziendali supportati		C	C	A	C	C	C	C	R	C	
Identificare tutti i costi IT (personale, tecnologia, etc.) e mapparli con i servizi IT sulla base dei costi unitari		C		A		C	C	C	R	C	
Definire e aggiornare la contabilità IT e il processo di controllo dei costi		C	C	A	C	C	C	C	R	C	
Definire e aggiornare politiche e procedure per il ribaltamento dei costi		C	C	A	C	C	C	C	R	C	

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS6 Identificare ed attribuire i costi

Il grado di strutturazione del processo *Identificare ed attribuire i costi* che soddisfa i requisiti aziendali per l'IT di *assicurare la trasparenza e la comprensione dei costi IT ed il miglioramento dell'efficienza attraverso un uso consapevole dei servizi IT*. è:

0 Non esistente quando

C'è un'assoluta mancanza di un processo riconoscibile per identificare ed allocare i costi relativi ai servizi informatici erogati. L'organizzazione non ha ancora riconosciuto che c'è un problema relativo alla contabilizzazione dei costi e non esiste alcuna comunicazione relativa.

1 Iniziale/*Ad Hoc* quando

C'è una conoscenza generale dei costi globali dei servizi informatici, ma non c'è la ripartizione dei costi per utente, per cliente, per dipartimento, per gruppi di utenti, per funzioni, per progetti o per servizio erogato. Non c'è un monitoraggio dei costi, ma solo la produzione di un report con i costi complessivi per la Direzione. I costi IT sono allocati come costi di gestione. L'azienda non ha alcuna informazione sui costi ed i benefici dei servizi a disposizione.

2 Ripetibile ma Intuitivo quando

C'è una generale consapevolezza della necessità di identificare ed allocare i costi. L'allocazione dei costi è basata su principi informali e rudimentali, ad es. i costi dell'hardware, e non c'è nessun collegamento con il centro di costo. I processi di allocazione dei costi sono ripetibili. Non c'è un addestramento formale e non vi sono procedure di comunicazione relativa all'identificazione dei costi standard e sulla loro allocazione. Non è assegnata la responsabilità per la raccolta o l'allocazione dei costi.

3 Definito quando

C'è un modello definito e documentato per il costo dei servizi informativi. È definito un processo per mettere in relazione i costi IT con i servizi forniti agli utenti. Esiste un appropriato livello di consapevolezza sui costi attribuibili ai servizi informativi. L'azienda riceve rudimentali informazioni sui costi.

4 Gestito e Misurabile quando

Le responsabilità di gestione dei costi dei servizi informatici sono definite e globalmente note a tutti i livelli e sono supportate da un formale addestramento. I costi diretti e indiretti sono identificati e comunicati in modo tempestivo e automatico alla Direzione, ai proprietari dei processi aziendali e agli utenti. Generalmente è in atto un monitoraggio e una valutazione dei costi e vengono intraprese delle azioni se è rilevato uno scostamento dei costi. Resoconti sulle informazioni dei costi di servizio sono collegati con gli obiettivi aziendali e i livelli di servizio concordati e sono controllati dai proprietari dei processi aziendali. Una funzione finanziaria revisiona la ragionevolezza del processo di allocazione dei costi IT. Un sistema automatico per il controllo dei costi esiste ma è focalizzato sulla funzione dei servizi informativi piuttosto che sui processi aziendali. Obiettivi e metriche per la misurazione dei costi sono stati concordati ma sono misurati in modo incoerente.

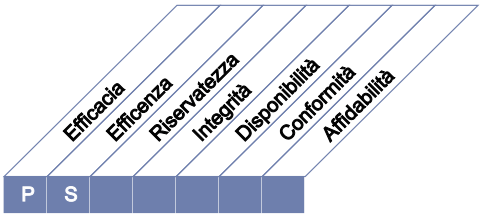
5 Ottimizzato quando

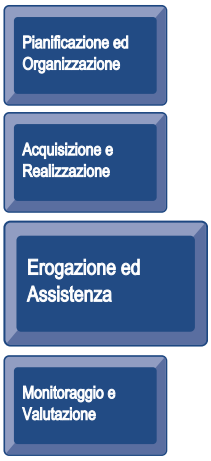
I costi dei servizi forniti sono identificati, acquisiti, riassunti e riportati alla Direzione, ai proprietari dei processi ed agli utenti. I costi sono identificati come servizi fatturabili e vengono sottoposti ad un sistema di ribaltamento che effettua la fatturazione agli utenti in maniera appropriata, in base ai servizi erogati ed al relativo utilizzo. Il dettaglio dei costi è di supporto per l'accordo sui livelli di servizio. Il monitoraggio e la valutazione del costo dei servizi sono utilizzati per ottimizzare il costo dell'utilizzo delle risorse IT. Le somme dei costi ottenute vengono utilizzate per la verifica dei benefici ricavati e vengono utilizzati nel processo di predisposizione del budget dell'azienda. Il resoconto sul costo del servizio informatico fornisce delle segnalazioni tempestive delle modifiche delle esigenze aziendali tramite un sistema intelligente di rendicontazione. Viene utilizzato un modello variabile di costo che deriva dai volumi delle elaborazioni per ogni servizio erogato. La gestione dei costi è stata affinata al livello di pratiche di settore, basata sui risultati del continuo miglioramento e sul confronto con altre organizzazioni. L'ottimizzazione dei costi è un processo in corso. La Direzione revisiona obiettivi e metriche come parte di un processo di miglioramento continuo ridisegnando sistemi di misurazione dei costi.

DESCRIZIONE DEL PROCESSO

DS7 Formare ed addestrare gli utenti

Un'efficace formazione di tutti gli utenti dei sistemi informativi, compresi coloro che fanno parte dell'IT, richiede l'identificazione dei fabbisogni formativi di ciascun gruppo di utenti. In aggiunta all'identificazione dei fabbisogni, questo processo include la definizione e l'attuazione di una strategia per un efficace addestramento e misurazione dei risultati. Un efficace programma di addestramento incrementa un efficace uso della tecnologia riducendo gli errori degli utenti, incrementando la produttività e incrementando la conformità con i controlli chiave quali le misure di sicurezza relative agli utenti.





Il controllo del processo IT

Formare ed addestrare gli utenti

che soddisfa i requisiti aziendali per l'IT di

utilizzare efficientemente ed efficacemente le applicazioni e le soluzioni tecnologiche ed assicurare la conformità degli utenti con le politiche e le procedure

ponendo l'attenzione su

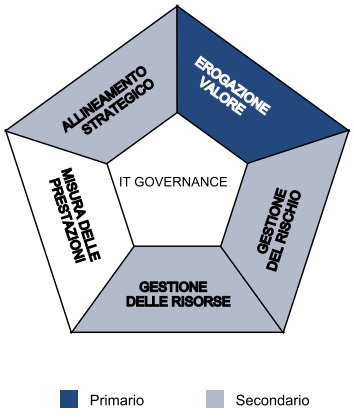
una chiara comprensione dei fabbisogni formativi, l'attuazione di una strategia di addestramento efficace e la misurazione dei risultati

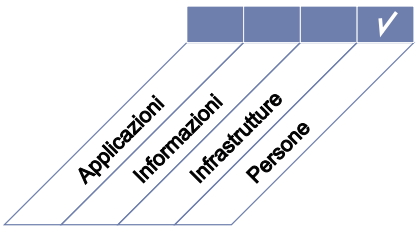
è ottenuto tramite

- la definizione dei curricoli di addestramento.
- l'organizzazione dell'addestramento
- l'erogazione dell'addestramento
- il monitoraggio e rendicontazione dell'efficacia dell'addestramento

e viene misurato tramite

- il numero di chiamate al servizio di help desk causate dalla mancanza di addestramento del personale
- la percentuale di personale interessato soddisfatto dall'addestramento ricevuto
- l'intervallo di tempo fra l'identificazione di un fabbisogno formativo e l'erogazione dell'addestramento





OBIETTIVI DI CONTROLLO

DS7 Formare ed addestrare gli utenti

DS7.1 Identificazione dei fabbisogni di formazione e di addestramento

Definire un regolare aggiornamento dei curricoli per ciascun gruppo di utenti individuato considerando:
• Strategie e necessità aziendali attuali e future
• Valore dell'informazione come bene
• Valori aziendali (valori etici, cultura sulla sicurezza e sul controllo, ecc.)
• Implementazione di nuove infrastrutture IT e software (ad esempio package ed applicazioni)
• Competenze attuali e future, profili di competenza e certificazioni necessarie come pure i requisiti di accreditamento
• Metodo di erogazione (ad esempio. classe, WEB), dimensione del gruppo individuato, disponibilità e coordinamento

DS7.2 Erogazione della formazione e dell'addestramento

Basandosi sui fabbisogni di formazione ed addestramento identificati, individuare il gruppo destinatario della formazione e i suoi membri, gli istruttori ed i mentor. Registrare l'iscrizione (includendo i prerequisiti), la partecipazione e la valutazione del corso di formazione.

DS7.3 Valutazione dell'addestramento ricevuto

Valutare l'erogazione dei contenuti della formazione e dell'aggiornamento in funzione di interesse, qualità, efficacia, conservazione della conoscenza, costi e valore aggiunto. I risultati di questa valutazione dovrebbero servire come contributo per la definizione dei futuri curricoli e l'erogazione di sessioni di aggiornamento.

LINEE GUIDA PER LA GESTIONE

DS7 Formare ed addestrare gli utenti

Da	Inputs
PO7	Capacità e competenza degli utenti, includendo l'addestramento individuale; requisiti di formazione specifica
AI4	Materiale per l'addestramento; requisiti per il trasferimento della conoscenza ai fini dell'implementazione di soluzioni
DS1	OLA
DS5	Requisiti di addestramento specifico sulla consapevolezza alla sicurezza
DS8	Rapporti sulla soddisfazione degli utenti

Outputs	A						
Relazioni sulla prestazione del processo	ME1						
Aggiornamenti della documentazione richiesta	AI4						

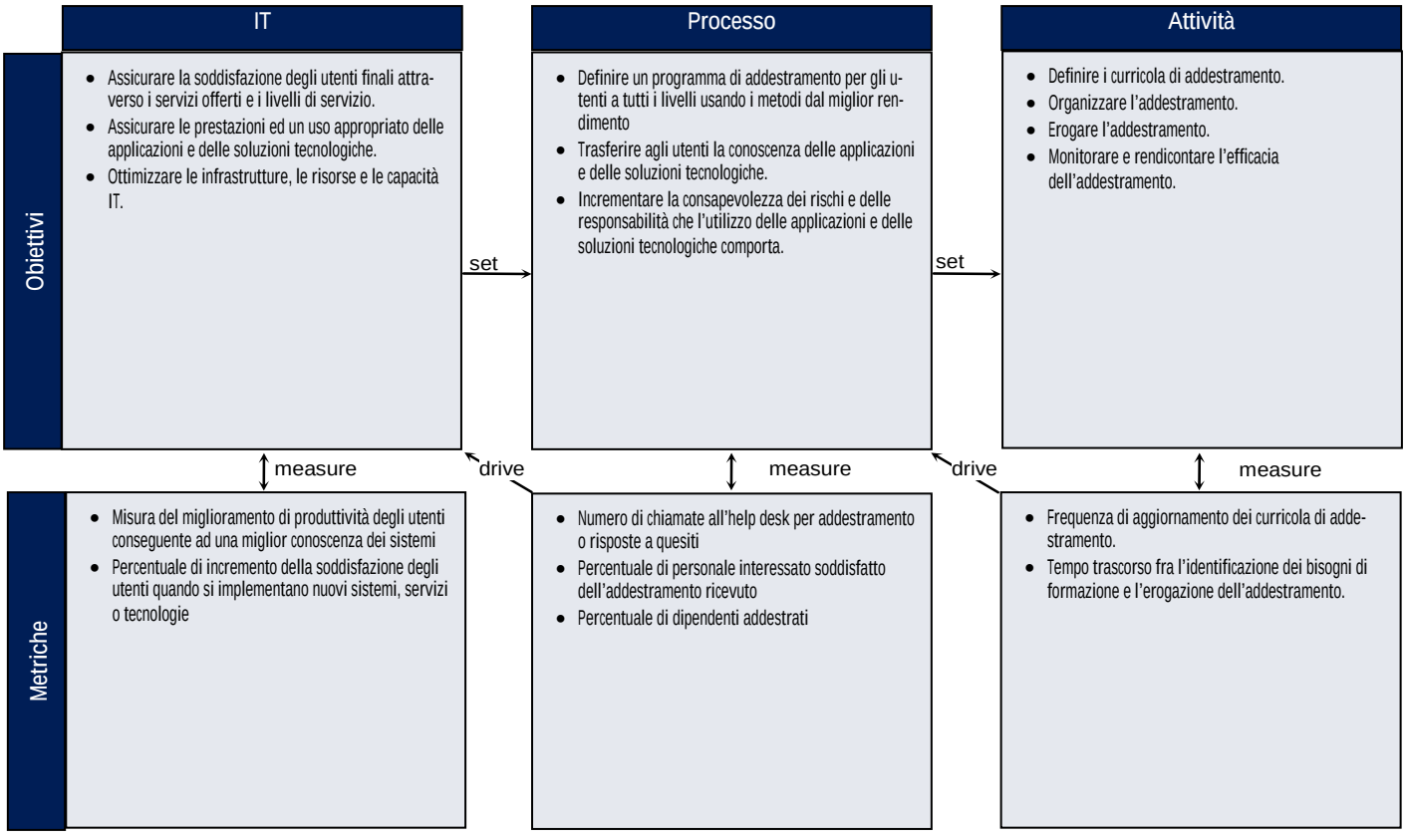
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Ufficio formazione
Identificare e specificare le necessità di addestramento degli utenti			C	A	R	C	C	C	C	C	C	R
Costruire un programma di addestramento			C	A	R	C	I	C	C	C	I	R
Eseguire delle attività di addestramento, formazione e consapevolezza			I	A	C	C	I	C	C	C	I	R
Eseguire la valutazione della formazione			I	A	R	C	I	C	C	C	I	R
Identificare e valutare i migliori metodi e strumenti per l'erogazione della formazione			I	A/R	R	C	C	C	C	C	C	R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS7 Formare ed addestrare gli utenti

Il grado di strutturazione del processo *Formare ed addestrare gli utenti* che soddisfa i requisiti aziendali per l'IT di *utilizzare efficientemente ed efficacemente le applicazioni e le soluzioni tecnologiche ed assicurare la conformità degli utenti con le politiche e le procedure* è:

0 Non esistente quando

C'è un'assoluta assenza di qualsiasi programma di addestramento e formazione. L'organizzazione non riconosce che, riguardo all'addestramento, esiste una situazione che va presa in considerazione e non c'è nessuna comunicazione in tal senso.

1 Iniziale/*Ad Hoc* quando

L'organizzazione ha riconosciuto l'esigenza di programmi di addestramento e formazione, ma non esistono dei processi standardizzati. In assenza di un programma organico, il personale identifica e partecipa ai corsi di formazione in base alla propria iniziativa. Alcuni di questi corsi sono orientati alla condotta etica, alla consapevolezza della sicurezza dei sistemi ed alle pratiche di sicurezza. L'approccio generale della Direzione manca di coerenza e vi sono solamente sporadiche e frammentarie comunicazioni in relazione all'orientamento delle attività di formazione e addestramento.

2 Ripetibile ma Intuitivo quando

C'è la consapevolezza dell'esigenza di un programma di addestramento e formazione e dei relativi processi relativi all'intera organizzazione. L'addestramento sta iniziando a essere previsto nei piani individuali relativi alle prestazioni del personale. I processi sono stati sviluppati a un livello in cui corsi informali di addestramento e formazione vengono impartiti da differenti istruttori, mentre vengono coperti i medesimi argomenti con approcci differenti. Alcuni corsi si orientano alla condotta etica, alla sicurezza dei sistemi e alle prassi. Si fa molto affidamento alle conoscenze dei singoli. C'è, comunque, una costante comunicazione dell'insieme delle novità e dell'esigenza di orientarle.

3 Definito quando

I programmi di formazione ed addestramento sono istituzionalizzati e comunicati, i dirigenti e i dipendenti identificano e documentano i fabbisogni di formazione. I processi di addestramento e formazione sono standardizzati e documentati. Sono stati stabiliti i budget, le risorse, i mezzi e gli istruttori per supportare i programmi di addestramento. Vengono forniti agli utenti specifici training sulla condotta etica e sulla sensibilizzazione della sicurezza dei sistemi nonché lezioni pratiche. Molti corsi vengono monitorati ma non tutte le deviazioni vengono rilevate dalla Direzione. Vengono effettuate solo occasionalmente delle analisi sui problemi relativi alla formazione.

4 Gestito e Misurabile quando

C'è un programma completo di addestramento e formazione che produce dei risultati misurabili. Le responsabilità sono chiare e la titolarità del processo è definita. L'addestramento e la formazione sono una componente dei percorsi di carriera del personale. La direzione sostiene e frequenta le sessioni di addestramento e formazione. Tutti gli impiegati ricevono la formazione sulla condotta etica e sulla conoscenza della sicurezza dei sistemi. Tutti i dipendenti ricevono l'appropriato livello di addestramento pratico rispetto alle misure di sicurezza contro i danni derivanti da anomalie che possano influenzare la disponibilità, la riservatezza e l'integrità. La Direzione controlla la conformità, rivedendo ed aggiornando costantemente i processi ed i programmi di formazione. I processi sono in fase di miglioramento e attuano le migliori prassi interne.

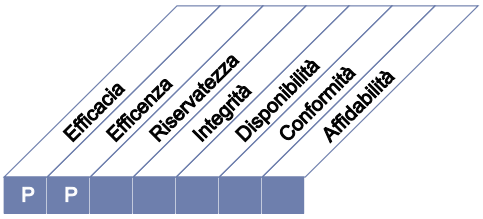
5 Ottimizzato quando

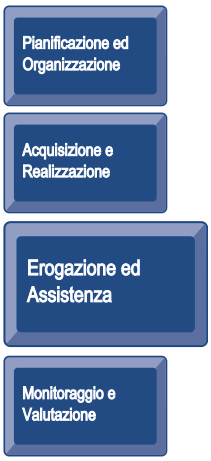
La formazione e l'addestramento producono un miglioramento delle prestazioni individuali. La formazione e l'addestramento costituiscono una componente critica del percorso di carriera del personale. Vengono stanziate sufficienti risorse finanziarie, mezzi, attrezzature ed istruttori per i programmi di formazione e addestramento. I processi sono stati opportunamente definiti e vengono continuamente migliorati traendo vantaggio dal confronto con le migliori prassi esterne e con il modello di maturità di altre organizzazioni. Tutti i problemi e gli scostamenti sono analizzati per scoprire le cause primarie e vengono identificate ed intraprese azioni opportune ed efficienti. C'è un atteggiamento positivo verso il rispetto della condotta etica e dei principi di sicurezza dei sistemi. L'IT viene utilizzato in maniera estesa, integrata e ottimizzata per fornire ed automatizzare gli strumenti di addestramento e formazione. Vengono utilizzati esperti di formazione esterni insieme a riferimenti standard come linee guida.

DESCRIZIONE DEL PROCESSO

DS8 Gestire il service desk e gli incidenti

Una risposta tempestiva ed efficace alle richieste ed ai problemi degli utenti IT richiede la presenza di un service desk correttamente progettato ed operativo e di un processo di gestione degli incidenti. Questo processo include la creazione di una funzione di service desk che preveda le fasi di registrazione, escalation degli incidenti, analisi dei trend e delle cause alla base degli incidenti, la risoluzione degli incidenti. I benefici per il business comprendono una accresciuta produttività attraverso la rapida risoluzione delle richieste degli utenti. In aggiunta, il business può gestire le cause alla base degli incidenti (come l'aggiornamento non adeguato degli utenti) attraverso un reporting efficace.





Il controllo del processo IT

Gestire il service desk e gli incidenti

che soddisfa i requisiti aziendali per l'IT di

abilitare un uso efficace dei sistemi assicurando la risoluzione e l'analisi delle richieste, delle domande e degli incidenti degli utenti finali.

ponendo l'attenzione su

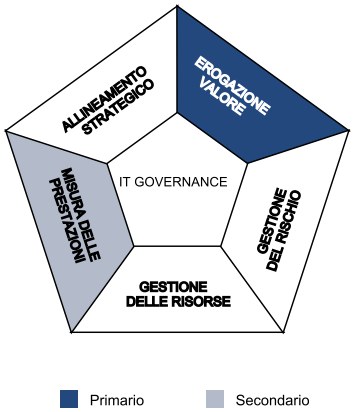
una funzione di service desk professionale con risposte rapide, chiare procedure di escalation, analisi delle soluzioni adottate e del trend

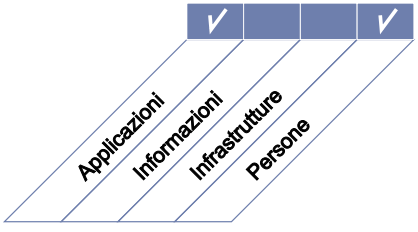
è ottenuto tramite

- l'installazione e attivazione di un service desk
- il monitoraggio e reporting dei trend
- la definizione di criteri e procedure di escalation chiare

e viene misurato tramite

- la soddisfazione degli utenti per il supporto di primo livello
- la percentuale di incidenti risolti entro un periodo di tempo concordato/accettabile
- la frequenza di abbandono della chiamata





OBIETTIVI DI CONTROLLO

DS8 Gestire il service desk e gli incidenti

DS8.1 Service Desk

Stabilire una funzione di service desk, che è l'interfaccia per gli utenti con l'IT, per registrare, comunicare, distribuire e analizzare tutte le chiamate, gli incidenti registrati, le richieste di servizio e le richieste di informazioni. Dovrebbero essere definite procedure di monitoraggio e di escalation basati su livelli di servizio concordati relativamente ad un appropriato SLA che consenta la classificazione e la messa in priorità di ogni elemento registrato come un incidente, una richiesta di servizio o una richiesta di informazione. Misurare la soddisfazione degli utenti finali rispetto alla qualità del service desk e dei servizi IT.

DS8.2 Registrazione delle richieste dei clienti

Definire una funzione ed un sistema per consentire il log ed il tracciamento delle chiamate, degli incidenti, delle richieste di servizio e di informazioni. La funzione dovrebbe lavorare in modo congiunto con altri processi come la gestione degli incidenti, la gestione dei problemi, la gestione del cambiamento, la gestione della capacità e la gestione della disponibilità. Gli incidenti dovrebbero essere classificati secondo una priorità di business e di servizio e, se necessario, indirizzati all'appropriato gruppo di gestione dei problemi. Quando necessario gli utenti dovrebbero essere informati dello stato di avanzamento delle loro richieste.

DS8.3 Escalation degli incidenti

Definire e attuare le procedure di service desk in modo che gli incidenti che non possono essere risolti immediatamente siano indirizzati in modo appropriato secondo i limiti definiti negli SLA e se opportuno siano effettuati degli approfondimenti e suggerite le azioni alternative necessarie per ripristinare l'operatività. Assicurare che la proprietà ed il monitoraggio del ciclo di vita degli incidenti rimangano sotto il controllo del service desk per incidenti che coinvolgono gli utenti, indipendentemente dal gruppo IT che sta lavorando alla risoluzione del problema.

DS8.4 Chiusura degli incidenti

Stabilire procedure per monitorare in modo tempestivo la risoluzione delle richieste dei clienti. Quando l'incidente è stato risolto, il service desk dovrebbe registrare le fasi di risoluzione dello stesso e confermare che l'azione intrapresa è stata concordata con l'utente. Registrare e riportare incidenti non risolti (errori conosciuti ed approfondimenti) al fine di fornire informazioni per un'appropriata gestione dei problemi.

DS8.5 Reporting e Analisi dei trend

Produrre rapporti dell'attività di service desk per consentire alla Direzione di misurare la performance ed i tempi di risposta del servizio e di identificare i trend o i problemi ricorrenti in modo che il servizio possa venire continuamente migliorato.

Linee Guida per la Gestione

DS8 Gestire il service desk e gli incidenti

Da	Inputs
AI4	Manuali utenti, operativi, di supporto, tecnici ed amministrativi
AI6	Autorizzazioni alla modifica
AI7	Elementi di configurazione rilasciati
DS1	SLA e OLA
DS4	Soglie di incidente e di disastro
DS5	Definizione di incidenti di sicurezza
DS9	Dettagli di configurazione e asset IT
DS10	Problemi noti, errori noti e approfondimenti
DS13	Ticket di incidente

Outputs	A						
Richieste di servizio e richieste di modifica	AI6						
Rapporti sugli incidenti	DS10						
Rapporti di performance dei processi	ME1						
Rapporti di soddisfazione utenti	DS7	ME1					

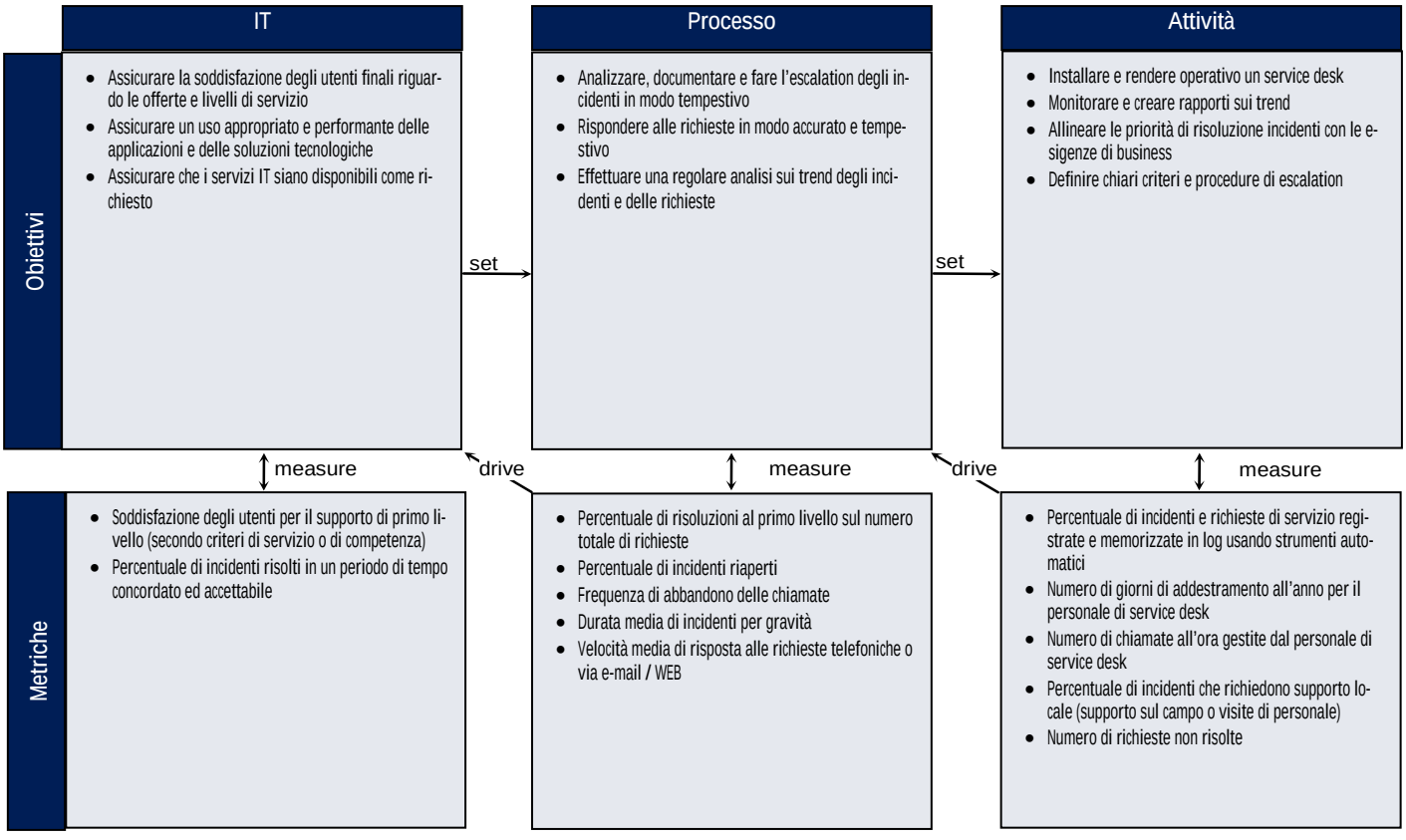
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Assistenza utenti/ Gestione incidenti
Creare una classificazione (severità e impatto) e procedure di escalation (funzionali e gerarchiche)				C	C	C	C	C	C		C	A/R
Individuare e registrare gli incidenti e le richieste di servizio e di informazioni												A/R
Classificare, analizzare e diagnosticare le richieste				I		C	C	C			I	A/R
Risolvere, ripristinare e chiudere gli incidenti					I	R	R	R			C	A/R
Informare gli utenti (ad esempio per gli aggiornamenti sullo stato della richiesta)				I	I							A/R
Produrre rapporti per la Direzione.	I			I	I	I			I		I	A/R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS8 Gestire il service desk e gli incidenti

Il grado di strutturazione del processo *Gestire il service desk e gli incidenti* che soddisfa i requisiti aziendali per l'IT di *abilitare un uso efficace dei sistemi assicurando la risoluzione e l'analisi delle richieste, delle domande e degli incidenti degli utenti finali.* è:

0 Non esistente quando

Non c'è supporto per rispondere alle richieste ed alle istanze degli utenti. Manca completamente un processo di gestione degli incidenti. L'organizzazione non riconosce che esiste un problema da gestire.

1 Iniziale/*Ad Hoc* quando

La Direzione ritiene che un processo, supportato da strumenti e da persone, sia necessario per rispondere alle richieste degli utenti e per gestire la risoluzione di incidenti. Non esiste tuttavia un processo standardizzato ed è fornito solo un supporto su base reattiva. La direzione non monitora le richieste degli utenti, gli incidenti o i trend. Non esiste un processo di escalation per assicurare la risoluzione dei problemi.

2 Ripetibile ma Intuitivo quando

Esiste la consapevolezza organizzativa del bisogno di una funzione di service desk e di un processo di gestione degli incidenti. L'assistenza è disponibile su base informale attraverso una rete di individui conosciuti. Questi individui hanno comuni strumenti per la risoluzione di in incidente. Non esiste formazione e comunicazione formale attraverso procedure standard, e la responsabilità è lasciata ai singoli individui.

3 Definito quando

L'esigenza di una funzione di service desk e di un processo di gestione incidenti è riconosciuto e accettato. Le procedure sono state standardizzate e documentate ed è definito un addestramento informale. Tuttavia è lasciata al singolo la scelta se essere addestrato e se seguire gli standard. Sono sviluppate elenchi di domande più frequenti (FAQ) e linee guida per l'utente, ma i singoli individui devono trovarle e possono non rispettarle. Le richieste e gli incidenti sono tracciati su base manuale e sono monitorate individualmente, ma non esiste un sistema formale di reportistica. La tempestività della risposta a domande e incidenti non è misurata e gli incidenti possono non essere risolti. Gli utenti hanno ricevuto una comunicazione chiara su dove e come registrare problemi e incidenti.

4 Gestito e Misurabile quando

Esiste una piena comprensione dei benefici di un processo di gestione degli incidenti a tutti i livelli dell'organizzazione e la funzione di service desk è stata definita in apposite unità organizzative. Gli strumenti e le tecniche sono automatizzate e vi è una funzione di gestione della conoscenza centralizzata. Il personale di service desk interagisce in modo stretto con il personale di gestione problemi. Le responsabilità sono chiare e l'efficacia è monitorata. Procedure per comunicare, scalare e risolvere gli incidenti sono definite e comunicate. Il personale di service desk è addestrato ed i processi sono migliorati attraverso l'uso di software specifici. La direzione ha sviluppato metriche per valutare le prestazioni del service desk.

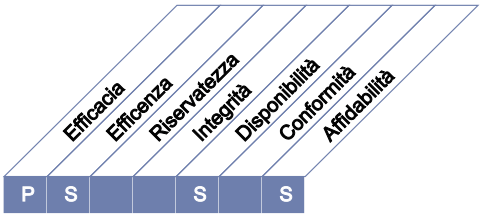
5 Ottimizzato quando

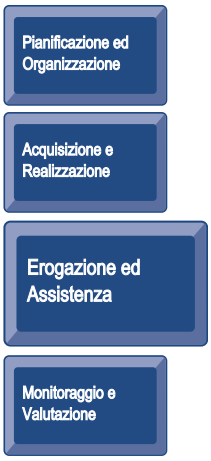
Il processo di gestione degli incidenti e la funzione di service desk sono definiti e ben organizzati e con un orientamento al servizio al cliente, in quanto sono conoscibili, focalizzati sul cliente e di aiuto. Le metriche sono sistematicamente misurate e rendicontate. Sono presenti FAQ comprensive e dettagliate che sono parte integrante della conoscenza sistematizzata. Sono utilizzati degli strumenti per consentire all'utente di individuare e risolvere gli incidenti. La consulenza è consistente e gli incidenti sono risolti velocemente con un processo di escalation strutturato. La Direzione utilizza uno strumento integrato per le statistiche sull'efficienza del processo di gestione degli incidenti e della funzione di service desk. I processi sono ottimizzati ad un livello di migliore prassi, in base ai risultati delle analisi degli indicatori di efficienza, di miglioramento continuo e di benchmark con altre organizzazioni.

DESCRIZIONE DEL PROCESSO

DS9 Gestire la configurazione

Assicurare l'integrità delle configurazioni hardware e software richiede che sia implementato ed aggiornato un repository delle configurazioni completo e accurato. Questo processo include la raccolta delle informazioni di configurazione iniziali, il consolidamento della configurazione in momenti precisi (schema base o baseline), la verifica e l'audit delle configurazioni e l'aggiornamento del repository di configurazione secondo necessità. Una gestione efficace delle configurazioni permette di ottenere una maggiore disponibilità dei sistemi, minimizza le problematiche relative alla produzione e risolve più rapidamente i problemi.





Il controllo del processo IT

Gestire la configurazione

che soddisfa i requisiti aziendali per l'IT di

ottimizzare l'infrastruttura, le risorse e le capacità IT, e la rendicontazione delle risorse IT

ponendo l'attenzione su

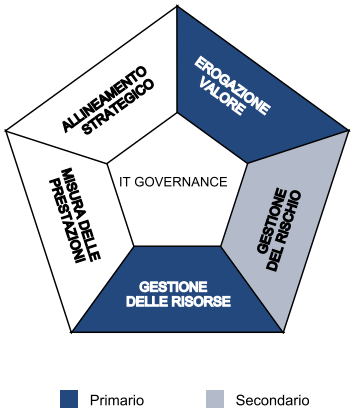
la realizzazione ed aggiornamento di un repository completo ed accurato contenente le caratteristiche della configurazione dei beni e delle baseline, e la comparazione di queste con l'attuale configurazione delle risorse

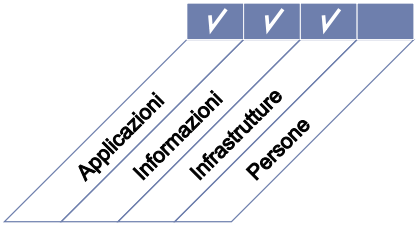
è ottenuto tramite

- la realizzazione di un repository centralizzato di tutti gli elementi di configurazione
- l'identificazione e l'aggiornamento di tutti gli elementi di configurazione
- la revisione dell'integrità dei dati di configurazione
-

e viene misurato tramite

- il numero di casi di problematiche di non conformità di business causati da configurazioni non corrette delle risorse
- il numero di difformità identificate tra le configurazioni attuali delle risorse e quelle presenti nel repository
- le percentuali di licenze acquisite e non registrate nel repository





OBIETTIVI DI CONTROLLO

DS9 Gestire la configurazione

DS9.1 Gestione del repository delle configurazioni e delle baseline

Definire uno strumento di supporto e un repository centralizzato che contenga tutte le informazioni rilevanti sugli elementi di configurazione. Monitorare e registrare tutte le risorse ed i cambiamenti alle stesse risorse. Dovrebbe essere gestito uno schema base (baseline) di elementi di configurazione per ogni sistema o servizio come punto di controllo a cui ritornare dopo le modifiche.

DS9.2 Identificazione ed aggiornamento degli elementi di configurazione

Stabilire procedure per supportare la gestione e la registrazione in log di tutti i cambiamenti nel repository delle configurazioni. Integrare queste procedure con quelle di gestione del cambiamento, gestione degli incidenti e dei problemi.

DS9.3 Revisione dell'integrità delle configurazioni

Rivedere in modo regolare gli elementi di configurazione per confermare e verificare l'integrità dei dati di configurazione attuali e storici. Rivedere periodicamente, rispetto alla politica di utilizzo del software, l'esistenza di qualsiasi software personale o senza licenza, o di ogni elemento di software in eccesso rispetto ai contratti di licenza attuali. Errori e difformità dovrebbero essere resi noti, documentati e corretti.

LINEE GUIDA PER LA GESTIONE

DS9 Gestire la configurazione

Da	Inputs
AI4	Manuali utenti, operativi, di supporto, tecnici ed amministrativi
AI7	Elementi di configurazione rilasciati
DS4	Criticità degli elementi di configurazione IT

Outputs	A						
Dettagli di configurazione IT delle risorse	DS8	DS10	DS13				
Richieste di modifica (dove e come applicare un correzione)	AI6						
Rapporti sulla performance del processo	ME1						

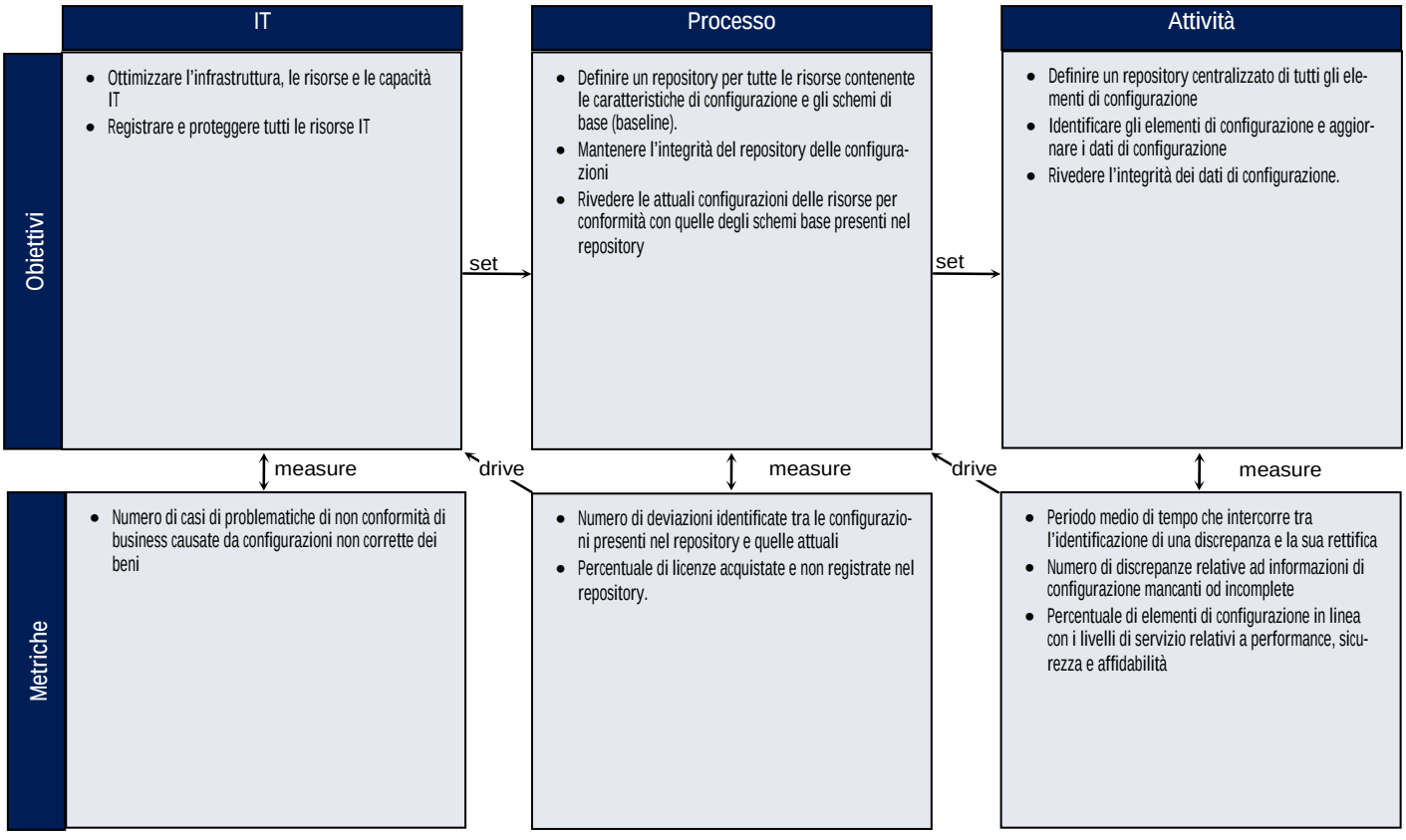
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Gestione configurazioni
Sviluppare procedure di pianificazione e gestione della configurazione					C	A	C	I	C		C	R
Raccogliere le informazioni iniziali di configurazione e stabilire degli elementi di base.						C	C	C			I	A/R
Verificare e revisionare le informazioni di configurazione (incluso l'individuazione di software non autorizzato)		I				A			I		I	A/R
Aggiornare il repository di configurazione.						R	R	R			I	A/R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS9 Gestire la configurazione

Il grado di strutturazione del processo *Gestire la configurazione* che soddisfa i requisiti aziendali per l'IT di *ottimizzare l'infrastruttura, le risorse e le capacità IT, e la rendicontazione delle risorse IT* è:

0 Non esistente quando

La Direzione non apprezza i benefici derivanti dall'adozione di un processo capace di rendicontare e gestire l'infrastruttura IT per le configurazioni sia hardware che software

1 Iniziale/*Ad Hoc* quando

L'esigenza di una gestione della configurazione è riconosciuta. Le attività di gestione delle configurazioni di base, come tenere aggiornati gli inventari di hardware e di software, sono svolte su base individuale. Non sono definite prassi standard.

2 Ripetibile ma Intuitivo quando

La Direzione è consapevole della necessità di controllare la configurazione IT e comprende i benefici di un'accurata e completa configurazione delle informazioni, ma esiste un implicito affidamento all'esperienza e la conoscenza del personale tecnico. Gli strumenti di gestione della configurazione sono impiegati solo fino ad un certo livello, ma sono differenti per piattaforma. Inoltre non sono definite prassi standard di lavoro. I dati di configurazione sono limitati e non utilizzati dai processi correlati, come la gestione del cambiamento e la gestione dei problemi.

3 Definito quando

Le procedure e le prassi di lavoro sono state documentate, standardizzate e comunicate, ma l'addestramento e l'applicazione di standard è lasciata ai singoli individui. Inoltre strumenti simili di gestione della configurazione sono implementati per piattaforme differenti. Le deviazioni dalle procedure hanno poca probabilità di essere individuate e verifiche fisiche sono svolte in modo inconsistente. Esiste qualche automazione in essere per tracciare le modifiche all'hardware e al software. I dati di configurazione sono usati dai processi correlati.

4 Gestito e Misurabile quando

L'esigenza di gestire la configurazione è riconosciuta a tutti i livelli dell'organizzazione e buone prassi sono in continua evoluzione. Procedure e standard sono comunicati e incorporati nell'addestramento e le deviazioni sono monitorate, tracciate e rendicontate. Strumenti automatici, come la push technology, sono utilizzati per far osservare gli standard e migliorare la stabilità. I sistemi di gestione della configurazione coprono la maggior parte delle risorse IT e permettono una gestione dei rilasci ed un controllo della distribuzione appropriati. Le analisi delle eccezioni, così come le verifiche fisiche, sono applicate in modo consistente e sono analizzate le principali cause dei problemi.

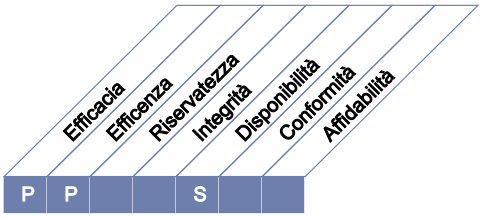
5 Ottimizzato quando

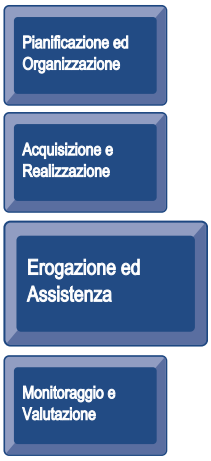
Tutte le risorse IT sono gestite in un sistema centrale di gestione della configurazione che contiene tutte le informazioni necessarie sui componenti, le loro relazioni e gli eventi. I dati di configurazione sono allineati con i cataloghi dei fornitori. Esiste una integrazione completa con i processi correlati, e questi utilizzano ed aggiornano i dati di configurazione in modo automatizzato. Rapporti di audit sullo schema base di configurazione forniscono dati essenziali su hardware e software per la riparazione, la gestione del servizio, la garanzia, l'aggiornamento e assessment tecnici di ogni unità individuale. Sono fatte osservare regole per limitare l'installazione di software non autorizzato. La Direzione effettua delle previsioni di riparazioni ed aggiornamenti sulla base dei rapporti di analisi che forniscono gli aggiornamenti programmati e gli adeguamenti delle capacità tecnologiche. Il tracciamento delle risorse ed il monitoraggio di risorse IT individuali consente la protezione da furti, utilizzo improprio e non autorizzato.

DESCRIZIONE DEL PROCESSO

DS10 Gestire i problemi

Una efficace gestione dei problemi richiede l'identificazione e la classificazione dei problemi, l'analisi delle cause di base e la risoluzione dei problemi. Il processo di gestione dei problemi include anche l'identificazione di raccomandazioni per il miglioramento, l'aggiornamento delle registrazioni dei problemi e la revisione dello stato delle azioni correttive. Un efficace processo di gestione dei problemi massimizza la disponibilità dei sistemi, migliora i livelli di servizio, riduce i costi e migliora la soddisfazione e la convenienza dei clienti.





Il controllo del processo IT

Gestire i problemi

che soddisfa i requisiti aziendali per l'IT di

assicurare la soddisfazione degli utenti finali relativamente all'offerta dei servizi ed ai livelli di servizio, e ridurre la soluzione di problemi e la presenza di difetti nei servizi erogati e ridurre le rilavorazioni

ponendo l'attenzione su

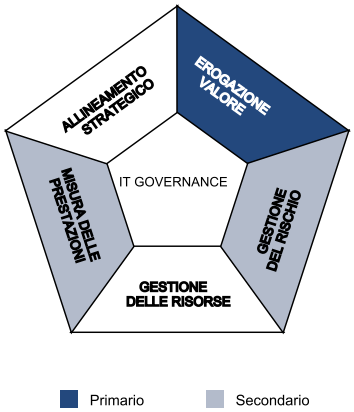
la registrazione, il tracciamento e la risoluzione dei problemi operativi; l'analisi delle cause principali di tutti i problemi significativi; la definizione delle soluzioni per i problemi operativi identificati

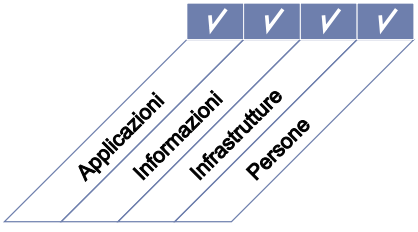
è ottenuto tramite

- l'analisi delle cause principali dei problemi registrati
- l'analisi dei trend
- l'assunzione di responsabilità per i problemi e degli avanzamenti della risoluzione degli stessi

e viene misurato tramite

- il numero di problemi ricorrenti con impatto sul business
- la percentuali di problemi risolti entro il periodo di tempo richiesto
- la frequenza dei rapporti o degli aggiornamenti ai problemi correnti, basati sulla severità dei problemi





OBIETTIVI DI CONTROLLO

DS10 Gestire i problemi

DS10.1 Identificazione e classificazione dei problemi

Implementare i processi per rendicontare e classificare i problemi che sono stati identificati come parte della gestione degli incidenti. I passi inerenti la classificazione dei problemi sono simili a quelli di classificazione degli incidenti; è necessario determinare la categoria, l'impatto, l'urgenza e la priorità. I problemi dovrebbero essere categorizzati in modo appropriato nell'ambito di gruppi o domini correlati (ad esempio hardware, software, software di supporto). Questi gruppi possono corrispondere alle responsabilità organizzative di utenti e clienti, e dovrebbero essere la base per allocare i problemi al personale di supporto.

DS10.2 Tracciamento e risoluzione dei problemi

Assicurare che il sistema di gestione dei problemi fornisca adeguati strumenti di audit trail che permettano di tracciare, analizzare e determinare le principali cause di tutti i problemi rendicontati considerando:
- tutti gli elementi di configurazione associati
- problemi e incidenti di grandi dimensioni
- errori conosciuti e sospettati
- tracciamento del trend dei problemi

Identificare ed attivare soluzioni sostenibili indirizzando le principali cause e le crescenti richieste di cambiamento attraverso il prestabilito processo di gestione del cambiamento. Attraverso il processo di risoluzione, il gestore dei problemi dovrebbe ottenere rapporti regolari dalla gestione delle modifiche sulla risoluzione di problemi ed errori. Il gestore dei problemi dovrebbe monitorare con continuità l'impatto dei problemi e degli errori conosciuti sui servizi agli utenti. Nel caso in cui questo impatto diventi critico, il gestore dei problemi dovrebbe scalare il problema, eventualmente comunicandolo ad un comitato appropriato per incrementare la priorità della richiesta di modifica (RFC) o se appropriata per implementare una modifica urgente. Il corso della risoluzione dei problemi dovrebbe essere monitorato tenendo in considerazione gli SLA.

DS10.3 Chiusura dei problemi

Mettere in opera una procedura per chiudere la registrazione di un problema o dopo la conferma di eliminazione con successo degli errori conosciuti o dopo l'accordo con il responsabile del processo utente su come gestire il problema in modo alternativo.

DS10.4 Integrazione della gestione della configurazione, degli incidenti e dei problemi

Integrare i processi correlati di gestione della configurazione, degli incidenti e dei problemi per assicurare una gestione efficace di problemi e rendere possibili i miglioramenti.

LINEE GUIDA PER LA GESTIONE

DS10 Gestire i problemi

Da	Inputs
AI6	Autorizzazione alle modifiche
DS8	Rapporti sugli incidenti
DS9	Dettagli di configurazione e degli asset IT
DS13	Log di errori

Outputs	A							
Richieste di modifica (dove e come applicare le correzioni)	AI6							
Registrazione dei problemi	AI6							
Rapporti di performance del processo	ME1							
Problemi conosciuti, errori conosciuti e azioni alternative	DS8							

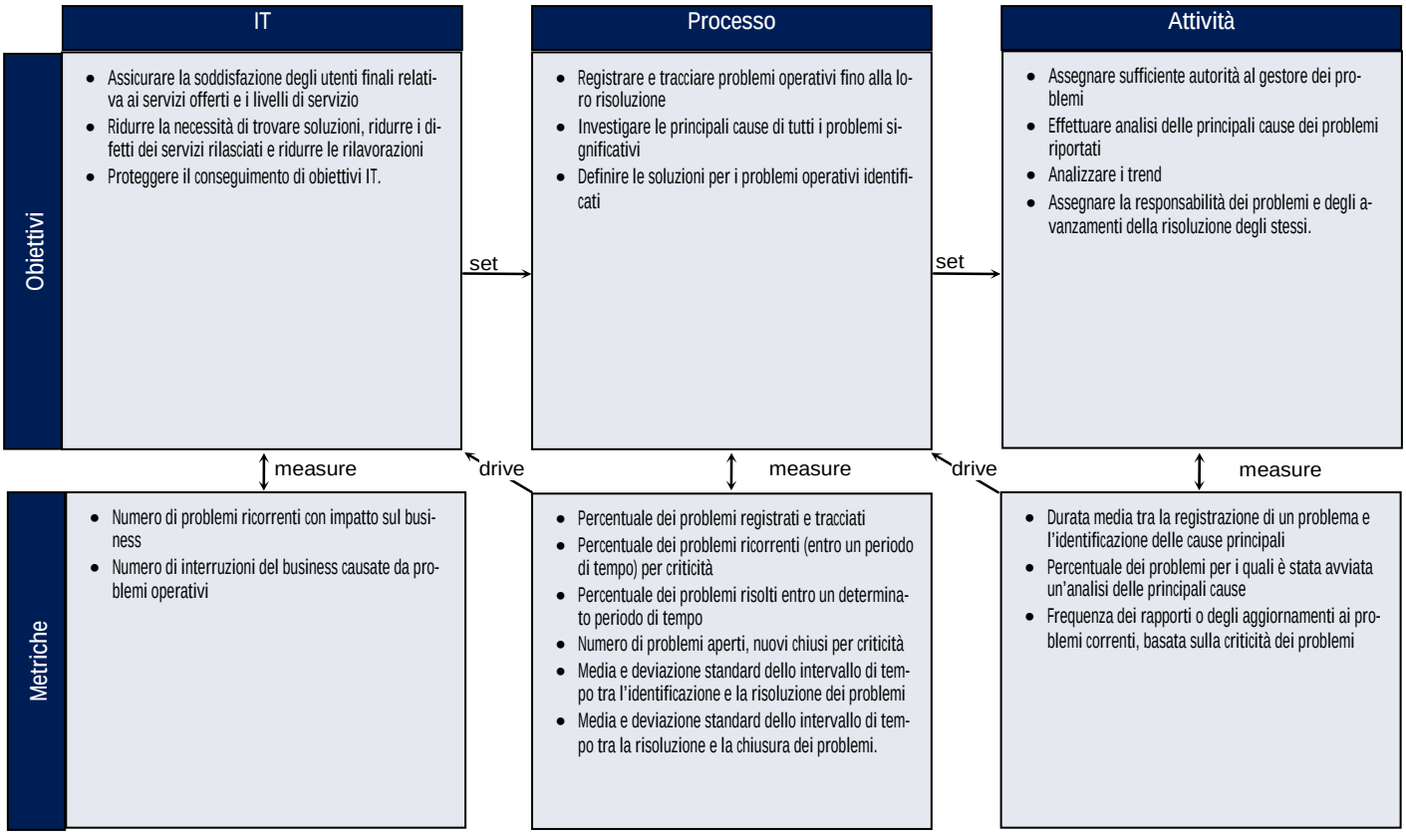
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process Owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Continuità, audit, rischio e sicurezza	Problem Manager
Identificare e classificare i problemi			I	I	C	A	C	C			I	R
Effettuare analisi delle cause principali						C		C				A/R
Risolvere i problemi					C	A	R	R		R	C	C
Rivedere lo stato dei problemi			I	I	C	A/R	C	C		C	C	R
Emettere raccomandazioni di miglioramento e creare una richiesta di modifica correlata					I	A	I	I		I		R
Aggiornare la registrazione dei problemi.					I	I		I			I	A/R

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS10 Gestire i problemi

Il grado di strutturazione del processo *Gestire i problemi* che soddisfa i requisiti aziendali per l'IT di *assicurare la soddisfazione degli utenti finali relativamente all'offerta dei servizi ed ai livelli di servizio, e ridurre la soluzione di problemi e la presenza di difetti nei servizi erogati e ridurre le rilavorazioni* è:

0 Non esistente quando

Non c'è una consapevolezza della necessità di gestire i problemi, così come non c'è differenziazione di problemi e incidenti. Perciò, a fronte degli incidenti non sono effettuate attività di identificazione delle cause.

1 Iniziale/*Ad Hoc* quando

Il personale riconosce il bisogno di gestire i problemi e risolvere le cause sottostanti. Individui chiave riconoscibili forniscono una certa assistenza per i problemi relativi alla loro area di pertinenza, ma la responsabilità della gestione dei problemi non è assegnata. L'informazione non è condivisa, con la conseguenza di creare problemi addizionali e di perdere tempo produttivo nella ricerca di risposte.

2 Ripetibile ma Intuitivo quando

Esiste un ampia consapevolezza dell'esigenza e dei benefici di gestire i problemi connessi all'IT all'interno sia delle unità di business sia della funzione relativa ai servizi informativi. Il processo di risoluzione dei problemi è evoluto ad un punto dove pochi individui chiave sono responsabili di identificare e risolvere i problemi. L'informazione è condivisa tra il personale in modo informale e reattivo. Il livello di servizio alla comunità degli utenti varia ed è vanificata da una insufficiente disponibilità della conoscenza strutturata per il gestore del problema.

3 Definito quando

L'esigenza di un sistema efficace ed integrato di gestione dei problemi è accettato ed evidenziato dal supporto della Direzione e sono disponibili budget per il personale e per la formazione. I processi di risoluzione e di escalation dei problemi sono stati standardizzati. La registrazione ed il tracciamento dei problemi e la loro risoluzione sono frammentati all'interno del team di risposta, utilizzando gli strumenti disponibili senza centralizzazione. Deviazioni dalle norme o dagli standard definiti hanno alta probabilità di non essere scoperti. L'informazione è condivisa tra il personale in modo proattivo e formale. La revisione della Direzione sugli incidenti e sull'analisi della identificazione e risoluzione dei problemi è limitata ed informale.

4 Gestito e Misurabile quando

Il processo di gestione dei problemi è compreso a tutti i livelli all'interno dell'organizzazione. Le responsabilità e la proprietà della gestione dei problemi sono chiare e definite. I metodi e le procedure sono documentati, comunicati e misurati per garantire l'efficacia. La maggior parte dei problemi sono identificati, registrati e riportati, ed è iniziata la risoluzione. La conoscenza e l'esperienza specifica sono coltivate, aggiornate e sviluppate ai più elevati livelli perché la funzione è vista come una risorsa e fornisce un contributo considerevole al conseguimento degli obiettivi IT ed al miglioramento dei servizi IT. La gestione dei problemi è bene integrata nei processi interrelati, come la gestione degli incidenti, dei cambiamenti, della disponibilità e della configurazione, ed assiste i clienti nel gestire i dati, le infrastrutture e l'operatività. Sono stati concordati obiettivi e metriche per il processo di gestione dei problemi.

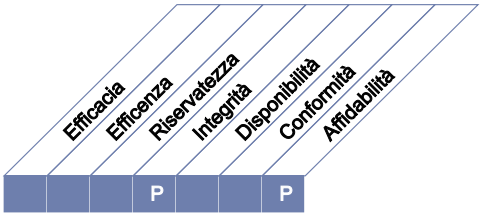
5 Ottimizzato quando

Il processo di gestione dei problemi è evoluto in modalità previdente e proattiva, contribuendo agli obiettivi IT. I problemi sono anticipati e prevenuti. La conoscenza riguardante gli elementi dei problemi passati e futuri è aggiornata attraverso contatti regolari con fornitori ed esperti. La registrazione, rendicontazione in rapporti e l'analisi dei problemi e la loro risoluzione sono automatizzati e completamente integrati nella gestione della configurazione dei dati. Gli obiettivi sono misurati in un modo consistente. La maggior parte dei sistemi sono dotati di meccanismi di individuazione automatica e di allerta, i quali sono tracciati e valutati in modo continuativo. Il processo di gestione dei problemi è analizzato per un miglioramento continuo basato sull'analisi delle metriche ed è oggetto di rendicontazione verso gli stakeholder.

DESCRIZIONE DEL PROCESSO

DS11 Gestire i dati

Una gestione efficace dei dati richiede l'identificazione dei requisiti dei dati stessi. Il processo di gestione dei dati comprende anche lo stabilire procedure efficaci per gestire la libreria dei supporti di memorizzazione, il salvataggio e il ripristino dei dati ed un'appropriata eliminazione dei supporti di memorizzazione. Un efficace processo di gestione dei dati aiuta ad assicurare la qualità, tempestività e la disponibilità dei dati aziendali.



Il controllo del processo IT

Gestire i dati

che soddisfa i requisiti aziendali per l'IT di

ottimizzare l'uso delle informazioni ed assicurare che le informazioni siano disponibili come richiesto

ponendo l'attenzione su

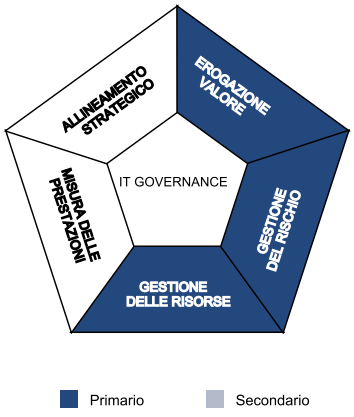
il mantenere la completezza, accuratezza, disponibilità e protezione dei dati

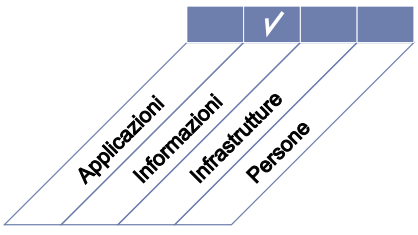
è ottenuto tramite

- il salvataggio dei dati ed i test di ripristino
- la gestione interna ed esterna del salvataggio dei dati
- l'eliminazione sicura di dati e supporti

e viene misurato tramite

- la percentuale di utenti soddisfatti per la disponibilità dei dati
- la percentuale di ripristini dei dati effettuati con successo
- il numero di incidenti nei quali i dati sensibili sono stati recuperati dopo l'eliminazione dei supporti di memorizzazione





OBIETTIVI DI CONTROLLO

DS11 Gestire i dati

DS11.1 Requisiti di business per la gestione dei dati

Verificare che tutti i dati richiesti per le elaborazioni siano ricevuti e processati completamente, accuratamente e tempestivamente, e tutti gli output siano distribuiti, coerentemente con i requisiti definiti dalle funzioni di business. Supportare adeguatamente i requisiti di riavvio delle elaborazioni e di rielaborazione dei dati.

DS11.2 Predisposizione di modalità operative per la memorizzazione e la conservazione dei dati

Definire e implementare procedure per una efficiente ed efficace memorizzazione, mantenimento e conservazione dei dati, al fine di raggiungere gli obiettivi aziendali ed essere conformi alla politica di sicurezza aziendale e alle normative.

DS11.3 Sistema di gestione della libreria dei supporti di memorizzazione

Definire e implementare procedure per mantenere un inventario dei supporti di memorizzazione e di conservazione ed assicurare la loro usabilità ed integrità.

DS11.4 Eliminazione

Definire e implementare procedure per assicurare che i requisiti di business per la protezione dei dati sensibili e del software siano soddisfatti quando i dati e l'hardware sono eliminati o trasferiti.

DS11.5 Salvataggio e Ripristino

Definire e implementare procedure per il salvataggio e il ripristino di sistemi, applicazioni, dati e documentazione in linea con i requisiti di business ed il piano di continuità.

DS11.6 Requisiti di sicurezza per la gestione dei dati

Definire ed implementare politiche e procedure per identificare ed attuare i requisiti di sicurezza applicabili in caso di ricezione, elaborazione, memorizzazione fisica ed output di dati al fine di raggiungere gli obiettivi aziendali ed essere conformi alla politica di sicurezza aziendale e alle normative.

LINEE GUIDA PER LA GESTIONE

DS11 Gestire i dati

Da	Inputs
PO2	Dizionario dei dati; classificazione dei dati definita
AI4	Manuali utente, operativi, di supporto tecnici e amministrativi
DS1	OLA
DS4	Piano di memorizzazione e protezione dei salvataggi
DS5	Piani e policy di sicurezza IT

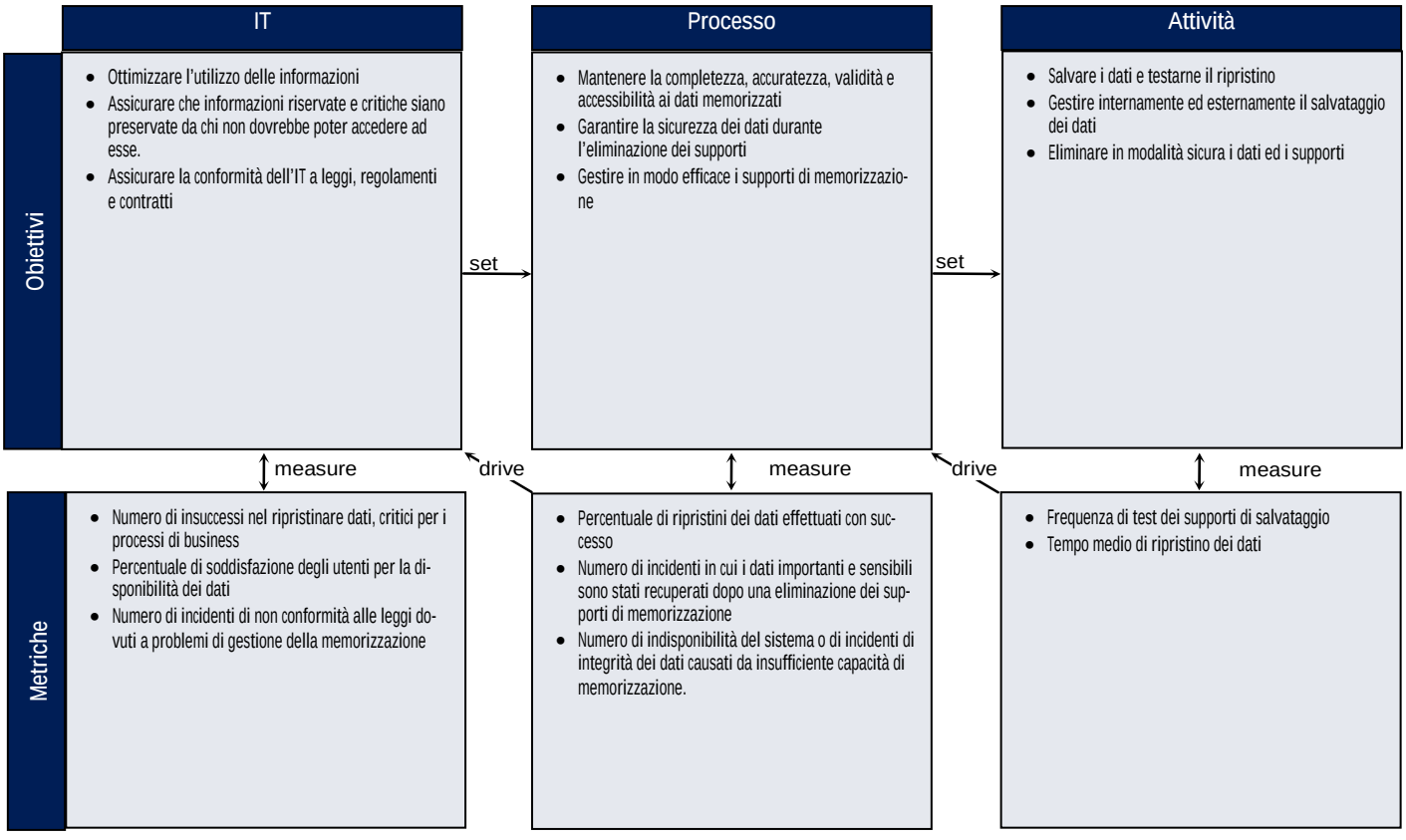
Outputs	A						
Rapporti sulla prestazione del processo	ME1						
Istruzioni operative per la gestione dati	DS13						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Tradurre i requisiti relativi alla memorizzazione e conservazione dei dati in procedure				A	I	C	R				C
Definire, aggiornare e implementare procedure per gestire la libreria dei supporti				A		R	C	C	I		C
Definire, aggiornare e implementare procedure per rendere sicura l'eliminazione di supporti e dei dispositivi				A	C	R			I		C
Salvare i dati secondo lo schema				A		R					
Definire, aggiornare e implementare procedure per il ripristino dei dati				A	C	R	C	C			I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS11 Gestire i dati

Il grado di strutturazione del processo *Gestire i dati* che soddisfa i requisiti aziendali per l'IT di *ottimizzare l'uso delle informazioni ed assicurare che le informazioni siano disponibili come richiesto* è:

0 Non esistente quando

I dati non sono riconosciuti come risorse e beni aziendali. Non è stata assegnata una proprietà dei dati o una responsabilità individuale per la gestione dei dati. La qualità e la sicurezza dei dati sono deboli o inesistenti.

1 Iniziale/*Ad Hoc* quando

L'azienda riconosce l'esigenza di una gestione accurata dei dati. Esiste un approccio ad hoc per specificare i requisiti di sicurezza per la gestione dei dati, ma non sono in essere procedure formali di comunicazione. Non è prevista alcuna formazione sulla gestione dei dati. La responsabilità della gestione dei dati non è chiara. Le procedure di salvataggio e ripristino e le modalità operative di eliminazione sono in essere.

2 Ripetibile ma Intuitivo quando

In ogni ambito dell'organizzazione c'è la consapevolezza dell'esigenza di una gestione dei dati efficace. La proprietà dei dati ad alto livello comincia a manifestarsi. I requisiti di sicurezza per la gestione dei dati sono documentati da personale chiave dell'organizzazione. Un monitoraggio all'interno dell'IT è effettuato sulle attività principali di gestione dei dati (es. salvataggio, ripristino, eliminazione). Le responsabilità per la gestione dei dati sono assegnate in modo informale al personale IT chiave.

3 Definito quando

L'esigenza di una gestione dei dati all'interno dell'IT e nell'organizzazione è compreso e accettato. La responsabilità per la gestione dei dati è definita. La proprietà dei dati è assegnata alla parte responsabile che ne controlla l'integrità e la sicurezza. Le procedure di gestione dei dati sono formalizzate all'interno dell'IT e sono utilizzati degli strumenti per il salvataggio e ripristino e per l'eliminazione dei dispositivi. Un monitoraggio è in essere per la gestione dei dati. Metriche di base sulle performance sono definite. L'addestramento del personale di gestione dei dati sta emergendo.

4 Gestito e Misurabile quando

La necessità di gestione dei dati è compreso e le azioni richieste sono accettate all'interno dell'organizzazione. Le responsabilità per la proprietà dei dati e per la gestione dei dati sono chiaramente definite, assegnate e comunicate all'interno dell'organizzazione. Le procedure sono formalizzate e ampiamente conosciute e la conoscenza condivisa. L'uso di strumenti sta emergendo. Gli indicatori di obiettivo e di prestazione sono concordati con i clienti e monitorati attraverso un processo ben definito. È presente un addestramento formale del personale per la gestione dei dati.

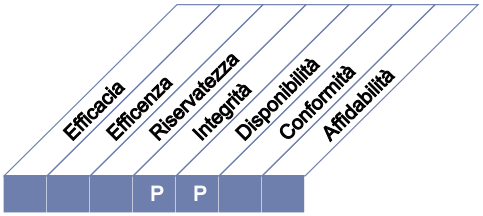
5 Ottimizzato quando

L'esigenza della gestione dei dati e la comprensione di tutte le azioni necessarie è compresa ed accettata all'interno dell'organizzazione. Le necessità ed i fabbisogni futuri sono esplorati in maniera proattiva. Le responsabilità per la proprietà dei dati e per la gestione dei dati sono chiaramente stabilite, ampiamente conosciute all'interno dell'organizzazione ed aggiornate in modo tempestivo. Le procedure sono formalizzate ed ampiamente conosciute, e la condivisione della competenza è una prassi standard. Strumenti sofisticati sono usati con il massimo dell'automazione della gestione dei dati. Gli indicatori di obiettivo e di efficienza sono concordati con i clienti, legati a obiettivi di business e monitorati in modo consistente usando processi ben definiti. Le opportunità di miglioramento sono costantemente esplorate. L'addestramento del personale di gestione dei dati è istituzionalizzato.

DESCRIZIONE DEL PROCESSO

DS12 Gestire l'ambiente fisico

La protezione dei dispositivi di elaborazione e delle persone richiede infrastrutture fisiche ben progettate e ben gestite. Il processo di gestione dell'ambiente fisico comprende la definizione dei requisiti del sito fisico, la scelta delle infrastrutture appropriate e la progettazione di processi efficaci per monitorare i fattori ambientali e la gestione degli accessi fisici. Una gestione efficace dell'ambiente fisico riduce le interruzioni dei processi di business causati da danni ai dispositivi di elaborazione ed al personale.



Il controllo del processo IT

Gestire l'ambiente fisico

che soddisfa i requisiti aziendali per l'IT di

proteggere le risorse di elaborazione e i dati di business e minimizzare i rischi di blocco ed interruzione del business

ponendo l'attenzione su

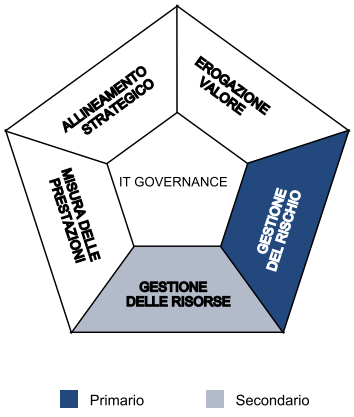
il fornire e mantenere un ambiente fisico adeguato a proteggere le risorse IT dall'accesso non desiderato, dal danneggiamento o dal furto

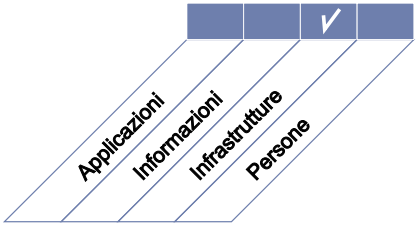
è ottenuto tramite

- l'implementazione di misure di sicurezza fisica
- la scelta e gestione delle infrastrutture

e viene misurato tramite

- il tempo di indisponibilità causato da incidenti nell'ambiente fisico
- il numero di incidenti dovuti a falle o debolezze di sicurezza fisica
- la frequenza delle valutazioni e delle revisioni del rischio fisico





OBIETTIVI DI CONTROLLO

DS12 Gestire l'ambiente fisico

DS12.1 Scelta e layout del sito fisico

Definire e scegliere i siti fisici per i dispositivi IT per supportare la strategia tecnologica connessa alla strategia di business. La scelta ed la progettazione della disposizione del sito fisico dovrebbe tenere conto del rischio associato ai disastri naturali e provocati dall'uomo, considerando leggi e regolamenti rilevanti come i regolamenti sulla salute fisica e sulla sicurezza dei lavoratori.

DS12.2 Misure di sicurezza fisica

Definire e implementare misure di sicurezza fisica in linea con i requisiti di business per rendere sicuri i locali e i beni fisici. Le misure di sicurezza fisica devono essere in grado di prevenire, identificare e mitigare efficacemente i rischi legati a furti, temperature, fuoco, fumo, acqua, terremoti, atti di vandalismo e di terrorismo, interruzioni dell'energia elettrica, prodotti chimici ed esplosivi.

DS12.3 Accesso fisico

Definire e implementare procedure per concedere, limitare e revocare gli accessi a locali, edifici ed aree secondo i requisiti di business incluse le emergenze. Gli accessi ai locali, edifici ed aree dovrebbero essere giustificati, autorizzati, registrati e monitorati. Questo si dovrebbe applicare a tutte le persone che entrano nei locali di edifici, incluso il personale dipendente, il personale temporaneo, i clienti, i fornitori, i visitatori od ogni altra terza parte.

DS12.4 Protezione contro fattori ambientali

Definire e implementare misure di protezione contro fattori ambientali. Installare dispositivi specializzati per monitorare e controllare l'ambiente.

DS12.5 Gestione delle infrastrutture fisiche

Gestire le infrastrutture, inclusi i dispositivi per l'energia e le comunicazioni, in linea con leggi e regolamenti, fabbisogni tecnici e di business, specifiche dei fornitori, e linee guida per garantire la salute e l'incolumità fisica.

LINEE GUIDA PER LA GESTIONE

DS12 Gestire l'ambiente fisico

Da	Inputs
PO2	Classificazione dei dati definita
PO9	Valutazione dei rischi
AI3	Requisiti dell'ambiente fisico

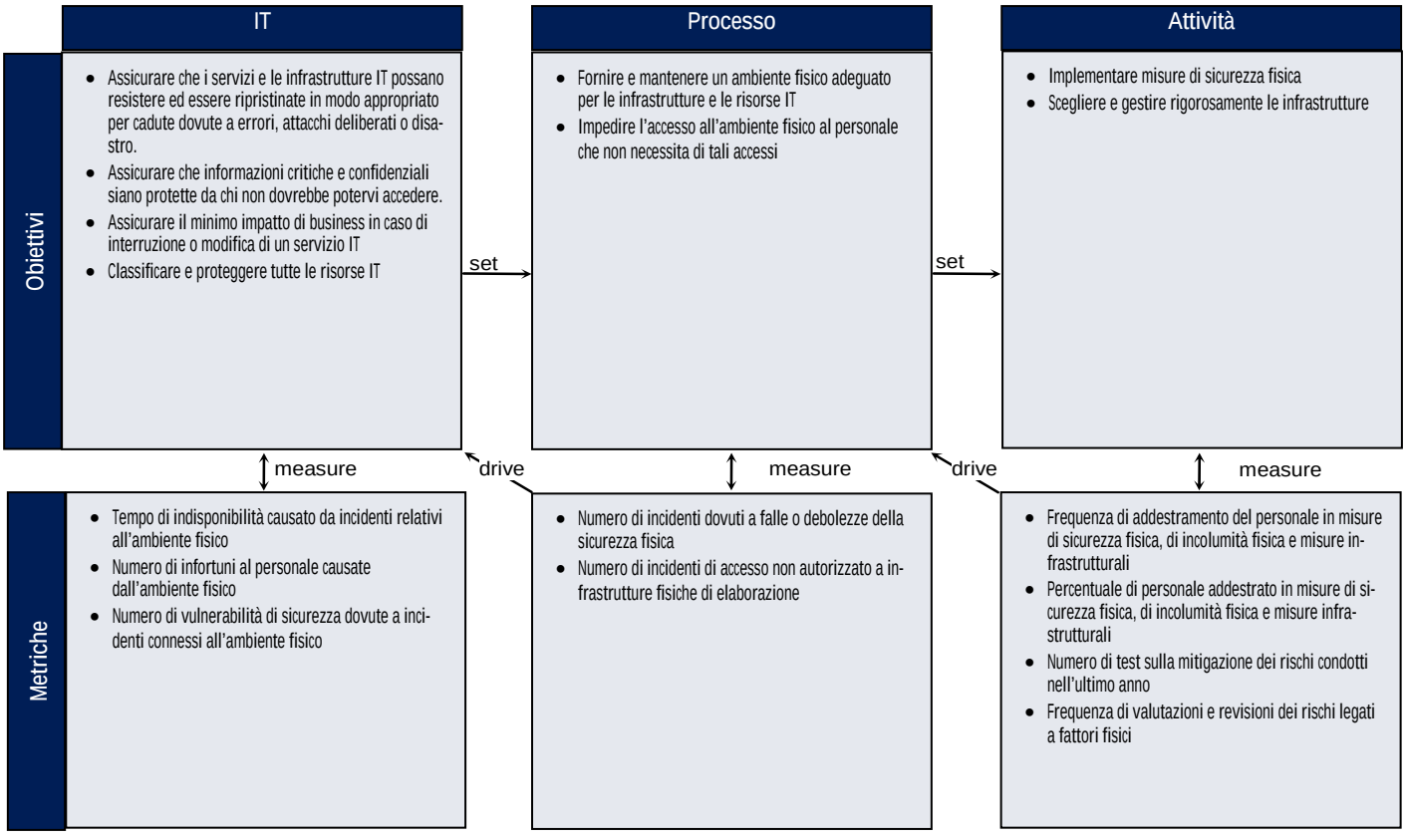
Outputs	A						
Rapporti sulle prestazioni del processo	ME1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire un livello di protezione fisica secondo i requisiti					C	A/R	C				C
Scegliere e commissionare il sito fisico (centro elaborazione dati, ufficio, ecc.)	I	C	C	C	C	A/R	C		C	C	C
Implementare misure fisico ambientali					I	A/R	I	I			C
Gestire l'ambiente fisico (incluso mantenimento, monitoraggio, e rendicontazione)						A/R	C				
Definire e implementare procedure per l'autorizzazione e l'aggiornamento dell'accesso fisico.				C	I	A/R	I	I	I		C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS12 Gestire l'ambiente fisico

Il grado di strutturazione del processo *Gestire l'ambiente fisico* che soddisfa i requisiti aziendali per l'IT di *proteggere le risorse di elaborazione e i dati di business e minimizzare i rischi di blocco ed interruzione del business* è:

0 Non esistente quando

Non c'è la consapevolezza dell'esigenza di proteggere le infrastrutture fisiche o gli investimenti in risorse elaborative. I fattori ambientali, inclusi protezione dal fuoco, polvere, energia, e eccessivo calore ed umidità, non sono né monitorate né controllate.

1 Iniziale/*Ad Hoc* quando

L'azienda riconosce come requisito del business di fornire un adeguato ambiente fisico che protegga le risorse e le persone contro eventi negativi naturali o causati dall'uomo. La gestione delle infrastrutture fisiche e dei dispositivi dipende dalla capacità personale e abilità di individui chiave. Le persone possono muoversi nelle infrastrutture fisiche senza restrizioni. La Direzione non monitora i controlli ambientali dell'infrastruttura fisica o i movimenti del personale.

2 Ripetibile ma Intuitivo quando

I controlli ambientali sono implementati e monitorati da personale operativo. La sicurezza fisica è un processo informale, guidato da un numero ristretto di impiegati che hanno un alto livello di preoccupazione per la sicurezza delle infrastrutture fisiche. Le procedure di manutenzione delle infrastrutture fisiche non sono ben documentate e si basano su buone prassi di pochi individui. Gli obiettivi di sicurezza fisica non sono basati su standard formali e la Direzione non assicura che gli obiettivi di sicurezza siano conseguiti.

3 Definito quando

L'esigenza di mantenere un ambiente fisico di elaborazione controllato è compresa e accettata all'interno dell'organizzazione. I controlli ambientali, la manutenzione preventiva e la sicurezza fisica sono elementi di budget approvati e tracciati dalla Direzione. Restrizioni di accesso sono applicate in modo che solo personale autorizzato abbia un accesso consentito alle infrastrutture fisiche di elaborazione. I visitatori sono registrati e scortati in base al tipo di individuo. Le infrastrutture fisiche sono di basso profilo e non identificabili in modo evidente. Le autorità civili monitorano la conformità con leggi e regolamenti sulla salute e l'incolumità fisica. I rischi sono assicurati con sforzo minimo per ottimizzare i costi assicurativi.

4 Gestito e Misurabile quando

L'esigenza di mantenere un ambiente fisico di elaborazione controllato è completamente compresa con evidenza fornita dalla struttura organizzativa e dall'allocazione di budget. I fabbisogni di sicurezza fisica ed ambientale sono documentati e l'accesso è strettamente controllato e monitorato. Le responsabilità e le assegnazioni di proprietà sono definite e comunicate. Il personale allocato alle infrastrutture fisiche è stato pienamente addestrato in situazioni di emergenza come anche a prassi per garantire la salute e la sicurezza personale. Meccanismi di controllo standardizzati sono in essere per limitare gli accessi alle infrastrutture e indirizzare i fattori ambientali e di sicurezza del personale. La Direzione monitora l'efficacia dei controlli e la conformità agli standard stabiliti. La Direzione ha stabilito obiettivi e metriche per misurare la gestione dell'ambiente fisico di elaborazione. La ripristinabilità delle risorse elaborative è incorporata all'interno di un processo organizzativo di gestione del rischio. L'informativa integrata è usata per ottimizzare la copertura assicurativa ed i relativi costi.

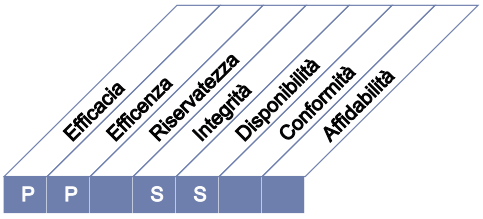
5 Ottimizzato quando

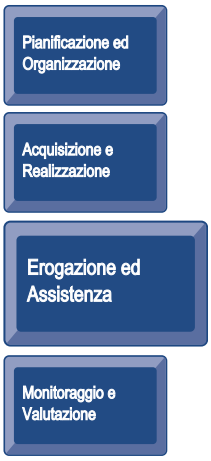
Esiste un piano condiviso di lungo termine per le infrastrutture necessarie a supportare l'ambiente fisico elaborativo dell'organizzazione. Sono definiti degli standard per tutte le infrastrutture fisiche, relativi alla scelta del sito, la costruzione, il controllo di guardia, la sicurezza fisica del personale, i sistemi meccanici ed elettrici e la protezione contro fattori ambientali (es. fuoco, esplosioni, allagamenti). Tutte la infrastrutture fisiche sono inventariate e classificate secondo il processo organizzativo corrente di gestione del rischio. L'accesso è strettamente controllato sulla base del fabbisogno lavorativo e monitorato continuamente e tutti i visitatori sono scortati tutte le volte. L'ambiente fisico è monitorato e controllato attraverso strumenti specializzati e le stanze dove sono presenti i dispositivi sono "gestiti senza la presenza fisica di personale". Gli obiettivi sono misurati e valutati in modo consistente. Programmi di manutenzione preventiva impongono un'aderenza stretta ad una pianificazione della manutenzione, e test regolari sono eseguiti su dispositivi importanti. Le strategie e gli standard di infrastruttura fisica sono allineate con gli obiettivi di disponibilità di servizio IT ed integrati con la pianificazione della continuità aziendale e con la gestione della crisi. La Direzione rivede e ottimizza su base continuativa le infrastrutture fisiche usando obiettivi e metriche, capitalizzando le opportunità di migliorare i contributi che può fornire al business.

DESCRIZIONE DEL PROCESSO

DS13 Gestire l'operatività

Una completa ed accurata elaborazione dei dati richiede un'efficace gestione dell'elaborazione dei dati e un'accurata manutenzione dell'hardware. Questo processo include la definizione di politiche e procedure operative per un'efficace gestione delle elaborazioni schedulate, la protezione di output con informazioni sensibili, il monitoraggio delle prestazioni infrastrutturali e la manutenzione preventiva dell'hardware. Una gestione efficace delle operazioni aiuta a mantenere l'integrità dei dati e riduce i ritardi di business ed i costi operativi dell'IT.





Il controllo del processo IT

Gestire l'operatività

che soddisfa i requisiti aziendali per l'IT di

mantenere l'integrità dei dati ed assicurare che l'infrastruttura IT possa resistere ed essere ripristinata dopo errori e guasti

ponendo l'attenzione su

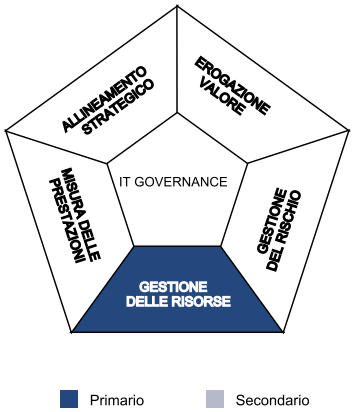
il conseguimento di livelli di servizio operativi (OLA) per l'elaborazione pianificata dei dati, la protezione gli output sensibili, il monitoraggio e la manutenzione dell'infrastruttura

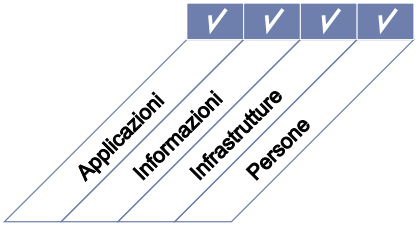
è ottenuto tramite

- un'operatività dell'ambiente IT in linea con i livelli di servizio concordati e le istruzioni definite
- la manutenzione dell'infrastruttura IT

e viene misurato tramite

- il numero di livelli di servizio impattati da incidenti operativi
- le ore di indisponibilità non pianificate e causate da incidenti operativi
- la percentuale di risorse hardware incluse nella manutenzione preventiva schedulata





OBIETTIVI DI CONTROLLO

DS13 Gestire l'operatività

DS13.1 Istruzioni e procedure operative

Definire, implementare e mantenere procedure standard per l'operatività IT ed assicurare che il personale IT sia a conoscenza di tutte le attività operative rilevanti. Le procedure operative dovrebbero coprire i cambi di turno (cambio formale di attività, aggiornamento sullo status, problemi operativi, procedure di escalation e rapporti sulle responsabilità correnti) per assicurare il raggiungimento dei livelli di servizio concordati e la continuità operativa.

DS13.2 Schedulazione dei job

Organizzare la schedulazione dei job, dei processi e delle attività nelle sequenze più efficienti, massimizzando il throughput e l'utilizzo delle risorse per soddisfare i requisiti definiti dal business.

DS13.3 Monitoraggio dell'infrastruttura IT

Definire e implementare procedure per monitorare l'infrastruttura IT e gli eventi correlati. Assicurare che una sufficiente informazione cronologica sia memorizzata in log operativi per consentire la ricostruzione, revisione ed esame delle sequenze temporali delle operazioni e le altre attività di contorno o di supporto alle operazioni.

DS13.4 Documenti sensibili e dispositivi di output

Definire e applicare appropriate tutele fisiche, prassi di rendicontazione e gestione dell'inventario per risorse IT sensibili come ad esempio moduli speciali, strumenti negoziabili, stampanti speciali o token di sicurezza.

DS13.5 Manutenzione preventiva dell'hardware

Definire ed implementare procedure per assicurare una manutenzione periodica dell'infrastruttura per ridurre la frequenza e l'impatto di guasti o un degrado delle prestazioni.

LINEE GUIDA PER LA GESTIONE

DS13 Gestire l'operatività

Da	Inputs
AI4	Manuali utente, operativo, di supporto, tecnico e amministrativo
AI7	Piani di passaggi in produzione, di rilascio e distribuzione del software.
DS1	SLA e OLA
DS4	Piano di esecuzione e protezione dei salvataggi.
DS9	Dettagli sulla configurazione/asset IT
DS11	Istruzioni operative per la gestione dei dati

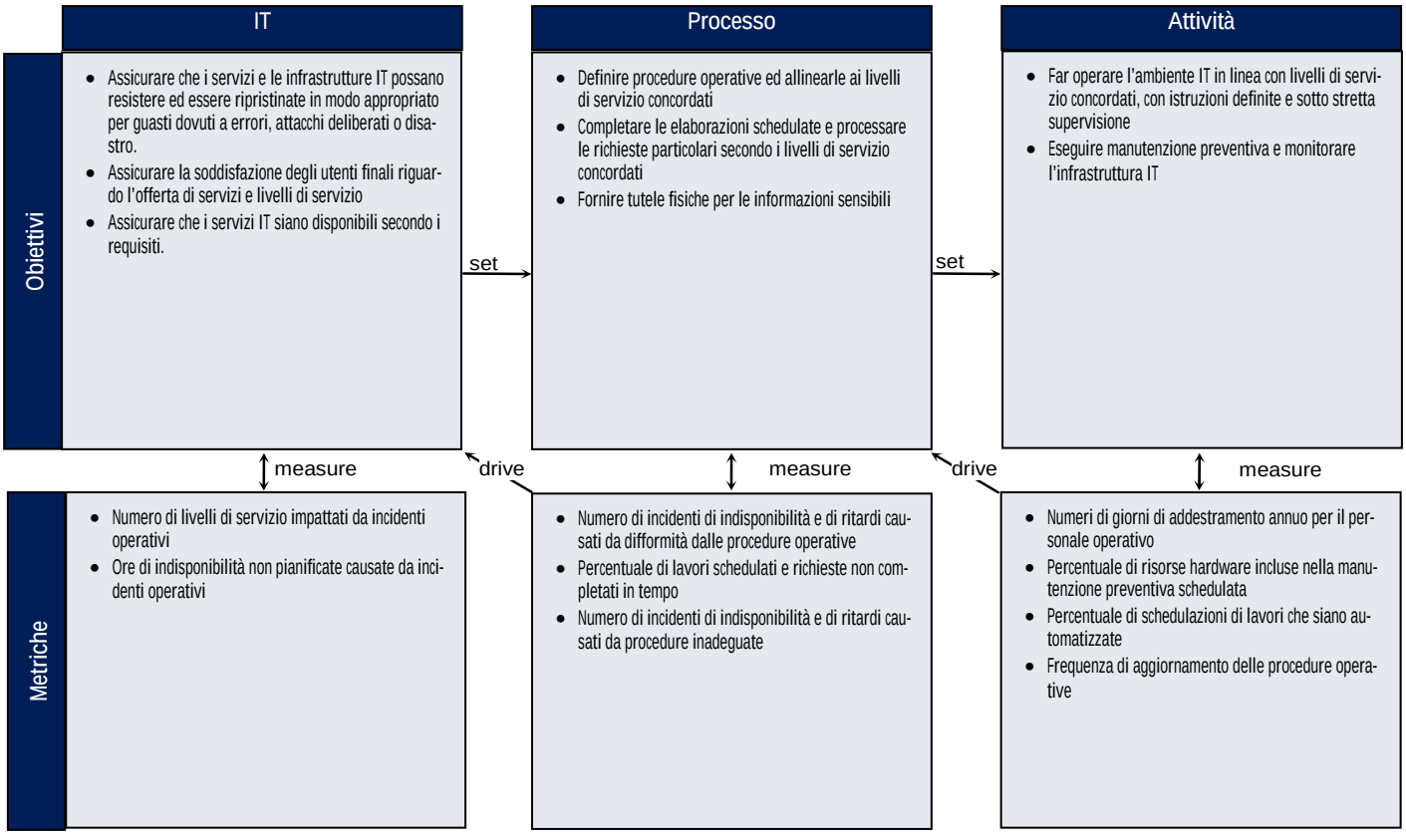
Outputs	A						
Ticket di incidenti	DS8						
Log di errori	DS10						
Rapporti sulle prestazioni del processo	ME1						

RACI Chart

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Creare/modificare le procedure operative (inclusi manuali, check list, piani di turno, documentazione operativa, procedure di escalation).						A/R					I
Schedulare i carichi elaborativi ed i job batch.					C	A/R	C	C			
Monitorare l'infrastruttura e l'elaborazione e risolvere i problemi.						A/R					I
Gestire e rendere sicuri gli output fisici (carta, supporti di memorizzazione, ecc.).						A/R					C
Applicare correzioni o modifiche alla schedulazione e all'infrastruttura.					C	A/R	C	C			C
Implementare un processo per salvaguardare i dispositivi di autenticazione contro interferenze, perdite o furti.				A		R			I		C
Schedulare ed effettuare una manutenzione preventiva.						A/R					

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

DS13 Gestire l'operatività

Il grado di strutturazione del processo *Gestire l'operatività* che soddisfa i requisiti aziendali per l'IT di *mantenere l'integrità dei dati ed assicurare che l'infrastruttura IT possa resistere ed essere ripristinata dopo errori e guasti* è:

0 Non esistente quando

L'azienda non dedica tempo e risorse per stabilire un supporto IT ed attività operative di base.

1 Iniziale/*Ad Hoc* quando

L'azienda riconosce l'esigenza di strutturare le funzioni di supporto IT. Poche procedure standard sono definite e le attività operative sono di natura reattiva. La maggior parte dei processi operativi sono schedulate informalmente e le richieste di elaborazioni sono accettate senza una validazione preventiva. Elaboratori, sistemi e applicazioni che supportano i processi di business sono frequentemente interrotti, ritardati ed indisponibili. Il personale perde tempo nell'attesa del ripristino di risorse. I supporti di memorizzazione degli output qualche volta si trovano in luoghi inaspettati o non si trovano del tutto.

2 Ripetibile ma Intuitivo quando

L'azienda è consapevole del ruolo chiave che le attività operative IT giocano nel fornire funzioni di supporto IT. È previsto un budget per acquisire strumenti, con un approccio "caso per caso". Le operazioni di supporto IT sono informali e intuitive. La dipendenza dagli skill e dalle capacità individuali è elevata. Le istruzioni di cosa fare, quando ed in quale ordine non sono documentate. Esiste un certo addestramento degli operatori ed esistono alcuni standard operativi formali.

3 Definito quando

L'esigenza della gestione delle operazioni è compresa ed accettata in azienda. Sono allocate risorse ed è effettuato un certo addestramento sul campo. Funzioni ripetitive sono formalmente definite, standardizzate, documentate e comunicate. Gli eventi e i risultati di attività completate sono registrate, con un scarsa reportistica per la Direzione. L'uso di strumenti di schedulazione automatica è introdotto per limitare l'intervento degli operatori. Controlli sono introdotti quando si aggiungono nuovi job all'operatività. Una politica formale è sviluppata per ridurre il numero di eventi non schedulati. Accordi di manutenzione e di servizio con i fornitori sono tuttora informali per natura.

4 Gestito e Misurabile quando

Le responsabilità per le operazioni di elaborazione e di supporto sono chiaramente definite e la proprietà del processo è assegnata. Le operazioni sono supportate attraverso budget per investimenti su capitale e risorse umane. L'addestramento è formalizzato e continuamente erogato. Le schedulazioni e le attività sono documentate e comunicate, sia all'interno della funzione IT sia ai clienti del business. Risulta possibile misurare e monitorare le attività giornaliere attraverso accordi standardizzati di efficienza e livelli di servizio stabiliti. Ogni scostamento da norme stabilite è velocemente affrontato e corretto. La direzione monitora l'uso delle risorse di elaborazione e il completamento dei lavori o delle attività assegnate. È presente uno sforzo continuo al fine di incrementare i livelli di automazione dei processi come modo per un miglioramento continuo. Una manutenzione formale e degli accordi di servizio sono definiti con i fornitori. Esiste un allineamento completo con i processi di gestione dei problemi, della capacità e della disponibilità, supportati da un'analisi delle cause degli errori e dei guasti.

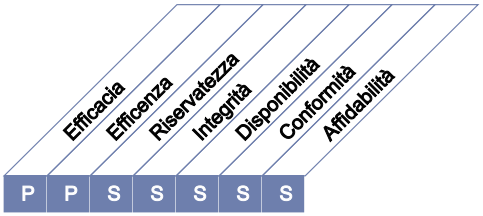
5 Ottimizzato quando

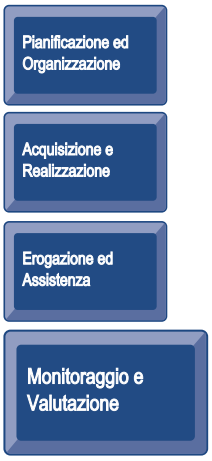
Le operazioni di supporto all'IT sono efficaci, efficienti e sufficientemente flessibili per conseguire il raggiungimento dei livello di servizio con minima perdita di produttività. I processi di gestione dell'operatività IT sono standardizzati e documentati sulla base delle competenze e sono soggetti a miglioramento continuo. I processi automatizzati che supportano i sistemi operano senza interruzioni e contribuiscono ad un ambiente operativo stabile. Tutti i problemi e le cadute elaborative sono analizzati per identificare le cause principali. Riunioni regolari con il personale per la gestione dei cambiamenti assicurano l'inclusione tempestiva di cambiamenti nelle schedulazioni di produzione. In collaborazione con i fornitori, i dispositivi sono analizzati riguardo ad obsolescenza ed a sintomi di malfunzionamento, la manutenzione è prevalentemente di natura preventiva.

DESCRIZIONE DEL PROCESSO

ME1 Monitorare e valutare le prestazioni dell'IT

Una gestione efficace delle prestazioni IT richiede un processo di monitoraggio. Tale processo comprende la definizione dei più importanti indicatori di prestazione, una informativa sistematica e tempestiva alla Direzione sulle prestazioni rilevate, l'individuazione di interventi solleciti in caso di scostamenti. Il monitoraggio è necessario per assicurarsi che siano adottate le giuste azioni e che esse siano in linea con le indicazioni e le politiche aziendali stabilite.





Il controllo del processo IT

Monitorare e valutare le prestazioni dell'IT

che soddisfa i requisiti aziendali per l'IT di

trasparenza e comprensione dei costi IT, dei benefici attesi, della strategia, delle politiche e dei livelli di servizio secondo quanto stabilito dai requisiti di governance aziendale

ponendo l'attenzione su

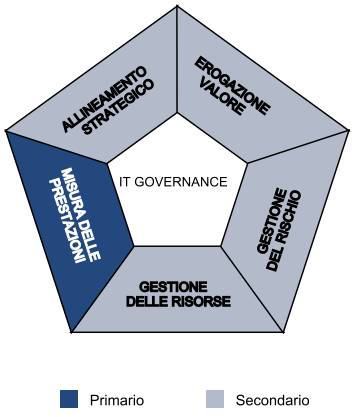
le metriche del processo di monitoraggio e di reporting e la individuazione e l'implementazione di azioni per il miglioramento delle prestazioni

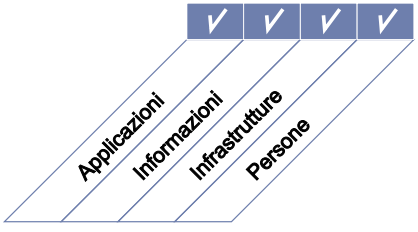
è ottenuto tramite

- il processo di raccolta delle informazioni sulle prestazioni e la loro traduzione in report per la Direzione
- la revisione delle prestazioni rispetto agli obiettivi concordati e l'avvio delle opportune azioni correttive

e viene misurato tramite

- la soddisfazione della Direzione e delle entità/comitati di governo dell'impresa delle informazioni disponibili sulle prestazioni dei processi IT dell'azienda
- il numero di azioni di miglioramento indotte dall'attività di monitoraggio
- la percentuale di processi critici monitorati





OBIETTIVI DI CONTROLLO

ME1 Monitorare e valutare le prestazioni dell'IT

ME1.1 Approccio al monitoraggio

Definire un quadro di riferimento e un approccio generale al monitoraggio, che stabilisca l'ambito, la metodologia e il processo da seguire per monitorare il contributo dell'IT ai risultati aziendali, alla erogazione di servizi e soluzioni. Integrare il quadro di riferimento con il sistema aziendale di misurazione delle prestazioni.

ME1.2 Definizione e raccolta di dati per il monitoraggio

Di concerto con le altre funzioni aziendali, definire un insieme bilanciato di obiettivi e farlo approvare dalle funzioni aziendali non-IT e dai principali stakeholder. Definire dei benchmark con cui confrontare gli obiettivi e identificare i dati disponibili per essere raccolti ed elaborati per misurare il raggiungimento degli obiettivi stessi. Definire i processi di misurazione in modo da poter raccogliere tempestivamente e accuratamente i dati per riferire sui progressi conseguiti rispetto agli obiettivi.

ME1.3 Metodo di monitoraggio

Identificare e tradurre operativamente un metodo di monitoraggio delle prestazioni (es. cruscotto aziendale o balanced scorecard) per registrare i risultati raggiunti e le misure effettuate, per fornire una sintetica vista complessiva delle prestazioni IT; il metodo deve essere in sintonia con il sistema di monitoraggio aziendale.

ME1.4 Valutazione delle prestazioni

Revisionare periodicamente le prestazioni rispetto agli obiettivi, effettuare un'analisi delle cause di ogni scostamento e avviare azioni correttive per rimuovere le cause stesse. Ogniqualvolta richiesto, effettuare un'analisi delle cause sulla base degli scostamenti.

ME1.5 Reporting ai vertici aziendali e al consiglio di amministrazione

Fornire analisi ai vertici aziendali per consentire loro di effettuare una valutazione del contributo dell'IT al perseguimento degli obiettivi aziendali, in particolare per quanto riguarda le prestazioni dei servizi/prodotti offerti dall'azienda, le iniziative di investimento facilitate dall'IT, i livelli di efficacia delle singole iniziative per l'erogazione del servizio e delle soluzioni. Inserire nelle analisi il grado di raggiungimento degli obiettivi pianificati, la quota di utilizzo del budget, gli obiettivi di prestazione raggiunti e i rischi mitigati. Anticipare la verifica della Direzione suggerendo le azioni correttive che riducano i principali scostamenti. Fornire il reporting alla Direzione, sollecitare un feedback dalla valutazione dei responsabili.

ME1.6 Azioni correttive

Identificare e avviare azioni correttive basate sul monitoraggio, sulle valutazioni e sui report riguardanti le prestazioni. Questo comprende il follow-up di tutti i monitoraggi, di tutte le valutazioni e di tutte le analisi, attraverso:

- la verifica, la negoziazione e la conferma delle risposte del management
- l'assegnazione delle responsabilità per le azioni correttive
- la tracciatura dei risultati delle azioni per cui il management si è impegnato.

LINEE GUIDA PER LA GESTIONE

ME1 Monitorare e valutare le prestazioni dell'IT

Da	Inputs
PO5	Analisi dei costi e dei benefici
PO10	Valutazione delle prestazioni dei progetti
AI6	Report sullo stato delle richieste di modifica
DS1-13	Analisi delle prestazioni dei processi
DS3	Piano delle performance e delle prestazioni (requisiti)
DS8	Analisi della soddisfazione degli utenti
ME2	Valutazione sull'efficacia dei controlli IT
ME3	Valutazione della conformità ai requisiti di legge e delle norme interne per le attività IT
ME4	Valutazione dello stato della governance del sistema informativo aziendale

Outputs	A						
Input alla pianificazione IT relativamente alle prestazioni	PO1	PO2	DS1				
Piani delle azioni correttive	PO4	PO8					
Eventi e serie storiche relativi ai rischi	PO9						
Analisi delle prestazioni dei processi	ME2						

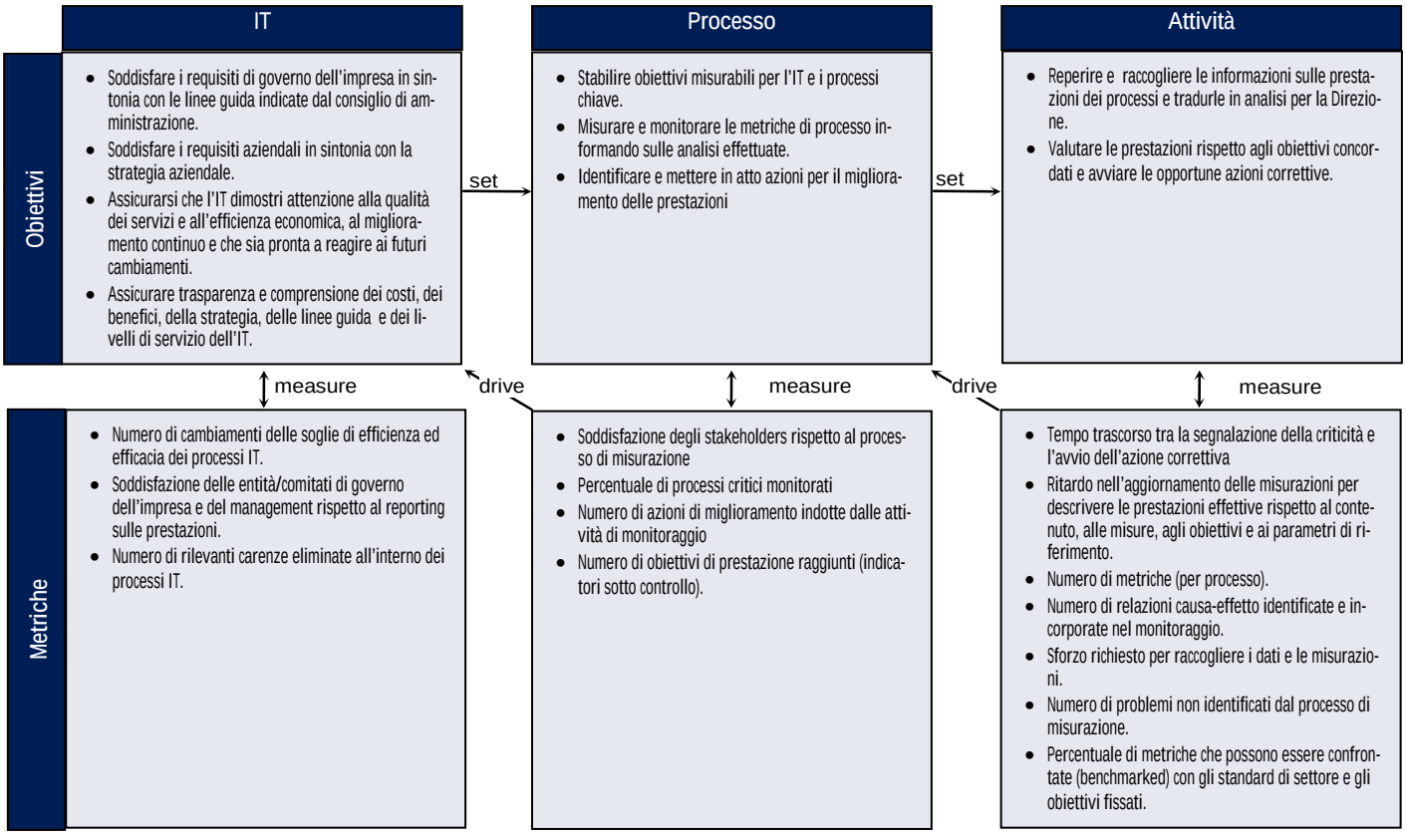
RACI Chart

Ruoli

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Definire l'approccio al monitoraggio		A	R	C	R	I	C	I	C	I		C
Identificare e raccogliere dati relativi a obiettivi misurabili che supportano gli obiettivi aziendali		C	C	C	A	R	R		R			
Creare cruscotti aziendali (scorecards)					A		R	C	R	C		
Misurare le prestazioni			I	I	A	R	R	C	R	C		
Analizzare le prestazioni	I	I	I	R	A	R	R	C	R	C		I
Identificare e monitorare le azioni di miglioramento delle prestazioni					A	R	R	C	R	C		C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME1 Monitorare e valutare le prestazioni dell'IT

Il grado di strutturazione del processo *Monitorare e valutare le prestazioni dell'IT* che soddisfa i requisiti aziendali per l'IT di *trasparenza e comprensione dei costi IT, dei benefici attesi, della strategia, delle politiche e dei livelli di servizio secondo quanto stabilito dai requisiti di governance aziendale* è:

0 Non esistente quando

L'organizzazione non dispone di processi di monitoraggio. L'IT non effettua autonomamente il monitoraggio di progetti e processi. Non sono disponibili informazioni utili, tempestive e accurate. Non è riconosciuta la necessità di obiettivi di processo definiti chiaramente.

1 Iniziale/*Ad Hoc* quando

La Direzione riconosce la necessità di raccogliere e valutare informazioni sul monitoraggio dei processi. Non sono stati identificati processi standard di raccolta e valutazione. Il monitoraggio è implementato e le metriche sono scelte caso per caso, in funzione delle necessità di specifici progetti e processi IT. Il monitoraggio è di norma attivato in reazione ad un incidente che ha causato una qualche perdita o imbarazzo all'Azienda. L'amministrazione svolge un monitoraggio delle misure economico - finanziare di base per l'IT.

2 Ripetibile ma Intuitivo quando

Sono stati identificati gli indicatori di base da monitorare. Esistono metodi e tecniche di raccolta e verifica, ma tali processi non sono stati adottati in tutta l'Azienda. L'analisi e l'interpretazione dei risultati dell'attività di monitoraggio si basano sulla competenza di individui chiave. Vengono identificati ed implementati strumenti limitati per la raccolta di informazioni, ma la raccolta delle informazioni non prevede un approccio strutturato.

3 Definito quando

La Direzione ha comunicato ed istituzionalizzato processi standard di monitoraggio. Sono stati attivati programmi di istruzione e formazione per il monitoraggio. È stata sviluppata una base di dati strutturata di informazioni sulle prestazioni storiche. Le valutazioni si riferiscono ancora a singoli processi o progetti IT e non esiste una visione complessiva e integrata tra tutti i processi. Sono stati definiti strumenti per il monitoraggio dei processi IT interni e per la misurazione dei livelli di servizio. Sono state definite metriche per la misurazione del contributo della funzione Sistemi Informativi alle prestazioni dell'Azienda, utilizzando criteri tradizionali di tipo sia economico - finanziario sia operativo. Sono state definite misurazioni delle prestazioni specifiche dell'IT, misurazioni non di tipo economico - finanziario, misurazioni dell'impatto strategico dell'IT, misurazioni della soddisfazione dei clienti e i livelli di servizio. È stato definito un modello per la misurazione delle prestazioni.

4 Gestito e Misurabile quando

La Direzione ha definito i limiti di tolleranza entro i quali devono operare i processi. Si sta standardizzando e normalizzando il reporting sui risultati del monitoraggio. Sono state integrate le metriche fra tutti i progetti e processi IT. I sistemi di monitoraggio aziendali per l'informativa della Direzione IT sono formalizzati. In tutta l'Azienda sono stati attivati e integrati strumenti automatizzati per raccogliere e monitorare informazioni operative sul portafoglio delle applicazioni, sui sistemi e sui processi IT. La Direzione è in grado di valutare le prestazioni sulla base di criteri concordati e approvati dagli stakeholder. Le misure della funzione IT sono allineate con gli obiettivi aziendali.

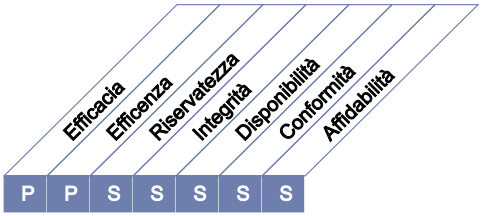
5 Ottimizzato quando

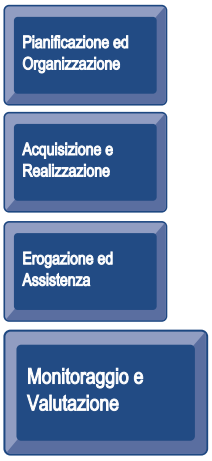
È stato sviluppato un processo di miglioramento continuo della qualità per aggiornare gli standard e le politiche di monitoraggio dell'intera organizzazione al fine di incorporare le migliori pratiche di settore. Tutti i processi di monitoraggio sono ottimizzati e supportano gli obiettivi dell'intera Azienda. Le metriche derivate dal core business sono usate correntemente per misurare le prestazioni e sono integrate in un quadro di riferimento per il monitoraggio strategico quale, ad esempio, l'IT Balanced Scorecard. Il monitoraggio e la continua riprogettazione dei processi sono coerenti con i piani di miglioramento dei processi di business dell'intera Azienda. Il confronto con il mercato e con i concorrenti di riferimento è effettuato con modalità formalizzate e con criteri di comparazione ben compresi.

DESCRIZIONE DEL PROCESSO

ME2 Monitorare e valutare i controlli interni

La realizzazione di un efficace programma di controllo interno per l'IT richiede un processo di monitoraggio ben definito. Tale processo riguarda il monitoraggio e l'informativa sulle eccezioni ai controlli, sui risultati delle autovalutazioni, sulle verifiche di terze parti. Un importante beneficio prodotto dal monitoraggio dei controlli interni è costituito dalla garanzia (assurance) riguardo l'efficienza e l'efficacia delle operazioni e la conformità a leggi e regolamenti.





Il controllo del processo IT

Monitorare e valutare i controlli interni

che soddisfa i requisiti aziendali per l'IT di

tutelare il raggiungimento degli obiettivi IT ed essere conformi alle leggi, ai regolamenti relativi all'IT ed ai contratti in essere

ponendo l'attenzione su

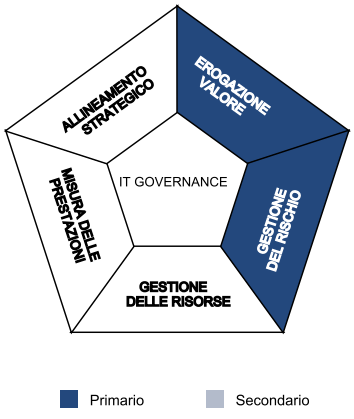
l'attività di verifica dei processi di controllo interno per le attività relative all'IT e sull'individuazione delle azioni di miglioramento

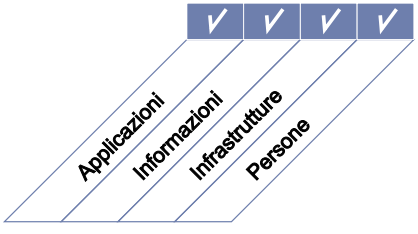
è ottenuto tramite

- la definizione di un sistema di controllo interno inserito nella struttura dei processi IT
- il monitoraggio e le segnalazioni sull'efficacia dei controlli interni IT
- il reporting alla Direzione sulle eccezioni ai controlli per consentire l'avvio delle azioni correttive

e viene misurato tramite

- numero di violazioni significative ai controlli
- numero di iniziative di miglioramento dei controlli
- numero e copertura delle iniziative di autovalutazione dei controlli





OBIETTIVI DI CONTROLLO

ME2 Monitorare e valutare i controlli interni

ME2.1 Valutazione del modello del sistema di controllo interno

Monitorare in modo continuo, effettuare benchmark e migliorare il sistema di controllo interno IT e il modello dei controlli per facilitare il raggiungimento degli obiettivi aziendali.

ME2.2 Controlli di supervisione

Monitorare e valutare l'efficacia e l'efficienza della verifica, da parte della management IT, sui controlli interni.

ME2.3 Eccezioni ai controlli

Registrare le informazioni riguardanti tutte le eccezioni ai controlli e assicurarsi che sia svolta un'analisi delle cause sottostanti. Le eccezioni debbono essere riportate ai livelli organizzativi superiori ove necessario e ove opportuno ai diversi stakeholder. Avviare le necessarie azioni correttive.

ME2.4 Attività di controllo promosse autonomamente (Self – assessment)

Valutare la completezza e l'efficacia dei controlli interni sui processi, sulle procedure e sui contratti dell'IT attraverso un programma continuo di autovalutazione.

ME2.5 Garanzie (Assurance) sui controlli interni

Ottenere, quando necessario, ulteriori garanzie (assurance) sulla completezza e sull'efficacia dei controlli interni attraverso verifiche svolte da terzi.

ME2.6 Controllo interno presso terze parti

Valutare lo stato del sistema di controllo interno di ogni terza parte fornitrice di servizi. Assicurarsi che il fornitore di servizi esterno sia conforme alle leggi e ai regolamenti e alle obbligazioni contrattuali.

ME2.7 Azioni correttive

Identificare, avviare e monitorare azioni correttive basate sulle analisi e valutazioni dei controlli.

LINEE GUIDA PER LA GESTIONE

ME2 Monitorare e valutare i controlli interni

Da	Inputs
ME1	Analisi delle prestazioni dei processi
AI7	Monitoraggio dei controlli interni

Outputs	A						
Informativa sull'efficacia dei controlli IT	PO4	PO6	ME1	ME4			

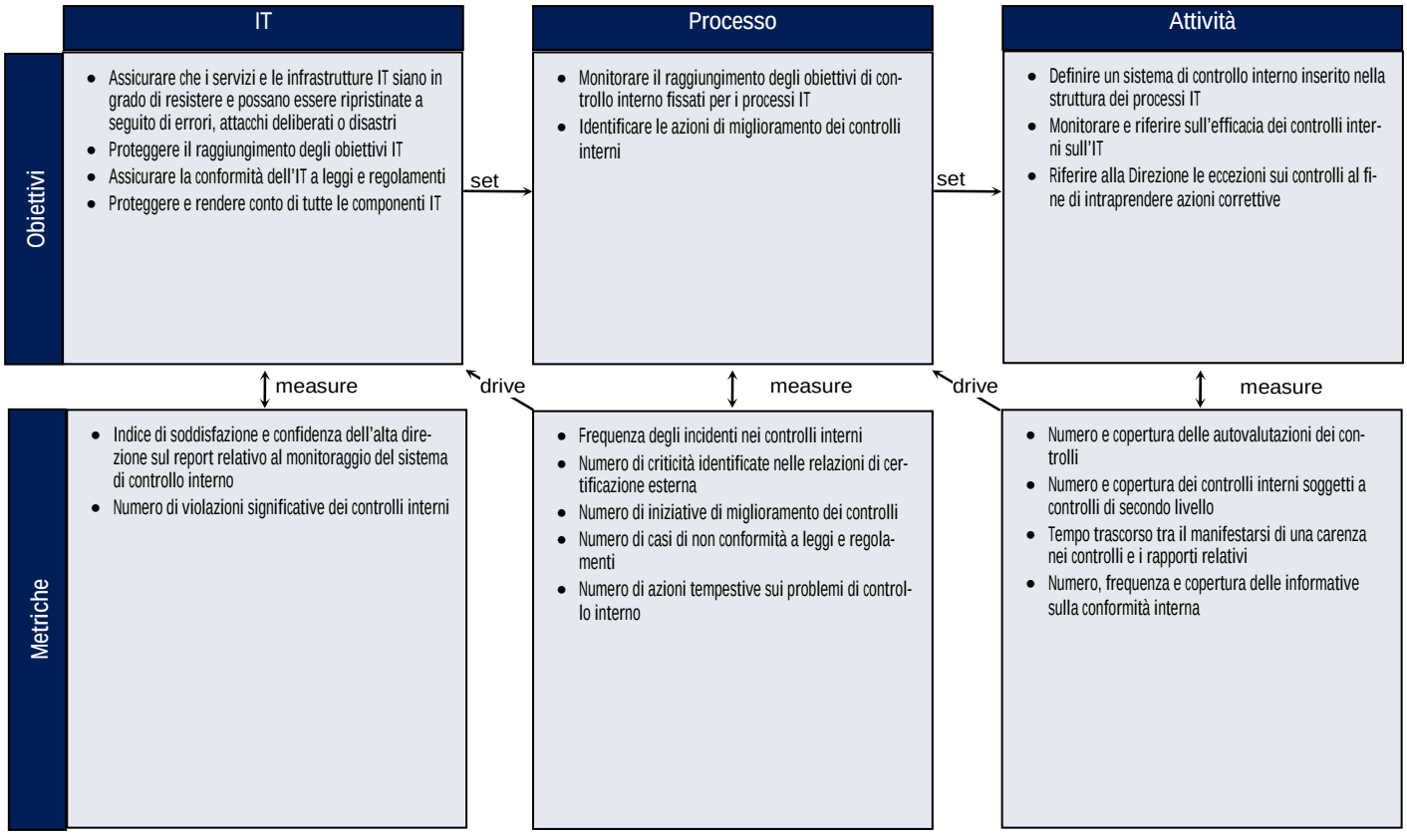
RACI Chart

Ruoli

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Monitorare e controllare le attività di controllo interno sull'IT					A		R		R	R		R
Monitorare il processo di autovalutazione				I	A		R		R	R		C
Monitorare le prestazioni di verifiche indipendenti, audit e ispezioni				I	A		R		R	R		C
Monitorare il processo per ottenere garanzia sui controlli operati da terze parti		I	I	I	A		R		R	R		C
Monitorare il processo per identificare e valutare le eccezioni ai controlli		I	I	I	A	I	R		R	R		C
Monitorare il processo per identificare e correggere le eccezioni ai controlli		I	I	I	A	I	R		R	R		C
Riferire alle parti interessate (key stakeholders)	I	I	I		A/R							I

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME2 Monitorare e valutare i controlli interni

Il grado di strutturazione del processo *Monitorare e valutare i controlli interni* che soddisfa i requisiti aziendali per l'IT di *tutelare il raggiungimento degli obiettivi IT ed essere conformi alle leggi, ai regolamenti relativi all'IT ed ai contratti in essere* è:

0 Non esistente quando

L'Azienda non dispone di procedure per monitorare l'efficacia dei controlli interni. Non vi sono metodi per riportare al management sul controllo interno. C'è una generalizzata mancanza di consapevolezza sugli aspetti di sicurezza delle attività IT e sull'esigenza di garanzia dell'operatività del controllo interno. La Direzione e il personale hanno una generale mancanza di consapevolezza del sistema dei controlli interni.

1 Iniziale/*Ad Hoc* quando

La Direzione riconosce il bisogno di una garanzia in merito alla corretta gestione e al controllo dell'IT. Sono utilizzate competenze individuali per la valutazione caso per caso dell'adeguatezza del controllo interno. La Direzione IT non ha assegnato formalmente la responsabilità del monitoraggio dell'efficacia dei controlli interni. La valutazione dei controlli interni IT è realizzata come parte degli audit contabili, con metodologie e competenze che non riflettono le necessità della funzione IT.

2 Ripetibile ma Intuitivo quando

L'Azienda utilizza relazioni informali sui controlli interni per attivare azioni correttive. La valutazione del sistema di controllo interno è dipendente dalle competenze di individui chiave. L'Azienda ha un'accresciuta consapevolezza sul monitoraggio del controllo interno. La Direzione dei Sistemi Informativi monitora su base regolare l'efficacia di quelli che ritiene siano i controlli interni critici. Metodologie e strumenti per il monitoraggio dei controlli interni iniziano ad essere usati ma non sulla base di un piano. I fattori di rischio specifici per l'ambiente IT sono identificati sulla base delle competenze degli individui.

3 Definito quando

La Direzione sostiene ed ha istituzionalizzato il monitoraggio del controllo interno. Sono state sviluppate politiche e procedure per la preparazione e la valutazione di rapporti sulle attività di monitoraggio dei controlli interni. È stato definito un programma di formazione per il monitoraggio del controllo interno. È stato definito un processo di autovalutazione e di verifiche di certificazione dei controlli interni, con ruoli per i manager aziendali e per i manager dell'IT. Si stanno utilizzando strumenti per la misurazione e per la valutazione dei controlli interni, ma essi non sono necessariamente integrati in tutti i processi. Sono utilizzate politiche per la valutazione dei rischi nell'ambito di un quadro di riferimento sviluppato specificamente per il controllo interno dell'IT. Sono definiti rischi specifici di processo e le relative azioni di mitigazione/riduzione del rischio.

4 Gestito e Misurabile quando

La Direzione ha realizzato una struttura per il monitoraggio dei controlli interni IT. L'azienda ha stabilito le soglie di tolleranza per il processo di monitoraggio del controllo interno. Sono stati implementati strumenti per standardizzare le valutazioni e per rilevare automaticamente le eccezioni ai controlli. È stata attivata una funzione formalmente definita per la gestione del controllo interno sull'IT, dotata di personale specializzato e certificato e che utilizza un quadro di riferimento di controllo formalizzato ed approvato dall'Alta Direzione. Personale IT competente partecipa regolarmente alle verifiche sui controlli interni. È stata realizzata una base di conoscenza storica di metriche sul monitoraggio del controllo interno. Sono state avviate attività di riesame fra pari grado per il monitoraggio del controllo interno.

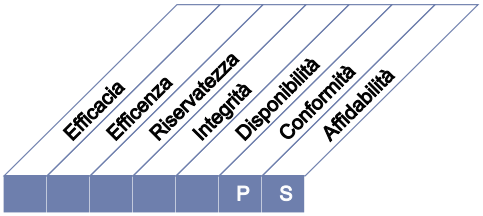
5 Ottimizzato quando

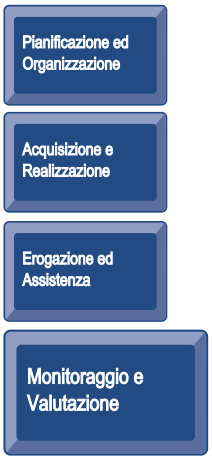
La Direzione ha stabilito un programma di miglioramento continuo per l'intera organizzazione, che prende in considerazione le esperienze maturate e le migliori prassi di settore per il monitoraggio del controllo interno. L'azienda utilizza strumenti integrati e aggiornati che, quando opportuno, permettono un efficace valutazione dei controlli IT critici e una rapida rilevazione degli incidenti nel monitoraggio dei controlli IT. La condivisione delle conoscenze, in particolare per la funzione Sistemi Informativi, è formalmente implementata. È formalizzato lo sviluppo di analisi comparative con gli standard di settore e con le pratiche di riferimento.

DESCRIZIONE DEL PROCESSO

ME3 Assicurare la conformità a leggi e normative esterne

Un'efficace supervisione del rispetto dei regolamenti richiede la definizione di un processo di valutazione per assicurare la conformità ai requisiti di legge, di norme e di contratti. Tale processo include l'identificazione dei requisiti di conformità, l'ottimizzazione e valutazione dei risultati, l'assicurazione che i requisiti di conformità sono stati effettivamente soddisfatti, infine, l'integrazione del reporting relativo alla conformità di competenza dell'IT nell'ambito del reporting di conformità aziendale.





Il controllo del processo IT

Assicurare la conformità a leggi e normative esterne

che soddisfa i requisiti aziendali per l'IT di

assicurare la conformità a leggi, regolamenti ed a requisiti contrattuali

ponendo l'attenzione su

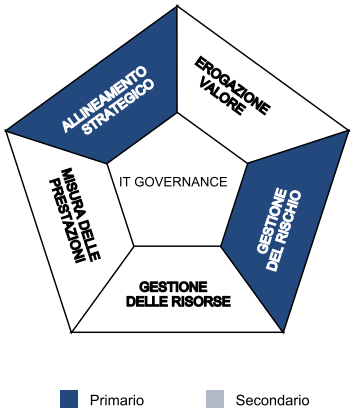
l'identificazione di tutte le leggi, regolamenti e requisiti contrattuali applicabili, sulla definizione del corrispondente livello di conformità richiesto all'IT ed infine sull'ottimizzazione dei processi IT per ridurre il rischio di non conformità

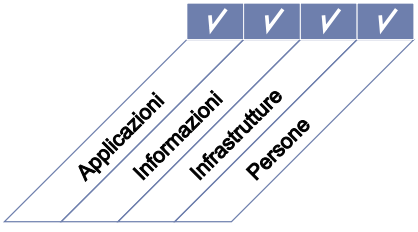
è ottenuto tramite

- l'identificazione dei requisiti legali, normativi e contrattuali relativi all'IT
- la valutazione dell'impatto dei requisiti legali e normativi
- il monitoraggio e il reporting sulla conformità a questi requisiti

e viene misurato tramite

- Costo della non conformità dell'IT, inclusi pagamenti e multe
- Tempo medio trascorso tra l'identificazione di problemi di conformità con norme esterne e la loro risoluzione
- Frequenza delle verifiche di conformità a leggi e regolamenti esterni





OBIETTIVI DI CONTROLLO

ME3 Assicurare la conformità a leggi e normative esterne

ME3.1 Identificazione dei requisiti esterni di compliance relativi a leggi, normative e contratti

Identificare, in modo sistematico, leggi nazionali ed internazionali, normative ed altri requisiti - di natura esogena rispetto all'azienda – che l'azienda deve rispettare, al fine di farli integrare nelle politiche, negli standard, nelle procedure e nelle metodologie specifici dell'IT.

ME3.2 Ottimizzazione della gestione dei requisiti normativi

Rivedere e adeguare le politiche, gli standard, le procedure ed i metodi IT per assicurare che i requisiti di legge, normativi e contrattuali siano efficientemente soddisfatti e conosciuti.

ME3.3 Valutazione del rispetto dei requisiti esterni

Confermare che le politiche, gli standard, le procedure e i metodi IT rispettano i requisiti normativi e di legge.

ME3.4 Garanzia di conformità

Ottenere e riferire sulla garanzia di conformità con e rispetto di tutte le politiche interne che derivano dall'applicazione di direttive interne o di leggi e normative esterne o di contratti; confermare che i proprietari dei processi interessati abbiano adottato le opportune azioni correttive per superare eventuali lacune di conformità.

ME3.5 Reporting integrato

Integrare, con analoghe informative provenienti da altre funzioni aziendali, il reporting dell'IT riguardante la conformità a requisiti di legge, normativi e contrattuali.

Linee Guida per la Gestione

ME3 Assicurare la conformità a leggi e normative esterne

Da	Inputs
*	Requisiti legali e normativi di conformità
PO6	Politiche IT

* Inputs dall'esterno di CobiT

Outputs	A						
Elenco (catalogue) dei requisiti di legge e normativi che si riferiscono alla fornitura di servizi IT	PO4	ME4					
Valutazione della conformità IT ai requisiti legali e normativi delle attività aziendali	ME1						

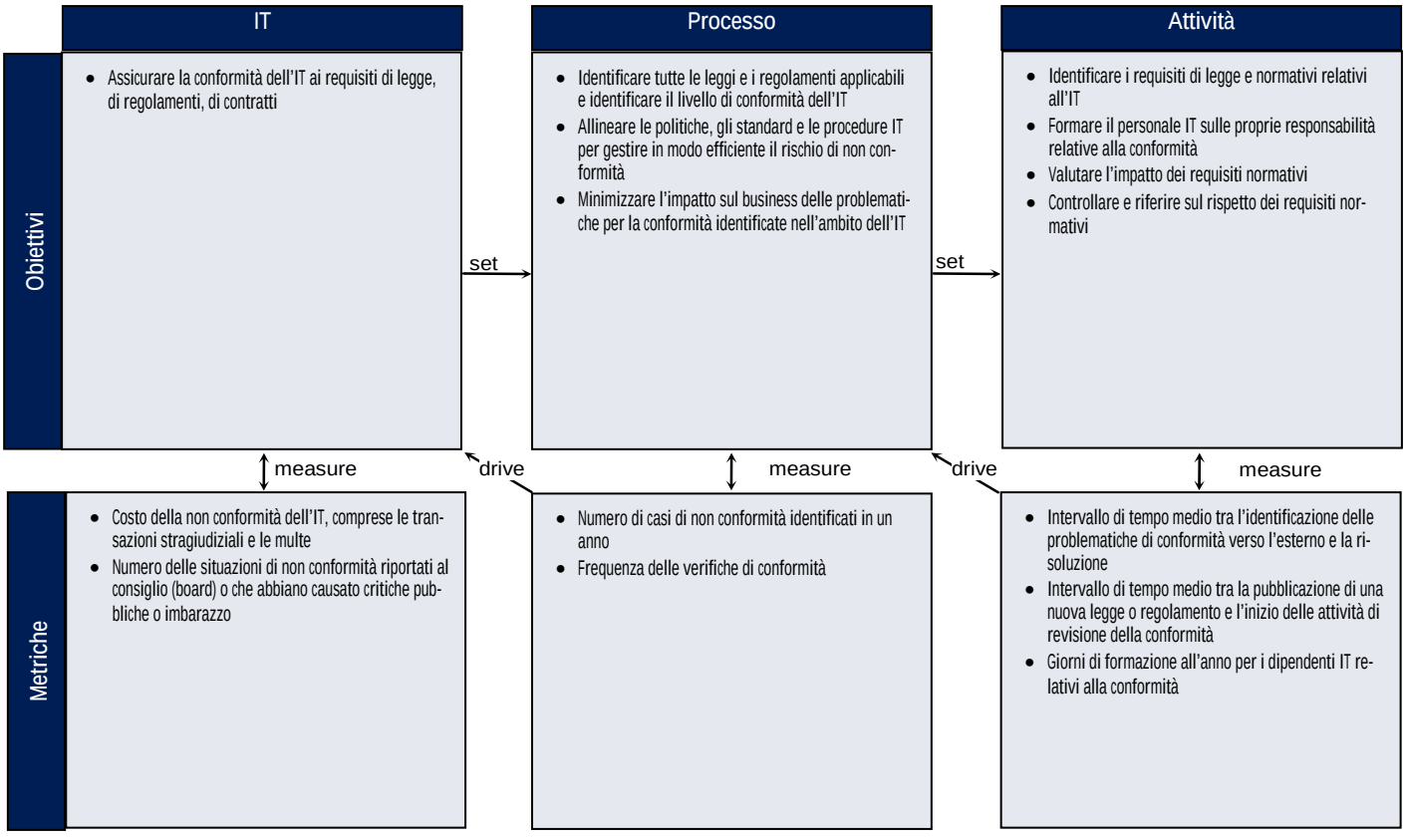
RACI Chart

Ruoli

Attività	Amm. Delegato o DG	Direttore Amministrativo	Direttore Utente IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architettura IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza	Consiglio d'amministrazione
definire e realizzare un processo per identificare i requisisti di legge, contrattuali, di policy e normativi				A/R	C	I	I	I	C	I	R	
valutare la conformità delle attività IT con le politiche , gli standard e le procedure IT	I	I	I	A/R	I	R	R	R	R	R	R	I
riferire in merito alla garanzia di conformità delle attività IT con le politiche, gli standard e le procedure IT				A/R	C	C	C	C	C	C	R	
definire le azioni (input) per allineare le politiche, le procedure e gli standard IT ai requisiti di conformità				A/R	C	C	C	C	C		R	
integrare il reporting sull'IT sui requisiti normativi con output analoghi delle altre funzioni di business				A/R		I	I	I	R	I	R	

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME3 Assicurare la conformità a leggi e normative esterne

Il grado di strutturazione del processo *Assicurare la conformità a leggi e normative esterne* che soddisfa i requisiti aziendali per l'IT di *assicurare la conformità a leggi, regolamenti ed a requisiti contrattuali* è:

0 Non esistente quando

C'è poca consapevolezza dei requisiti esterni che influiscono sull'ambito IT, non c'è un processo riguardante la conformità con normative, con requisiti di natura legale o contrattuale.

1 Iniziale/*Ad Hoc* quando

Si è consapevoli dell'impatto che hanno sull'azienda le norme, i contratti o la legislazione. Vengono adottate procedure informali per garantire la compliance, ma solo a seguito di un'esigenza emersa in un nuovo progetto o come reazione ad una verifica o ad una ispezione.

2 Ripetibile ma Intuitivo quando

È compresa la necessità di rispettare le regole esterne e tale esigenza è comunicata. Ogniqualvolta la compliance diventa un obbligo ricorrente, come nel caso di normative del settore finanziario o della legislazione sulla privacy, sono sviluppate procedure particolari, applicate con cadenza annuale. Tuttavia non esiste un approccio standard. Si fa molto affidamento sull'esperienza e sulla responsabilità dei singoli individui, e di conseguenza sono possibili errori. La formazione sui regolamenti esterni e su quanto concerne il loro rispetto è fatta in modo informale.

3 Definito quando

Politiche, procedure e piani che garantiscono il rispetto di norme, leggi e contratti sono stati sviluppati, documentati e comunicati ma non sempre vengono rispettati ed in alcuni casi possono essere superati o di difficile applicazione. Il controllo è limitato e non tutte le esigenze di adeguamento sono state prese in considerazione. La formazione viene fornita per quanto riguarda i requisiti legali e normativi che interessano l'organizzazione ed i processi di compliance definiti. Per ridurre i rischi relativi alle responsabilità contrattuali sono disponibili fac-simili di contratti e di procedure legali.

4 Gestito e Misurabile quando

I problemi e i rischi connessi al rispetto di requisiti legali esterni e l'esigenza di garantirne l'osservanza a tutti i livelli sono fortemente compresi. Un piano di formazione è definito per garantire che tutto il personale conosca le regole da rispettare. Le responsabilità sono chiare e note, in particolare è assegnata la responsabilità di ciascun processo. Il processo di compliance include un'analisi della situazione attuale per identificare le regole da rispettare e via via i cambiamenti da apportare. Esiste un meccanismo per controllare il non rispetto delle regole esterne, per garantire l'applicazione delle procedure interne e per adottare azioni correttive. I problemi di non rispetto delle regole sono analizzati in modo standard per ricercarne le cause, con l'obiettivo di individuare le soluzioni sostenibili. Prassi operative interne standard, vengono utilizzate per esigenze specifiche quali ad esempio le disposizioni permanenti e i contratti di servizio ricorrenti.

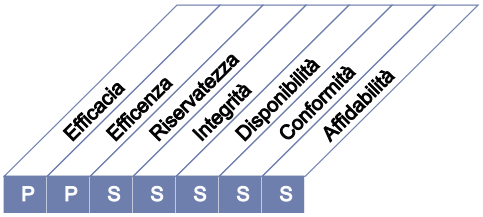
5 Ottimizzato quando

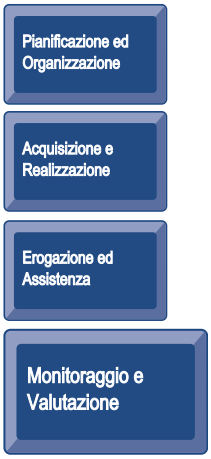
Esiste un processo ben organizzato, efficiente e rispettato di conformità alle regole esterne, basato su una singola funzione centrale che fornisce guida e coordinamento a tutta l'azienda. C'è una conoscenza approfondita delle norme da applicare, delle relative future evoluzioni, delle modifiche prevedibili e dell'esigenza di nuove soluzioni. Per capire ed influenzare la definizione delle normative esterne che possono interessarla, l'azienda partecipa ad iniziative di natura normativa promosse dalle autorità. Sono state sviluppate regole interne per garantire una efficiente conformità con le normative esterne, tali regole hanno ridotto al minimo i casi di non rispetto delle norme. Esiste un sistema centrale di registrazione valido per tutta l'azienda, tale funzione consente alla direzione di documentare i flussi operativi e di misurare e migliorare la qualità e l'efficacia del processo di supervisione della compliance. Viene utilizzato ed affinato, a livello di regola interna, un processo di auto-valutazione relativo ai requisiti normativi esterni. Lo stile e la cultura dei responsabili aziendali riguardo al rispetto delle regole esterne sono sufficientemente forti, il processo è ben definito in modo tale da consentire che l'addestramento sia limitato al nuovo personale o al verificarsi di cambiamenti significativi.

DESCRIZIONE DEL PROCESSO

ME4 Istituire l'IT Governance

Istituire un'efficace struttura per la governance che includa la definizione delle strutture organizzative, dei processi, della leadership, dei ruoli e delle responsabilità al fine di garantire che gli investimenti dell'impresa in tecnologie informatiche siano allineati ed erogati in accordo con le strategie e con gli obiettivi aziendali.





Il controllo del processo IT

Istituire l'IT Governance

che soddisfa i requisiti aziendali per l'IT di

integrare l'IT governance con gli obiettivi di corporate governante e di conformità con leggi, regolamenti e contratti

ponendo l'attenzione su

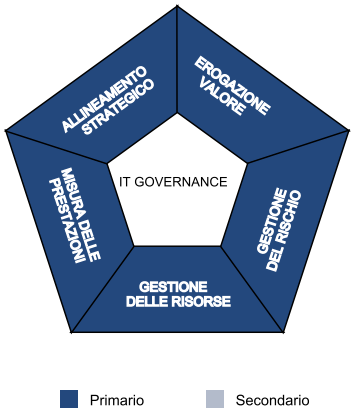
l'attività di redazione di reportistica indirizzata al board in merito a strategie, prestazioni e rischi legati all'IT, e sull'attività di soddisfacimento dei requisiti di governance coerentemente con le indicazioni del board

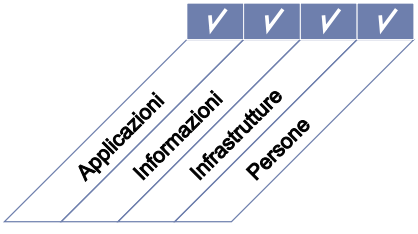
è ottenuto tramite

- l'istituzione di una struttura di IT governance integrata con la corporate governance
- l'ottenimento di una valutazione indipendente sullo stato dell'IT governance

e viene misurato tramite

- frequenza delle comunicazioni indirizzate agli stakeholder in merito alle tematiche IT, anche con riferimento al grado di strutturazione dei processi IT
- frequenza della reportistica dell'IT al board, anche con riferimento al grado di strutturazione dei processi IT
- frequenza delle verifiche indipendenti in merito alla conformità dei processi IT





OBIETTIVI DI CONTROLLO

ME4 Istituire l'IT Governance

ME4.1 Istituzione di un quadro di riferimento per l'IT Governance

Definire, realizzare un quadro di riferimento per la governance dell'IT e mantenerlo allineato con il contesto stabilito per la governante ed il controllo dell'intera azienda. Il quadro di riferimento dovrebbe essere basato su un adeguato modello di controllo e dei processi IT e indicare responsabilità non ambigue e procedure che consentano di prevenire errori nell'ambito di attività di controllo e di supervisione. Confermare che il quadro di riferimento per la governance dell'IT è funzionale a garantire la conformità con la legislazione e le normative, l'allineamento alle strategie aziendali ed il perseguimento degli obiettivi aziendali. Definire un sistema di reporting che relazioni sullo stato e sulle problematiche dell'IT Governance.

ME4.2 Allineamento strategico

Facilitare la comprensione da parte del Consiglio di Amministrazione e dell'Alta Direzione delle problematiche strategiche dell'IT, come il ruolo dell'IT, le caratteristiche e le potenzialità delle tecnologie informatiche in azienda. Assicurarsi che il potenziale contributo dell'IT alla strategia aziendale sia compreso sia dall'azienda sia dalla funzione sistemi informativi. Collaborare con il Consiglio di Amministrazione al fine di definire ed implementare organismi di controllo, come il Comitato Strategico per l'IT, con l'obiettivo di fornire un orientamento strategico al management che si deve relazionare con l'IT, in modo da assicurare che strategia ed obiettivi siano diffusi all'interno delle unità operative sia di business sia delle singole funzioni IT, e che tra utenti aziendali e specialisti della funzione sistemi informativi si sviluppi un rapporto di fiducia reciproca. Facilitare l'allineamento dell'IT all'azienda per quanto riguarda strategia e processi operativi, incoraggiando la condivisione di responsabilità fra process owner e l'IT al fine di pervenire a decisioni strategiche e produrre valore a fronte di investimenti in tecnologie informatiche.

ME4.3 Apporto di valore

Gestire i programmi di investimento dove l'IT è fattore abilitante e di altre risorse e servizi IT in modo che possano apportare il maggiore valore possibile nel perseguimento della strategia e degli obiettivi dell'impresa. Assicurarsi che i risultati degli investimenti IT attesi dall'azienda e che tutti gli sforzi necessari per ottenerli vengano compresi, che siano prodotti e approvati dagli stakeholder degli studi di fattibilità significativi e coerenti, che le risorse e gli investimenti siano controllati durante tutto il loro ciclo di vita economico e che ci sia una gestione finalizzata alla realizzazione dei benefici, come il contributo a nuovi servizi, guadagni in efficienza e una maggiore capacità di risposta alla domanda del cliente. Assicurare una gestione puntuale a livello di portafoglio, di programmi e di progetti, incoraggiando l'assunzione di responsabilità da parte delle strutture e dei processi di business sugli investimenti favoriti dall'IT e che la funzione sistemi informativi garantisca un efficiente ed efficace supporto.

ME4.4 Gestione delle risorse

Supervisionare gli investimenti, l'utilizzo e l'allocazione delle risorse IT attraverso una attività di verifica sistematica delle iniziative e delle operazioni IT assicurandosi che la funzione sistemi informativi disponga di una quantità sufficiente di risorse competenti e allineate con gli attuali e futuri obiettivi strategici ed esigenze irrinunciabili dell'azienda.

ME4.5 Gestione del rischio

Collaborare con il Consiglio di Amministrazione al fine di definire la propensione al rischio IT dell'impresa; ottenere una ragionevole garanzia che le modalità di gestione del rischio informatico siano appropriate e che il rischio informatico attuale non superi il livello stabilito dal Consiglio. Incorporare le responsabilità di gestione del rischio nell'organizzazione, assicurando che l'azienda e l'IT valutino e comunichino in maniera sistematica i rischi correlati all'IT ed il loro impatto sui processi di business. La posizione assunta dall'azienda nei confronti del rischio IT dovrebbe essere trasparente e nota a tutti gli stakeholder.

ME4.6 Valutazione delle prestazioni

Confermare che gli obiettivi IT sui quali si è raggiunto un accordo sono stati raggiunti o superati, o che i miglioramenti nel perseguimento degli obiettivi IT è coerente con le aspettative. Ove gli obiettivi non siano stati raggiunti o le aspettative siano state insoddisfatte, verificare gli interventi risolutivi adottati dalla Direzione. verso Fornire al Consiglio informazioni dettagliate sugli aspetti più importanti legati al portafoglio delle iniziative che riguardano l'IT, ai programmi e alle prestazioni dei processi IT, attraverso dei report che mettano in condizione la Direzione di verificare i progressi dell'azienda verso gli obiettivi definiti.

ME4.7 Certificazione indipendente

Ottenere una certificazione indipendente (interna o esterna) relativamente alla conformità dell'IT con la legislazione e le normative vigenti; con le politiche, gli standard e le procedure dell'azienda, con le pratiche generalmente accettate, con l'attesa efficienza ed efficacia delle performance IT.

LINEE GUIDA PER LA GESTIONE

ME4 Istituire l'IT Governance

Da	Inputs
PO4	Quadro di riferimento dei processi IT
PO5	Reporting sul rapporto costi/benefici
PO9	Valutazione del rischio e reporting
ME2	Report sull'efficacia dei controlli IT
ME3	Elenco (catalogue) dei requisiti di legge e normativi che si riferiscono alla fornitura di servizi IT

Outputs	A						
Miglioramenti del quadro di riferimento dei processi	PO4						
Valutazione dello stato della governance del sistema informativo aziendale	PO1	ME1					
Benefici attesi dall'azienda relativamente agli investimenti IT	PO5						
Orientamento strategico dell'impresa verso l'IT	PO1						
Propensione ai rischi IT dell'azienda	PO9						

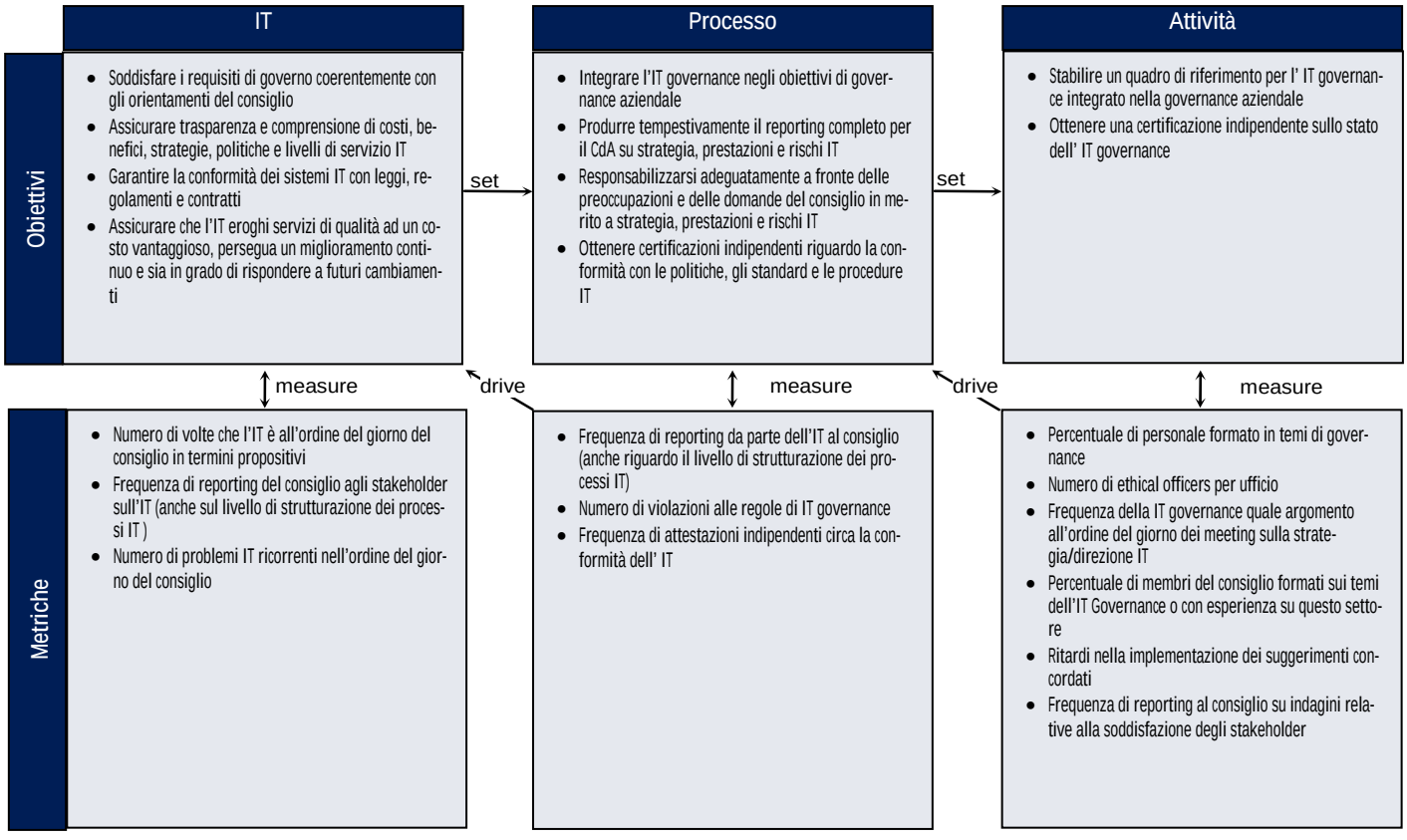
RACI Chart

Ruoli

Attività	Consiglio d'amministrazione	Amm. Delegato o DG	Direttori Amministrativi	Direttori Unità IT	Direttore IT	Process owner	Responsabile operativo	Responsabile architetture IT	Responsabile sviluppo IT	Responsabile amministrativo IT	PMO	Conformità, audit, rischio e sicurezza
Stabilire la supervisione e la promozione delle attività di IT da parte del Consiglio di Amministrazione e dell'Alta Direzione	A	R	C	C	C							C
Analizzare, approvare, allineare e comunicare le performance, la strategia , la gestione del rischio e delle risorse IT rispetto alla strategia aziendale	A	R	I	I	R							C
Ottenere periodicamente valutazioni indipendenti relativamente alle prestazioni e alla conformità con politiche, standard e procedure	A	R	C	I	C		I	I	I	I	I	R
Risolvere i rilievi individuati dalle valutazioni indipendenti ed assicurare l'implementazione da parte della direzione dei suggerimenti concordati	A	R	C	I	C		I	I	I	I	I	R
Produrre un report sull'IT governance	A	C	C	C	R	C	I	I	I	I	I	C

La tabella **RACI** identifica chi è **R**esponsible (Incaricato di eseguire o far eseguire), **A**ccountable (Responsabile), **C**onsulted (Consultato) e/o **I**nformed (Informato).

Obiettivi e metriche



GRADO DI STRUTTURAZIONE DEL PROCESSO

ME4 Istituire l'IT Governance

Il grado di strutturazione del processo *Istituire l'IT Governance* che soddisfa i requisiti aziendali per l'IT di *integrare l'IT governance con gli obiettivi di corporate governante e di conformità con leggi, regolamenti e contratti* è:

0 Non esistente quando

C'è una completa mancanza di qualsiasi processo riconoscibile di IT governance. L'azienda non si è ancora resa conto che c'è un problema che deve essere affrontato e di conseguenza non c'è comunicazione riguardo al problema.

1 Iniziale/*Ad Hoc* quando

C'è la consapevolezza che le problematiche di IT governance esistono e devono essere considerate. Sono presenti approcci ad hoc attuati su base individuale o su casi specifici. L'approccio della Direzione è di tipo reattivo, esiste solo una comunicazione sporadica e non coerente sui problemi e sugli approcci necessari per affrontarli. La Direzione riceve soltanto indicazioni approssimative circa il contributo fornito dall'IT alla performance aziendale. Il management affronta e risolve gli incidenti che hanno causato qualche perdita o problemi di immagine all'azienda solo con un approccio reattivo.

2 Ripetibile ma Intuitivo quando

Esiste consapevolezza in merito alle problematiche legate al governo dell'IT. Le attività di IT governance, e gli indicatori di prestazione, fra cui la pianificazione, l'erogazione e i processi di monitoraggio dell'IT sono in fase di sviluppo. L'identificazione dei processi IT da migliorare è effettuata sulla base di decisioni individuali. La Direzione ha identificato metodi e tecniche di valutazione elementari; il processo non è tuttavia ancora stato applicato all'intera azienda. La comunicazione degli standard e delle responsabilità di governo viene lasciata ai singoli, i quali guidano i processi di governance all'interno di vari progetti e processi IT. I processi, gli strumenti e le metriche dell'IT governance sono limitati e possono non essere utilizzati appieno per una mancanza di conoscenza delle loro caratteristiche.

3 Definito quando

L'importanza e la necessità dell'IT governance sono comprese dal management e comunicate all'organizzazione. È sviluppato un insieme di indicatori di base per l'IT governance, dove i collegamenti fra le misure dei risultati e i parametri delle prestazioni sono definiti e documentati. Le procedure sono standardizzate e documentate. La Direzione ha comunicato le procedure standardizzate e sono definite delle procedure di formazione. Sono identificati gli strumenti per supportare il monitoraggio dell'IT governance. Sono stati sviluppati dei cruscotti, parte integrante delle Balanced Business Scorecard in ambito IT. Tuttavia è lasciato al singolo di dedicarsi alla formazione, seguire gli standard ed applicarli. I processi possono essere monitorati, ma mentre molto viene fatto sulla base dell'iniziativa personale per gestire le deviazioni, queste ultime sono difficilmente identificate dalla Direzione.

4 Gestito e Misurabile quando

Esiste consapevolezza delle problematiche legate all'IT governance a tutti i livelli. Il cliente dei servizi forniti dall'IT è chiaramente identificato e le responsabilità sono definite e monitorate tramite accordi sui livelli di servizio. Le responsabilità sono chiaramente definite e la responsabilità del processo è stata attribuita. I processi IT e l'IT governance sono allineati ed integrati con la strategia aziendale e la strategia IT. I miglioramenti dei processi IT sono basati principalmente su di un approccio di natura quantitativa ed è possibile misurare e monitorare la conformità con le procedure e le metriche di processo. Tutti gli stakeholder del processo sono consapevoli dei rischi, dell'importanza dell'IT e delle opportunità che essa è in grado di offrire. La Direzione ha definito i livelli di tolleranza con riferimento ai quali devono essere strutturati i processi. C'è un limitato, principalmente tattico, uso della tecnologia, basato su tecniche mature e strumenti standard consolidati. L'IT governance è stata integrata nella pianificazione operativa e strategica e nei processi di monitoraggio. Gli indicatori di prestazione relativi a tutte le attività di IT Governance sono stati identificati e tracciati consentendo miglioramenti estesi a tutta la realtà aziendale. La responsabilità generale delle prestazioni dei processi chiave è chiara e il management è premiato sulla base delle misure chiave di prestazione.

5 Ottimizzato quando

Esiste una comprensione avanzata ed orientata al futuro delle problematiche di IT Governance e delle relative soluzioni. Addestramento e comunicazione sono supportati da concetti e tecniche all'avanguardia. I processi sono stati portati ad un livello coerente con le migliori pratiche di settore sulla base dei risultati di un'attività di miglioramento continuo e di raffronto con altre realtà aziendali in relazione al modello di strutturazione dei processi IT. La realizzazione delle politiche IT ha condotto ad una struttura organizzativa, organico del personale e processi IT che sono rapidi ad adattarsi e a supportare pienamente i requisiti di IT governance. Le cause di tutti i problemi e di tutte le discrepanze sono analizzate e si dà corso ad azioni correttive efficaci. L'IT è usato in modo coerente, integrato ed ottimizzato, tale da automatizzare i flussi di lavoro e fornire strumenti per migliorare qualità ed efficacia. I rischi come i benefici dei processi IT sono definiti, bilanciati e comunicati a tutta l'azienda. Si fa leva su esperti esterni e i benchmark sono usati come riferimento. Il monitoraggio, l'auto-valutazione e la comunicazione delle aspettative di governance pervadono tutta l'azienda e c'è un uso ottimale della tecnologia a supporto di attività di misurazione, analisi, comunicazione e formazione. Il governo dell'impresa ed il governo dell'IT sono collegati strategicamente, facendo leva su tecnologia, risorse umane e finanziarie per aumentare il vantaggio competitivo dell'azienda. Le attività di IT governance sono integrate con i processi di governance dell'impresa.

Appendix I

Tables Linking Goals and Processes

This appendix provides a global view of how generic business goals relate to IT goals, the IT processes and information criteria. There are three tables:

1. The first table maps the business goals, organised according to a balanced scorecard, to the IT goals and information criteria. This helps show, for a given generic business goal, the IT goals that typically support this goal and the CobiT information criteria that relate to the business goal. The set of 17 business goals should not be regarded as a complete set of all possible business goals; it is a selection of relevant business goals that can have a clear impact on IT (IT-related business goals).
2. The second table maps the IT goals to CobiT's IT processes and the information criteria on which the IT goal is based.
3. The third table provides a reverse mapping showing for each IT process the IT goals that are supported.

The tables help demonstrate the scope of CobiT and the overall business relationship between CobiT and business drivers, enabling typical IT-related business goals to be mapped via IT goals to the IT processes needed to support them. The tables are based on generic goals and, therefore, should be used as a guide and tailored for a specific enterprise.

To provide a link back to the information criteria used for business requirements in CobiT 3rd Edition, the tables also provide an indication of the most important information criteria supported by the business and IT goals.

Notes:

1. The information criteria in the business goals chart are based on an aggregation of the criteria for the related IT goals and a subjective assessment of those that are most relevant to the business goal. No attempt has been made to indicate primary or secondary. These are only indicative and users can follow a similar process when assessing their own business goals.
2. The information criteria primary and secondary references in the IT goals chart are based on an aggregation of the criteria for each IT process and a subjective assessment of what is primary and secondary for the IT goal, as some processes have more of an impact on the IT goal than others. These are only indicative and users can follow a similar process when assessing their own IT goals.

LINKING BUSINESS GOALS TO IT GOALS

		Business Goals	IT Goals								CobiT Information Criteria						
											Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24									✔					
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22			✔	✔	✔		
	3	Improve corporate governance and transparency.	2	18													✔
Customer Perspective	4	Improve customer orientation and service.	3	23							✔						
	5	Offer competitive products and services.	5	24							✔	✔					
	6	Establish service continuity and availability.	10	16	22	23					✔				✔		
	7	Create agility in responding to changing business requirements.	1	5	25						✔	✔					
	8	Achieve cost optimisation of service delivery.	7	8	10	24						✔					
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26				✔			✔			✔
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11						✔	✔					
	11	Lower process costs.	7	8	13	15	24					✔					
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27				✔			✔	
	13	Provide compliance with internal policies.	2	13									✔			✔	
	14	Manage business change.	1	5	6	11	28				✔	✔					
	15	Improve and maintain operational and staff productivity.	7	8	11	13					✔	✔					
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28						✔	✔					
	17	Acquire and maintain skilled and motivated people.	9								✔	✔					

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes											CobiT Information Criteria: Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4							P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Optimise the use of information.	PO2	DS11											S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3								P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6									P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5									P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5										S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5										P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2											P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7									P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8							P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9											S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5									P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12								P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13								P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6										S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10										P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5										P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4										S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4								P	P					P

IT PROCESS TO IT GOALS MATRIX

	1 Respond to business requirements in alignment with the business strategy.	2 Respond to governance requirements in line with board direction.	3 Ensure satisfaction of end users with service offerings and service levels.	4 Optimise use of information.	5 Create IT agility.	6 Define how business functional and control requirements are translated in effective and efficient automated solutions.	7 Acquire and maintain integrated and standardised application systems.	8 Acquire and maintain an integrated and standardised IT infrastructure.	9 Acquire and maintain an integrated and respond to the IT strategy.	10 Ensure mutual satisfaction of third-party relationships.	11 Ensure seamless integration of applications into business processes.	12 Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	13 Ensure proper use and performance of the applications and technology solutions.	14 Account for and protect all IT assets.	15 Optimise the IT infrastructure, resources and capabilities.	16 Reduce solution and service delivery defects and rework.	17 Protect the achievement of IT objectives.	18 Establish clarity on the business impact of risks to IT objectives and resources.	19 Ensure that critical and confidential information is withheld from those who should not have access to it.	20 Ensure that automated business transactions and information exchanges can be trusted.	21 Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	22 Ensure minimum business impact in the event of an IT service disruption or change.	23 Make sure that IT services are available as required.	24 Improve IT's cost-efficiency and its contribution to business profitability.	25 Deliver projects on time and on budget, meeting quality standards.	26 Maintain the integrity of information and processing infrastructure.	27 Ensure IT compliance with laws, regulations and contracts.	28 Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.
Plan and Organise																													
PO1 Define a strategic IT plan.	✔	✔																											
PO2 Define the information architecture.	✔			✔	✔						✔																		
PO3 Determine technological direction.							✔								✔														
PO4 Define the IT processes, organisation and relationships.	✔	✔			✔																								
PO5 Manage the IT investment.												✔													✔				✔
PO6 Communicate management aims and direction.												✔	✔						✔	✔	✔	✔							
PO7 Manage IT human resources.					✔				✔																				
PO8 Manage quality.			✔													✔										✔			
PO9 Assess and manage IT risks.														✔			✔	✔											
PO10 Manage projects.	✔	✔																								✔			
Acquire and Implement																													
AI1 Identify automated solutions.	✔					✔																							
AI2 Acquire and maintain application software.						✔	✔																						
AI3 Acquire and maintain technology infrastructure.					✔			✔							✔														
AI4 Enable operation and use.			✔								✔		✔			✔													
AI5 Procure IT resources.							✔	✔	✔																				
AI6 Manage changes.	✔					✔										✔						✔					✔		
AI7 Install and accredit solutions and changes.	✔										✔		✔			✔				✔	✔								
Deliver and Support																													
DS1 Define and manage service levels.	✔		✔									✔																	
DS2 Manage third-party services.			✔							✔		✔																	
DS3 Manage performance and capacity.	✔														✔									✔					
DS4 Ensure continuous service.																					✔	✔	✔						
DS5 Ensure systems security.														✔					✔	✔	✔					✔			
DS6 Identify and allocate costs.												✔													✔				✔
DS7 Educate and train users.			✔										✔		✔														
DS8 Manage service desk and incidents.			✔										✔											✔					
DS9 Manage the configuration.														✔	✔														
DS10 Manage problems.			✔													✔	✔												
DS11 Manage data.				✔															✔								✔		
DS12 Manage the physical environment.														✔					✔		✔	✔							
DS13 Manage operations.			✔																		✔		✔						
Monitor and Evaluate																													
ME1 Monitor and evaluate IT performance.	✔	✔										✔																	✔
ME2 Monitor and evaluate internal control.														✔			✔				✔							✔	
ME3 Ensure compliance with external requirements.																												✔	
ME4 Provide IT governance.		✔										✔																✔	✔

Appendix II

Mapping IT Processes to IT Governance Focus Areas, COSO, CobiT IT Resources and CobiT Information Criteria

This appendix provides a mapping between the CobiT IT processes and the five IT governance focus areas, the components of COSO, IT resources and the information criteria. The table also provides a relative importance indicator (high, medium and low) based on benchmarking via CobiT Online. This matrix demonstrates on one page and at a high level how the CobiT framework addresses IT governance and COSO requirements, and shows the relationship between IT processes and the IT resources and information criteria. P is used when there is a primary relation and S when there is only a secondary relation. No P or S does not mean that there is no relation, only that it is less important, or marginal. The importance values are based on a survey and the opinions of experts, and are provided only as a guide. Users should consider what processes are important within their own organisations.

Appendix II—Mapping IT Processes to IT Governance Focus Areas, COSO, CobiT IT Resources and CobiT Information Criteria

	IMPORTANCE	IT Governance Focus Areas					COSO					CobiT IT Resources				CobiT Information Criteria						
		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring	Application	Information	Infrastructure	People	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Plan and Organise																						
PO1 Define a strategic IT plan.	H	P		S	S			P		S	S	✓	✓	✓	✓	P	S					
PO2 Define the information architecture.	L	P	S	P	S				P	P		✓	✓			S	P	S	P			
PO3 Determine technological direction.	M	S	S	P	S			S	P	S		✓		✓		P	P					
PO4 Define the IT processes, organisation and relationships.	L	S		P	P		P			S	S				✓	P	P					
PO5 Manage the IT investment.	M	S	P	S		S		S	P			✓		✓	✓	P	P					S
PO6 Communicate management aims and direction.	M	P			P		P			P			✓		✓	P					S	
PO7 Manage IT human resources.	L	P		P	S	S	P			S					✓	P	P					
PO8 Manage quality.	M	P	S		S		P		P	S	P	✓	✓	✓	✓	P	P		S			S
PO9 Assess and manage IT risks.	H	P			P			P				✓	✓	✓	✓	S	S	P	P	P	S	S
PO10 Manage projects.	H	P	S	S	S	S	S	S	P		S	✓		✓	✓	P	P					
Acquire and Implement																						
AI1 Identify automated solutions.	M	P	P	S	S				P			✓		✓		P	S					
AI2 Acquire and maintain application software.	M	P	P		S				P			✓				P	P		S			S
AI3 Acquire and maintain technology infrastructure.	L			P					P					✓		S	P		S	S		
AI4 Enable operation and use.	L	S	P	S	S				P	S		✓		✓	✓	P	P		S	S	S	S
AI5 Procure IT resources.	M		S	P					P			✓	✓	✓	✓	S	P				S	
AI6 Manage changes.	H		P	S				S	P		S	✓	✓	✓	✓	P	P		P	P		S
AI7 Install and accredit solutions and changes.	M	S	P	S	S	S			P	S	S	✓	✓	✓	✓	P	S		S	S		
Deliver and Support																						
DS1 Define and manage service levels.	M	P	P	P		P	S		P	S	S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS2 Manage third-party services.	L		P	S	P	S	P	S	P		S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS3 Manage performance and capacity.	L	S	S	P	S	S			P		S	✓		✓		P	P			S		
DS4 Ensure continuous service.	M	S	P	S	P	S	S		P	S		✓	✓	✓	✓	P	S			P		
DS5 Ensure systems security.	H				P				P	S	S	✓	✓	✓	✓			P	P	S	S	S
DS6 Identify and allocate costs.	L		S	P		S			P			✓	✓	✓	✓		P					P
DS7 Educate and train users.	L	S	P	S	S		P			S					✓	P	S					
DS8 Manage service desk and incidents.	L		P			S	S			P	P	✓			✓	P	P					
DS9 Manage the configuration.	M		P	P	S				P			✓	✓	✓		P	S			S		S
DS10 Manage problems.	M		P		S	S			P	S	S	✓	✓	✓	✓	P	P			S		
DS11 Manage data.	H		P	P	P				P				✓						P			P
DS12 Manage the physical environment.	L			S	P			S	P					✓					P	P		
DS13 Manage operations.	L			P					P	S		✓	✓	✓	✓	P	P		S	S		
Monitor and Evaluate																						
ME1 Monitor and evaluate IT performance.	H	S	S	S	S	P				S	P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME2 Monitor and evaluate internal control.	M		P		P						P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME3 Ensure compliance with external requirements.	H	P			P				P	S	S	✓	✓	✓	✓						P	S
ME4 Provide IT governance.	H	P	P	P	P	P	P	S		S	P	✓	✓	✓	✓	P	P	S	S	S	S	S

P=Primary enabler S=Secondary enabler

Note: The COSO mapping is based on the original COSO framework. The mapping also applies generally to the later COSO *Enterprise Risk Management—Integrated Framework*, which expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. Whilst it is not intended to and does not replace the original COSO internal control framework, but rather incorporates the internal control framework within it, users of CobiT may choose to refer to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.

Page intentionally left blank

Appendix III

Maturity Model for Internal Control

This appendix provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimised level. The model provides a high-level guide to help CobiT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

APPENDIX III—MATURITY MODEL FOR INTERNAL CONTROL

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilties for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organisation benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Page intentionally left blank

Appendix IV

CobiT 4.1 Primary Reference Material

APPENDIX IV—COBIT 4.1 PRIMARY REFERENCE MATERIAL

For the earlier COBIT development and updating activities, a broad base of more than 40 international detailed IT standards, frameworks, guidelines and good practices was used to ensure the completeness of COBIT in addressing all areas of IT governance and control.

Because COBIT is focused on *what* is required to achieve adequate management and control of IT, it is positioned at a high level. The more detailed IT standards and good practices are at a lower level of detail describing *how* to manage and control specific aspects of IT. COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements.

For this COBIT update (COBIT 4.1), six of the major global IT-related standards, frameworks and practices were focused on as the major supporting references to ensure appropriate coverage, consistency and alignment. These are:

- COSO:
  Internal Control—Integrated Framework, 1994
  Enterprise Risk Management—Integrated Framework, 2004
- Office of Government Commerce (OGC®):
  IT Infrastructure Library® (ITIL®), 1999-2004
- International Organisation for Standardisation:
  ISO/IEC 27000
- Software Engineering Institute (SEI®):
  SEI Capability Maturity Model (CMM®), 1993
  SEI Capability Maturity Model Integration (CMMI®), 2000
- Project Management Institute (PMI®):
  A Guide to the Project Management Body of Knowledge (PMBOK®), 2004
- Information Security Forum (ISF):
  The Standard of Good Practice for Information Security, 2003

Additional references used in the development of COBIT 4.1 include:

- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, IT Governance Institute, USA, 2006
- *CISA Review Manual*, ISACA, 2006

Page intentionally left blank

Appendix V

Cross-references Between CobiT 3rd Edition and Cobit 4.1

APPENDIX V—CROSS-REFERENCES BETWEEN COBIT 3RD EDITION AND COBIT 4.1

FRAMEWORK-LEVEL CHANGES

The major changes to the COBIT framework as a result of the COBIT 4.0 update were as follows:
- The M domain became ME, standing for Monitor and Evaluate.
- M3 and M4 were audit processes and not IT processes. They were removed, as they were adequately covered by a number of IT audit standards, but references were provided within the updated framework to highlight management's need for, and use of, assurance functions.
- ME3 is the process related to regulatory oversight, which was previously covered by PO8.
- ME4 covers the process of governance oversight over IT, in keeping with COBIT's purpose as an IT governance framework. By positioning that process as the last in the chain, it underscores the support that each prior process provides to the ultimate aim of implementing effective IT governance in the enterprise.
- With the removal of PO8 and the need to keep the numbering for PO9 *Assess risk* and PO10 *Manage projects* consistent with COBIT 3rd Edition, PO8 became *Manage quality*, the old PO11 process. The PO domain now has 10 processes instead of 11.
- The AI domain required two changes: the addition of a procurement process and the need to include in AI5 the aspects of release management. The latter change suggested that this should be the last process in the AI domain so it became AI7. The slot this created at AI5 was used to add the new procurement process. The AI domain now has seven processes instead of six.

COBIT 4.1, an incremental update to COBIT 4.0, includes:
- Enhanced executive overview
- Explanation of goals and metrics in the framework section
- Better definitions of the core concepts. It is important to mention that the definition of a control objective changed, shifting more toward a management practice statement.
- Improved control objectives resulting from updated control practices and Val IT development activity. Some control objectives were grouped and/or reworded to avoid overlaps and make the list of control objectives within a process more consistent. These changes resulted in the renumbering of the remaining control objectives. Some other control objectives were reworded to make them more action-oriented and consistent in wording. Specific revisions include:
  – AI5.5 and AI5.6 were combined with AI5.4
  – AI7.9, AI7.10 and AI7.11 were combined with AI7.8
  – ME3 was revised to include compliance with contractual requirements in addition to legal and regulatory requirements
- Application controls have been reworked to be more effective, based on work to support controls effectiveness assessment and reporting. This resulted in a list of six application controls replacing the 18 application controls in COBIT 4.0, with further detail provided in *COBIT Control Practices, 2nd Edition.*
- The list of business goals and IT goals in appendix I was improved, based on new insights obtained during validation research executed by the University of Antwerp Management School (Belgium).
- The pull-out has been expanded to provide a quick reference list of the COBIT processes, and the overview diagram depicting the domains has been revised to include reference to the process and application control elements of the COBIT framework.
- Improvements identified by COBIT users (COBIT 4.0 and COBIT Online) have been reviewed and incorporated as appropriate.

CONTROL OBJECTIVES

As can be seen from the above description of the framework-level changes and the work to clarify and focus the control objective content, the updating of the COBIT framework has significantly changed the control objectives within it. These components have been reduced from 215 to 210, because all generic materials are now retained only at the framework level and not repeated in each process. Also, all references to applications controls were moved to the framework and specific control objectives were aggregated into new statements. To support transitional activity in relation to control objectives, the following two sets of tables show the cross-references between the new and old control objectives.

MANAGEMENT GUIDELINES

Inputs and outputs have been added to illustrate what processes need from others and what the processes typically deliver. Activities and associated responsibilities have also been provided. Inputs and activity goals replace the critical success factors of COBIT 3rd Edition. Metrics are now based on a consistent cascade of business goals, IT goals, process goals and activity goals. The COBIT 3rd Edition metrics set has also been reviewed and enhanced to make it more representative and measurable.

Cross-reference: COBIT 3rd Edition to COBIT 4.1

COBIT 3rd Edition	COBIT 4.1
PO1 Define a strategic IT plan.	
1.1 IT as part of the organisation's long- and short-range plan	1.4
1.2 IT long-range plan	1.4
1.3 IT long-range planning —approach and structure	1.4
1.4 IT long-range plan changes	1.4
1.5 Short-range planning for the IT function	1.5
1.6 Communication of IT plans	1.4
1.7 Monitoring and evaluating of IT plans	1.3
1.8 Assessment of existing systems	1.3
PO2 Define the information architecture.	
2.1 Information architecture model	2.1
2.2 Corporate data dictionary and data syntax rules	2.2
2.3 Data classification scheme	2.3
2.4 Security levels	2.3
PO3 Determine technological direction.	
3.1 Technological infrastructure planning	3.1
3.2 Monitor future trends and regulations.	3.3
3.3 Technological infrastructure contingency	3.1
3.4 Hardware and software acquisition plans	3.1, AI3.1
3.5 Technology standards	3.4, 3.5
PO4 Define the IT organisation and relationships.	
4.1 IT planning or steering committee	4.3
4.2 Organisational placement of the IT function	4.4
4.3 Review of organisational achievements	4.5
4.4 Roles and responsibilities	4.6
4.5 Responsibility for quality assurance	4.7
4.6 Responsibility for logical and physical security	4.8
4.7 Ownership and custodianship	4.9
4.8 Data and system ownership	4.9
4.9 Supervision	4.10
4.10 Segregation of duties	4.11
4.11 IT staffing	4.12
4.12 Job or position descriptions for IT staff	4.6
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
PO5 Manage the IT investment.	
5.1 Annual IT operating budget	5.3
5.2 Cost and benefit monitoring	5.4
5.3 Cost and benefit justification	1.1, 5.3, 5.4, 5.5
PO6 Communicate management aims and direction.	
6.1 Positive information control environment	6.1
6.2 Management's responsibility for policies	6.3, 6.4, 6.5
6.3 Communication of organisation policies	6.3, 6.4, 6.5
6.4 Policy implementation resources	6.4
6.5 Maintenance of policies	6.3, 6.4, 6.5
6.6 Compliance with policies, procedures and standards	6.3, 6.4, 6.5
6.7 Quality commitment	6.3, 6.4, 6.5
6.8 Security and internal control framework policy	6.2
6.9 Intellectual property rights	6.3, 6.4, 6.5
6.10 Issue-specific policies	6.3, 6.4, 6.5
6.11 Communication of IT security awareness	6.3, 6.4, 6.5
PO7 Manage human resources.	
7.1 Personnel recruitment and promotion	7.1
7.2 Personnel qualifications	7.2
7.3 Roles and responsibilities	7.4
7.4 Personnel training	7.5
7.5 Cross-training or staff backup	7.6
7.6 Personnel clearance procedures	7.7
7.7 Employee job performance evaluation	7.8
7.8 Job change and termination	7.8
PO8 Ensure compliance with external requirements.	
8.1 External requirements review	ME3.1
8.2 Practices and procedures for complying with external requirements	ME3.2
8.3 Safety and ergonomic compliance	ME3.1
8.4 Privacy, intellectual property and data flow	ME3.1
8.5 Electronic commerce	ME3.1
8.6 Compliance with insurance contracts	ME3.1
PO9 Assess risks.	
9.1 Business risk assessment	9.1, 9.2, 9.4
9.2 Risk assessment approach	9.4
9.3 Risk identification	9.3
9.4 Risk measurement	9.1, 9.2, 9.3, 9.4
9.5 Risk action plan	9.5
9.6 Risk acceptance	9.5
9.7 Safeguard selection	9.5
9.8 Risk assessment committment	9.1
PO10 Manage projects.	
10.1 Project management framework	10.2
10.2 User department participation in project initiation	10.4
10.3 Project team membership and responsibilities	10.8
10.4 Project definition	10.5
10.5 Project approval	10.6
10.6 Project phase approval	10.6
10.7 Project master plan	10.7
10.8 System quality assurance plan	10.10
10.9 Planning of assurance methods	10.12
10.10 Formal project risk management	10.9
10.11 Test plan	AI7.2
10.12 Training plan	AI7.1
10.13 Post-implementation review plan	10.14 (part)
PO11 Manage quality.	
11.1 General quality plan	8.5
11.2 QA approach	8.1
11.3 QA planning	8.1
11.4 QA review of adherence to IT standards and procedures	8.1, 8.2
11.5 System development life cycle (SDLC) methodology	8.2, 8.3
11.6 SDLC methodology for major changes to existing technology	8.2, 8.3
11.7 Updating of the SDLC methodology	8.2, 8.3
11.8 Co-ordination and communication	8.2
11.9 Acquisition and maintenance framework for the technology infrastructure	8.2
11.10 Third-party implementor relationships	8.2, DS2.3
11.11 Programme documentation standards	AI4.2, AI4.3, AI4.4
11.12 Programme testing standards	AI7.2, AI7.4
11.13 System testing standards	AI7.2, AI7.4
11.14 Parallel/pilot testing	AI7.2, AI7.4
11.15 System testing documentation	AI7.2, AI7.4
11.16 QA evaluation of adherence to development standards	8.2
11.17 QA review of the achievement of IT objectives	8.2
11.18 Quality metrics	8.6
11.19 Reports of QA reviews	8.2

CobiT 3rd Edition	CobiT 4.1
AI1 Identify automated solutions.	
1.1 Definition of information requirements	1.1
1.2 Formulation of alternative courses of action	1.3, 5.1, PO1.4
1.3 Formulation of acquisition strategy	1.3, 5.1, PO1.4
1.4 Third-party service requirements	5.1, 5.3
1.5 Technological feasibility study	1.3
1.6 Economic feasibility study	1.3
1.7 Information architecture	1.3
1.8 Risk analysis report	1.2
1.9 Cost-effective security controls	1.1, 1.2
1.10 Audit trails design	1.1, 1.2
1.11 Ergonomics	1.1
1.12 Selection of system software	1.1, 1.3
1.13 Procurement control	5.1
1.14 Software product acquisition	5.1
1.15 Third-party software maintenance	5.4
1.16 Contract application programming	5.4
1.17 Acceptance of facilities	5.4
1.18 Acceptance of technology	3.1, 3.2, 3.3, 5.4
AI2 Acquire and maintain application software.	
2.1 Design methods	2.1
2.2 Major changes to existing systems	2.1, 2.2, 2.6
2.3 Design approval	2.1
2.4 File requirements definition and documentation	2.2

CobiT 3rd Edition	CobiT 4.1
2.5 Programme specifications	2.2
2.6 Source data collection design	2.2
2.7 Input requirements definition and documentation	2.2
2.8 Definition of interfaces	2.2
2.9 User-machine interface	2.2
2.10 Processing requirements definition and documentation	2.2
2.11 Output requirements definition and documentation	2.2
2.12 Controllability	2.3, 2.4
2.13 Availability as a key design factor	2.2
2.14 IT integrity provisions in application programme software	2.3, DS11.5
2.15 Application software testing	2.8, 7.4
2.16 User reference and support materials	4.3. 4.4
2.17 Reassessment of system design	2.2
AI3 Acquire and maintain technology infrastructure.	
3.1 Assessment of new hardware and software	3.1, 3.2, 3.3
3.2 Preventive maintenance for hardware	DS13.5
3.3 System software security	3.1, 3.2, 3.3
3.4 System software installation	3.1, 3.2, 3.3
3.5 System software maintenance	3.3
3.6 System software change controls	6.1, 7.3
3.7 Use and monitoring of system utilities	3.2, 3.3, DS9.3

CobiT 3rd Edition	CobiT 4.1
AI4 Develop and maintain procedures.	
4.1 Operational requirements and service levels	4.1
4.2 User procedures manual	4.2
4.3 Operations manual	4.4
4.4 Training materials	4.3, 4.4
AI5 Install and accredit systems.	
5.1 Training	7.1
5.2 Application software performance sizing	7.6, DS3.1
5.3 Implementation plan	7.2, 7.3
5.4 System conversion	7.5
5.5 Data conversion	7.5
5.6 Testing strategies and plans	7.2
5.7 Testing of changes	7.4, 7.6
5.8 Parallel/pilot testing criteria and performance	7.6
5.9 Final acceptance test	7.7
5.10 Security testing and accreditation	7.6
5.11 Operational test	7.6
5.12 Promotion to production	7.8
5.13 Evaluation of meeting user requirements	7.9
5.14 Management's post-implementation review	7.9
AI6 Manage changes.	
6.1 Change request initiation and control	61, 6.4
6.2 Impact assessment	6.2
6.3 Control of changes	7.9
6.4 Emergency changes	6.3
6.5 Documentation and procedures	6.5
6.6 Authorised maintenance	DS5.3
6.7 Software release policy	7.9
6.8 Distribution of software	7.9

CobiT 3rd Edition	CobiT 4.1
DS1 Define and manage service levels.	
1.1 SLA framework	1.1
1.2 Aspects of SLAs	1.3
1.3 Performance procedures	1.1
1.4 Monitoring and reporting	1.5
1.5 Review of SLAs and contracts	1.6
1.6 Chargeable items	1.3
1.7 Service improvement programme	1.6
DS2 Manage third-party services.	
2.1 Supplier interfaces	2.1
2.2 Owner relationships	2.2
2.3 Third-party contracts	AI5.2
2.4 Third-party qualifications	AI5.3
2.5 Outsourcing contracts	AI5.2
2.6 Continuity of services	2.3

CobiT 3rd Edition	CobiT 4.1
2.7 Security relationships	2.3
2.8 Monitoring	2.4
DS3 Manage performance and capacity.	
3.1 Availability and performance requirements	3.1
3.2 Availability plan	3.4
3.3 Monitoring and reporting	3.5
3.4 Modelling tools	3.1
3.5 Proactive performance management	3.3
3.6 Workload forecasting	3.3
3.7 Capacity management of resources	3.2
3.8 Resources availability	3.4
3.9 Resources schedule	3.4
DS4 Ensure continuous service.	
4.1 IT continuity framework	4.1

CobiT 3rd Edition	CobiT 4.1
4.2 IT continuity plan strategy and philosophy	4.1
4.3 IT continuity plan contents	4.2
4.4 Minimising IT continuity requirements	4.3
4.5 Maintaining the IT continuity plan	4.4
4.6 Testing the IT continuity plan	4.5
4.7 IT continuity plan training	4.6
4.8 IT continuity plan distribution	4.7
4.9 User department alternative processing backup procedures	4.8
4.10 Critical IT resources	4.3

COBIT 3rd Edition	COBIT 4.1
4.11 Backup site and hardware	4.8
4.12 Offsite backup storage	4.9
4.13 Wrap-up procedures	4.10
DS5 Ensure systems security.	
5.1 Manage security measures.	5.1
5.2 Identification, authentication and access	5.3
5.3 Security of online access to data	5.3
5.4 User account management	5.4
5.5 Management review of user accounts	5.4
5.6 User control of user accounts	5.4, 5.5
5.7 Security surveillance	5.5
5.8 Data classification	PO2.3
5.9 Central identification and access rights management	5.3
5.10 Violation and security activity reports	5.5
5.11 Incident handling	5.6
5.12 Reaccreditation	5.1
5.13 Counterparty trust	5.3, AC6
5.14 Transaction authorisation	5.3
5.15 Non-repudiation	5.11
5.16 Trusted path	5.11
5.17 Protection of security functions	5.7
5.18 Cryptographic key management	5.8
5.19 Malicious software prevention, detection and correction	5.9
5.20 Firewall architectures and connections with public networks	5.10
5.21 Protection of electronic value	13.4
DS6 Identify and allocate costs.	
6.1 Chargeable items	6.1
6.2 Costing procedures	6.3
6.3 User billing and chargeback procedures	6.2, 6.4
DS7 Educate and train users.	
7.1 Identification of training needs	7.1
7.2 Training organisation	7.2
7.3 Security principles and awareness training	PO7.4

COBIT 3rd Edition	COBIT 4.1
DS8 Assist and advise customers.	
8.1 Help desk	8.1, 8.5
8.2 Registration of customer queries	8.2, 8.3, 8.4
8.3 Customer query escalation	8.3
8.4 Monitoring of clearance	10.3
8.5 Reporting and trend analysis	10.1
DS9 Manage the configuration.	
9.1 Configuration recording	9.1
9.2 Configuration baseline	9.1
9.3 Status accounting	9.3
9.4 Configuration control	9.3
9.5 Unauthorised software	9.3
9.6 Software storage	AI3.4
9.7 Configuration management procedures	9.2
9.8 Software accountability	9.1, 9.2
DS10 Manage problems and incidents.	
10.1 Problem management system	10.1, 10.2, 10.3, 10.4
10.2 Problem escalation	10.2
10.3 Problem tracking and audit trail	8.2, 10.2
10.4 Emergency and temporary access authorisations	5.4, 12.3, AI6.3
10.5 Emergency processing priorities	10.1, 8.3
DS11 Manage data.	
11.1 Data preparation procedures	AC1
11.2 Source document authorisation procedures	AC1
11.3 Source document data collection	AC1
11.4 Source document error handling	AC1
11.5 Source document retention	DS11.2
11.6 Data input authorisation procedures	AC2
11.7 Accuracy, completeness and authorisation checks	AC3
11.8 Data input error handling	AC2, AC4
11.9 Data processing integrity	AC4
11.10 Data processing validation and editing	AC4
11.11 Data processing error handling	AC4
11.12 Output handling and retention	AC5, 11.2
11.13 Output distribution	AC5, AC6

COBIT 3rd Edition	COBIT 4.1
11.14 Output balancing and reconcilation	AC5
11.15 Output review and error handling	AC5
11.16 Security provision for output reports	11.6
11.17 Protection of sensitive information during transmission and transport	AC6, 11.6
11.18 Protection of disposed sensitive information	11.4, AC6
11.19 Storage management	11.2
11.20 Retention periods and storage terms	11.2
11.21 Media library management system	11.3
11.22 Media library management responsibilities	11.3
11.23 Backup and restoration	11.5
11.24 Backup jobs	11.4
11.25 Backup storage	4.9, 11.3
11.26 Archiving	11.2
11.27 Protection of sensitive messages	11.6
11.28 Authentication and integrity	AC6
11.29 Electronic transaction integrity	5.11
11.30 Continued integrity of stored data	11.2
DS12 Manage facilities.	
12.1 Physical security	12.1, 12.2
12.2 Low profile of the IT site	12.1, 12.2
12.3 Visitor escort	12.3
12.4 Personnel health and safety	12.1, 12.5, ME3.1
12.5 Protection against environmental factors	12.4, 12.9
12.6 Uninterruptible power supply	12.5
DS13 Manage operations.	
13.1 Processing operations procedures and instructions manual	13.1
13.2 Start-up process and other operations documentation	13.1
13.3 Job scheduling	13.2
13.4 Departures from standard job schedules	13.2
13.5 Processing continuity	13.1
13.6 Operation logs	13.1
13.7 Safeguard special forms and output devices	13.4
13.8 Remote operations	5.11

COBIT 3rd Edition	COBIT 4.1
M1 Monitor the processes.	
1.1 Collecting monitoring data	1.2
1.2 Assessing performance	1.4
1.3 Assessing customer satisfaction	1.2
1.4 Management reporting	1.5
M2 Assess internal control adequacy.	
2.1 Internal control monitoring	2.2
2.2 Timely operation of internal controls	2.1
2.3 Internal control level reporting	2.2, 2.3
2.4 Operational security and internal control assurance	2.4
M3 Obtain independent assurance.	
3.1 Independent security and internal control certification/accreditation of IT services	2.5, 4.7
3.2 Independent security and internal control certification/accreditation of third-party service providers	2.5, 4.7
3.3 Independent effectiveness evaluation of IT services	2.5, 4.7
3.4 Independent effectiveness evaluation of third-party service providers	2.5, 4.7
3.5 Independent assurance of compliance with laws, regulatory requirements and contractual commitments	2.5, 4.7
3.6 Independent assurance of compliance with laws, regulatory requirements and contractual commitments by third-party service providers	2.5, 2.6, 4.7
3.7 Competence of independent assurance function	2.5, 4.7
3.8 Proactive audit involvement	2.5, 4.7
M4 Provide for independent audit.	
4.1 Audit charter	2.5, 4.7
4.2 Independence	2.5, 4.7
4.3 Professional ethics and standards	2.5, 4.7
4.4 Competence	2.5, 4.7
4.5 Planning	2.5, 4.7
4.6 Performance of audit work	2.5, 4.7
4.7 Reporting	2.5, 4.7
4.8 Follow-up activities	2.5, 4.7

Cross-reference: COBIT 4.1 to COBIT 3rd Edition

COBIT 4.1	COBIT 3rd Edition
PO1 Define a strategic IT plan.	
1.1 IT value management	5.3
1.2 Business-IT alignment	New
1.3 Assessment of current capability and performance	1.7, 1.8
1.4 IT strategic plan	1.1, 1.2, 1.3, 1.4, 1.6, AI1.2, AI1.3
1.5 IT tactical plans	1.5
1.6 IT portfolio management	New
PO2 Define the information architecture.	
2.1 Enterprise information architecture model	2.1
2.2 Enterprise data dictionary and data syntax rules	2.2
2.3 Data classification scheme	2.3, 2.4, DS5.8
2.4 Integrity management	New
PO3 Determine technological direction.	
3.1 Technological direction planning	3.1, 3.3, 3.4
3.2 Technological infrastructure plan	New
3.3 Monitoring of future trends and regulations	3.2
3.4 Technology standards	3.5
3.5 IT architecture board	3.5
PO4 Define the IT processes, organisation and relationships.	
4.1 IT process framework	New
4.2 IT strategy committee	New
4.3 IT steering committee	4.1
4.4 Organisational placement of the IT function	4.2
4.5 IT organisational structure	4.3
4.6 Establishment of roles and responsibilities	4.4, 4.12
4.7 Responsibility for IT quality assurance	4.5
4.8 Responsibility for risk, security and compliance	4.6
4.9 Data and system ownership	4.7, 4.8
4.10 Supervision	4.9
4.11 Segregation of duties	4.10
4.12 IT staffing	4.11
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
PO5 Manage the IT investment.	
5.1 Financial management framework	New
5.2 Prioritisation within IT budget	New
5.3 IT budgeting	5.1, 5.3
5.4 Cost management	5.2, 5.3
5.5 Benefit management	5.3
PO6 Communicate management aims and direction.	
6.1 IT policy and control environment	6.1
6.2 Enterprise IT risk and control framework	6.8
6.3 IT policies management	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Policy, standards and procedures rollout	6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 Communication of IT objectives and direction	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 Manage IT human resources.	
7.1 Personnel recruitment and retention	7.1
7.2 Personnel competencies	7.2
7.3 Staffing of roles	New
7.4 Personnel training	7.3, DS7.3
7.5 Dependence upon individuals	7.4
7.6 Personnel clearance procedures	7.5
7.7 Employee job performance evaluation	7.6
7.8 Job change and termination	7.7, 7.8
PO8 Manage quality.	
8.1 Quality management system	11.2, 11.3, 11.4
8.2 IT standards and quality practices	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 Development and acquisition standards	11.5, 11.6, 11.7
8.4 Customer focus	New
8.5 Continuous improvement	New
8.6 Quality measurement, monitoring and review	11.18
PO9 Assess and manage IT risks.	
9.1 IT risk management framework	9.1, 9.4, 9.8
9.2 Establishment of risk context	9.1, 9.4
9.3 Event identification	9.3, 9.4
9.4 Risk assessment	9.1, 9.2, 9.4
9.5 Risk response	9.5, 9.6, 9.7
9.6 Maintenance and monitoring of a risk action plan	New
PO10 Manage projects.	
10.1 Programme management framework	New
10.2 Project management framework	10.1
10.3 Project management approach	New
10.4 Stakeholder commitment	10.2
10.5 Project scope statement	10.4
10.6 Project phase initiation	10.5, 10.6
10.7 Integrated project plan	10.7
10.8 Project resources	10.3
10.9 Project risk management	10.10
10.10 Project quality plan	10.8
10.11 Project change control	New
10.12 Project planning of assurance methods	10.9
10.13 Project performance measurement, reporting and monitoring	New
10.14 Project closure	10.13 (part)

COBIT 4.1	COBIT 3rd Edition
AI1 Identify automated solutions.	
1.1 Definition and maintenance of business functional and technical requirements	1.1, 1.9, 1.10, 1.11, 1.12
1.2 Risk analysis report	1.8, 1.9, 1.10
1.3 Feasibility study and formulation of alternative courses of action	1.3, 1.7, 1.12
1.4 Requirements and feasibility decision and approval	New
AI2 Acquire and maintain application software.	
2.1 High-level design	2.1, 2.2
2.2 Detailed design	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Application control and auditability	2.12, 2.14
2.4 Application security and availability	2.12
2.5 Configuration and implementation of acquired application software	New
2.6 Major upgrades to existing systems	2.2
2.7 Development of application software	New
2.8 Software quality assurance	2.15
2.9 Applications requirements management	New
2.10 Application software maintenance	New
AI3 Acquire and maintain technology infrastructure.	
3.1 Technological infrastructure acquisition plan	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Infrastructure resource protection and availability	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Infrastructure maintenance	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 Feasibility test environment	New
AI4 Enable operation and use.	
4.1 Planning for operational solutions	4.1
4.2 Knowledge transfer to business management	PO11.11, 4.2
4.3 Knowledge transfer to end users	PO11.11, 2.16, 4.4
4.4 Knowledge transfer to operations and support staff	PO11.11, 2.16, 4.3, 4.4
AI5 Procure IT resources.	
5.1 Procurement control	1.2, 1.3, 1.4, 1.13, 1.14
5.2 Supplier contract management	DS2.3, DS2.5
5.3 Supplier selection	1.4, DS2.4
5.4 IT resources acquisition	1.15, 1.16, 1.17, 1.18
AI6 Manage changes.	
6.1 Change standards and procedures	3.6, 6.1
6.2 Impact assessment, prioritisation and authorisation	6.2
6.3 Emergency changes	DS10.4, 6.4
6.4 Change status tracking and reporting	6.1
6.5 Change closure and documentation	6.5
AI7 Install and accredit solutions and changes.	
7.1 Training	PO10.11, PO10.12, 5.1
7.2 Test plan	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 Implementation plan	3.6, 5.3
7.4 Test environment	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 System and data conversion	5.4, 5.5
7.6 Testing of changes	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Final acceptance test	5.9
7.8 Promotion to production	5.12
7.9 Post-implementation review	5.13, 5.14

COBIT 4.1	COBIT 3rd Edition
DS1 Define and manage service levels.	
1.1 Service level management framework	1.1, 1.3
1.2 Definition of services	New
1.3 SLAs	1.2, 1.6
1.4 OLAs	New
1.5 Monitoring and reporting of service level achievements	1.4
1.6 Review of SLAs and contracts	1.5, 1.7
DS2 Manage third-party services.	
2.1 Identification of all supplier relationships	2.1
2.2 Supplier relationship management	2.2
2.3 Supplier risk management	PO11.10, 2.6, 2.7
2.4 Supplier performance monitoring	2.8
DS3 Manage performance and capacity.	
3.1 Performance and capacity planning	AI5.2, 3.1, 3.4
3.2 Current performance and capacity	3.7
3.3 Future performance and capacity	3.5, 3.6
3.4 IT resources availability	3.2, 3.8, 3.9
3.5 Monitoring and reporting	3.3
DS4 Ensure continuous service.	
4.1 IT continuity framework	4.1, 4.2
4.2 IT continuity plans	4.3
4.3 Critical IT resources	4.4, 4.10
4.4 Maintenance of the IT continuity plan	4.5
4.5 Testing of the IT continuity plan	4.6
4.6 IT continuity plan training	4.7
4.7 Distribution of the IT continuity plan	4.8
4.8 IT services recovery and resumption	4.9, 4.11
4.9 Offsite backup storage	4.12, 11.25
4.10 Post-resumption review	4.13
DS5 Ensure systems security.	
5.1 Management of IT security	5.1, 5.12
5.2 IT security plan	New
5.3 Identity management	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 User account management	5.4, 5.5, 5.6, 5.13, 10.4
5.5 Security testing, surveillance and monitoring	5.6, 5.7, 5.10
5.6 Security incident definition	5.11
5.7 Protection of security technology	5.17
5.8 Cryptographic key management	5.18

COBIT 4.1	COBIT 3rd Edition
5.9 Malicious software prevention, detection and correction	5.19
5.10 Network security	5.20
5.11 Exchange of sensitive data	5.15, 5.16 11.29, 13.8
DS6 Identify and allocate costs.	
6.1 Definition of services	6.1
6.2 IT accounting	6.3
6.3 Cost modelling and charging	6.2
6.4 Cost model maintenance	6.3
DS7 Educate and train users.	
7.1 Identification of education and training needs	7.1
7.2 Delivery of training and education	7.2
7.3 Evaluation of training received	New
DS8 Manage service desk and incidents.	
8.1 Service desk	8.1
8.2 Registration of customer queries	8.2, 10.3
8.3 Incident escalation	8.2, 8.3, 10.5
8.4 Incident closure	8.2

COBIT 4.1	COBIT 3rd Edition
8.5 Reporting and trend analysis	8.1
DS9 Manage the configuration.	
9.1 Configuration repository and baseline	9.1, 9.2, 9.8
9.2 Identification and maintenance of configuration items	9.7, 9.8
9.3 Configuration integrity review	9.3, 9.4, 9.5
DS10 Manage problems.	
10.1 Identification and classification of problems	8.5, 10.1, 10.5
10.2 Problem tracking and resolution	New
10.3 Problem closure	8.4, 10.1
10.4 Integration of configuration, incident and problem management	New, 10.1
DS11 Manage data.	
11.1 Business requirements for data management	New
11.2 Storage and retention arrangements	11.12, 11.19, 11.20, 11.26, 11.30

COBIT 4.1	COBIT 3rd Edition
11.3 Media library management system	11.21, 11.22, 11.25
11.4 Disposal	11.18, 11.24
11.5 Backup and restoration	AI2.14, 11.23
11.6 Security requirements for data management	11.16, 11.17, 11.27
DS12 Manage the physical environment.	
12.1 Site selection and layout	12.1, 12.2, 12.4
12.2 Physical security measures	12.1, 12.2
12.3 Physical access	10.4, 12.3
12.4 Protection against environmental factors	12.5
12.5 Physical facilities management	12.4, 12.6, 12.9
DS13 Manage operations.	
13.1 Operations procedures and instructions	13.1, 13.2, 13.5, 13.6
13.2 Job scheduling	13.3, 13.4
13.3 IT infrastructure monitoring	New
13.4 Sensitive documents and output devices	5.21, 13.7
13.5 Preventive maintenance for hardware	AI3.2

COBIT 4.1	COBIT 3rd Edition
ME1 Monitor and evaluate IT performance.	
1.1 Monitoring approach	1.0*
1.2 Definition and collection of monitoring data	1.1, 1.3
1.3 Monitoring method	New
1.4 Performance assessment	1.2
1.5 Board and executive reporting	1.4
1.6 Remedial actions	New
ME2 Monitor and evaluate internal control.	
2.1 Monitoring of internal control framework	2.0*, 2.2
2.2 Supervisory review	2.1, 2.3
2.3 Control exceptions	New

COBIT 4.1	COBIT 3rd Edition
2.4 Control self-assessment	2.4
2.5 Assurance of internal control	New
2.6 Internal control at third parties	3.6
2.7 Remedial actions	New
ME3 Ensure compliance with external requirements.	
3.1 Identification of external legal, regulatory and contractual compliance requirements	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 Optimisation of response to external requirements	PO8.2
3.3 Evaluation of compliance with external requirements	New

COBIT 4.1	COBIT 3rd Edition
3.4 Positive assurance of compliance	New
3.5 Integrated reporting	New
ME4 Provide IT governance.	
4.1 Establishment of an IT governance framework	New
4.2 Strategic alignment	New
4.3 Value delivery	New
4.4 Resource management	New
4.5 Risk management	New
4.6 Performance measurement	New
4.7 Independent assurance	New

* ME1.0 and ME2.0 introduced in *Control Practices* published by ITGI in 2004.

Appendix VI

Approach to Research and Development

APPENDIX VI—APPROACH TO RESEARCH AND DEVELOPMENT

Development of the COBIT framework content is supervised by the COBIT Steering Committee, formed by international representatives from industry, academia, government, and the IT governance, assurance, control and security profession. International working groups have been established for the purpose of quality assurance and expert review of the project's interim research and development deliverables. Overall project guidance is provided by ITGI.

PREVIOUS COBIT EDITIONS

Starting with the COBIT framework defined in the first edition, the application of international standards, guidelines and research into good practices led to the development of the control objectives. Audit guidelines were next developed to assess whether these control objectives are appropriately implemented. Research for the first and second editions included the collection and analysis of identified international sources and was carried out by teams in Europe (Free University of Amsterdam), the US (California Polytechnic University) and Australia (University of New South Wales). The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing, and industry practices and requirements, as they relate to the framework and to individual control objectives. After collection and analysis, the researchers were challenged to examine each domain and process in depth, and suggest new or modified control objectives applicable to that particular IT process. Consolidation of the results was performed by the COBIT Steering Committee.

The COBIT 3rd Edition project consisted of developing the management guidelines and updating COBIT 2nd Edition based on new and revised international references. Furthermore, the COBIT framework was revised and enhanced to support increased management control, introduce performance management and further develop IT governance. To provide management with an application of the framework, so it can assess and make choices for control implementation and improvements over its information and related technology, as well as measure performance, the management guidelines include maturity models, critical success factors, KGIs and KPIs related to the control objectives.

The management guidelines were developed by using a worldwide panel of 40 experts from academia, government, and the IT governance, assurance, control and security profession. These experts participated in a residential workshop guided by professional facilitators and using development guidelines defined by the COBIT Steering Committee. The workshop was strongly supported by the Gartner Group and PricewaterhouseCoopers, who not only provided thought leadership but also sent several of their experts on control, performance management and information security. The results of the workshop were draft maturity models, CSFs, KGIs and KPIs for each of COBIT's 34 process descriptions. Quality assurance of the initial deliverables was conducted by the COBIT Steering Committee, and the results were posted for exposure on the ISACA web site. The management guidelines document offered a new management-oriented set of tools, while providing integration and consistency with the COBIT framework.

The update to the control objectives in COBIT 3rd Edition, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of COBIT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the control objectives, but to provide an incremental update process. The results of the development of the management guidelines were then used to revise the COBIT framework, especially the considerations, goals and enabler statements of the process descriptions. COBIT 3rd Edition was published in July 2000.

THE LATEST UPDATE PROJECT ACTIVITY

In its effort to continuously evolve the COBIT body of knowledge, the COBIT Steering Committee has initiated over the last two years research into several detailed aspects of COBIT. These focused research projects addressed components of the control objectives and the management guidelines. Some specific areas that were addressed follow.

Control Objectives Research

- COBIT—IT governance bottom-up alignment
- COBIT—IT governance top-down alignment
- COBIT and other detailed standards—Detailed mapping between COBIT and ITIL, CMM, COSO, PMBOK, ISF's *Standard of Good Practice for Information Security* and ISO 27000 to enable harmonisation with those standards in language, definitions and concepts

Management Guidelines Research

- KGI-KPI causal relationships analysis
- Review of the quality of the KGIs/KPIs/CSFs—Based on the KPI/KGI causal relationship analysis, splitting CSFs into 'what you need from others' and 'what you need to do yourself'
- Detailed analysis of metrics concepts—Detailed development with metrics experts to enhance the metrics concepts, building up a cascade of 'process-IT-business' metrics and defining quality criteria for metrics
- Linking of business goals, IT goals and IT processes—Detailed research in eight different industries resulting in a more detailed insight into how COBIT processes support the achievement of specific IT goals and, by extension, business goals; results then generalised
- Review of maturity model contents—Ensured consistency and quality of maturity levels between and within processes, including better definitions of maturity model attributes

All of these projects were initiated and overseen by the COBIT Steering Committee, while day-to-day management and follow-up were executed by a smaller COBIT core team. The execution of most of the aforementioned research projects was based heavily on the expertise and volunteer team of ISACA members, COBIT users, expert advisors and academics. Local development groups were set up in Brussels (Belgium), London (England), Chicago (Illinois, USA), Canberra (Australian Capital Territory), Cape Town (South Africa), Washington (DC, USA) and Copenhagen (Denmark), in which five to 10 COBIT users gathered on average two to three times per year to work on specific research or review tasks assigned by the COBIT core team. In addition, some specific research projects were assigned to business schools such as the University of Antwerp Management School (UAMS) and the University of Hawaii.

The results of these research efforts, together with feedback provided by COBIT users over the years and issues noted from the development of new products such as the control practices, have been fed into the main COBIT project to update and improve the COBIT control objectives, management guidelines and framework. Two major development labs, each involving more than 40 IT governance, management and control experts (managers, consultants, academics and auditors) from around the world, were held to review and thoroughly update the control objectives and management guidelines content. Further smaller groups worked on refining or finalising the significant output produced by these major events.

The final draft was subject to a full exposure review process with approximately 100 participants. The extensive comments received were analysed in a final review workshop by the COBIT Steering Committee.

The results of these workshops have been processed by the COBIT Steering Committee, the COBIT core team and ITGI to create the new COBIT material available in this volume. The existence of COBIT Online means that the technology now exists to keep the core COBIT content up to date more easily, and this resource will be used as the master repository of COBIT content. It will be maintained by feedback from the user base as well as periodic reviews of specific content areas. Periodic publications (paper and electronic) will be produced to support offline reference to COBIT content.

APPENDICE VII—GLOSSARIO

Access control—Il processo che limita e controlla l'accesso alle risorse di un sistema; un controllo fisico o logico progettato per proteggere da accessi o utilizzi non autorizzati.

Accountable—In un diagramma RACI, si riferisce alla persona o al gruppo che ha la responsabilità di approvare o accettare l'esecuzione di un attività

Activity—Le azioni principali per applicare il CobiT

Application program—Un programma che elabora i dati dati attraverso attività come immissione di dati, aggiornamenti o richieste. È diverso dai programmi di sistema, come il sistema operativo o dai programmi di gestioni di rete, e degli altri programmi per la copia o l'ordinamento.

Audit charter—Un documento approvato da una commessione che definisce scopo, autorizzazioni e responsabilità dell'attività interna di audit

Authentication—L'atto di verifica dell'identità di un entità di sistema (es. User, system, network node) e dell'autorizzazione di accesso alle informazioni computerizzate. Pensata per proteggere da accessi fraudolenti, l'autenticazione può anche riferirsi alla verifica della correttezza dei dati.

Automated application control—Un insieme di controlli presenti in soluzioni automatizzate (applicazioni).

Balanced scorecard—Un insieme di misure di performance organizzate in quattro categorie. Includono i tradizionali indicatori finanziari, ma aggiungono clienti, processi di business interni, e la crescita delle prospettive. È stata sviluppata da Robert S.Kaplan and David P. Norton nel 1992.

Benchmarking—L'approccio sistematico nel comparare le performance delle organizzazioni nei confronti dei concorrenti allo scopo di comprendere il modo migliore di condurre il business (e.g., benchmarking of quality, logistical efficiency and various other metrics).

Best practice—Un attività o un processo che è stato utilizzato con successo da più organizzazioni.

Business process—Vedi Process.

Capability—Avere le caratteristiche necessari per potare a termine un compito.

Capability Maturity Model (CMM)—Il CMM per il Software, redatto dal Software Engineering Institute (SEI). Un modello usato da molte organizzazioni per identificare le linee guida utili nell'aiutarle a valutare e aumentare il livello dei loro software di processo.

CEO—Amministratore delegato; la carica individuale più alta in un'organizzazione.

CFO—Chief financial officer; il responsabile primario per la gestione del rischio finanziario di un organizzazione.

CIO—Chief information officer; il responsabile IT. In alcuni casi il CIO ha ruoli aggiuntivi e diventa chief knowledge officer (CKO), che ha deleghe non solo per quanto riguarda l'IT.

CTO—Chief technology officer; centrato sulle soluzioni tecniche in un'organizzazione. Il titolo CTO è associato spesso come sinonimo di CIO.

Configuration item (CI)—Componenti di un infrastruttura—o un entità, come una richiesta di cambio, associate con un infrastruttura—che è sotto il controllo di configurazioni personalizzabili. I CI possono variare in complessità, grandezza e tipo partendo da un un intero sistema(incluso tutto l'hardware, software e documentazione) e arrivando a un singolo modulo o componente hardware.

Configuration management—Il controllo delle modifiche delle configurazioni attraverso una serie di configurazioni in un sistema.

Consulted—In un diagramma RACI, si riferisce a quella persone le cui opinioni sono richieste su un'attività (comunicazione bidirezionale)

Continuity—Prevenire, mitigare e recuperare da una distruzione. I termini 'business resumption planning', 'disaster recovery planning' e 'contingency planning' possono essere usati in questo contesto; tutti si concentrano negli aspetti di recupero.

Control framework—Un insieme dei controlli fondamentali che facilita lo scarico di responsabilità del responsabile del business, per impedire perdite finanziarie o di dati informative in un'organizzazione.

Control objective—Una dichiarazione del risultato o dello scopo che vuole essere ottenuto applicando le procedure di controllo in un particolare processo

Control practice—Meccanismo chiave di controllo, che sostiene il successo degli obiettivi di controllo con un uso responsabile delle risorse, con un management adatto del rischio ed allineamento degli apparati IT con il business.

COSO—Committee of Sponsoring Organisations of the Treadway Commission. Il suo 1992 report *Internal Control—Integrated Framework* è uno standard internazionale per la corporate governance. Vedere *www.coso.org*.

CSF—Fattore critico di successo; problematiche o azioni più importanti per il management per realizzare il controllo sui relative processi IT.

Dashboard—Un tool per la definizione delle aspettative di un'organizzazione ad ogni livello di responsabilità e il continuo monitoraggio delleprestazioni a fronte degli obiettivi prefissati.

Data classification scheme—Uno schema per classificare i dati a livello aziendale in base a fattori quali criticità, sensibilità e proprietà

Data dictionary—Una base di dati che contiene il nome, il tipo, la gamma di valori, la fonte e l'autorizzazione per l'accesso ai dati. Inoltre indica quali programmi applicativi usano quei dati in modo che quando una struttura di dati è contemplata, una lista dei programmi interessati può essere generata. Il dizionario di dati può essere un sistema d'informazione autonomo usato per il management o generare documentazione, o può tracciare le operazioni su una base di dati.

Data owners—Persone, normalmente manager o dirigenti, che hanno la responsabilità dell'integrità, della reportistica e dell'uso dei dati

Detective control—Un controllo utilizzato per identificare gli eventi (indesiderati o voluti), gli errori ed altri casi che un'azienda ha evidenziato con possibili effetti materiali su un processo o su un prodotto finale

Domain—In COBIT, il raggruppamento degli obiettivi di controllo in fasi logiche del ciclo di vita IT degli investimenti che coinvolgono l'IT stesso (Pianificazione e Organizzazione, Acquisto e Implementazione, Rilascio e Supporto e Monitoraggio e Valutazione)

Enterprise—Un gruppo di persone che lavorano insieme per uno scopo comune, tipicamente all'interno del contesto di una forma organizzativa quali una società, un'agenzia pubblica, un ente di beneficenza o una associazione

Enterprise architecture—Descrizione del disegno fondamentale dei componenti del sistema di business, o di un elemento del sistema di business (es. tecnologia), i rapporti fra loro ed il modo in cui sostengono gli obiettivi dell'organizzazione

Enterprise architecture for IT—Descrizione del disegno fondamentale dei componenti del sistema IT, o di un elemento del sistema IT, i loro rapporti ed il modo in cui sostengono gli obiettivi dell'organizzazione

Enterprise governance—Un insieme delle responsabilità e delle pratiche dell'amministrazione dell'esecutivo con l'obiettivo di fornire un senso strategico, accertandosi che gli obiettivi siano realizzati, accertandosi che i rischi siano correttamente controllati e verificando che le risorse dell'azienda siano usate responsabilmente

Framework—Vedi Control framework.

General computer controls—Controlli, diversi dai controlli applicativi, che si riferiscono all'ambiente su cui i sistemi applicativi sono sviluppati, mantenuti e operativi e che quindi possono essere applicati a tutte le applicazioni. Gli obiettivi dei controlli generali sono quelli di accertare lo sviluppo e l'implementazione adeguata delle applicazioni, l'integrità dei dati e dei programmi e il funzionamento dei calcolatori. Come i controlli applicativi, i comandi generali possono essere manuali o programmati. Esempi di comandi generali sono includere lo sviluppo e l'implementazione di una strategia IS e una politica di sicurezza IS, l'organizzazione di personale IS per separare le funzioni in conflitto e la progettazione per la disaster prevention e disaster recovery.

Guideline—Descrizione di una particolare modo da seguire per completare qualcosa che è meno formale di una procedura

Information architecture—Un componente dell'architettura IT (insieme alle applicazioni ed alla tecnologia). Vedere architettura

Informed—In un diagramma RACI, si riferisce a quelle persone cje sono aggiorante nel progresso di un attività (comunicazione unidirezionale).

Internal control—Le politiche, i programmi, le procedure e le strutture organizzative per fornire l'assicurazione ragionevole che gli obiettivi di business saranno realizzati e gli eventi indesiderati saranno evitati o rilevati e corretti

ISO 9001:2000—Code of practice for quality management from the International Organisation for Standardisation (ISO). ISO 9001:2000, che specifica i requisiti di un sistema di management di qualità per tutta l'organizzazione che deve dimostrare la relativa abilità nel fornire costantemente prodotto o assistenza che incontrano determinati target di qualità.

ISO 17799—Uno standard internazionale che definisce controlli relativi alla riservatezza, integrità e disponibilità delle informazioni.

ISO 27001—*Information Security Management—Specification with Guidance for Use*; rimpiazza la BS7799-2. Intende fornire il fondamento per la verifica di terzi ed è armonizzato con altri standard, quale ISO/IEC 9001 and 14001.

IT—Information technology; l'hardware, il software, le comunicazioni e le altre risorse usate per input, store, processi, transmissioni e output di dati in qualunque forma.

IT architecture—Descrizione della struttura di fondo fondamentale dei componenti IT del business, dei rapporti fra loro ed il modo in cui sostengono gli obiettivi dell'organizzazione

ITIL—The UK Office of Government Commerce (OGC) IT Infrastructure Library; Una raccolta di guide di management e fornitura di servizi IT.

IT incident—Qualsiasi evento che non fa parte del funzionamento ordinario di un servizio e che causa, o può causare, un'interruzione o una riduzione , della qualità di un determinato servizio (allineato a ITIL)

IT investment dashboard—Un tool per la definizione delle aspettative per un'organizzazione ad ogni livello e per il monitoraggio continuo delle prestazioni verso gli obiettivi prefissati per le spese ed il ritorno dai progetti di investimento IT, in termini di valori di affari

IT strategic plan—Un programma di lunga durata, tre o cinque anni, in cui il businesss e l'IT management contribuiscono con gli obiettivi stategici dell'azienda(obiettivi)

IT strategy committee—Il comitato a livello della comissione dei direttori per accertarsi che la commissione sia coinvolta nelle decisioni più importanti. Il comitato è soprattutto responsabile per il controllo dei portafogli di investimento, servizi IT e altre risorse IT. Il comitato è il proprietario del portafoglio.

IT tactical plan—Un programma a medio termine, tra I 6 e I 18 mesi, che traduce la direzione del piano strategico IT in iniziative richieste, in requisiti delle risorse e nei modi nei quali le risorse e i benefits saranno controllati e monitorati.

IT user—Una persona che utilizza strumeti IT per sostenere o realizzare un obiettivo di business

Key management practices—Quelle line di business richieste per per eseguire con successo dei progetti.

KGI—Indicatori chiave di un obiettivo; indici che segnalano all'amministrazione, dopo un determinato avvenimento, se un processo IT sta realizzando i relativi requisiti di business, espressi solitamente in termini di test.

KPI—Indici chiave di prestazioni; gli indici che determinano come il processo sta evolvendo per raggiungere l'obiettivo prefissato. Sono gli indicatori più significativi per capire come un obiettivo è raggiunto, e sono buoni indici per valutare le capacità, le professioni e le abilità. Misurano gli scopi delle attività, che sono le azioni che i responsabili di processo devono intraprendere per raggiungere le performance effettive per il processo.

Maturity—In business, indica il grado di affidabilità o dipendenza che un attività di business può avere nei confronti di un processo per raggiungere gli obiettivi desiderati.

Measure—Uno standard per valutare e comunicare le performance nel raggiungere risultati fissati. Le misure sono normalmente quantitative come numeri, valute, percentuali, etc., ma possono anche valorizzare informazioni qualitative come la soddisfazione dei clienti. Presentare e monitorare le misure aiuta un'organizzazione a calibrare un progresso verso l'effettiva implementazione di una strategia.

Metrics—Descrizioni specifiche di come una valutazione quantitativa e periodica delle prestazioni deve essere misurata. Una metrica completa definisce l'unità utilizzata, la frequenza, il valore ideale da raggiungere, la procedura per effettuare la misura e la procedura per interpretare le valutazioni.

OLA—Operational level agreement; un accordo interno che riguarda il delivery dei servizi che sostengono l'organizzazione IT nel suo relative delivery dei servizi.

Organisation—Il modo in cui un azienda è strutturata; può anche intendere un ente.

Outcome measures—Le misure che rappresentano le conseguenze di azioni precedentemente intraprese e spesso si considerano come indicatori di ritardi. Frequentemente focalizzano i risultati alla conclusione di un periodo di tempo e caratterizzano le prestazioni storiche. Sono anche relazionati agli indicatori chiave (KGIs) e di solito indicano se gli obiettivi sono stati raggiunti. Questi possono essere misurati solo dopo il fatto in considerazione e per questo sono chiamati 'lag indicators'.

Performance—In IT, l'esecuzione o il successo reale di un processo

Performance drivers—Misure che sono considerati i 'driver' degli indicatori di ritardi. Possono essere misurati prima che il risultato sia definito, perciò sono anche chiamati 'lead indicators'. C'è una relazione presupposta tra i due che suggerisce che le prestazioni migliorate di un indicatore principale guideranno prestazioni più brillanti nei 'laggin indicator'. Sono anche relazionati agli indicatori di performance (KPIs) e di solito indicano se gli obiettivi stanno per essere raggiunti.

Performance management—In IT, la capacità di controllare qualsiasi tipo di misura, compreso l'impiegato, squadra, processo, misure operative e finanziarie. Il termine indica in circuito chiuso di contollo e monitoraggio regolare delle misure.

PMBOK—Project Management Body of Knowledge; un project management standard sviluppato dal Project Management Institute (PMI)

PMO—Project management officer; la funzione individuale responsabile dell'implementazione di una specifica iniziativa per supportare un ruolo di project management e avanzate discipline di project management.

Policy—Generalmente, un documento che registra un principio o una linea di condotta ad alto livello che è stata stabilita. Lo scopo di una policy è di influenzare e guidare le decisioni presenti e future per essere in conformità con la filosofia, gli obiettivi e i programmi strategici stabiliti dai team manager dell'azienda. Oltre al contenuto stesso, le policy devono descrivere le conseguenze del non aderire alle policy stesse, il modo di gestire le eccezionie il modo in cui la conformità alle policy sarà controllata e misurata.

Portfolio—Un gruppo di programmi, progetti, servizi o risorse selezionati, gestiti e monitorati per ottimizzare il ritorno di business

Preventive control—Un controllo interno che è usato per prevenire eventi indesiderati, errori e altri eventi, determinati dall'organizzazione, che possono avere sonseguenze materiali negative su un processo o un prodotto finale.

PRINCE2—Projects in a Controlled Environment, sviluppato da OGC; un metodo di project management che copre la gestione, il controllo e l'organizzazione di un progetto.

Problem—Nell'IT, la causa sconosciuta che causa uno o più incidenti.

Procedure—Un documento che contiene I passi che specificano come realizzare un attività. Le procedure sono definite come la parte di un processo.

Process—Generalmente, un insieme di procedure influenzate dalle policy di un organizzazione e procedure che sono alimentate da un numero di sorgenti, includendo gli altri processi, e procedure che manipolano gli input e le procedure di output, includendo gli altri processi. I processi hanno una chiara ragione per esistere, responsabili, ruoli ben definiti e responsabilità sull'esecuzione del processo ed i mezzi per misurare le prestazioni.

Programme—Un gruppo strutturato di progetti interdipendenti che include lo scopo di business, processi, persone, tecnologie e attività organizzative che richiedono (necessario e sufficente) per raggiungere un ben definito risultato di business.

Project—Un insieme di attività strutturate interessate nel fornire all'azienda una capacità definite (che è necessaria, ma non sufficente per raggiungere un risultato richiesto) basata su un programma e un budget concordato.

QMS—Quality management system; un sistema che descrive le policy e le procedure necessarie per migliorare e controllare i vari processi che alla fine condurranno al miglioramento delle prestazioni dell'organizzazione.

RACI chart—Riportano chi è il responsabile, consultato e informato del quadro organizzativo.

Resilience—In business, la proprietà di un sistema o di una rete di ripararsi automaticamente da un guasto, tipicamente con minime conseguenze rilevabili.

Responsible—In un diagramma RACI, si riferisce una persona che deve assicurarsi che le attività siano completate con successo.

Risk—In business, la probabilità che una data minaccia sfrutti le vulnerabilità di una risorsa o di un gruppo di risorse per causare la perdita e/o il danneggiamento degli stessi; misurato solitamente tramite una combinazione di effetti e le probabilità con cui può verificarsi.

Root cause analysis—Processo di diagnosi per stabilire l'origine di un evento, che può essere usato per imparare dalle conseguenze, tipicamente di errori e problemi.

SDLC—System development life cycle; le fasi impiegate nello sviluppo o nell'acquisiszione di un sistema software. Una fase tipica include lo studio di fattibilità, l'analisi dei requisiti, la definizione dei requisiti, una progettazione dettagliata, lo sviluppo software, la fase di test, l'installazione e il supporto post-implementazione, ma non include il delivery dei servizi o realizzazione di attività supplementari.

Segregation/separation of duties—Un controllo interno basilare che previene o rileva errori e irregolarità assegnando a individui separati responsabilità per avviare e registrare tranzazioni e assegnare in custodia le risorse ad individui separati. Comunemente è usato in grandi organizzazioni IT, in modo che nessuna singola persona sia in una posizione per introdurre codice fraudolento o malevolo senza che questo sia rilevato.

Service desk—Un punto di contatto con l'organizzazione IT per gli utenti dei servizi IT.

Service provider—Entità esterna che fornisce servizi a un organizzazione.

SLA—Service level agreement; un accordo, preferibilmente documentato, tra un fornitore di servizi e i clienti/utenti che definisce gli obiettivi minimi di performance per un servizio e come questi sono misurati.

Standard—Un requisito obbligatorio. Alcuni esempi: ISO/IEC 20000 (standart internazionale), uno standard interno di sicurezza per le configurazioni di UNIX o uno standard governativo che definisce come le note finanziarie devono essere mantenute. Il termine 'standard' è usato anche per far riferimento a in insieme di specifiche o procedure pubblicate da un organismo per la definizione degli standards come ISO o BSI.

TCO—Total cost of ownership; in IT include:

- Costo iniziale dei computer e del software
- Aggiornamenti hardware software
- Attività di manutenzione
- Technical support
- Training
- Alcune attività sviluppate dagli utenti

Technology infrastructure plan—Un piano per le teconoglie, risorse umane e risorse che consentono l'uso attuale e futuro delle applicazioni.

Page intentionally left blank

Appendix VIII

CobiT and Related Products

APPENDIX VIII—COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.0 and higher, includes all of the following:
- Framework—Explains how COBIT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:
- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- COBIT Online—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition.*
- *IT Assurance Guide: Using COBIT*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in *Audit Guidelines* for auditing and self-assessment against the control objectives in COBIT 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit
- COBIT *Quickstart*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- COBIT *Security Baseline*—Focuses on essential steps for implementing information security within the enterprise. The second edition is in development at the time of this writing.
- COBIT Mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*
  - *COBIT Mapping: Overview of International IT Guidance, 2nd Edition*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT Mapping: Mapping of PMBOK With COBIT 4.0*
  - *COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
  - *COBIT Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:
- *Enterprise Value: Governance of IT Investments—The Val IT Framework*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters and other framework-specific information, visit *www.isaca.org/cobit* and *www.isaca.org/valit*.

Page intentionally left blank

Leading the IT Governance Community

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*