Gruppo di Ricerca

C. Bacchieri – E. Boati – M. Rinalducci

AUDITING CON LO STANDARD BS7799

Realizzato con la collaborazione di

PRICEWATERHOUSECOOPERS
Global Management Solutions

L'AIEA, Associazione Italiana Information Systems Auditors è un Capitolo ISACA

Information Systems Audit and Control Association®

Indice

1. Introduzione

L'attività dell'Auditor dei sistemi informativi impone a tutti coloro i quali svolgono questa professione un costante aggiornamento su tutte le principali tematiche della sicurezza ITC. Il compito è alquanto difficile non tanto per la necessità di dover apprendere sempre nuove conoscenze al sorgere di nuove soluzioni tecnologiche, bensì per l'elevato grado di professionalità che richiede il saper discernere di volta in volta quali sono le effettive implicazioni in termini di potenziali rischi per il Sistema Informativo aziendale che un'innovazione porta con sé. Accade ad esempio che uno strumento quale un firewall, oggetto pensato, realizzato, commercializzato ed utilizzato comunemente come mezzo di tutela della sicurezza ITC in azienda, possa addirittura trasformarsi nella fonte primaria di rischio. Ciò avviene, ovviamente, solo in determinate circostanze. Ma sono proprio quelle circostanze le implicazioni che un buon I.S. Auditor deve saper riconoscere.
Oltre alla capacità di individuare i rischi nascosti – e quindi le relative contromisure – un secondo elemento che contribuisce a rendere la professione dell'auditor innanzitutto una sfida, è la capacità di valorizzare, capitalizzare e costruire sui risultati ottenuti. Data l'estrema dinamicità del mondo informatico, se non si sviluppa una simile capacità si ricadrebbe in una sorta di supplizio *tantalico* del terzo millennio: ricostruire un sistema di controlli efficace ed efficiente ad ogni nuova minaccia portata dall'evoluzione tecnologica.
Ecco perché si è voluto intraprendere un Gruppo di lavoro AIEA che si occupasse di approfondire le implicazioni – teoriche e pratiche – di auditing dell'affermazione dello standard di sicurezza britannico BS7799. Le domande alle quali si è cercato di dare risposta sono pertanto: quali sono i risvolti per la mia attività che lo standard porta? Come faccio ad usarlo? In che modo con questo standard posso dare valore aggiunto a quanto ho sinora fatto?

Sperando di essere riusciti in tale impresa non ci resta che augurarvi: buona lettura e buon lavoro!

Claudio Bacchieri – AEM
Massimiliano Rinalducci – Gruppo Unicredit
Emanuele Boati, CISA – Consigliere AIEA

2. Obiettivi del lavoro

Il presente documento è stato redatto con il preciso scopo di costituire una guida essenziale, nei suoi riferimenti teorici, e pratica nell'uso quotidiano. L'oggetto trattato è lo standard di sicurezza inglese BS7799 che si è oramai affermato a livello di mercato internazionale.

3. Perché utilizzare lo standard

Con lo sviluppo della nuova era dell'informatica le diverse nazioni industrializzate del mondo si sono buttate nell'arena dei fornitori di servizi "high-tech", in forte competizione l'una contro l'altra. Sull'onda di ciò le aziende si stanno facendo sempre più carico di responsabilità nei confronti dei propri clienti; responsabilità derivanti dalla gestione di informazioni riservate e dall'effettuazione di transazioni on-line quali anche pagamenti di beni e servizi. Entrambe queste attività sono ad alto rischio. La gestione dell'Information Security si concentra verso l'identificazione di tali rischi informativi e verso l'adozione di adeguate ed efficaci contromisure per annullarne o mitigarne i possibili effetti negativi.

Lo standard, a suo tempo promosso dal governo britannico, ha appunto lo scopo di guidare i potenziali clienti internazionali nell'individuare quali aziende dispongono di servizi realmente sicuri ed affidabili. L'ISO/IEC 17799:2000 permette alle aziende certificate di dimostrare in modo pubblico e formalmente riconoscibile che esse possono adeguatamente proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite e conservate per conto dei propri clienti. Tutto ciò si tramuta in un efficace strumento per catalizzare le opportunità di business e conseguire un vantaggio strategico rispetto ai concorrenti nazionali ed internazionali. Come riportato negli allegati, sono oramai 104 le aziende che nel mondo hanno sfruttato l'opportunità offerta dalla certificazione. E' da notare a riguardo che i settori cui queste appartengono coprono praticamente l'intero spettro delle realtà di mercato: dalle aziende di servizi alle società finanziarie, dalle banche agli enti pubblici sino agli ospedali. Una simile varietà testimonia, al di là di ogni dubbio, della possibilità di inserire con successo queste "buone prassi" in qualunque contesto economico.

4. Breve storia dello Standard BS7799

Agli inizi degli anni '90, il DTI (Department of Trade and Industry) britannico ha istituito un Gruppo di lavoro, in risposta ad un'esigenza emersa in ambito industriale, finalizzato a fornire alle aziende una guida per il governo della sicurezza del loro patrimonio informativo. Il Gruppo ha pubblicato nel 1993 una raccolta di "best practice" (Code of Practice for Information Security Management) che costituì la base per lo standard britannico BS779 pubblicato dal BSI (British Standard Institution) nel 1995. Nel 1998 fu aggiunta una seconda parte allo standard (Specification for Information Security Mangement Systems) che fu poi sottoposto ad una revisione complessiva conclusasi con la pubblicazione, nell'aprile del 1999, di una nuova versione delle sue due parti. Lo standard BS7799 riguarda nominalmente ogni forma di gestione dell'informazione ma di fatto gli aspetti informatici risultano fortemente predominanti.

Nel 1995 la Gran Bretagna sottopose lo standard BS7799 all'ISO/IEC JTC1 SC27 affinché venisse approvato come standard ISO ma, seppure di stretta misura, la proposta non fu accettata. Nel frattempo però l'Australia, la Nuova Zelanda e l'Olanda hanno sviluppato schemi nazionali di certificazione basati sullo standard BS7799 e l'interesse intorno a tale standard è cresciuto anche in molti altri paesi (tra i quali: Brasile, Danimarca, Giappone, Norvegia, Polonia, Sud Africa, Svezia, Svizzera, etc.) tanto che la proposta di trasformarlo in uno standard internazionale è stata nuovamente presentata all'ISO nell'autunno del 1999 e la parte 1 dello standard BS7799 è divenuta uno standard internazionale ISO (IS 17799) alla fine del 2000. La parte 2 sarà successivamente sottoposta all'ISO perché divenga anch'essa uno standard internazionale.

Lo standard ruota intorno ai due concetti di politica di sicurezza e di sistema di governo della sicurezza (di cui la prima costituisce uno degli aspetti) secondo un approccio simile a quello degli standard della serie ISO9000 per la certificazione di qualità di un'azienda. I concetti di politica di qualità e di sistema di gestione della qualità sui quali tali serie si basa, sono sostituiti da quelli di politica di sicurezza dell'informazione e di sistema di governo della sicurezza dell'informazione o ISMS (Information Security Management System).
La politica di sicurezza è la specificazione ad alto livello degli obiettivi di sicurezza (espressi, come di consueto in termini di volontà di salvaguardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce) che l'organizzazione si propone di conseguire.

L'ISMS, invece, è il complesso di procedure per il governo della sicurezza attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento della politica di sicurezza.
La Parte 2 dello standard BS7799 propone il modello di ISMS (rappresentato in Fig. 1). Si tratta di un modello dinamico nel quale vengono individuate 6 fasi di analisi e gestione del problema. I risultati delle analisi e le scelte di gestione vengono permanentemente messe in discussione in modo da garantire la capacità dell'azienda di mantenere nel tempo la sicurezza del proprio patrimonio informativo anche in presenza degli inevitabili cambiamenti dovuti a fattori esterni o interni all'azienda stessa.

La Parte 1 dello standard è un elenco di funzioni di sicurezza (controlli) di tipo organizzativo, logico, fisico, che costituiscono la prassi corrente per garantire la sicurezza dell'informazione in ambito industriale. Lo standard propone un insieme di 127 controlli raggruppati in 10 categorie, più avanti illustrate nel dettaglio.

Nell'insieme dei 127 controlli previsti vanno selezionati, attraverso un processo di analisi del rischio, quelli che soddisfano le esigenze di protezione dell'organizzazione. I controlli prescelti costituiscono una sorta di regolamento di sicurezza che l'azienda si impone di rispettare. Tali controlli dovranno essere realizzati: attraverso meccanismi hardware o software (sistemi di autenticazione tramite password e/o smart-card, prodotti per la protezione crittografica dei dati, firewall, etc.), nel caso dei controlli attuati mediante misure di sicurezza di tipo tecnico; attraverso l'installazione di sistemi anti-intrusione, telecamere, casseforti, contenitori ignifughi, etc. nel caso dei controlli che richiedono misure di sicurezza fisiche; attraverso la creazione di apposite strutture o cariche aziendali e la definizione di precise procedure per la messa in atto dei controlli di tipo procedurale (ad esempio l'istituzione del forum aziendale per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di indottrinamento periodico del personale, le procedure per l'accettazione di visitatori all'interno dell'azienda, etc.).

Lo standard BS 7799 è utilizzato in Gran Bretagna e in altri paesi, come riferimento per la certificazione di un'azienda rispetto alla sua capacità di garantire la sicurezza del proprio patrimonio informativo o di quello di terzi a lei affidato. La certificazione avviene a seguito di una revisione della documentazione dell'ISMS (durata: 2-3 settimane) e di una verifica iniziale, sul campo, che quanto stabilito dall'ISMS sia stato efficacemente e correttamente realizzato (durata: 4-10 giorni). Il mantenimento del certificato richiede visite ispettive periodiche (semestrali) e la ripetizione completa delle verifiche ogni 3 anni.

5. Schema dell'ISMS – Information Security Mananagement System

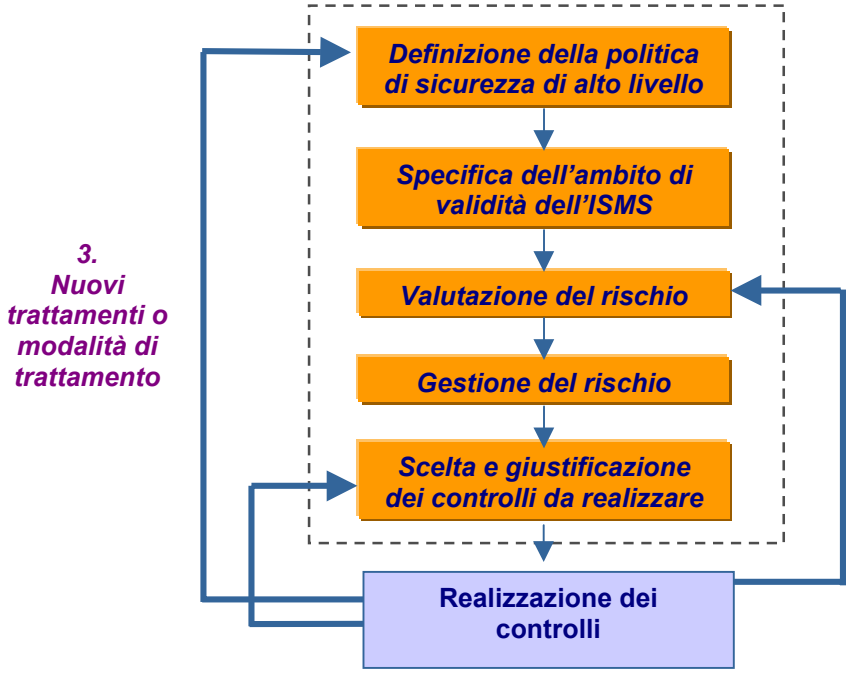


Fig. 1 - Il modello di ISMS proposto dallo standard BS7799

6. Riferimenti incrociati con CobiT

REPORT SULLA CORRELAZIONE TRA ISO 17799 E COBIT

Il ruolo di IS Auditor che ricopriamo ed il lavoro di ricerca sull'argomento degli standard di sicurezza ci hanno portato ad esplorare anche altre realtà che, pur essendo lontane per cultura e per dislocazione geografica, si avvicinano a noi per l'approccio utilizzato al problema della sicurezza e per gli strumenti individuati per rispondere alle Politiche adottate.

È il caso dell'Agenzia di Stato dell'Oregon (USA) che, nella propria politica di e-Government, ha adottato, tra gli altri, COBIT e ISO 17799 per raggiungere gli obiettivi inseriti nelle proprie Politiche di sicurezza sviluppando, laddove possibile, una matrice di correlazione tra le due metodologie.

Riportiamo qui di seguito la traduzione di uno stralcio della documentazione sull'argomento citato.

Relazione tra le Politiche di Sicurezza basate sugli standard ISO 17799 e lo standard COBIT - un riferimento incrociato

Introduzione alle Politiche

Le Politiche di Sicurezza sono una espressione gestionale direttiva e di intenti. Non sono documenti tecnici o spiegazioni dettagliate di metodi e approcci ai sistemi di sicurezza, ma è l'autorità ed il riferimento per linee guida successive e standard per attuare i requisiti e gli intenti delle Politiche.

Le Politiche sono il fondamento per una buona struttura di sicurezza delle informazioni. Senza il fondamento di queste, nessuno sforzo è efficace.

Insieme con molti altri benefici, una comunicazione chiara delle Politiche crea consapevolezza sui problemi di sicurezza, una consapevolezza della responsabilità del management e degli utenti di aderire alle procedure di sicurezza, e una mappa per gli auditor e per gli enti addetti all'emissione di regolamenti al fine di capire gli intendimenti del management nel limitare i rischi, circoscrivere le conseguenti responsabilità e quindi individuare e reagire alle violazioni delle Politiche stesse.

L'uso degli standard

La necessità di creare Politiche efficaci e significative è difficile sia per i governi che per l'industria. Quanto lo stesore delle Politiche è in grado di sapere che tutto è coperto adeguatamente? Qualche elemento è stato dimenticato o è sfuggito? Per questo motivo una grande quantità di sforzi e iniziative sono stati impiegati nello sviluppo di manuali e standard internazionali come COSO, Cadbury, TCSEC, COBIT e ISO 17799. Ciascuno ha i suoi punti di forza e debolezza nel contempo. Di solito questi punti di forza e di debolezza sono relativi all'area per i quali sono stati emessi - TCSEC per un focus di alta confidenzialità per il Ministero della Difesa USA, COBIT dal mondo dell'audit dell'IT per l'ISACA (Information Systems Audit and Control Association), e ISO 17799 dagli interessi del British Government Information Security.

Nessuno standard può dirsi completo senza il contributo degli altri. Lo Stato dell'Oregon ha adottato il COBIT come lo standard per l'Audit e la Governance dell'IT nella guida del Governo. Questa è una linea guida importante per assicurare che la pianificazione, lo sviluppo e gli sforzi operativi in ambito IT siano strutturati, controllati e strettamente collegati con i requisiti di business.

[Nota: *decidere l'adozione di COBIT è stato più che una dichiarazione di intenti. Sembra che poche tra le Agenzie di Stato siano attente nel seguire la struttura del COBIT. Uno dei motivi potrebbe essere la mancanza di politiche e di linee guida per l'IT governance. L'IT è ancora vista come un'area di controllo separata invece che strettamente connessa con le unità di business.*]

Il COBIT è un metodo chiave per misurare la maturità e le performance di un sistema IT. Il COBIT si rivolge ai sistemi durante le quattro fasi del ciclo di vita del sistema. Questi sono "Pianificazione e Organizzazione", "Acquisizione e Implementazione", "Rilascio e Supporto" e "Monitoraggio". Un sistema può essere rivisto in qualsiasi fase esso attualmente risieda. Da queste asserzioni, le valutazioni standard del sistema possono essere fatte in base alle revisioni dettagliate del processo. Le parti del processo sono raggruppate in 34 sezioni, ulteriormente suddivise i 318 obiettivi di controllo dettagliati. Questo metodo di valutazione permette ad un responsabile, ad un utente o ad un auditor di conoscere lo stato o la maturità del sistema in relazione alle best practice, agli obiettivi, alla sicurezza e ai rischi. Se usato appropriatamente, il COBIT è un elemento chiave per assicurare che i sistemi informativi e relativi processi, stanno operando in qualità, sicurezza e con strumenti di business affidabili (in conformità con leggi e regolamenti). La cosa più importante, forse, è che COBIT ha un focus iniziale primario sui requisiti di business, e garantisce che i sistemi informativi supportino la soluzione di business che è stato previsto indirizzassero.

Il COBIT tenta di misurare i processi valutandoli rispetto alle politiche e ai piani di sicurezza dello Stato dell'Oregon. Queste politiche sono attualmente in sviluppo e sono proposte in base agli standard ISO 17799. Gli ISO 17799 dividono il mondo dell'Information System Security in dieci categorie: Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Enviromental Security, Communications and Operations Management, Access Control, System Developement and Maintenance, Business Continuity Management, e Compliance.

Non c'è diretta correlazione fra gli standard ISO e il COBIT. Essi hanno origini diverse e, mentre si rispettano a vicenda, non si relazionano con facilità.

L'intento della stesura delle Politiche di Sicurezza emanate dall'IT Security Subcommittee, è quello di fornire linee guida per i diversi ministeri su come sviluppare le loro proprie politiche di sicurezza che riflettono l'ambiente nel quale essi operano. Le politiche del Security Subcommittee saranno ulteriormente sviluppate in modelli e linee guida che formeranno una struttura base per essere utilizzate dai ministeri per sviluppare la loro propria policy. L'utilizzo di questi modelli assicurerà che la policy sviluppata in ciascun ministero sia completa, aggiornata, con forma corretta e appropriatamante comunicata. Quindi i responsabili, gli utenti e gli auditor saranno in grado di utilizzare i principi del COBIT per assicurare (misurare) che la tecnologia, le apparecchiature, le applicazioni, i dati e gli utilizzatori siano conformi alle Politiche.
Il motivo per usare gli standard ISO 17799 è quello di assicurare che tutte le Politiche sviluppate raggiungano ciascuna area dell'information security. Di seguito vengono schematizzati i dieci domini degli standard ISO 17799 e alcuni degli elementi chiave che sono utili per indirizzarli. Vengono inclusi anche i requisiti del COBIT e le sezioni di valutazione dei processi che dipendono dalle policy di settore per le considerazioni sulla conformità.

MATRICE DI CORRELAZIONE ISO 17799 - COBIT

Dominio	PUNTI ISO 17799 DA VERIFICARE	RIFERIMENTI COBIT
Security policy	• Supporto di gestione per le policy • Dichiarazione di Agenzia sulla Privacy • Compensi e Penali • Ruolo del Security Manager	PO6 Communicate Management Aims and Direction
Security Organization	• Ruoli e responsabilità dei proprietari dei dati, degli utenti, del personale sistemistico • Gestione dell'outsourcing • Procedura per rispondere a richieste di informazioni esterne • Gestione delle risposte ad incidenti • Aggiornamento delle policy	PO4 Define the IT organization and relationships PO9 Assess Risks AI1 Identify Automated Solutions AI4 Develop and Maintain Procedures DS6 Identify and Allocate Costs DS10 Manage Problems and Incidents
Asset Classification and Control	• Livelli di classificazione di sistemi e dati • Metodi per classificare e qualificare documenti, media, files, ecc.	PO2.3 Data Classification Scheme DS 11 Manage Data
Personnel Security	• Programmi di formazione e di crescita di consapevolezza • Applicazione della normativa e monitoraggio • Errori e controlli sull'aggiornamento	PO7 Manage Human Resources DS7 Educate and Train users
Physical and Environmental Security	• Protezione delle apparecchiature - edifici, locali di telecomunicazione, attrezzature e personale da incendi, furti, vandalismi, interruzione di servizi, disastri naturali	DS12 Manage Facilities
Communications and Operations Management	• Adeguamento della sicurezza delle operazioni • Minimizzazione del rischio di disservizi • Integrità del software e delle informazioni • Integrità delle comunicazioni • Protezione dal danneggiamento della rete • Sicurezza del trasferimento interdipartimentale delle informazioni • Distruzione delle attività di business	PO2 Define Information Architecture AI3 Acquire and Maintain Technology Infrastructure DS1 Define and Manage Service levels DS3 Manage Performance and Capacity DS6 Identify and Allocate Costs DS8 Assist and Advise Customers DS9 Manage configuration DS13 Manage Operations M1 Monitor the Process
Access Control	• Controllo, rilevazione e prevenzione accessi non autorizzati da soggetti interni ed esterni • Controllo delle comunicazioni mobile computing	DS5 Ensure Systems Security
Systems Development and Maintenance	• Processo di sviluppo strutturato • Requisiti di sicurezza nei progetti • Backup appropriati, documentazione e standard di sviluppo applicativo • Integrità dell'elaborazione delle applicazioni	PO1.0 Define a Strategic IT Plan - PO2.2.2 Corporate Data Dictionary and Data Syntax Rules PO3.0 Determine Technological Direction PO10 Manage Projects PO11 Manage Quality (SDLC) AI2 Acquire and Maintain software AI5 Install and accredit systems AI6 Change Management
Business Continuity Management	• Preparazione e pianificazione per gestire le interruzioni di business e disservizi di sistema	DS4 Ensure Continuous service
Compliance	• Assicurazione che leggi e regolamenti siano rispettati • Fedeltà dei processi alle policy • Massimizzazione dell'efficacia dell'audit • Universalità delle policy - applicata ai dipendenti, appaltatori, fornitori, ecc.	PO8.0 Ensure compliance with external requirements PO11.10 Third Party Implementer relationships DS2 Manage Third party Services M2 Assess Internal Control Adequacy M3 Obtain Independent Assurance M4 Provide for Independent Audit

MATRICE DI CORRELAZIONE COBIT - BS7799

STRUTTURA COBIT		STRUTTURA BS7799	
Ref:	**PLANNING & ORGANISATION**	**Ref:**	**BS7799 Framework**
1,0	**Define a Strategic Information Technology Plan**		
1,1	Information Technology as Part of the Long- and Short-Range Plan		
1,2	Information Technology Long-Range Plan		
1,3	Information Technology Long-Range Plan -- Approach and Structure		
1,4	Information Technology Long-Range Plan Changes		
1,5	Short-Range Planning for the Information Services Function		
1,6	Assessment of Existing Systems		
2,0	**Define the Information Architecture**		
2,1	Information Architecture Model		
2,2	Corporate Data Dictionary and Data Syntax Rules		
2,3	Data Classification Scheme		
2,4	Security Levels	3.2.1	Classification guidelines (accountability of assets)
3,0	**Determine the Technology Direction**		
3,1	Technological Infrastructure Planning		
3,2	Monitor Future Trends and Regulations		
3,3	Technological Infrastructure Contingency		
3,4	Hardware and Software Acquisition Plans		
3,5	Technology Standards		
4,0	**Define the IT Organisation and Relationships**		
4,1	The Information Services Function Planning or Steering Committee	2.1.1	Management information security forum
4,2	Organisational Placement of Information Services Function		
4,3	Review of Organisational Achievements		
4,4	Roles and Responsibilities	2.1.3	Allocation of information security responsibilities
		3.1.1	Inventory of assets
		4.1.1	Personnel security including security in job titles
4,5	Responsibility for Quality Assurance		
4,6	Responsibility for Logical and Physical Security	2.1.3	Allocation of information security responsibilities
		2.1.4	Specialist information security advice
		3.1.1	Inventory of assets
4,7	Ownership and Custodianship	3.1.1	Inventory of assets
4,8	Data and System Ownership	3.2.1	Classification guidelines (accountability of assets)
4,9	Supervision		
4,1	Segregation of Duties	6.1.3	Computer and network management - segregation of duties
4,1	Information Technology Staffing		

STRUTTURA COBIT		STRUTTURA BS7799	
Ref:	**PLANNING & ORGANISATION**	**Ref:**	**BS7799 Framework**
4,1	Job or Position Descriptions for Information Services Function Staff		
4,1	Key Information Technology Personnel		
4,1	Contracted Staff Procedures		
4,2	Relationships		
5,0	**Manage the Investment in Information Technology**		
5,1	Annual Information Services Function Operating Budget		
5,2	Cost and Benefit Monitoring		
5,3	Cost and Benefit Justification		
6,0	**Communicate Management Aims and Direction**		
6,1	Positive Information Control Environment		
6,2	Management's Responsibility for Policies		
6,3	Communication of Organisation Policies		
6,4	Policy Implementation Resources		
6,5	Maintenance of Policies		
6,6	Compliance with Polices, Procedures and Standards	12,2	Reviews of security policy and technical compliance
6,7	Quality Commitment		
6,8	Security and Internal Control Framework Policy	1,1	Information security policy document
6,9	Intellectual Property Rights	12.1.2	Intellectual property rights
6,1	Issue Specific Policies		
6,1	Communication of IT security Awareness		
7,0	**Manage Human Resources**		
7,1	Personnel Recruitment and Promotion	4.1.3	Personnel security including confidentiality agreements
7,2	Personnel Qualifications		
7,3	Personnel Training	4.2.1	Information security education and training
7,4	Cross-Training or Staff Backup	4.2.1	Information security education and training
7,5	Personnel Clearance Procedures	4.1.2	Personnel screening policy
7,6	Employee Job Performance Evaluation		
7,7	Job Change and Termination	4.3.4	Disciplinary process
8,0	**Ensure Compliance with External Requirements**		
8,1	External Requirements Review	12,1	Compliance with legal requirements
8,2	Practices and Procedures for Complying with External Requirements		
8,3	Safety and Ergonomic Compliance		
8,4	Privacy, Intellectual Property and Data Flow	12.1.2	Intellectual property rights
		12.1.4	Data protection and privacy of personal information
8,5	Electronic Commerce	8.7.3	Electronic commerce security
8,6	Compliance with Insurance Contracts		

STRUTTURA COBIT		STRUTTURA BS7799	
Ref:	**PLANNING & ORGANISATION**	**Ref:**	**BS7799 Framework**
9,0	**Assess Risks**	2.2.1	Identification of risks from third party access
9,1	Business Risk Assessment		
9,2	Risk Assessment Approach		
9,3	Risk Identification		
9,4	Risk Measurement		
9,5	Risk Action Plan		
9,6	Risk Acceptance		
10,0	**Manage Projects**		
10,1	Project Management Framework		
10,2	User Department Participation in Project Initiation		
10,3	Project Team Membership and Responsibilities		
10,4	Project Definition		
10,5	Project Approval		
10,6	Project Phase Approval		
10,7	Project Master Plan		
10,8	System Quality Assurance Plan		
10,9	Planning of Assurance Methods		
10,1	Formal Project Risk Management		
10,1	Test Plan		
10,1	Training Plan		
10,1	Post-Implementation Review Plan		
11,0	**Manage Quality**		
11,1	General Quality Plan		
11,2	Quality Assurance Approach		
11,3	Quality Assurance Planning		
11,4	The Quality Assurance Review of Adherence to Standards and Procedures		
11,5	System Development Life Cycle Methodology		
11,6	System Development Life Cycle Methodology for Major Changes to Existing Technology		
11,7	Updating the System Development Life Cycle Methodology		
11,8	Coordination and Communication		
11,9	Acquisition and Maintenance Framework for the Technology Infrastructure		
11,1	Third-Party Implementor Relationships		
11,1	Program Documentation Standards		
11,1	Program Testing Standards		
11,1	System Testing Standards		

STRUTTURA COBIT		STRUTTURA BS7799	
Ref:	**PLANNING & ORGANISATION**	**Ref:**	**BS7799 Framework**
11,1	Parallel/Pilot Testing		
11,2	System Testing Documentation		
11,2	Quality Assurance Evaluation of Adherence to Development Standards		
11,2	Quality Assurance Review of the Achievement of IT Function objectives		
11,2	Quality Metrics		
11,2	Reports of Quality Assurance Reviews		

STRUTTURA COBIT		STRUTTURA BS7799	
	ACQUISITION & IMPLEMENTATION		
1,0	**Identify Solutions**		
1,1	Definition of Information Requirements		
1,2	Formulation of Alternative Courses of Action		
1,3	Formulation of Acquisition Strategy		
1,4	Third Party Service requirements		
1,5	Technological Feasibility Study		
1,6	Economic Feasibility Study		
1,7	Information Architecture		
1,8	Risk Analysis Report	8.1.1	Security requirements analysis and specification
1,9	Cost-Effective Security Controls		
1,1	Audit Trails Design		
1,1	Ergonomics		
1,1	Selection of System Software		
1,1	Procurement Control		
1,1	Software Product Acquisition		
1,2	Third-Party Software Maintenance		
1,2	Contract Application Programming		
1,2	Acceptance of Facilities		
1,2	Acceptance of Technology		
2,0	**Acquire and Maintain Application Software**		
2,1	Design Methods		
2,2	Major Changes to Existing Systems		
2,3	Design Approval		
2,4	File Requirements Definition and Documentation		
2,5	Program Specifications		
2,6	Source Data Collection Design		
2,7	Input Requirements Definition and Documentation		
2,8	Definition of Interfaces		
2,9	User-Machine Interface		
2,1	Processing Requirements Definition and Documentation		
2,1	Output Requirements Definition and Documentation		
2,1	Controllability		
2,1	Availability as Key Design Factor		
2,1	IT Integrity Provisions in Application Program Software	8.2.1	Input data validation
2,2	Application Software Testing		
2,2	User Reference and Support Materials		

STRUTTURA COBIT		STRUTTURA BS7799	
	ACQUISITION & IMPLEMENTATION		
2,2	Re-assessment of System Design	10.2.2	Technical conformity checking
3,0	**Acquire and Maintain Technology Architecture**		
3,1	Assessment of New Hardware and Software		
3,2	Preventative Maintenance for Hardware	5.2.4	Equipment maintenance
3,3	System Software Security	8.3.1	Policy on the use of cryptographic controls
		8.4.1	Control of operational software
		10.2.2	Technical conformity checking
3,4	System Software Installation		
3,5	System Software Maintenance		
3,6	System Software Change Controls	8.5.2	Technical review of operating system changes
4,0	**Develop and Maintain Information Technology Procedures**		
4,1	Future Operational Requirements and Service Levels		
4,2	User Procedure Manual		
4,3	Operations Manual		
4,4	Training Materials		
5,0	**Install and Accredit Systems**		
5,1	Training		
5,2	Application Software Performance Sizing		
5,3	Conversion		
5,4	Testing of Changes	8.4.2	Protection of system test data
5,5	Parallel / Pilot Testing Criteria and Performance		
5,6	Final Acceptance Test	6.2.2	System acceptance
5,7	Security Testing and Accreditation		
5,8	Operational Test		
5,9	Promotion to Production		
5,1	Evaluation of Meeting User Requirements		
5,1	Management's Post-Implementation Review		

STRUTTURA COBIT		STRUTTURA BS7799	
	ACQUISITION & IMPLEMENTATION		
6,0	**Managing Changes**		
6,1	Change Request Initiation and Control	8.5.1	Change control procedures
6,2	Impact Assessment	8.5.1	Change control procedures
6,3	Control of Changes	8.5.3	Restrictions on changes to software packages
		8.5.1	Change control procedures
6,4	Documentation and Procedures	8.5.1	Change control procedures
6,5	Authorized Maintenance	8.5.1	Change control procedures
6,6	Software Release Policy	8.5.1	Change control procedures
6,7	Distribution of Software	8.5.1	Change control procedures

STRUTTURA COBIT		STRUTTURA BS7799	
	DELIVERY & SUPPORT		
1,0	**Define Service Levels**		
1,1	Service Level Agreement Framework		
1,2	Aspects of Service Level Agreements		
1,3	Performance Procedures		
1,4	Monitoring and Reporting		
1,5	Review of Service Level Agreements and Contracts		
1,6	Chargeable Items		
1,7	Service Improvement Program		
2,0	**Manage Third-Party Services**		
2,1	Supplier Interfaces	2.2.1	Identification of risks from third party access
2,2	Owner Relationships		
2,3	Third-Party Contracts	2.2.2	Security requirments in third party contracts
2,4	Third-Party Qualifications	6.1.5	External facilities management
2,5	Outsourcing Contracts	8.5.5	Outsourced software development
2,6	Continuity of Services	2.2.2	Security requirments in third party contracts
2,7	Security Relationships	2,2	Security of thrid party access
2,8	Monitoring		
3,0	**Manage Performance and Capacity**		
3,1	Availability and Performance Requirements	6.2.1	Capacity planning
3,2	Availability Plan		
3,3	Monitoring and Reporting		
3,4	Modeling Tools		
3,5	Proactive Performance Management		
3,6	Workload Forecasting		
3,7	Capacity Management of Resources		
3,8	Resources Availability		
3,9	Resource Schedule		

STRUTTURA COBIT		STRUTTURA BS7799	
	DELIVERY & SUPPORT		
4,0	**Ensure Continuous Service**		
4,1	The Disaster Recovery/Contingency Framework	9.1.1	Business continuity management process
		9.1.4	Business continuity planning framework
4,2	Disaster Recovery/Contingency Plan		
4,3	Disaster Recovery/Contingency Plan Strategy and Philosophy	9.1.2	Business continutiy and impact analysis
4,4	Maintaining and Testing the Disaster Recovery/Contingency Plan	9.1.3	Writing and implementing continuity plans
4,5	User Department Alternative Processing Back-Up Procedures		
4,6	Disaster Recovery/Contingency Plan Training		
4,7	Critical Information Technology Applications		
4,8	Backup Site and Hardware		
4,1	Disaster Recovery/Contingency Plan Contents		
5,0	**Ensure Systems Security**		
5,1	Authentication and Access	6.5.1	Network controls
		7.1.1	Access control policy
		7.1.2	Access control rules
		7.4.2	Enforced path
		7.4.3	User authentication for external connections
		7.4.4	Node authentication
		7.4.5	Remote diagnostic port protection
		7.4.6	Segregation in networks
		7.4.7	Network connection controls
		7.4.8	Network routing controls
		7.4.9	Security of network services
		7.5.1	Automatic terminal identification
		7.5.2	Terminal log-on procedures
		7.5.3	User identification and authentication
		7.5.4	Password management system
		7.5.5	Use of system utilities
		7.5.6	Duress alarm to safeguard users
		7.5.7	Terminal time-out
		7.5.8	Limitation of connection time
		7.8.1	Information access restriction
		7.8.2	Sensitive system isolation
5,2	Security of Online Access to Data	7.2.1	User registration
5,3	User Account Management	7.2.2	Privilage management
		7.2.3	User password management

STRUTTURA COBIT		STRUTTURA BS7799	
	DELIVERY & SUPPORT		
		7.2.4	Review of user access rights and privilages
5,4	Management Review of User Account		
5,5	Data Classification	8.2.4	Output data validation
5,6	Central Identification and Access Rights Management		
5,7	Violation and Security Activity Reports	4.3.1	Reporting security incidents
5,8	Incident Handling	4.3.1	Reporting security incidents
5,9	Re-accreditation		
5,1	Public Key Cryptography	8.3.2	Encryption
5,1	Security of Cryptographic Modules		
5,1	Cryptographic Key Management	8.3.5	Key management
5,1	Virus Prevention and Detection	6.3.1	Controls against malicious software
6,0	**Identify and Allocate Costs**		
6,1	Chargeable Items		
6,2	Costing Procedures		
6,3	User Billing and Chargeback Procedures		
7,0	**Educate and Train Users**		
7,1	Identification of Training Needs		
7,2	Training Organisation	7.3.1	User responsibilities - password use
7,3	Security Principles and Awareness Training	7.4.1	Policy on the use of networked services
8,0	**Assisting and Advising Information Technology Customers**		
8,1	Help Desk	6.4.3	Fault logging
8,2	Registration of Customer Queries	6.4.3	Fault logging
8,3	Customer Query Escalation	6.4.3	Fault logging
8,4	Monitoring of Clearance		
8,5	Trend Analysis and Reporting	6.4.3	Fault logging
9,0	**Manage the Configuration**		
9,1	Configuration Recording		
9,2	Configuration Baseline		
9,3	Status Accounting		
9,4	Configuration Control		
9,5	Unauthorized Software		
9,6	Software Storage		

STRUTTURA COBIT		STRUTTURA BS7799	
	DELIVERY & SUPPORT		
10,0	**Manage Problems and Incidents**		
10,1	Problem Management System	4.3.3	Reporting software malfunctions
		6.1.2	Incident management procudures
10,2	Problem Escalation	4.3.3	Reporting software malfunctions
		6.1.2	Incident management procudures
10,3	Problem Tracking and Audit Trail	4.3.3	Reporting software malfunctions
		6.1.2	Incident management procudures
11,0	**Manage Data**		
11,1	Data Preparation Procedures		
11,2	Source Document Authorization Procedures		
11,3	Source Document Data Collection		
11,4	Source Document Error Handling		
11,5	Source Document Retention		
11,6	Data Input Authorization Procedures		
11,7	Accuracy, Completeness and Authorization Checks		
11,8	Data Input Error Handling		
11,9	Data Processing Integrity		
11,1	Data Processing Validation and Editing		
11,1	Data Processing Error Handling		
11,1	Output Handling and Retention	5.1.4	Working in clear areas - clear desk policy
11,1	Output Distribution		
11,1	Output Balancing and Reconciliation		
11,2	Output Review and Error Handling	11,12	Information handling procedures
11,2	Security Provision for Output Reports	6.6.4	Security of systems documentation
11,2	Protection of Sensitive Information	5.2.3	Cabling security
11,2	Protection of Disposed Sensitive Information	5.2.6	Secure disposal and re-use of equipment
		6.6.2	Disposal of media
11,2	Storage Management		
11,2	Retention Periods and Storage		
11,2	Media Library Management System	6.6.1	Management of removable computer media
11,2	Media Library Management Responsibilities		
11,2	Back-Up and Restoration	8.4.1	Information back-up
11,2	Back-Up Jobs		
11,3	Back-Up Storage		

STRUTTURA COBIT		STRUTTURA BS7799	
	DELIVERY & SUPPORT		
12,0	**Manage Facilities**		
12,1	Physical Security	5.1.1	Physical security perimeter
		5.1.3	Securing of data centres and computer rooms
		5.2.5	Security of equipment off-premesis
12,2	Low Profile of the Information Technology Site	5.1.1	Physical security perimeter
12,3	Visitor Escort	5.1.5	Isolated delivery and loading areas
12,4	Personnel Health and Safety		
12,5	Protection Against Environmental Factors	5.1.3	Securing of data centres and computer rooms
		5.2.1	Equipment siting and protection
12,6	Uninterruptable Power Supply	5.2.2	Power supplies
		5.2.1	Equipment siting and protection
13,0	**Manage Operations**		
13,1	Processing Operations Procedures and Instructions Manual	6.1.1	Documented operating procedures
13,2	Startup Process and Other Operations Documentation	6.1.1	Documented operating procedures
13,3	Job Scheduling		
13,4	Departures from Standard Job Schedules		
13,5	Processing Continuity		
13,6	Operations Logs		
13,7	Remote Operations		

STRUTTURA COBIT		STRUTTURA BS7799	
	MONITORING		
1,0	**Monitor the Process**		
1,1	Collecting Monitoring Data	10.3.1	System audit controls
1,2	Management Reporting		
1,3	Internal Control Monitoring		
1,4	Timely Operation of Internal Controls		
1,5	Internal Control Level Reporting		
1,6	Operational Security and Internal Control Assurance	2.1.6	Independent review of information security
		10.2.1	Compliance with security policy
2,0	**Obtain Independent Assurance**		
2,1	Audit Charter		
2,2	Adherence to Codes Of Ethics and Professional Standards		
2,3	Auditor Independence		
2,4	Audit Plan		
2,5	The Performance of Audit Work		
2,6	Seeking Independent Audit Involvement		
2,7	The Technological Competence of Audit Personnel		
2,8	Audit Personnel's Continuing Education		
2,9	Audit Reporting		
2,1	Follow Up Activities		
3,0	**Obtain Independent Assurance**		
3,1	Independent Security and Control Certification/Accreditation of IT Services	2.1.7	Independent review of information security
3,2	Independent Security and Control Certification/Accreditation of Third-Party Service Providers	2.1.7	Independent review of information security
3,3	Independent Effectiveness Evaluation of IT Services	2.1.7	Independent review of information security
3,4	Independent Effectiveness Evaluation of Third-Party Service Providers	2.1.7	Independent review of information security
3,5	Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments	2.1.7	Independent review of information security
3,6	Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers	2.1.7	Independent review of information security
3,7	Competence of Independent Assurance Function		
3,8	Proactive Audit Involvement		

STRUTTURA COBIT		STRUTTURA BS7799	
	MONITORING		
4,0	**Provide for Independent Audit**		
4,1	Audit Charter		
4,2	Independence		
4,3	Professional Ethics and Standards		
4,4	Competence		
4,5	Planning		
4,6	Performance of Audit Work		
4,7	Reporting		
4,8	Follow-up Activities		

Fonte CobiT-List ISACA

7. Introduzione ai diversi ambiti

SECURITY POLICY

La difficoltà nel comprendere l'importanza della salvaguardia del patrimonio informativo aziendale, è ampiamente diffusa nella mentalità dell'operare quotidiano nelle nostre aziende; la costruzione della consapevolezza deve partire da lontano e le indicazioni, le informazioni e le norme approntate top-down e messe a disposizione di tutta la popolazione aziendale, aiutano a formare le fondamenta sulle quali poi continuare a costruire per consolidare il concetto di sicurezza delle informazioni.
Anche se non presenti sotto forma di classici documenti formalizzati, a volte possono essere rappresentate anche in forme più vicine agli utenti, ad esempio nei calendari da tavolo.
Un altro elemento che dovrebbe emergere è che la sicurezza è ormai un elemento strategico per l'azienda in chiave di Business. Consideriamo, ad esempio, le recenti emanazioni del Comitato di Basilea, le quali hanno incluso il rischio operativo nel rating degli istituti finanziari (definito come il rischio di subire perdite a causa di processi interni, persone, sistemi o eventi esterni). Tali aspetti dovranno portare inevitabilmente ad una maggiore sensibilizzazione interna sulle tematiche di sicurezza.

Questa sezione introduttiva sottolinea la necessità di descrivere le politiche di sicurezza in un documento chiaro da distribuire a tutto il personale che dovrà riguardare i seguenti aspetti:
- Politiche di sicurezza, definizione della sicurezza informatica
- Revisioni e valutazione delle politiche

ORGANISATIONAL SECURITY

Il primo elemento da costruire, dopo aver pubblicato le politiche di sicurezza, è sicuramente un'organizzazione, supportata dal Vertice aziendale, in grado di identificare, gestire, aggiornare e promuovere le politiche stesse; si sottolinea l'importanza, in questo progetto, di creare coesione tra tutte quelle funzioni aziendali che, a vario titolo, operano nell'ambito della sicurezza, della gestione del rischio e degli obblighi di legge. Tale organizzazione, preferibilmente posta ai vertici dell'azienda, dovrà essere costituita da risorse con adeguato skill professionale. Nella sua attività, dovrà considerare la sicurezza con una visione d'insieme agendo su diverse aree, e non solo su quelle tecnologiche.

Questa sezione spiega come gestire la sicurezza all'interno dell'organizzazione.
In particolare si deve:
- Costituire un "forum" per comunicare, controllare e coordinare gli eventi di sicurezza
- Definire il coordinamento per l'implementazione dei controlli di sicurezza informatica
- Assegnare le responsabilità per la sicurezza informatica
- Istituire un processo per approvare l'acquisto di nuovi hardware e software
- Favorire la collaborazione con organizzazioni, autorità, operatori nel campo della sicurezza informatica
- Organizzare revisioni/audit delle pratiche organizzative
- Identificare i rischi per l'accesso di terze parti (p.e. outsourcing, consulenti esterni ecc.)
- Sviluppare clausole di sicurezza per i contratti con terze parti, compreso l'outsourcing

ASSET CLASSIFICATION AND CONTROL

La condizione per poter applicare le misure di sicurezza è di avere la conoscenza dettagliata delle risorse da proteggere. Quella dell'inventario e della classificazione è un'attività complessa e dispendiosa se effettuata partendo da zero: molte aziende hanno effettuato il censimento degli asset in occasione del millenium bug, tenendo poi sotto controllo questa attività con aggiornamenti periodici; si ricorda che i dati dell'inventario sono uno degli input dell'analisi dei rischi, attività fondamentale nella definizione delle politiche di sicurezza.

Questa sezione interessa la sicurezza degli asset:

- Tutti gli asset (informazioni, software, hardware, servizi) devono essere opportunamente inventariati e per ognuno si deve definire un responsabile
- Le informazioni, in particolare, devono essere appropriatamente classificate e per ogni classe bisogna definire il tipo di trattamento e le relative contromisure.

PERSONNEL SECURITY

Le informazioni statistiche ricavate dai dati conosciuti relativamente a frodi, furti di dati, perdite di informazioni, affermano che la maggior parte di questi sono da imputare ad azioni causate da personale interno delle aziende; da qui si deduce la necessità di una forte attenzione nel trattamento della risorsa umana appartenente all'organizzazione, a partire dalla selezione, durante la sua attività lavorativa, fino al momento della risoluzione del suo contratto lavorativo. Questo si raggiunge regolamentando opportunamente le attività, motivando il personale e promuovendo il concetto di etica professionale, implementando i relativi controlli. L'attenzione alle risorse umane è un tassello fondamentale per poter costruire un efficace sistema di sicurezza, che non può basarsi solo su presidi di tipo tecnologico. E' necessario che le risorse percepiscano l'enfasi che l'azienda pone alle tematiche di sicurezza.

Questa sezione riguarda la protezione di dati e di sistemi da azioni umane intenzionali e/o accidentali quali la frode, il furto e l'errore:

- Descrizione formale della mansione di lavoro comprendente le responsabilità sulla sicurezza
- Verifiche e controlli sul personale nella fase di selezione
- Riferimenti contrattuali sulla responsabilità per la sicurezza delle informazioni
- Addestramento del personale per il corretto utilizzo degli assets nel rispetto della sicurezza
- Definizione di una struttura per accertarsi che gli incidenti e i malfunzionamenti vengano segnalati e attivino i canali corretti.

PHYSICAL AND ENVIRONMENTAL SECURITY

Non si può pensare di risolvere il problema della sicurezza informatica senza affrontare come un tutt'uno anche quello della sicurezza fisica e ambientale. A questo scopo deve essere prevista una politica di security e di piani di emergenza in stretta relazione con la politica di sicurezza informatica, in modo da minimizzare il rischio di lasciare scoperto qualche aspetto importante relativo alla protezione degli asset informativi.

Questa sezione riguarda la sicurezza fisica e ambientale:
- Stabilire zone sicure, attraverso barriere fisiche, per prevenire accessi non autorizzati ad informazioni riservate
- Proteggere fisicamente le attrezzature per impedire i furti o i sabotaggi
- Proteggere la struttura fisica delle reti
- Equipaggiarsi contro il rischio di disastri ambientali, incendi, esplosioni ecc.…
- Regolamentare l'utilizzo, al di fuori dei locali di lavoro abituali, di apparecchiature adibite alla gestione dell'informazione (p.e. telefoni cellulari, PC portatili, documenti cartacei, ecc.)
- Identificare regole che diminuiscano il rischio di fuga di informazioni (p.e. clear desk, clear screen, ecc.).

COMMUNICATIONS AND OPERATIONS MANAGEMENT

Gli aspetti di un sistema informativo da considerare rispetto alle esigenze di protezione sono molteplici e complessi; per ognuno di questi è opportuno effettuare un'analisi evidenziandone i rischi rispetto alla riservatezza, all'integrità e alla disponibilità al fine di poter implementare gli adeguati meccanismi di sicurezza. Questi possono essere valutati solo con una fotografia accurata e rispondente al reale del proprio ambiente informatico in modo da metterli nella corretta relazione con i reali rischi delle singole aree.

Questa è una sezione molto ampia e si occupa della sicurezza dei sistemi di elaborazione. Definisce le zone principali di rischio di cui si deve essere informati.
In particolare si dovranno prendere in considerazione:
- La documentazione delle procedure operative di sicurezza
- Controllo dei cambiamenti
- Procedure per la gestione degli incidenti
- Separazione dei ruoli
- Separazione tra sviluppo e servizi operativi
- Gestione dei servizi esterni
- Capacity planning
- Identificazione dei criteri di accettazione di nuove soluzioni informatiche
- Controlli contro virus e software dannosi
- Back-up delle informazioni
- Gestione dei file di log
- Controlli sulla sicurezza in rete
- Gestione dei media di supporto dati
- Sicurezza della documentazione del sistema
- Sicurezza e-commerce ed e-mail.

ACCESS CONTROL

Il controllo degli accessi, pur avendo delle norme di applicazione riconosciute ovunque, ha il suo punto di maggior difficoltà nel definire e applicare le regole di gestione del turn-over interno/esterno del personale, con le conseguenti modifiche nei diritti di accesso alle applicazioni e ai data base: è frequente che il personale in

possesso di una user ID abbia dei diritti di accesso sovrabbondanti rispetto a quelli che la sua mansione comporterebbe, con un rischio latente di trattamento non autorizzato e di perdita o manomissione dei dati. Lo sforzo da perpetrare è nella direzione di una maggior sensibilizzazione nella definizione delle policy e nella loro puntuale osservanza.

Questa sezione tratta il controllo degli accessi per proteggere il sistema da utenti non autorizzati.
In particolare sono previste:

- Gestione degli accessi:
  - assegnazione user ID e password con attenzione agli utenti privilegiati
  - tempo massimo di accesso ed expiration date
- Accesso fisico ai terminali
- Collaborazione da parte degli utenti sulle policy di sicurezza scelte (responsabilizzazione)
- Controllo degli accessi ai servizi di Rete, alle applicazioni e degli accessi da Lap-Top e teleworking
- Monitoraggio del sistema per rendere effettive e controllabili le politiche adottate.

SYSTEM DEVELOPMENT AND MAINTENANCE

La sicurezza, per arrivare al suo obiettivo di protezione, deve partire da lontano; questo concetto deve far parte dei sistemi e delle applicazioni sin dalla loro progettazione. Devono essere disegnati tenendo conto di queste esigenze, nonché della flessibilità richiesta dalla necessaria manutenzione adattativa ed evolutiva, facendo ricorso alle nuove frontiere in fatto di approcci metodologici e tecnologie di sviluppo, completando il tutto con il ricorso alle moderne tecniche di progettazione e di controllo.

Ovvero le regole per assicurarsi che la sicurezza sia una parte integrante nello sviluppo di nuovi sistemi e che essa rimanga integra nel corso del ciclo di vita:

- Procedure per l'acquisizione del software
- Procedure per lo sviluppo del software
- Procedure di configuration management
- Procedure di change management
- Protezione dei dati di test
- Tecniche di validazione dei dati di input
- Protezione dei file e dei flussi
- Controlli sulla crittografia
- Sviluppo di software da parte di terzi.

BUSINESS CONTINUITY MANAGEMENT

Le esperienze dovute alla preparazione dell'anno 2000 e gli effetti di un evento catastrofico come quello delle Twin Towers, ci aiutano a comprendere l'importanza di vedere la nostra azienda anche come un'entità a rischio nella sua continuità operativa e, di conseguenza, nella sua capacità di produrre business. La predisposizione di un piano di disaster recovery mirato a salvaguardare gli aspetti legati ai processi portanti dell'organizzazione è un fattore da prendere in considerazione, vista la sempre crescente dipendenza del business dai processi informatici e la possibilità di sfruttare nuovi strumenti di trasmissione dati e di memorizzazione. In fase di stesura di un piano di Business Continuity, in considerazione degli elevati costi richiesti per l'implementazione, è fondamentale effettuare una valutazione costi/benefici.

Questa sezione si focalizza sulla protezione del business riferendosi in particolare ai processi critici per il "business continuity plan".
Sarà necessario quindi identificare i rischi e ridurli, limitare le conseguenze degli incidenti e assicurare un ripristino in tempi brevi delle operazioni essenziali al business.
Il piano di continuità dovrà essere quindi:

- Disegnato
- Implementato
- Testato
- Sottoposto a manutenzione.

COMPLIANCE

Oggi le battaglie nel campo della sicurezza si stanno combattendo anche sul piano della normativa e del diritto. La conoscenza di questi fattori, quindi, è decisiva al fine di allineare i propri sforzi nel campo della salvaguardia del proprio patrimonio informativo con la realtà quotidiana del vivere sociale, con la realtà del rapporto tra gli individui e nei rapporti della civiltà industriale. Avere i giusti riferimenti per essere allineati con questi aspetti e intraprendere le azioni da questi derivanti è senz'altro un fattore qualificante delle nostre politiche di sicurezza e del nostro sistema di protezione.
Tali aspetti normativi possono inoltre essere utilizzati, negli ambienti più ostici, per poter affrontare con maggiore determinazione specifici argomenti o per spingere l'attuazione di alcune Policy.

Un sistema di sicurezza deve prevedere la conformità legale dei dati, del software, dei processi e del personale addetto. È importante quindi essere sempre in contatto con esperti in materia per avere pareri sull'utilizzo del sistema informativo conforme ai regolamenti e alle norme.
In particolare l'attenzione andrà posta su:

- Copyrights
- Salvaguardia dei dati conservati
- Protezione dei dati personali
- Utilizzo delle informazioni al di fuori degli scopi di business
- Raccolta delle prove per poter procedere legalmente contro persone od organizzazioni
- Revisione delle politiche di sicurezza e conformità tecnica
- Considerazioni sull'audit di sistema.

8. Link utili e Bibliografia

LINK

Registro internazionale società certificate: http://www.xisec.com/Register.htm

Società di certificazione: http://www.gammassl.co.uk/topics/hot1.html
http://www.dnv.it/

British Standard Institute: http://www.bsi-global.com/index.xalter

ISCACA http://www.isaca.org

Vari http://www.thewindow.to/bs7799/index.htm
http://www.itsecurity.com/papers/trinity5.htm
http://www.itsc.org.sg/standards_news/2001-09/TaewanPark-Korea-Business-Experience-of-BS7799-Certification.pdf

BIBLIOGRAFIA

British Standard Institute:

Are You Ready for a BS 7799 Audit? (DISC PD 3003)
Guide to BS 7799 Auditing (DISC PD 3004)

ALLEGATI

ELENCO SOCIETÀ CERTIFICATE BS7799 NEL MONDO

Name of Company	Country	Certificate Number	Certification Body
7 Global Ltd	UK	IS 67048	BSI
A3 Security Consulting Co Ltd	Korea	IS 69428	BSI
ABB Facilities Management AB	Sweden	0001-2000-AIS-SKM-SWEDAC	DNV
Accordis Acetate Chemicals Ltd, Derby	UK	IS 58457	BSI
Alenia Marconi Systems Ltd, Dorchester	UK	IS 61581	BSI
American Society of Quality	USA	IS 60206	BSI
AMOUN Pharmaceutical Co, Cario	Egypt	IS 54501	BSI
Attenda Ltd, Staines and Heathrow	UK	IS 60764	BSI
Baltimore Technologies, Dublin	Ireland	964558	LRQA
Bank SinoPac, Information Technology Division	Taiwan, ROC	02022-2001-AIS-LDN-UKAS	DNV
BBS	Norway	0003-2002-AIS-OSL-NA	DNV
BNL Multiservizi S.p.A.	**ITALIA**	**0007-2002-AIS-SKM-SWEDAC**	**DNV**
Britannic Money plc	UK	1	KPMG Certification Services
Brite Voice Systems Group	UK	K/50820	SGS ICS Limited
BSC Consulting	UK	01798-2000-AIS-LDN-UKAS	DNV
BT Exact Technologies, Security Practice, Ipswich	UK	962885	LRQA
BT Security, Milton Keynes	UK	959494	LRQA
BT Ignite Solutions - Secure Business Services, Milton Keynes	UK	964973	LRQA
BT Ignite Trust Services, Cardiff	UK	961984	LRQA
Business Coach IT Management, Swansea	UK	IS 53093	BSI
Buytel Ltd	Ireland	2001/03	Certification Europe
C2 Management AB	Sweden	0002-2000-AIS-SKM-SWEDAC	DNV
CADWEB Ltd, London	UK	IS 40831	BSI
CAMELOT Group plc, Watford and Aintree	UK	IS 52025	BSI
Capita Business Services	UK	IS 66036	BSI
Chatham Archive Ltd	UK	K/52880	SGS ICS Limited
Churchill India (P) Ltd, New Delhi	India	ISMS/01/1002	STQC Certification Services
Citibank N.A, Asia Pacific Processing Center	Singapore	ISMS-2001-0004	PSB Certification
Name of Company	**Country**	**Certificate Number**	**Certification Body**
Conax AS	Norway	904001	Nemco
Cognizant Technology Solutions, Chennai	India	ISMS/01/1006	STQC Certification Services
Dacom Corporation	Korea	IS 68556	BSI

Data Centres, Networks and Internet Managed Services, Fujitsu Services Ltd	UK	IS 67990	BSI
DBI Consulting, Kenilworth	UK	IS 51756	BSI
Dental Practice Board	UK	IS 66140	BSI
Detica Limited	UK	01712-2000-AIS-LDN-UKAS	DNV
Digex	UK	IS 67703	BSI
DNP Facility Services Co Ltd	Japan	IS 60381	BSI
DTI IMPE	UK	6	KPMG Certification Services
Eastlands Benefits Administration, Basingstoke	UK	IS 55770	BSI
e-Cop.net Ltd	Hong Kong	ISMS-2002-0005	PSB Certification
e-Cop.net Ltd	Singapore	ISMS-2001-0003	PSB Certification
Elopak AS	Norway	904002	Nemco
Energis UK, Reading	UK	964173	LRQA
ErgoIntegration	Norway	0002-2002-AIS-OSL-NA	DNV
Ericsson ESPA A S.A	Spain	IS 53616	BSI
Eurotronik Rt.	Hungary	0006-2002-AIS-SKM-SWEDAC	DNV
Foreign and Colonial Management Ltd	UK	01709-2000-AIS-LDN-UKAS	DNV
Fuji Xerox Co, Ltd.	Japan		JACO-IS
Fujitsu Invia Oyj	Finland	2086-03	SFS Certification
Fujitsu Limited	Japan	IC02J0002	JACO-IS
Fujitsu Oita Software Laboratories Ltd.	Japan	JQA-IS0001	JQA
GESAB Engineering AB publ.	Sweden	0003-2001-AIS-SKM-SWEDAC	DNV
GLAXO WELLCOME Manufacturing	Singapore	IS 57662	BSI
GLAXOSMITHKLINE, Montrose and Speke	UK	IS 56186	BSI
Global Security Experts Inc	Japan	IS.....	BSI
GTECH Ireland Corporation	Ireland	01959-2001-AIS-LDN-UKAS	DNV
GTECH UK Limited	UK	02064-2002-AIS-LDN-UKAS	DNV
Guangdong Shengyi Sci. Tech. Co., Ltd	China	02063-2002-AIS-LDN-UKAS	DNV
HackersLab Taiwan Co Ltd	Taiwan, ROC	IS 61595	BSI
Hanvit Bank Info Tech Unit	Korea	IS 59994	BSI
Hanwha Solutions & Consulting	Korea	IS 62291	BSI
Name of Company	**Country**	**Certificate Number**	**Certification Body**
Hays Commercial Services	UK	10854	BVQI
Hitachi netBusiness Ltd, Okayama	Japan	IC02J0005	JACO-IS
HM Government Communications Centre	UK	964695	LRQA
HM Land Registry, London & UK District Offices	UK	964052	LRQA
Huangdao Power Plant of Shandong	China	02020-2001-AIS-LDN-UKAS	DNV

Hughes Software System, Gurgaon (Haryana)	India	ISMS/01/1004	STQC Certification Services
Hungarian Banknote Printing Corporation	Hungary	0008-2002-AIS-SKM-SWEDAC	DNV
Hyundai Information Technology	Korea	IS 62290	BSI
Icfox International	Hong Kong	IS 67394	BSI
IMServe Europe, Milton Keynes	UK	959399	LRQA
Insight Consulting Limited	UK	01173-98-AIS-LDN-UKAS	DNV
Insurance Technology Solutions plc, Leeds	UK	961737	LRQA
Intergalis	UK	IS 65890	BSI
International Integrated Systems Inc	Taiwan, ROC	IS 61910	BSI
Intermail plc, Newbury	UK	964683	LRQA
JMC Co Ltd	Japan	IS 69111	BSI
Kensington Mortgage Co, London	UK	IS 61291	BSI
KPMG	UK	25211	BVQI
Larsen & Toubro Ltd, Engneering and construction division, Mumbai and Vadodara	India	ISMS/01/1001	STQC Certification Services
LEDU	UK	K/50098	SGS ICS Limited
Legal Document Management	UK	IS 67129	BSI
Link Interchange Network ltd	UK		KPMG Certification Services
Logic Systems Management	UK	IS 59736	BSI
Logica UK Limited	UK	01337-99-AIS-LDN-UKAS	DNV
Luottokunta	Finland	2225-01	SFS Certification
Luton Borough Council, I.M. Div	UK	S0002	National Quality Assurance
Marconi Secure Systems	UK	01761-2000-AIS-LDN-UKAS	DNV
Marine Systems Associates Co. Ltd	Japan	IS....	BSI
McCarthy & Associates	UK	K/52879	SGS ICS Limited

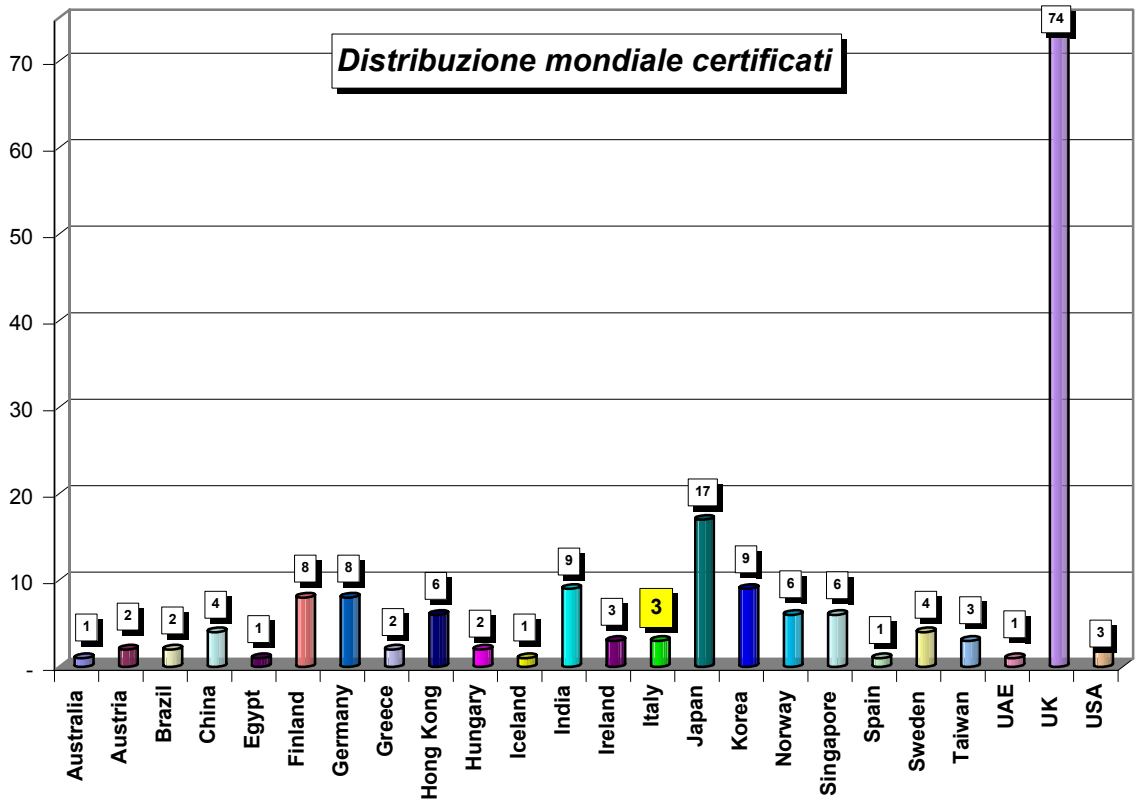
Name of Company	Country	Certificate Number	Certification Body
Macquarie Corporate Telecommunications Pty Ltd	Australia	IS 61344	BSI
MetroMail	UK	IS 67169	BSI
MIDAS-KAPITI International, London	UK	IS 51772	BSI
Miles Smith	UK	IS 68104	BSI
Miotec Oy	Finland	2275-01	SFS Certification
Mitsue Links Co Ltd	Japan	IS 60384	BSI
Mizuho Corporate Bank Ltd, London	UK	IS 55405	BSI
Modulo Security Solutions S.A	Brazil	02154-2002-AIS-LDN-UKAS	DNV
NDS NongShim Data System Co Ltd, Seoul	Korea	220305 IS	DQS
Netstore plc, Berkshire	UK	IS 56436	BSI
NHS PASA	UK	IS 66373	BSI
Nihon Unisys Ltd	Japan	3	KPMG Certification Services
Norsk Informasjonssikkerhet AS	Norway	0001-2001-AIS-OSL-NA	DNV
NTT Communications Corporation	Japan	IS 70369	BSI
NTT Data Corp (2 locations)	Japan	IS 67397	BSI
NTT DATA ITSC Group	Japan	IS 60186	BSI
Panacea Services Ltd, London	UK	963030	LRQA
Panafon S.A.	Greece	S0003	National Quality Assurance
Panafon Vodafone	Greece	S0001	National Quality Assurance
Paramount Computer Systems, Dubai Internet City	UAE	IS 59182	BSI
PCCW Business eSolutions HK	Hong Kong	IS 67432	BSI
PCCW Powerbase Data Center Services	Hong Kong	IS 66182	BSI
PICC, Xiamen Branch	China	0004-2001-AIS-SKM-SWEDAC	DNV
Prism Communications Corp 47116242	Korea	IS 68245	BSI
RAG Informatik GmbH, Gelsenkirchen	Germany	56771 IS	DQS
Red Island Consulting, London	UK	4000415	LRQA
Royal Mail	UK	01998-2001-AIS-LDN-UKAS	DNV
S-Cube Inc, Seoul	Korea	IS 59583	BSI
Samsung Electronics Co Ltd	Korea	IS 69872	BSI

Name of Company	Country	Certificate Number	Certification Body
Satyam Computer Systems, Secundrabad	India	ISMS/01/1005	STQC Certification Services
Securicor Information Systems Ltd	UK	IS 70610	BSI
Serasa, São Paulo	Brazil	262326 IS	DQS
Serco Consultancy, Malvern	UK	IS 56881	BSI
SecGo Service Centre	Finland	2263-01	SFS Certification
Serious Fraud Office	UK	IS 66329	BSI
Shilquan Power Plant of Shandong International Power Development Stock Co..	China	02152-2002-AIS-LND-UKAS	DNV
Siemens Business Services GmbH & Co Wien	Austria	102391 IS	DQS
Siemens Business Services GmbH & Co Wien	Austria	001/02	CIS
Siemens Business Services GmbH & Co. OHG Siemens IT Service Region Deutschland, München (includes 17 subsidiary sites)	Germany	099322 IS	DQS
Siemens Business Services GmbH & Co. OHG (includes 5 subsidiary sites)	Germany	249717 IS	DQS
Siemens Business Services Trust Center, Munich	Germany	IS 61545	BSI
Siemens Financial Services	UK	7	KPMG Certification Services
Siemens Network Systems Ltd	UK	IS 67042	BSI
S.I.A Spa	**ITALIA**	**0005-2002-AIS-SKM-SWEDAC**	**DNV**
Singapore Telecommunications Limited	Singapore	ISMS-2002-0006	PSB Certification
Sony Bank Inc	Japan	IS 67393	BSI
Sony Information System Solutions (Asia Pacific) - A division company of Sony Electronics (S) Pte. Ltd	Singapore	ISMS-2001-0002	PSB Certification
Sony Facility Management Corporation	Japan	IC02J0003	JACO-IS
Stiki EHF Iceland	Iceland	IS 67383	BSI
ST Microelectronics Ltd, Noida	India	ISMS/01/1003	STQC Certification Services
Stonewood Electronics	UK	31322	BVQI
Syan Ltd, High Wycombe	UK	22278	BVQI
Symantec Security Services	UK and USA	5	KPMG Certification Services

Name of Company	Country	Certificate Number	Certification Body
Synstar International	UK	01941-2001-AIS-LDN-UKAS	DNV
System Sikkerhet ASA	Norway	904003	Nemco
Taisei Corp, Design Division	Japan	IS 67782	BSI
Telecom Italia S.p.A	**ITALIA**	**0007-2002-AIS-SKM-SWEDAC**	**DNV**
Terrington Systems Limited	UK	K/51792	SGS ICS Limited
The Co-operative Bank plc, Lancashire and Salford	UK	IS 53362	BSI
The University of Texas	USA	IS 53841	BSI
TietoEnator Oyj, Processing and Networks	Finland & Sweden	1930-06	SFS Certification
Title Research	UK	IS 67403	BSI
T-Mobile (UK) Ltd, Hatfield, Herts	UK	964753	LRQA
Toijala Health Center	Finland	1931-02	SFS Certification
Toshiba IS Corporate, Tokyo	Japan	IC02J0004	JACO-IS
Total Network Solutions Ltd, Oswertry	UK	IS 57259	BSI
TPG Information Systems	UK	K54605	SGS ICS Limited
TQM Consultants Ltd	Hong Kong	IS 57846	BSI
T-Systems Computing & Desktop Services (includes 20 subsidiary sites)	Germany	063383 IS	DQS
T-Systems International GmbH, Frankfurt	Germany	255901 IS	DQS
T-Systems Global Computing, Darmstadt	Germany	256236 IS	DQS
Trustis Limited, London	UK	964889	LRQA
Unilever GIO Asia	Singapore	ISMS-2001-0001	PSB Certification
Unisys Ltd, Milton Keynes	UK	IS 58442	BSI
Vaestorekisterikeskus (The Population Register Centre)	Finland	2261-01	SFS Certification
Veikkaus Oy Ab	Finland	2115-01	SFS Certification
Vhsoft Technologies Co. Ltd	Hong Kong	02015-2001-AIS-LDN-UKAS	DNV
Vodafone Telecommerce GMBH, Ratingen	Germany	IS 58064	BSI
Volex Group plc, Warrington	UK	IS 51701	BSI
Weboutcome Ltd, London	UK	IS 67922	BSI
Whyte & Company	UK	S0004	National Quality Assurance
Wipro Technologies	India	02186-2002-AIS-ROT-UKAS	DNV
Xansa	India	15497	BVQI
Xansa (India) Ltd	India	02072-2002-AIS-LND-UKAS	DNV

Fonte: International Register Aggiornamento al 05.12.2002

DISTRIBUZIONE TERRITORIALE



Fonte: International Register del 5.12.2002

ALLEGATI OPERATIVI

9. Nomenclatura

Ci sono due domande base che potrebbero riguardare ciascun requisito di controllo. Le domande sono:

Q1 – È stato implementato il requisito adeguato?
Sono possibili tre risposte:

- **SI** – significa che le misure sono applicate con buona soddisfazione dei requisiti;
  Qualora lo si ritenesse necessario possono essere fornite alcune spiegazioni per meglio giustificare questa risposta;
- **PARZIALMENTE** – alcune misure sono applicate secondo i requisiti indicati ma non sono sufficienti per rispondere "SI";
- **NO** – nessuna misura è stata presa rispetto ai requisiti indicati. Questa è anche la risposta appropriata dove il controllo non è adeguato al sistema sotto revisione. Per esempio, la verifica sulla protezione mediante crittografia di dati altamente sensibili non è appropriata per i sistemi che non contengono dati simili. In queste circostanze la risposta corretta alla domanda è perciò "NO". Ad una successiva domanda correlata (ad es. quale sistema di crittografia viene utilizzato) si dovrebbe rispondere segnando la casella "Non Applicabile" (vedi sotto). Una risposta "NO" potrebbe anche essere data se un requisito di controllo è rilevante ma è implementato attraverso un altro tipo di controllo.

Q2 – Se un requisito non è pienamente implementato, perché non lo è stato?
È importante capire i motivi della parziale o mancata implementazione. Questi sono classificati secondo le seguenti categorie, con la possibilità di più risposte contemporanee:

- **RISCHIO** – non giustificato dall'esposizione al rischio;
- **BUDGET** – ci sono spesso limitazioni finanziarie sulla misure di sicurezza che devono essere implementata;
- **AMBIENTE** – fattori ambientali, come la disponibilità di spazio, le condizioni climatiche, la geografia naturale ed urbana circostante, potrebbero influenzare la scelta delle misure di protezione;
- **TECNOLOGIA** – alcune misure sono tecnicamente irrealizzabili a causa dell'incompatibilità dell'hardware e del software;
- **CULTURA** - le limitazioni sociologiche sull'implementazione dei requisiti potrebbero riguardare una nazione, un settore o una organizzazione. Le misure potrebbero essere inefficaci se non sono accettate dal personale e/o dai clienti;
- **TEMPO** - non tutti i requisiti possono essere implementati immediatamente. Alcuni potrebbero aver bisogno di più tempo a causa del budget, altri di un'opportunità adatta per essere inseriti in un più vasto piano di miglioramento, per esempio una ristrutturazione di uno stabile che permette l'implementazione di una cablatura più sicura ad un costo più basso rispetto a quella di una sola parte di essa;
- **Non Applicabile -** per esempio, quando l'organizzazione non ritiene di avere dimensioni tali da necessitare di un comitato inter-funzionale per coordinate le misure di sicurezza o, nel caso dei requisiti di protezione dei dati, potrebbero non essere trattati dati altamente sensibili e perciò non esistere la necessità di crittografare i dati;
- **ALTRO -** ci potrebbero essere ulteriori motivi per la mancata implementazione oltre quelli sopra elencati;

OSSERVAZIONE - in tutti i casi di mancata implementazione dovrebbero essere forniti ulteriori commenti per chiarirne i motivi. Questi potrebbero comprendere:

- Dove i requisiti di controllo sono stati implementati può essere utile, ma non essenziale, descrivere il modo in cui sono stati attivati. Questo in sé potrebbe portare al riconoscimento che devono essere eseguiti ancora ulteriori interventi in quell'area.

  In alternativa, la precisazione delle misure implementate può indicare che è stato fatto più di quanto necessario e che può essere operato un risparmio riducendo talune misure;
- Dove non è specificato il motivo per una mancata o parziale implementazione (per esempio quando ricade nella categoria ALTRO), dovrebbe essere fornita una spiegazione di dettaglio;
- Dove il motivo per una mancata o parziale implementazione è tra quelli identificati nelle categorie sopra elencate, dovrebbero essere fornite le opportune spiegazioni;
- In ogni caso dovrebbe essere fornita un'indicazione su quali azioni dovranno essere intraprese e con quali tempi si potrà andare a coprire l'assenza dei requisiti richiesti;
- Dove i requisiti sono stati coperti solo parzialmente, deve essere indicato chiaramente cosa deve essere ancora fatto;
- In alcuni casi potrebbe essere stata presa una decisione per non implementare ulteriori misure in una determinata area: effettivamente è stata assunta la decisione di accettare il livello di rischio. In questi casi dovrebbe essere ampiamente spiegato il motivo di tale decisione.

10. Check-list

Categoria:

3	**CARATTERISTICHE GENERALI DEL SISTEMA DI GOVERNO DELLA SICUREZZA**
3.2	***STRUTTURA DEL GOVERNO DELLA SICUREZZA***

Obiettivo:

Verificare l'attuazione da parte dell'azienda di un sistema per il governo della sicurezza, che a partire dalla definizione di un'opportuna politica, identifichi le aree aziendali di maggior rischio.

NOTA BENE:

- Considerare gli aspetti relativi a 2.2.a e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
3.2.1.a	Sono presenti politiche sulla sicurezza?											
3.2.1.b	E' stato definito lo scopo del sistema di governo della sicurezza in termini di caratteristiche dell'azienda, sua ubicazione, beni e tecnologia?											
3.2.1.c	E' presente di un'appropriata valutazione dei rischi, che individua le minacce ai beni, le vulnerabilità e il loro impatto sull'azienda, determinandone il grado di rischio?											
3.2.1.d	E' stata identificata l'area del rischio da governare basandosi sulla politica di sicurezza e sul grado di garanzia richiesto?											

Categoria:

3	**CARATTERISTICHE GENERALI DEL SISTEMA DI GOVERNO DELLA SICUREZZA**
3.3	***IMPLEMENTAZIONE***

Obiettivo:

Implementare i controlli adeguati alla realtà organizzativa

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
3.3.1.a	Gli obiettivi di controllo e i controlli selezionati sono implementati dall'azienda?											
3.3.1.b	L'efficacia delle procedure adottate per implementare i controlli è verificata sulla base delle indicazioni di cui al par. 4.10.2?											

Categoria:

3	**CARATTERISTICHE GENERALI DEL SISTEMA DI GOVERNO DELLA SICUREZZA**
3.4	***DOCUMENTAZIONE***

Obiettivo:

Verificare che la documentazione relativa al sistema di governo della sicurezza contenga l'informativa riguardante le procedure aziendali adottate per l'applicazione dei controlli dettati dalle politiche.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
3.4.1.a	Verifica delle azioni avviate, come specificate al punto 3.2											
3.4.1.b	Sono presenti ed adottate procedure aziendali per applicare i controlli, con la descrizione obbligatoria delle responsabilità e delle azioni rilevanti?											
3.4.1.c	Sono presenti procedure che riguardano la gestione e le operazioni del sistema di governo della sicurezza?											

Categoria:

3	**CARATTERISTICHE GENERALI DEL SISTEMA DI GOVERNO DELLA SICUREZZA**
3.5	***CONTROLLO DELLA DOCUMENTAZIONE***

Obiettivo:

Verificare che la documentazione relativa alle procedure aziendali, sull'applicazione dei controlli, siano aggiornate ed opportunamente conservate per un periodo determinato.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
3.5.1.a	La documentazione è risultata prontamente disponibile?											
3.5.1.b	La documentazione è periodicamente rivista e rivisitata, se necessario, in base alla politica di sicurezza dell'azienda?											
3.5.1.c	La documentazione è mantenuta nella versione aggiornata e resa disponibile in tutte le postazioni dove sono eseguite operazioni essenziali all'effettivo funzionamento del sistema di governo della sicurezza?											
3.5.1.d	La documentazione è prontamente ritirata quando obsoleta?											
3.5.1.e	La documentazione è identificata e conservata, quando obsoleta, se necessaria per scopi pratici e/o legali?											

Categoria:

3	**CARATTERISTICHE GENERALI DEL SISTEMA DI GOVERNO DELLA SICUREZZA**
3.6	***REGISTRAZIONI***

Obiettivo:

Verificare che la documentazione relativa alle procedure aziendali, sull'applicazione dei controlli, siano aggiornate ed opportunamente conservate per un periodo determinato.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
3.6.1.a	Le registrazioni (per es. autorizzazioni all'accesso, registro dei visitatori…) sono mantenute per un tempo adeguato?											
3.6.1.b	Esistono procedure che regolano la tenuta delle registrazioni?											
3.6.1.c	Le registrazioni sono protette dal danneggiamento o perdita?											

Categoria:

4.1	**SECURITY POLICY**
4.1.1	***DOCUMENTO DI SECURITY POLICY E RESPONSABILE DELLA SICUREZZA***

Obiettivo:

Verificare la presenza di un documento sulle politiche di sicurezza e relativi contenuti, nonché la presenza di un Responsabile della Sicurezza che si occupi delle revisione periodica del documento.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.1.1.1.a	***Documento di information security policy*** Nel documento di Security Policy è presente una definizione di sicurezza dell'informazione, con evidenza dei suoi obiettivi e scopi generali ?											
4.1.1.1.b	Nel documento di Security Policy è presente breve esposizione delle politiche di sicurezza, dei principi, degli standard e dei requisiti di conformità di particolare importanza per l'azienda ?											
4.1.1.1.c	Nel documento di Security Policy è presente definizione delle responsabilità generali e specifiche per il governo della politica di sicurezza ?											
4.1.1.1.d	Nel documento di Security Policy sono presenti rinvii a documenti che possono supportare la politica di sicurezza ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.1.1.2	***Revisione e valutazione*** E' stato nominato un Responsabile della Sicurezza che si occupi del mantenimento e della revisione della politica di sicurezza ?											

Categoria:

4.2	**ORGANIZZAZIONE DELLA SICUREZZA**
4.2.1	***INFRASTRUTTURA DI SICUREZZA - GESTIRE LA SICUREZZA DEI SISTEMI INFORMATIVI ALL'INTERNO DELL'AZIENDA***

Obiettivo:

Verifica dei principali presidi organizzativi di gestione della sicurezza dei sistemi informativi aziendali.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.1.1	***Comitato di gestione della sicurezza delle informazioni*** I criteri di gestione della sicurezza sono forniti da un comitato direttivo di alto livello aziendale ?											
4.2.1.2	***Coordinamento della sicurezza delle informazioni*** E' stato nominato un comitato per il coordinamento delle misure di sicurezza, composto di persone provenienti da diverse aree aziendali ?											
4.2.1.3	***Affidamento delle responsabilità della sicurezza delle informazioni*** Esiste una chiara definizione dei ruoli e delle responsabilità delle risorse aziendali che gestiscono aspetti della sicurezza?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.1.4	***Processo autorizzativo per le nuove componenti informatiche*** Sono previste richieste di autorizzazione per l'installazione di nuove componenti IT (hardware e software) ?											
4.2.1.5	***Consulenza di specialisti di sicurezza delle informazioni*** Sono stati individuati consulenti o istituiti focal point sulla sicurezza delle informazioni ? *(La qualità della loro valutazione del rischio e la consulenza sui controlli determina l'efficacia della sicurezza dell'informazione. Devono essere consultati al più presto possibile in caso di incidenti e di violazioni alla sicurezza).*											
4.2.1.6	***Collaborazione fra organizzazioni*** E' prevista la cooperazione con specialisti esterni all'azienda nel campo della sicurezza dei sistemi informativi, come legali, authorities, organismi regolatori, fornitori di servizi informativi e operatori delle telecomunicazioni, per garantire un'azione adeguata e immediata in risposta ad eventuali incidenti che investano la sicurezza ?											
4.2.1.7	***Revisione indipendente di information security*** E' previsto un esame indipendente della politica di sicurezza, da parte della funzione interna di audit, di un manager esterno o di una terza parte specializzata in tali revisioni ?											

Categoria:

4.2	**ORGANIZZAZIONE DELLA SICUREZZA**
4.2.2	***SICUREZZA DELL'ACCESSO DI TERZE PARTI***

Obiettivo:

La verifica di presidi tecnico-organizzativi relativi all'accesso di terze parti in azienda.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.2.1.a	***Identificazione dei rischi di accesso di terze parti*** Sono stati analizzati i rischi derivanti dagli accessi fisici e logici delle terze parti e devono essere adottati adeguati controlli della sicurezza ?											
4.2.2.1.b	Sono presenti terze parti che prestano la loro opera all'interno dell'azienda per un periodo definito dal loro contratto che possono anche dare origine a debolezze nella sicurezza ? *(Esempi di terze parti in azienda sono: lo staff di supporto e manutenzione dell'hardware e del software, le imprese di pulizia, di catering, le guardie giurate e tutti gli altri servizi di supporto affidati in outsourcing, stage e altro personale temporaneo, consulenti.)*											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.2.2.a	***Requisiti di sicurezza nei contratti con terze parti*** L'accesso alle informazioni e alle componenti IT delle terze parti non è consentito fino a quando non siano stati implementati gli opportuni controlli e non sia stato sottoscritto un contratto che definisce i termini di connessione o di accesso ?											
4.2.2.2.b	Sono previste apposite clausole riguardanti gli aspetti di sicurezza nei contratti con terze parti che prevedono accessi alle componenti IT ?											

Categoria:

4.2	**ORGANIZZAZIONE DELLA SICUREZZA**
4.2.3	***OUTSOURCING***

Obiettivo:

Verifica del presidio sulla sicurezza delle informazioni dell'informazione quando la responsabilità per il trattamento delle informazioni è affidata ad un'altra organizzazione.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.3.1.a	***Requisiti di sicurezza nei contratti di outsourcing*** I contratti prevedono specifiche clausole su come soddisfare gli adempimenti di legge, relativi alla normativa sulla protezione dei dati ?											
4.2.3.1.b	I contratti prevedono specifiche clausole su come mantenere e controllare l'integrità e la riservatezza dei beni aziendali ?											
4.2.3.1.c	I contratti prevedono specifiche clausole di sicurezza su quali controlli fisici e logici usare per limitare l'accesso alle informazioni sensibili dell'azienda ai soli utenti autorizzati?											
4.2.3.1.d	I contratti prevedono specifiche clausole relative al diritto di Audit da parte dell'outsourcer ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.2.3.1.e	I contratti prevedono specifiche clausole che indicano come mantenere l'accessibilità dei servizi in caso di disastro ?											
4.2.3.1.f	I contratti prevedono specifiche clausole relative ai livelli di sicurezza fisica da approntare per il personale dell'outsourcer ?											

Categoria:

4.3	**CLASSIFICAZIONE E CONTROLLO DEI BENI**
4.3.1	***CENSIMENTO DEI BENI***

Obiettivo:

Mantenere un'adeguata protezione dei beni aziendali.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.3.1.1.a	***Inventario degli asset*** Le risorse informatiche (hardware e software) sono opportunamente censite per fornire livelli di protezione commisurati al valore e all'importanza dei beni da proteggere ?											
4.3.1.1.b	Ciascuna risorsa è chiaramente identificato, individuato il possessore e il livello di sicurezza adeguato al bene, insieme alla sua attuale collocazione ?											

Categoria:

4.3	**CLASSIFICAZIONE E CONTROLLO DEI BENI**
4.3.2	***CLASSIFICAZIONE DELLE INFORMAZIONI***

Obiettivo:

Verificare la presenza di un adeguato livello di protezione delle informazioni.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.3.2.1	***Linee guida sulla classificazione*** Sono state redatte linee guida per la classificazione delle informazioni/dati in termini di Riservatezza, Integrità, Disponibilità, che tengano conto delle esigenze di condivisione e dell'eventuale impatto derivante da accessi non autorizzati o danni alle informazioni ?											
4.3.2.2	***Catalogazione e gestione delle informazioni*** Le informazioni sono classificate e contrassegnate in modo da evidenziare i dati maggiormente critici che necessitano di un maggiore livello di protezione o di trattamenti particolari ?											

Categoria:

4.4	**ASPETTI GESTIONALI DEL PERSONALE**
4.4.1	***SICUREZZA NELL'ASSEGNAZIONE/DEFINIZIONE DELLE MANSIONI E NELLA FASE DI SELEZIONE DEL PERSONALE***

Obiettivo:

Verificare i presidi organizzativi inerenti la riduzione dei rischi di errori umani, truffe, furti o cattivo uso delle componenti I.T.; verificare, inoltre, che le responsabilità in materia sicurezza siano considerate fin dalla fase di reclutamento, incluse nel contratto e monitorate durante lo svolgimento dell'impiego.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.4.1.1.a	***Inclusione della sicurezza nelle responsabilità di lavoro*** I compiti riguardanti la sicurezza sono stati descritti, ove possibile nell'ambito dei ruoli e delle responsabilità ?											
4.4.1.1.b	E' stata realizzata una procedura per la selezione e la verifica delle persone che accedono ad informazioni critiche ?											
4.4.1.2	***Policy e controlli sul personale*** I controlli di verifica sul personale di ruolo sono effettuati fin dal momento della domanda d'impiego? *(Queste informazioni devono essere trattate in conformità con la legislazione applicabile).*											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.4.1.3	***Accordi di confidenzialità*** E' prevista la sottoscrizione di un impegno di riservatezza per gli addetti, interni ed esterni, all'uso di componenti dei sistemi informativi aziendali ?											
4.4.1.4	***Termini e condizioni di impiego*** Il regolamento aziendale disciplina la responsabilità prevista per i dipendenti per quanto attiene agli aspetti di sicurezza ?											

Categoria:

4.4	**ASPETTI GESTIONALI DEL PERSONALE**
4.4.2	***FORMAZIONE DEGLI UTENTI***

Obiettivo:

Garantire che gli utenti siano consapevoli dei rischi e delle minacce alla sicurezza dei sistemi informativi e che abbiano gli strumenti per seguire la policy di sicurezza nello svolgimento delle mansioni.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.4.2.1	***Formazione sulla sicurezza delle informazioni*** E' stata svolta un'attività di formazione del personale utente, anche di terze parti, su policy di sicurezza e procedure organizzative, corretto uso delle componenti dei sistemi informativi aziendali ?											

Categoria:

4.4	**ASPETTI GESTIONALI DEL PERSONALE**
4.4.3	***RISPOSTA AGLI INCIDENTI E AI MALFUNZIONAMENTI***

Obiettivo:

Verificare la presenza di una procedura di gestione degli incidenti o malfunzionamenti inerenti la sicurezza, che consenta di analizzare e prevenire futuri incidenti.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.4.3.1	***Rapporti sugli incidenti di sicurezza*** E' stata redatta una procedura di reporting degli eventi rilevanti ai fini della sicurezza per riferirli il più rapidamente possibile al management aziendale? *(Tutti i dipendenti devono essere a conoscenza delle procedure per riportare gli incidenti).*											
4.4.3.2	***Rapporti sulle criticità di sicurezza*** La procedura prevede che gli utenti forniscano rapporti sulle vulnerabilità osservate e/o sospette?											
4.4.3.3	***Rapporti sui malfunzionamenti del software*** E' stata redatta una procedura che consenta agli utenti di fornire un rapporto sui malfunzionamenti del software?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.4.3.4	***Apprendere dagli incidenti*** E' stata realizzata procedure di valutazione degli incidenti o dei malfunzionamenti (tipo, volumi, costi)?											
4.4.3.5	***Processo di disciplina*** Sono state previste sanzioni per le violazioni delle procedure di sicurezza?											

Categoria:

4.5	**SICUREZZA FISICA ED AMBIENTALE**
4.5.1	***AREE DI SICUREZZA***

Obiettivo:

Verificare la presenza di procedure e misure atte a prevenire accessi non autorizzati, danni e interferenze ai servizi dell'IT.
Verificare che gli elaboratori di informazioni sensibili o critiche siano localizzati in locali protetti (o in aree di sicurezza) mediante perimetri definiti di sicurezza e con controlli di accesso.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.1.1.a	***Perimetro di sicurezza fisica*** E' stato chiaramente definito il perimetro dell'area da proteggere ?											
4.5.1.1.b	Il perimetro di un edificio o sito che contiene elaboratori di informazioni è in buone condizioni (non devono esistere varchi che consentano facili irruzioni), con i muri esterni solidi e tutte le porte esterne opportunamente protette da accessi non autorizzati (per es. con meccanismi di controllo, cancelli, allarmi, serrature, ecc.) ?											
4.5.1.1.c	E' predisposta una reception vigilata o altri mezzi di controllo dell'accesso fisico al luogo o all'edificio ?											
4.5.1.1.d	Gli accessi sono limitati al solo personale autorizzato ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.1.1.e	Se necessario sono estendse le barriere fisiche a tutto il volume del sito, dai sottopavimenti ai controsoffitti, per prevenire ingressi non autorizzati e contaminazioni ambientali come quelle causate da incendi e allagamenti?											
4.5.1.1.f	Le porte antincendio dentro il perimetro di sicurezza devono sono allarmate e dotate di un sistema di blocco automatico?											
4.5.1.2.a	***Controllo accessi fisici*** I visitatori sono sorvegliati o identificati e la data e l'ora del loro ingresso registrate?											
4.5.1.2.b	L'accesso a informazioni sensibili e agli elaboratori è controllato e limitato alle sole persone autorizzate? *(Tramite l'utilizzo di dispositivi di autenticazione, come ad esempio badge dotati di sistemi di identificazione, per autorizzare e convalidare tutti gli accessi; il tracciamento di tutti gli accessi deve essere conservato per sicurezza.).*											
4.5.1.2.c	Tutto il personale adotta misure di identificazione a vista e deve essere esortato a chiedere il riconoscimento degli estranei non accompagnati e di chiunque non indossi misure di riconoscimento a vista?											
4.5.1.2.d	I diritti di accesso alle aree protette devono essere regolarmente rivisti e aggiornati?											
4.5.1.3.a	***Sicurezza degli uffici, stanze e apparecchiature*** Sono implementati meccanismi di chiusura per impedire l'accesso al pubblico ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.1.3.b	Gli edifici sono inaccessibili e fornire un'indicazione minima della loro destinazione, senza segnali riferibili a una presenza di attività di trattamento delle informazioni, né all'interno né all'esterno ?											
4.5.1.3.c	Materiali e attrezzature per l'ordinaria gestione, per es. fotocopiatrici, fax, sono collocati in maniera adeguata all'interno dell'area ?											
4.5.1.3.d	Porte e finestre sono chiuse (quando i locali non sono presidiati) e devono essere applicate protezioni esterne alle finestre, soprattutto al piano terra ?											
4.5.1.3.e	Sono applicati sistemi antintrusione (progettati con standard internazionali certificati) a tutte le porte esterne ed alle finestre raggiungibili e testati regolarmente,? Le aree non presidiate sono sempre allarmate?											
4.5.1.3.f	Gli elaboratori delle informazioni utilizzati dall'azienda sono fisicamente separati da quelli gestiti da terze parti?											
4.5.1.3.g	Tutti i documenti (localizzazione, rubriche telefoniche, ecc.) che identificano l'ubicazione di elaboratori di informazioni critiche sono non accessibili al pubblico?											
4.5.1.3.h	I materiali pericolosi o infiammabili sono immagazzinati a una distanza di sicurezza dall'area protetta ?											
4.5.1.3.i	I ricambi, l'equipaggiamento tecnico di emergenza e i dati di backup sono riposti a una distanza di sicurezza per evitare danneggiamenti derivanti da un disastro occorso al sito principale ?											
4.5.1.4.a	***Lavoro nell'area protetta*** Il personale è messo a conoscenza delle attività dell'area protetta soltanto per il minimo necessario?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.1.4.b	E' evitato nell'area protetta il lavoro non sorvegliato, sia per ragioni di sicurezza sia per evitare attività malevole?											
4.5.1.4.c	Le aree protette non presidiate sono fisicamente chiuse e periodicamente controllate?											
4.5.1.4.d	Le terze parti a supporto del personale di servizio hanno un accesso limitato all'area protetta o agli elaboratori di informazioni sensibili, solo per quanto necessario e richiesto dalle attività di supporto svolte? [*Tale accesso deve essere autorizzato e controllato. Ulteriori barriere e perimetri per il controllo dell'accesso fisico possono rendersi necessari tra aree con differenti diritti di accesso all'interno del perimetro protetto*]											
4.5.1.4.e	Apparecchiature fotografiche, audio-video o di altro tipo, sono ammesse solo su autorizzazione?											
4.5.1.5.a	***Aree isolate di consegna e carico*** L'accesso ad aree di attesa dall'esterno è ristretto al personale identificato e autorizzato?											
4.5.1.5.b	L'area è strutturata in maniera tale che le forniture possano essere scaricate senza che gli addetti alle consegne abbiano accesso ad altre parti dell'edificio?											
4.5.1.5.c	Gli accessi esterni all'area sono chiusi quando le porte interne sono aperte?											
4.5.1.5.d	Il materiale in entrata è ispezionato contro potenziali atti illeciti prima che sia introdotto nelle postazioni di utilizzo?											
4.5.1.5.e	Il materiale in entrata è registrato all'entrata nel sito?											

Categoria:

4.5	**SICUREZZA FISICA ED AMBIENTALE**
4.5.2	***SICUREZZA DEGLI STRUMENTI***

Obiettivo:

Verificare la presenza di misure atte a proteggere i principali presidi tecnologici.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.2.1.a	***Posizionamento e protezione degli strumenti*** Le apparecchiature sono collocate in modo da ridurre al minimo gli accessi non necessari nelle aree di lavoro ?											
4.5.2.1.b	Gli elaboratori per il trattamento e la conservazione dei dati sensibili sono posti in modo da ridurre i rischi di accessi a letture non autorizzate durante il loro utilizzo ?											
4.5.2.1.c	Le applicazioni che richiedono una speciale difesa sono isolate per ridurre il livello generale di protezione richiesto?											
4.5.2.1.d	Sono adottati controlli per minimizzare il rischio di potenziali minacce, quali furti, incendi, esplosivi, fumo, acqua (o mancanza di fornitura), polvere, vibrazioni, effetti chimici, interferenze delle forniture elettriche, radiazioni elettromagnetiche ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.2.1.e	E' stata definita una politica interna per disciplinare la possibilità di mangiare, bere e fumare in prossimità di elaboratori di informazioni ?											
4.5.2.1.f	Sono monitorate le condizioni ambientali che potrebbero influire negativamente sulle operazioni di elaborazione ?											
4.5.2.1.g	E' considerato l'impatto di accadimenti disastrosi nelle vicinanze dell'area protetta, ad esempio un incendio in un edificio vicino ecc.. ?											
4.5.2.1.h	E' considerato l'uso di speciali metodi di protezione per le attrezzature in ambiente industriale ?											
4.5.2.2.a	***Alimentazione d'emergenza*** Sono presenti sistemi di continuità nella fornitura di energia come l'alimentazione multipla (privilegiata) per ovviare a guasti al sistema di alimentazione; o l'alimentazione di emergenza (UPS – uninterruptable power supply) o generatore di riserva ?											
4.5.2.3.a	***Sicurezza del cablaggio*** Le linee elettriche e di telecomunicazione sono interrate o protette alternativamente in modo adeguato ?											
4.5.2.3. b	Il cablaggio delle reti è protetto da intercettazioni non autorizzate o da danni, per esempio usando canaline o evitando passaggi attraverso zone pubbliche ?											
4.5.2.3.c	I cavi elettrici devono essere isolati da quelli di trasmissione per prevenire interferenze ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.2.3.d	I sistemi sensibili o critici ulteriori includono l'installazione in canaline o tubi blindati e box o stanze chiuse nei punti di controllo e di terminazione (punti di permutazione) ?											
4.5.2.3.e	I sistemi sensibili o critici ulteriori includono l'uso di instradamenti alternativi o mezzi di trasmissione alternativi?											
4.5.2.3.f	I sistemi sensibili o critici ulteriori includono l'uso di cablaggio a fibre ottiche?											
4.5.2.3.g	I sistemi sensibili o critici ulteriori includono sistemi di deviazione dei flussi a causa di derivazioni non autorizzate?											
4.5.2.4.a	***Manutenzione delle attrezzature*** La manutenzione rispetta le istruzioni dei produttori?											
4.5.2.4.b	E' utilizzato solo personale specializzato per le riparazioni?											
4.5.2.4.c	Sono registrati di tutti i guasti sospetti o concreti e della manutenzione preventiva e correttiva?											
4.5.2.4.d	Controlli accurati sono effettuati quando la strumentazione è mantenuta all'esterno?											
4.5.2.5.a	***Sicurezza delle attrezzature usate all'esterno dei locali aziendali*** L'equipaggiamento portato all'esterno dell'azienda è custodito in aree pubbliche e i computer portatili devono essere trasportati in valige apposite e "mascherati" durante il trasporto?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.2.5.b	Le istruzioni fornite dal fabbricante sono osservate per proteggere gli apparati e le attrezzature da possibili minacce esterne, per esempio per la protezione da campi elettromagnetici?											
4.5.2.5.c	Sono prese in considerazione adeguate coperture assicurative?											
4.5.2.5.d	I dati sono cancellati in modo non recuperabile prima della dismissione o del riutilizzo dei supporti?											
4.5.2.6	***Cancellazione delle informazioni*** Le informazioni memorizzate vengono cancellate dagli apparati prima del loro smaltimento o reimpiego?											

Categoria:

4.5	**SICUREZZA FISICA ED AMBIENTALE**
4.5.3	***CONTROLLI GENERALI***

Obiettivo:

Verificare la presenza di misure di sicurezza per prevenire accessi non autorizzati, danni e furti d'informazioni e di strumenti di elaborazione.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.3.1.a	***Policy del clear desk and screen*** La documentazione e i supporti informatici sono riposti in armadi di sicurezza quando non usati, specialmente al di fuori dell'orario di lavoro?											
4.5.3.1.b	Informazioni critiche sono riposte in armadi di sicurezza ignifughi?											
4.5.3.1.c	I personal computer e i terminali sono protetti da accessi non autorizzati mediante chiavi di chiusura, password?											
4.5.3.1.b	I fax e i punti di accesso ai servizi di posta sono protetti?											
4.5.3.1.e	Le informazioni riservate e classificate, quando stampate, vengono tolte immediatamente dalla stampante?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.5.3.2.	***Trasferimento di proprietà*** E' regolamentato il trasferimento di beni aziendali (strumenti, informazioni e software, ecc)?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.1	***RESPONSABILITÀ E PROCEDURE OPERATIVE***

Obiettivo:

Verificare l'adozione di idonee procedure che consentano un corretto e sicuro funzionamento degli elaboratori di produzione. Verificare inoltre la presenza di ambienti di test e produzione separati alfine di evitare modifiche e/o accessi non idonei ai dati di produzione aziendali.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.1.1.a	***Documentazione delle procedure operative*** Sono state documentate e mantenute aggiornate le procedure di produzione per il corretto funzionamento, la manutenzione ed il test di tutti i sistemi ?											
4.6.1.1.b	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione, inclusa l'elaborazione e il trattamento delle informazioni ?											
4.6.1.1.c	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione, inclusi i requisiti di scheduling ?											
4.6.1.1.d	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione, inclusi le istruzioni per la gestione degli errori o di altre situazioni eccezionali ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.1.1.e	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione, inclusa l'assistenza nei casi di difficoltà tecniche ?											
4.6.1.1.f	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione incluso le istruzioni per il trattamento di speciali output?											
4.6.1.1.g	Sono state realizzate procedure per gestire i log delle modifiche dei dati e degli ambienti di produzione?											
4.6.1.1.h	Le procedure specificano le istruzioni per l'esecuzione dettagliata di ciascuna mansione incluso il riavvio del sistema e le procedure di recovery nell'ipotesi di guasti di sistema?											
4.6.1.2	***Controlli sulle modifiche operative*** Sono stati individuati dei controlli per le modifiche alle apparecchiature e ai sistemi?											
4.6.1.3	***Procedure di gestione degli incidenti*** Sono state realizzate procedure per la gestione degli incidenti, al fine di assicurare una pronta, efficace e corretta risposta agli incidenti rilevanti per la sicurezza ?											
4.6.1.3.a	***Separazione dei compiti*** Sono state separate le responsabilità di conduzione da quelle di approvazione?											
4.6.1.4.b	E' stato separato l'ambiente di sviluppo e test da quello di produzione per ridurre il rischio di modifiche accidentali o accessi non autorizzati al software di produzione e ai dati aziendali?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.1.5.a	***Separazione tra ambiente operativo e di sviluppo*** Sono presenti controlli tra il software di sviluppo e quello di produzione, che ove possibile dovrebbero essere gestiti da processori o domini o directory differenti?											
4.6.1.5.b	Sono opportunamente separate le attività di Test e di sviluppo?											
4.6.1.5.c	E' limitato l'accesso ai sistemi di produzione di compilatori e altre analoghe utilità di sistema ?											
4.6.1.5.d	Sono usate diverse procedure di log-on per i sistemi di produzione e di test al fine di ridurre il rischio di errore? *(Gli utenti devono essere incoraggiati all'uso di differenti password per questi sistemi, e i menù devono mostrare adeguati messaggi di identificazione).*											
4.6.1.5.e	Lo staff di sviluppo utilizza e possiede la password di produzione esclusivamente quando sono necessari controlli al sistema di produzione ?											
4.6.1.5.f	Sono stati implementati controlli che assicurino l'effettivo cambiamento delle password dopo l'utilizzo ?											
4.6.1.6	***Gestione dei contratti esterni*** I contratti di outsourcing prevedono appropriate misure di sicurezza? *(I rischi devono essere valutati preventivamente e controlli adeguati devono essere concordati con l'outsourcer e inseriti nel contratto).*											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.2	***PIANIFICAZIONE DI UN SISTEMA ED ACCETTAZIONE***

Obiettivo:

Verificare le misure atte a minimizzare il rischio di indisponibilità del sistema.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.2.1	***Capacity planning*** E' stato realizzato un Capacity Planning (piano di dimensionamento) per assicurarsi la disponibilità di capacità e di risorse adeguate, prendendo in considerazione le attuali e future tendenze nei processi informativi dell'azienda?											
4.6.2.2	***Approvazione dei nuovi sistemi*** Sono stati stabiliti i criteri per la delibera di acquisizione di nuovi sistemi o nuove versioni di prodotti?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.3	***PROTEZIONE DA SOFTWARE MALEVOLO***

Obiettivo:

Verifica la presenza di presidi tecnico-organizzativi atti a preservare l'integrità dei dati e del software, principalmente dai cosiddetti Virus.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.3.a	***Controlli sui software malevoli*** E' presente una policy formale che tenga conto delle licenze software e proibisca l'uso di software non autorizzato?											
4.6.3.b	E' stata adottata una politica formale di protezione contro i rischi derivanti da file o software ottenuti sia da reti esterne o da altre vie, che indichi quali misure protettive adottare?											
4.6.3.c	Sono stati installati e regolarmente aggiornati idonei prodotti antivirus?											
4.6.3.d	Sono pianificate ed eseguite verifiche periodiche sul software e sui dati che supportano processi critici?											
4.6.3.e	Ogni file di origine non certa è passato sotto il controllo dell'antivirus?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.3.f	Ogni allegato di posta elettronica è verificato da un antivirus sia dal server sia dal client ?											
4.6.3.g	Sono stati sensibilizzati gli utenti verso i rischi connessi ai virus e alle misure protettive esistenti ?											
4.6.3.h	Sono stati individuati ruoli, responsabilità e procedure di gestione per relazionare e ripristinare i sistemi dagli attacchi dei virus, includendo il back-up dei dati e del software e le procedure di recovery ?											
4.6.3.i	Sono state predisposte procedure di verifica di tutte le informazioni relative ai virus malevoli, e devono garantirsi bollettini accurati e istruttivi ?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.4	***MANUTENZIONE***

Obiettivo:

Verificare la predisposizione di procedure per il mantenimento dell'integrità e della disponibilità dei dati e servizi.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.4.1	***Back-up delle informazioni*** Sono state predisposte adeguate procedure di backup?											
4.6.4.2	***Log operativi*** Il personale mantiene una registrazione delle operazioni svolte sui sistemi?											
4.6.4.3.a	***Logging degli errori*** Sono registrati sia gli errori sia le azioni correttive intraprese?											
4.6.4.3.b	Esistono chiare regole per riportare gli errori di trattamento?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.5	***GESTIONE DELLE RETI***

Obiettivo:

Verificare l'adozione di misure tecnico-organizzative per assicurare la sicurezza delle informazioni in transito sulle reti e delle infrastrutture di supporto

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.5.1.a	***Controlli sulla rete*** Sono separate le responsabilità di gestione delle reti dalle responsabilità di gestione degli elaboratori?											
4.6.5.1.b	Sono state definite le responsabilità e le procedure per la gestione di apparati remoti?											
4.6.5.1.c	Sono state adottate opportune misure di sicurezza al fine di proteggere l'integrità e la riservatezza dei dati e la disponibilità dei sistemi?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.6	***UTILIZZO DEI SUPPORTI E SICUREZZA***
4.6.6.1	

Obiettivo:

Verificare la predisposizione di procedure mirate alla gestione dei supporti rimovibili degli elaboratori (dischi, nastri, cassette, ecc).

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.6.1.a	***Gestione dei supporti rimovibili*** Sono stati cancellati, se non più necessari, i contenuti precedenti dei supporti riutilizzabili che devono essere eliminati dall'azienda?											
4.6.6.1.b	E' stata richiesta l'autorizzazione per tutti i supporti da eliminare e conservata una loro registrazione come documento di verifica?											
4.6.6.1.c	Tutti i supporti sono stati immagazzinati in ambienti sicuri nl rispetto delle istruzioni d'uso?											
4.6.6.2.a	***Eliminazione dei supporti*** I supporti riguardanti informazioni sensibili sono stati archiviati e collocati al sicuro da pericoli, ad esempio stracciati, oppure riempiti di nuovi dati per essere riutilizzati nell'azienda ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.6.2.b	Sono state adottate disposizioni di sicurezza anche per: documenti cartacei, registrazioni vocali o di altro tipo, carta carbone, nastri di stampa usa e getta, nastri magnetici, dischi o cassette rimovibili, liste di programma, dati sui test, documentazione di sistema ?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.6	***UTILIZZO DEI SUPPORTI E SICUREZZA***

Obiettivo:

Verificare l'adozione di misure di sicurezza per il trattamento ed archiviazione dei dati.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.6.3	***Procedure per il trattamento delle informazioni*** Sono state realizzate procedure per il trattamento e l'archiviazione dei dati ?											
4.6.6.4	***Sicurezza della documentazione di sistema*** La sicurezza dei documenti di sistema (processi applicativi, procedure, dati, processi di autorizzazione) è stata garantita dagli accessi non autorizzati ?											

Categoria:

4.6	GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ
4.6.7	**SCAMBIO DI DATI E SOFTWARE**

Obiettivo:

Verificare l'adozione di procedure atte a considerare i rischi di perdite, modifiche o uso scorretto dei dati scambiati, in particolare con la posta elettronica.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.7.1	***Accordi sullo scambio di software e informazioni*** Sono stati stipulati accordi formali per lo scambio di dati e software ?											
4.6.7.2	***Sicurezza dei media in transito*** Il trasporto di supporti magnetici contenenti dati è adeguatamente protetto?											
4.6.7.3	***Sicurezza nel commercio elettronico*** Il commercio elettronico è adeguatamente protetto contro i rischi di attività fraudolenta, controversie contrattuali e divulgazione e/o modifica di informazioni?											
4.6.7.4.a	***Sicurezza della posta elettronica*** L'azienda ha emesso una policy specifica riguardante lo stato e l'uso dell'e-mail ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.7.4.b	La valutazione dei i rischi per la sicurezza, creati dalla posta elettronica includono la vulnerabilità dei messaggi da accessi non autorizzati o modificazioni o indisponibilità di servizio?											
4.6.7.4.c	La valutazione dei rischi per la sicurezza creati dalla posta elettronica includono valutazioni legali, come la necessità delle prove della provenienza, dell'invio, della spedizione e dell'accettazione?											
4.6.7.4.d	La valutazione dei rischi per la sicurezza creati dalla posta elettronica includono le implicazioni della pubblicazione delle liste del personale accessibili dall'esterno?											
4.6.7.4.e	La valutazione dei rischi per la sicurezza creati dalla posta elettronica includono il controllo dell'accesso da parte di utenti remoti all'account di posta elettronica?											
4.6.7.4.f	La valutazione dei rischi per la sicurezza creati dalla posta elettronica includono la vulnerabilità rispetto agli errori e la generale affidabilità e disponibilità del servizio?											
4.6.7.4.g	La valutazione dei rischi per la sicurezza creati dalla posta elettronica includono l'impatto di un cambiamento dei mezzi di comunicazione sui processi commerciali (per es. gli effetti dell'aumentata rapidità di invio o gli effetti dell'invio di messaggi formali indirizzati a singoli piuttosto che all'azienda)?											
4.6.7.4.h	Le politiche sull'uso della posta elettronica considerano gli attacchi all'e-mail, ad esempio virus ed intercettazioni?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.7.4.i	Le politiche sull'uso della posta elettronica considerano la protezione degli attachments di posta elettronica ?											
4.6.7.4.l	Le politiche sull'uso della posta elettronica indicano quando non usare la posta elettronica ?											
4.6.7.4.m	Le politiche sull'uso della posta elettronica considerano la responsabilità dei dipendenti per non compromettere la compagnia (es. inviando messaggi elettronici diffamatori, o utilizzando l'e-mail per molestie, per acquisti non autorizzati) ?											
4.6.7.4.n	Le politiche sull'uso della posta elettronica considerano l'uso di tecniche crittografiche per proteggere la riservatezza e l'integrità dei messaggi ?											
4.6.7.4.o	Le politiche sull'uso della posta elettronica considerano la conservazione dei messaggi che potrebbero essere utili in caso di vertenze legali ?											
4.6.7.4.p	Le politiche sull'uso della posta elettronica considerano controlli addizionali per verificare i messaggi che non possono essere autenticati ?											

Categoria:

4.6	**GESTIONE DELLE COMUNICAZIONI E DELL'OPERATIVITÀ**
4.6.7	**SCAMBIO DI DATI E SOFTWARE**

Obiettivo:
Verificare l'emanazione di policy e linee guida per i prodotti di office automation e l'adozione di provvedimenti per la protezione dei dati pubblicati in rete.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.7.5.a	***Sicurezza dei prodotti di office automation*** Sono state realizzate policy e linee guida per l'utilizzo dei prodotti di office automation ?											
4.6.7.5.b	Sono stati adottati provvedimenti per garantire l'integrità dei dati pubblicati in rete, in modo che l'informazione sia ottenuta rispettando la normativa sulla protezione dei dati?											
4.6.7.6.a	***Sistemi disponibili al pubblico*** Sono stati adottati provvedimenti per garantire l'integrità dei dati pubblicati in rete, in modo che l'informazione inserita e elaborata dal sistema pubblico sia processata completamente e in modo tempestivo?											
4.6.7.6.b	Sono stati adottati provvedimenti per garantire l'integrità dei dati pubblicati in rete, in modo che le informazioni sensibili siano protette durante i processi di raccolta e di conservazione?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.6.7.6.c	Sono stati adottati provvedimenti per garantire l'integrità dei dati pubblicati in rete, in modo che l'accesso al sistema pubblico non consenta ingressi fortuiti alle reti con cui è connesso?											
4.6.7.7	***Altre forme di scambio di dati*** Gli scambi di informazioni telefoniche, tramite fax, ecc. sono state regolate e il personale adeguatamente istruito?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.1	***ESIGENZE DI GOVERNO DEGLI ACCESSI***

Obiettivo:
Verificare la definizione di una politica sul controllo degli accessi ai dati.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.1.1.a	***Politica di controllo degli accessi*** Le policy e le regole per l'accesso ai dati sono state definite e documentate?											
4.7.1.1.b	L'accesso alle informazioni e ai processi aziendali è stato controllato sulla base dei requisiti di sicurezza?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.2	***GESTIONE DELL'ACCESSO DEGLI UTENTI***

Obiettivo:

Verificare l'adozione di procedure mirate ad evitare accessi non autorizzati ai dati aziendali di business.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.2.1.a	***Registrazione degli utenti*** E' utilizzata un'unica ID per utente, così che gli utilizzatori siano collegati e resi imputabili delle loro azioni ? *(L'uso di ID di gruppo deve essere consentito solo se sono necessarie all'attività da compiere).*											
4.7.2.1.b	L'utente è stato autorizzato all'accesso dal titolare del sistema informativo ? *(Può anche essere ammessa l'approvazione separata per i diritti di accesso da parte della direzione)*											
4.7.2.2.a	***Gestione dei privilegi*** Il livello di accesso garantito è adatto agli scopi ed è compatibile con la politica di sicurezza ?											
4.7.2.2.b	E' stato consegnato agli utenti un documento scritto che contempli i loro diritti di accesso ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.2.2.c	Gli l'utenti hanno firmato il documento, dichiarando di avere capito le condizioni di accesso ?											
4.7.2.3	***Gestione delle password utente*** E' garantito che i service providers non permettano l'accesso prima della conclusione delle procedure di autorizzazione ?											
4.7.2.4.a	***Revisione dei diritti di accesso degli utenti*** Sono immediatamente ritirati i diritti di accesso degli utenti che hanno cambiato lavoro o lasciato l'organizzazione ?											
4.7.2.4.b	Sono periodicamente controllate e rimosse le ID in eccesso che identificano uno stesso utente e documentare tale rimozione ?											
4.7.2.4.c	Non sono di solito rilasciate, ad altri utenti, le ID in eccesso che sono state rimosse ?											
4.7.2.4.d	Sono conservate le registrazioni formali delle persone ammesse all'uso del servizio ?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.3	***RESPONSABILITÀ DEGLI UTENTI***

Obiettivo:
Verificare l'emissione di linee guida per la scelta e la gestione sicura delle password.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.3.1.a	***Utilizzo delle password*** Gli utenti sono stati avvisati di tenere la password riservata ?											
4.7.3.1.b	Gli utenti sono stati avvisati di cambiare la password quando può apparire in qualche modo compromessa ?											
4.7.3.1.c	Gli utenti sono stati avvisati di scegliere password affidabili con una lunghezza minima di sei caratteri, che siano facilmente ricordabili, non facilmente individuabili, con caratteri alfanumerici diversi ?											
4.7.3.1.d	Gli utenti sono stati avvisati cambiare le password a intervalli regolari o in base al numero degli accessi e evitare di riutilizzarne di vecchie ?											
4.7.3.1.e	Gli utenti sono stati avvisati cambiare la password provvisoria alla prima registrazione ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.3.1.f	Gli utenti sono stati avvisati non includere la password in processi automatici di registrazione ?											
4.7.3.1.g	Gli utenti sono stati avvisati non condividere le password individuali di altri utenti ?											
4.7.3.2.a	***Dispositivi degli utenti lasciati incustoditi*** Gli utenti sono stati invitati a terminare le sessioni attive quando è terminato il lavoro, a meno che il terminale non sia protetto da meccanismi quali screen saver con password ?											
4.7.3.2.b	Gli utenti sono stati invitati a procedere al log-off del server quando la sessione è terminata ?											
4.7.3.2.c	Gli utenti sono stati invitati a proteggere i PC o i terminali dall'uso non autorizzato mediante l'uso di chiavi d'accesso?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.4	***CONTROLLO DELL'ACCESSO ALLA RETE***

Obiettivo:
Verificare l'adozione di politiche e procedure mirate alla protezione delle risorse accessibili tramite la rete telematica aziendale.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Inserisci, nello spazio "COMMENTI", una più ampia spiegazione delle ragioni indicate in Q2

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.4.1	***Politiche sull'utilizzo dei servizi di rete*** E' stata realizzata una policy sull'uso delle reti e dei servizi connessi?											
4.7.4.2.a	***Rafforzamento dei percorsi di rete*** Sono state preventivamente determinate e controllate le possibilità di accesso alle risorse di rete?											
4.7.4.2.b	Sono stati adottati controlli che restringono il percorso tra il terminale dell'utente e i servizi a cui è autorizzato l'accesso, (che riducono il rischio di accessi o operazioni sulle informazioni non autorizzate), limitando le opzioni di percorso in diversi punti della rete, sulla base di scelte predefinite. Sono state assegnate linee o numeri telefonici dedicati ?											
4.7.4.2.c	Sono presenti porte a connessione automatica per sistemi di specifiche applicazioni o ingressi di sicurezza?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.4.2.d	Sono presenti menu limitati e opzioni di submenù per utenti individuali?											
4.7.4.2.e	Sono previste limitazioni sul roaming in rete illimitato?											
4.7.4.2.f	Sono previste misure di rinforzamento dell'uso di sistemi e/o ingressi di sicurezza per utenti di reti esterne?											
4.7.4.2.g	Sono previsti controlli attivi sui punti origine autorizzati a comunicazioni verso qualsiasi destinazione tramite gateway di sicurezza, ad esempio firewall, ecc.?											
4.7.4.3.a	***Autenticazione utente per le connessioni esterne*** Sono previste restrizioni dell'accesso alla rete mediante l'installazione di domini logici separati?											
4.7.4.3.b	E' autenticato l'accesso alle risorse di rete?											
4.7.4.4	***Autenticazione dei nodi*** Sono autenticate le connessioni a sistemi remoti soprattutto quando il controllo della rete non è effettuato dall'azienda? *(L'autenticazione dei nodi può essere un modo alternativo per autenticare gruppi di utenti remoti)*											
4.7.4.5	***Protezione delle porte di gestione da remoto*** E' controllato l'accesso alle porte di gestione degli elaboratori con adeguati meccanismi di sicurezza, come chiavi di accesso e procedure per garantire che tali porte siano accessibili solo in virtù di accordi tra i responsabili del servizio e il personale di supporto hw/sw che richiede l'accesso?											
4.7.4.6	***Separazione delle reti*** Sono inseriti meccanismi di separazione logica delle reti?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.4.7	***Controllo delle connessioni di rete*** E' controllata la possibilità di connessione degli utenti a reti condivise in accordo con la politica di controllo accessi definita?											
4.7.4.8	***Controllo del routing di rete*** Sono presenti meccanismi di instradamento per le reti condivise che consentano di controllare i flussi delle informazioni ?											
4.7.4.9	***Sicurezza dei servizi di rete*** Tutti i meccanismi di sicurezza adottati sono chiaramente e formalmente descritti ?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.5	***CONTROLLO DELL'ACCESSO AI SISTEMI OPERATIVI***

Obiettivo:

Verificare l'adozione di procedure e misure per prevenire l'accesso non autorizzato agli elaboratori aziendali, mediate apposite procedure di Logon e sistemi gestione della password.

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.5.1	***Autenticazione automatica del terminale*** Sono previste procedure di identificazione automatica del terminale o dell'apparecchiatura portatile utilizzate?											
4.7.5.2.a	***Procedure di Logon per l'accesso alle risorse*** Sono previste procedure di logon per l'accesso alle risorse informatiche?											
4.7.5.2.b	La procedura di logon evita di mostrare informazioni sul sistema o l'applicazione fino a che il processo di logon sia concluso con successo?											
4.7.5.2.c	La procedura di logon evidenzia che il computer può essere usato solo dagli utenti autorizzati all'accesso?											
4.7.5.2.d	La procedura di logon evita di fornire alcuna indicazione che possa facilitare accessi non autorizzati?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.5.2.e	La procedura di logon convalida le informazioni di logon solo dopo il completamento dell'inserimento dei dati ? *(se si presenta un errore, il sistema non deve indicare quale dato è corretto e quale non corretto*).											
4.7.5.2.f	La procedura di logon limita il numero di tentativi infruttuosi di logon (sono raccomandati tre) e: registra tali tentativi, impone un tempo d'attesa prima di accettare ulteriori procedure di logon o rigetta ogni altro tentativo senza specifica autorizzazione, disconnette la connessione con i link dei dati?											
4.7.5.2.g	La procedura di logon limita il tempo massimo e minimo concesso per le procedure di logon, superato il quale il sistema interrompe la procedura ?											
4.7.5.2.h	La procedura di logon mostra dopo il completamento della procedura la data e l'ora del precedente logon positivo e i dettagli di ogni tentativo infruttuoso di logon fin dall'ultimo logon riuscito ?											
4.7.5.3.a	***Identificazione e autenticazione degli utenti*** Gli utenti (incluso lo staff di supporto tecnico) sono stati identificati e autenticati da ID personali ?											
4.7.5.3.b	E' stato realizzato un sistema di gestione delle password che fa rispettare l'uso delle password individuali per garantire il tracciamento ?											
4.7.5.4.a	***Sistema di gestione delle password*** E' stato realizzato un sistema di gestione delle password, ove se opportuno, autorizza gli utenti a selezionare e cambiare la loro password e includere una procedura di conferma per tenere conto degli errori ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.5.4.b	E' stato realizzato un sistema di gestione delle password che promuovere una scelta di password di qualità, come descritto al punto 4.7.3 ?											
4.7.5.4.c	E' stato realizzato un sistema di gestione delle password che una volta selezionata la password, spingere gli utenti a cambiare quella provvisoria alla prima registrazione ?											
4.7.5.4.d	E' stato realizzato un sistema di gestione delle password che conserva la registrazione delle precedenti password, per esempio degli ultimi dodici mesi, e prevenirne il riutilizzo ?											
4.7.5.4.e	E' stato realizzato un sistema di gestione delle password che mantiene i file delle password separati dai dati del sistema applicativo ?											
4.7.5.4.f	E' stato realizzato un sistema di gestione delle password che conserva le password in forma criptata usando algoritmi di tipo hash?											
4.7.5.4.g	E' stato realizzato un sistema di gestione delle password che modifica le password standard del rivenditore successivamente all'installazione del software ?											
4.7.5.5	***Uso di utility di sistema*** Sono state definite e controllate le utilità di sistema a disposizione degli utenti. ?											
4.7.5.6	***Avvisi per rischi di coercizione a salvaguardia degli utenti*** Ci sono rischi di imposizioni dove gli utenti potrebbero essere obiettivo di coercizione?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.5.7	***Time-out dei terminali*** Sono state realizzate procedure temporizzate di shut-down per i terminali inattivi ?											
4.7.5.8	***Limitazione del tempo di connessione*** Sono previste restrizioni temporali per l'accesso, usando, per esempio, tempi predefiniti o limitando l'accesso al solo orario di ufficio ?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.6	***CONTROLLO DELL'ACCESSO ALLE APPLICAZIONI***

Obiettivo:
Verificare l'adozione di misure per prevenire l'accesso non autorizzato alle informazioni contenute negli elaboratori.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.6.1	***Restrizione all'accesso delle informazioni*** L'accesso alle applicazioni è stato limitato secondo quanto definito nella politica di controllo accessi?											
4.7.6.2.a	***Isolamento dei sistemi sensibili*** I sistemi critici hanno ambienti dedicati (isolati), con individuazione e documentazione delle criticità del Sistema?											
4.7.6.2.b	Quando un'applicazione critica è stata inserita in un ambiente condiviso, il sistema applicativo con cui deve spartire le risorse, è stato identificato e concordato con il titolare dell'applicazione critica?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.7	***MONITORAGGIO DELL'ACCESSO E DELL'USO DEL SISTEMA***

Obiettivo:
Verificare l'adozione di misure finalizzate al monitoraggio dell'accesso ai sistemi per il controllo di accessi e/o attività non autorizzate.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.7.1.a	***Logging degli eventi*** I dati di tracciamento e di audit sono raccolti e conservati per un periodo stabilito ?											
4.7.7.1.b	I dati tracciamento e di audit includono l'identificazione degli utenti?											
4.7.7.1.c	I dati tracciamento e di audit includono date e orari di registrazione e di uscita ?											
4.7.7.1.d	I dati tracciamento e di audit includono identità del terminale o postazione se è possibile ?											
4.7.7.1.e	I dati tracciamento e di audit includono registrazioni dei tentativi riusciti e respinti di accesso al sistema ?											
4.7.7.2.a	***Monitoraggio dell'utilizzo dei sistemi*** L'utilizzo dei sistemi è monitorato per controllare che gli utenti eseguano solo le operazioni che sono state esplicitamente autorizzate, in particolare ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.7.2.b	Sono stabilite procedure per il monitoraggio dell'utilizzo dei dati ?											
4.7.7.2.c	I risultati delle attività di monitoraggio sono valutati con periodicità definita ?											
4.7.7.2.d	I risultati dell'analisi dei file di log è finalizzata alla comprensione delle minacce ?											
4.7.7.3	***Sincronizzazione dei clock*** Gli orologi degli elaboratori sono opportunamente sincronizzati ?											

Categoria:

4.7	**GOVERNO DEGLI ACCESSI**
4.7.8	***COMPUTER PORTATILI E TELELAVORO***

Obiettivo:
Verificare la presenza di procedure per assicurare la sicurezza dei dati nell'utilizzo dei computer portatili e del telelavoro.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.7.8.1	***Computer portatili*** E' stata emessa una procedura di utilizzo dei portatili, soprattutto in luoghi pubblici, che preveda istruzioni per la protezione fisica del portatile e di controllo dell'accesso, tecniche crittografiche, backup, e protezione contro i virus?											
4.7.8.2	***Telelavoro*** Sono adottate policy e procedure di autorizzazione e controllo del telelavoro, in linea con la politica di sicurezza aziendale?											

Categoria:

4.8	**SVILUPPO E MANUTENZIONE DEI SISTEMI**
4.8.1	***REQUISITI DI SICUREZZA DEI SISTEMI***

Obiettivo:
Verificare la presenza di procedure per assicurare la sicurezza dei dati nell'utilizzo dei computer portatili e del telelavoro.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.1.1	***Analisi e descrizione dei requisiti di sicurezza*** La valutazione di nuovi sistemi o di modifiche ai sistemi in uso tiene conto delle esigenze di sicurezza derivate dalle esigenze di business?											

Categoria:

4.8	**SVILUPPO E MANUTENZIONE DEI SISTEMI**
4.8.2	***SICUREZZA NEI SISTEMI APPLICATIVI***

Obiettivo:
Verificare la presenza di procedure per assicurare la sicurezza dei dati nell'utilizzo dei computer portatili e del telelavoro.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.2.1	***Validazione dei dati di input*** I dati in input ai sistemi applicativi sono validati ai fini della valutazione sulla loro correttezza?											
4.8.2.2	***Controlli sulle elaborazioni*** I controlli di validazione sono incorporati nei sistemi al fine della intercettazione di corruzione dei dati?											
4.8.2.3	***Autenticazione dei messaggi*** L'autenticazione dei messaggi è utilizzata dove c'è esigenza di protezione rispetto all'integrità del contenuto dei messaggi?											
4.8.2.4	***Validazione dei dati di output*** I dati di output dei sistemi applicativi sono validati ai fini della valutazione sulla loro correttezza?											

Categoria:

4.8	**SVILUPPO E MANUTENZIONE DEI SISTEMI**
4.8.3	***ESIGENZE DI SICUREZZA DEL SISTEMA E CONTROLLI CRITTOGRAFICI***

Obiettivo:
Verificare l'adozione di procedure e misure che garantiscono la sicurezza nei sistemi, nonchè la riservatezza, l'integrità e l'autenticità dei dati.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.3.1.a	***Politiche sull'utilizzo dei controlli crittografici*** E' stato eseguito un risk assessment per determinare le modalità di utilizzo dei meccanismi crittografici ?											
4.8.3.1.b	Se si, è stato considerato l'approccio aziendale all'uso dei meccanismi crittografici di controllo nell'organizzazione, compresi i principi generali in base ai quali l'informazione aziendale deve essere protetta ?											
4.8.3.1.c	Se si, è stato considerato l'approccio alla gestione delle chiavi, inclusi i metodi per affrontare il recupero delle informazioni criptate in caso di perdita, compromissione o danneggiamento delle chiavi stesse ?											
4.8.3.1.d	Se si, sono stati considerati ruoli e responsabilità ?											
4.8.3.1.e	Se si, è stato considerata l'implementazione della politica dei controlli crittografici ?											
4.8.3.1.f	Se si, è stato considerato il governo delle chiavi ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.3.1.g	Se si, è stato considerato come deve essere determinato il giusto livello di protezione crittografica ?											
4.8.3.1.h	Se si, sono stati considerati gli standard da adottare per l'effettiva applicazione attraverso tutta l'organizzazione?											
4.8.3.2	***Crittografazione*** E' stata adottata la cifratura dei dati per garantire la riservatezza dei dati considerati critici ?											
4.8.3.3	***Firma digitale*** E' stata adottata la firma digitale per garantire l'autenticità e l'integrità dei documenti elettronici ?											
4.8.3.4	***Servizi di non-ripudio*** Sono adottati sistemi di non ripudio per garantire la certezza e l'origine di eventi definiti ?											
4.8.3.5.a	***Gestione delle chiavi di crittografia*** Sono adottati sistemi di gestione delle chiavi crittografiche per garantire l'utilizzo delle tecniche di cifratura ?											
4.8.3.5.b	E' presente un sistema di gestione di chiavi fondato su un complesso concordato di standard, procedure e metodi ?											
4.8.3.5.c	Se si, gli standard e le procedure considerano la generazione di chiavi per diversi sistemi crittografici e differenti applicazioni ?											
4.8.3.5.d	Se si, gli standard e le procedure considerano la generazione e la certificazione delle chiavi pubbliche ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.3.5.e	Se si, gli standard e le procedure considerano la fase di distribuzione delle chiavi per gli utenti designati, incluse le istruzioni per attivarle ?											
4.8.3.5.f	Se si, gli standard e le procedure considerano il deposito delle chiavi, comprese le modalità di autorizzazione degli utenti per l'accesso alle chiavi ?											
4.8.3.5.g	Se si, gli standard e le procedure considerano il cambiamento o l'aggiornamento delle chiavi, comprese le regole su quando le chiavi devono essere cambiate e come questo deve essere fatto ?											
4.8.3.5.h	Se si, gli standard e le procedure considerano le chiavi compromesse ?											
4.8.3.5.i	Se si, gli standard e le procedure considerano la revocare delle chiavi, incluse le modalità di ritiro o disattivazione, per es. quando le chiavi sono state compromesse o quando l'utente lascia l'azienda (nel qual caso la chiave va anche archiviata) ?											
4.8.3.5.l	Se si, gli standard e le procedure considerano il recupero delle chiavi perse o compromesse come politica di continuity management ?											
4.8.3.5.m	Se si, gli standard e le procedure considerano l'archiviazione delle chiavi ?											
4.8.3.5.n	Se si, gli standard e le procedure considerano la distruzione delle chiavi ?											
4.8.3.5.o	Se si, gli standard e le procedure considerano la registrazione e la verifica delle attività relative al governo delle chiavi ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.3.5.p	Se si, gli standard e le procedure considerano la probabilità di compromissioni, e sono fissati i tempi di attivazione e disattivazione in maniera tale che le chiavi possano essere usate solo per un determinato periodo ?											

Categoria:

4.8	**SVILUPPO E MANUTENZIONE DEI SISTEMI**
4.8.4	***LA SICUREZZA DEI FILE DI SISTEMA***

Obiettivo:
Verificare l'adozione di misure per assicurare la protezione del software di sistema.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.4.1	***Controlli sul software operativo*** Deve essere esercitato uno stretto controllo sull'implementazione del software di sistema in ambiente di produzione ?											
4.8.4.2	***Protezione dei dati di system test*** I dati usati per i test sono protetti e controllati ?											
4.8.4.3	***Controllo accessi a programmi nelle librerie sorgente*** E' mantenuto uno stretto controllo sulle librerie dei sorgenti ?											

Categoria:

4.8	**SVILUPPO E MANUTENZIONE DEI SISTEMI**
4.8.5	***LA SICUREZZA NELLO SVILUPPO E NELLE ATTIVITÀ DI SUPPORTO***

Obiettivo:
Verifica della presenza di misure di sicurezza sui sistemi applicativi e sui dati.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.5.1	***Procedure di controllo delle modifiche*** Sono presenti procedure di controllo sulle modifiche del ciclo di vita del sistema ?											
4.8.5.2	***Revisione tecnica delle modifiche dei sistemi*** I sistemi applicativi sono riveduti e testati quando vengono effettuate modifiche? ?											
4.8.5.3	***Restrizioni sulle modifiche ai pacchetti software*** Le modifiche ai pacchetti applicativi sono completamente testate e documentate, in modo da poter essere applicate se necessario agli aggiornamenti futuri del software ?											
4.8.5.4	***Canali nascosti e codice Trojan*** L'acquisto, l'utilizzo e le modifiche al software sono controllate per evitare l'introduzione di backdoors e di Trojans ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.8.5.5	***Sviluppo di software all'esterno*** Sono adottati opportuni controlli sullo sviluppo in outsourcing del software ?											

Categoria:

4.9	**GESTIONE DEL PIANO DI BUSINESS CONTINUITY**
4.9.1	***ASPETTI DEL PIANO DI BUSINESS CONTINUITY***

Obiettivo:
Verifica la presenza di procedure che consentono di contenere gli effetti di un'interruzione dell'attività di business e la sua ripresa.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.9.1.1.a	***Gestione del processo di Business Continuity*** E' presente un processo che abbia lo scopo di gestire lo sviluppo e il supporto dei piani di Business Continuity aziendale?											
4.9.1.1.b	Se si, è considerata l'identificazione dei rischi, compresa l'identificazione e l'assegnazione di priorità dei processi di business critici?											
4.9.1.1.c	Se si, è considerata l'identificazione dell'impatto delle interruzioni sull'azienda e determinazione degli obiettivi degli strumenti di trattamento delle informazioni?											
4.9.1.1.d	Se si, è considerata la valutazione dell'opportunità di sottoscrivere una specifica assicurazione come parte del piano di B.C?											
4.9.1.1.e	Se si, il piano di B.C. è documentato ed opportunamente formalizzato?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.9.1.1.f	Se si, sono considerati gli aspetti di formazione?											
4.9.1.1.g	Se si, sono considerati test e aggiornamenti regolari dei piani e dei processi individuati?											
4.9.1.1.h	Se si, sono individuati i livelli di responsabilità relativi?											
4.9.1.2.a	***Business continuity e analisi d'impatto*** La struttura del piano di B. C. parte dall'identificazione degli eventi che possono causare interruzioni ai processi aziendali, e in seguito valutare i rischi per determinare l'impatto di queste interruzioni (in termini di grado del danno e tempi di ripristino), considerando tutti i processi aziendali e non limitarsi agli strumenti di trattamento delle informazioni?											
4.9.1.2.b	Una volta formulato, il piano è stato approvato dalla direzione?											
4.9.1.3	***Stendere e implementare i piani di continuità*** Sono sviluppati i piani per mantenere o ripristinare le operazioni aziendali secondo i passi e i tempi previsti											
4.9.1.4.a	***Struttura della piano di Business Continuity*** E' mantenuta un'unica struttura di piani di B.C. che tiene conto delle condizioni per azionare i piani, che descrivano il processo da seguire (come valutare la situazione, chi deve essere coinvolto) prima che ciascun piano sia reso attivo?											
4.9.1.4.b	E' mantenuta un'unica struttura di piani di B.C. che tiene conto delle procedure d'emergenza che descrivano le azioni che devono essere prese in seguito ad un incidente che metta in pericolo operazioni aziendali e/o vite umane?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.9.1.4.c	E' mantenuta un'unica struttura di piani di B.C. che tiene conto delle procedure di fallback che descrivano le azioni da intraprendere per trasferire attività aziendali o servizi di supporto in posti provvisori e per riportare i processi aziendali alla normalità nei tempi previsti?											
4.9.1.4.d	E' mantenuta un'unica struttura di piani di B.C. che considera le procedure di ripresa, con descrizione delle azioni da assumere per ritornare alle normali operazioni aziendali?											
4.9.1.4.e	E' mantenuta un'unica struttura di piani di B.C che considera un programma di mantenimento che specifichi come e quando il piano deve essere testato, e il processo per mantenere lo stesso piano?											
4.9.1.4.f	E' mantenuta un'unica struttura di piani di B.C che considera le attività di formazione per ottenere coscienza del processo di B.C. e garantire l'efficacia dei processi?											
4.9.1.4.g	E' mantenuta un'unica struttura di piani di B.C che considera le responsabilità individuali che individuino le competenze per l'esecuzione di ciascuna parte del piano?											
4.9.1.5	***Test, manutenzione e rivalutazione dei piani di Business Continuity*** I piani di B.C. sono testati, mantenuti aggiornati e periodicamente rivialutati?											

Categoria:

4.10	**CONFORMITÀ**
4.10.1	***CONFORMITÀ AI REQUISITI LEGALI***

Obiettivo:

Verificare la presenza di politiche e procedure atte ad evitare violazioni di qualunque regola penale o civile, statutaria, regolamentare o di obbligazioni contrattuali e di ogni altro requisito di sicurezza (in particolare Copyright e Privacy).

NOTA BENE:

- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.1.1	***Identificazione delle leggi applicabili*** Tutti i requisiti statutari, regolamentari e contrattuali rilevanti sono definiti esplicitamente e documentati, con individuazione dei controlli e le responsabilità relative?											
4.10.1.2.a	***Diritti di proprietà intellettuale*** Sono considerati i Diritti di proprietà intellettuale (IPR)?											
4.10.1.2.b	Sono state applicate procedure per garantire il rispetto dei precetti legali nell'utilizzo di materiali protetti da diritti di proprietà intellettuale, come copyright, design right e trade marks?											
4.10.1.2.c	E' stata definita una politica di compliance con il copyright del software?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.1.2.d	Sono presenti standard per le procedure di acquisizione dei prodotti software?											
4.10.1.2.e	Il personale è stato informato sulle norme che regolano il copyright con le azioni disciplinari previste in caso di loro violazione?											
4.10.1.2.f	Sono conservate le prove della titolarità della licenza, dei dischi master, dei manuali, ecc.?											
4.10.1.2.g	E' controllato che non sia superato il numero massimo di utenti consentiti? E' controllato che non siano installati solo software autorizzati e prodotti con licenza?											
4.10.1.2.h	E' stata stabilita una politica per mantenere adeguate condizioni di licenza?											
4.10.1.2.i	Vi è adeguamento ai termini ed alle condizioni per i software e le informazioni ottenute da reti pubbliche?											
4.10.1.3.a	***Salvaguardia della documentazione organizzativa*** Sono mantenuti e protetti i registri dei beni?											
4.10.1.3.b	I documenti importanti sono protetti contro danni distruzioni e falsificazioni?											
4.10.1.3.c	Sono state emanate linee guida sulla conservazione, il trattamento e la cessione di documenti e informazioni?											
4.10.1.3.d	E' presente un inventario delle sorgenti di informazioni chiave?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.1.3.e	Sono implementati controlli adeguati per proteggere i documenti e le informazioni da perdite, distruzioni e falsificazioni?											
4.10.1.4	***Privacy e protezione dei dati personali*** La conformità con la legislazione sulla protezione dei dati personali richiede una struttura organizzativa adeguata (organigramma, nomine e procedure) e dei controlli. Il titolare del trattamento ha istruito i responsabili sulle modalità e finalità del trattamento dei dati in base alla legislazione vigente ?											
4.10.1.5	***Prevenzione all'uso non corretto di apparecchiature informatiche*** La direzione ha autorizzare l'uso degli strumenti di trattamento delle informazioni e sono applicati controlli per prevenirne l'abuso ?											
4.10.1.6	***Regolamentazione dei controlli crittografici*** I controlli in atto assicurano le verifiche di conformità con gli accordi nazionali, leggi, regolamenti e altri strumenti che regolano l'accesso e l'utilizzo di controlli crittografici?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.1.7	***Raccolta delle prove*** E' necessario avere prove sufficienti per supportare eventuali azioni contro singoli o organizzazioni. Quando questa azione è di tipo disciplinare la prova deve essere espressamente prevista nelle procedure interne. Per le azioni legali di tipo civile o penale, sono rispettate le prescrizioni della legge applicabile ?											

Categoria:

4.10	**CONFORMITÀ**
4.10.2	***REVISIONI DELLA POLITICA DI SICUREZZA E CONFORMITÀ TECNICA***

Obiettivo:
Verificare la conformità dei sistemi con le politiche e gli standard di sicurezza.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Se segnato argomenti di "Q2", inserire in calce una più ampia spiegazione delle motivazioni

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.2.1	***Conformità alle politiche di sicurezza*** I manager garantiscono che tutte le procedure di sicurezza all'interno della loro area di responsabilità siano eseguite correttamente ?											
4.10.2.2.a	***Verifiche di conformità tecnica*** Sono periodicamente controllate tutte le aree dell'organizzazione per garantire la loro conformità alla politica e agli standard di sicurezza; in particolare, quelle relative ai sistemi informativi, ai provider di sistema, ai titolari dell'informazione e alle informazioni, agli utenti e al management ?											

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.2.2.b	I sistemi informativi sono regolarmente controllati per garantirne la conformità con gli standard di implementazione della sicurezza? I test di conformità tecnica comprendono per esempio l'esame delle operazioni di sistema per verificare che i controlli dell'hardware e del software siano stati implementati correttamente, e i test di penetrazione? *(Tutti i controlli devono essere eseguiti da, o sotto la supervisione di, personale competente e autorizzato).*											

Categoria:

4.10	**CONFORMITÀ**
4.10.3	***CONSIDERAZIONI SUGLI AUDIT DI SISTEMA***

Obiettivo:
Verifica della presenza di misure tendenti a massimizzare l'efficacia e minimizzare le interferenze al/dal processo di audit del sistema.

NOTA BENE:
- Considerare gli aspetti relativi alla Categoria e, quindi, segnare la casella appropriata in Q1
- Se segnato "PARZ." oppure "NO" indicare in Q2, segnando una o più caselle appropriate, la ragione corrispondente
- Inserisci, nello spazio "COMMENTI", una più ampia spiegazione delle ragioni indicate in Q2

Rif. BS	FUNZIONE	Q1			Q2							
		SI	PARZ.	NO	RISCHIO	BUDGET	AMBIENTE	TECNOLOGIA	CULTURA	TEMPO	N/A	ALTRO
4.10.3.1	***Controlli di system audit*** I requisiti e le attività di audit che comprendono check sui sistemi di produzione sono attentamente pianificate e concordate per minimizzare il rischio di interruzione dei processi aziendali ?											
4.10.3.2.a	***Protezione dei tool di system audit*** L'accesso agli strumenti di audit è protetto per prevenire qualsiasi possibile uso scorretto o compromissione ?											
4.10.3.2.b	Se adottati, questi strumenti di audit sono separati dai sistemi di sviluppo e di produzione, e non sono conservati nelle librerie degli utenti senza aver firnito un livello adeguato di protezione addizionale ?											