Governance IT

Continua evoluzione dei modelli per gestirla

D. D'Agostini, A. Piva, A. Rampazzo

Con il termine "Governance IT" si intende quella parte del più ampio governo di impresa che si occupa della gestione dei sistemi informatici. In questo articolo vengono presentati gli schemi concettuali, definiti a livello internazionale, che possono aiutare le organizzazioni nella gestione ottimale del problema.

1. Introduzione

I venti di crisi che si stanno abbattendo sulle borse mondiali stanno provocando ripercussioni di notevole entità sull'intero sistema di *Governance* delle organizzazioni. Come è ovvio aspettarsi, tra le vittime - lo stiamo constatando giorno dopo giorno - vi è il settore dell'*Information Tecnology*.
Con il termine *governance IT* si intende quella parte del più ampio governo d'impresa che si occupa della gestione dei sistemi IT, ossia dell'*Information Tecnology*.

Il governo d'impresa si è notevolmente espanso in seguito ai recenti sviluppi normativi[1] tanto da avere ingenti ripercussioni anche sulla gestione dei sistemi informativi. A ciò si inserisce anche la *Compliance* normativa (letteralmente conformità) che è la funzione atta a prevenire il rischio connesso alla possibilità di giungere a danni di immagine o perdite finanziarie, in seguito al cattivo funzionamento e\o comportamento rispetto a determinate norme, alle regole o standard e alle leggi.
Gli obiettivi principali della *governance IT* sono:

- assicurare che gli investimenti IT generino valore per l'azienda;
- gestire e mitigare i rischi associati con l'IT.

[1] *Sarbanes-Oxley Act* in USA (maggiore responsabilità per il management per quanto concerne l'accuratezza delle informazioni contabili sui bilanci), Basilea III nel settore bancario Europeo, Legge 262/2005 in Italia (disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari) e tante altre.

Questi obiettivi possono essere raggiunti definendo e realizzando una struttura logistica nell'organizzazione con ruoli e responsabilità ben chiari per quanto riguarda i temi correlati ai sistemi informativi: sicurezza, processi aziendali, infrastruttura, analisi dei rischi, applicazioni, ecc.

Un aiuto alle organizzazioni per ottenere i succitati obiettivi è dato da diversi *framework* (schemi) concettuali per un corretto approccio ai temi dell'*IT governance*.

I principali Framework sono:

- "*Control Objectives for IT*" (**COBIT**) e **Val IT** *frameworks* a cura dell' IT *Governance Institute* e di ISACA che approfondiscono il tema del controllo dei processi aziendali e degli investimenti;
- "*IT Infrastructure Library*" (**ITIL**) sviluppato dall'*United Kingdom's Office of Government Commerce* in partenariato con l'*IT Service Management Forum*;
- i sistemi di gestione proposti dall'ISO (*International Organization for Standardization*):
  - **ISO 38500** requisiti per la "**Corporate governance of IT"**;
  - **ISO 31000** gestione del rischio;
  - **ISO 9001** Sistema di Gestione della Qualità (applicato al software e al mondo IT);
  - **ISO 20000**, serie di standard sviluppato per la gestione dei servizi IT;
  - **ISO 27000**, serie di standard dedicati al vasto tema della sicurezza dei sistemi informativi;
- le proposte normative del *BSI - British Standards Institute*:
  - **BS 10012** norma per sviluppare un Sistema di gestione delle Informazioni personali;
  - **BS 25999** serie di standard sviluppato per la gestione della Continuità Operativa (o *Business Continuity*).

La definizione di *frameworks* o modelli internazionali può solamente facilitare lo sviluppo e l'adozione della gestione dell'IT, in particolare quando sono effettivamente applicabili in tutte le organizzazioni, dalla più piccola alla più grande, indipendentemente dagli obiettivi e dalla struttura organizzativa in quanto rappresentano un riconosciuto strumento di controllo e gestione delle problematiche aziendali, attraverso l'individuazione delle criticità e la corretta pianificazione delle risorse interne.

2. COBIT® – VAL IT

COBIT® (*Control Objectives for Information and related Technology*) vers. 4.1 è un f*ramework* per la gestione e la disponibilità di servizi di qualità basati sulla tecnologia e fornisce le *best practice* per contribuire, con i mezzi adeguati, al processo di creazione del valore in azienda.

COBIT® fornisce ai manager, agli auditor e agli utenti dei sistemi IT una griglia di riferimento costituita da:

- una struttura dei processi della funzione IT, rispetto alla quale si è venuto formando il consenso degli esperti del settore;
- una serie di strumenti teorici e pratici collegati ai processi.

Ha l'obiettivo di valutare se è in atto un efficace governo della funzione IT (*IT governance*) o di fornire una guida per instaurarlo.
COBIT® è ormai riconosciuto a livello internazionale: l'Unione Europea ha indicato COBIT come uno dei tre standard utilizzabili per garantire la sicurezza dei sistemi informativi[2].

Val IT vers. 2.0 si basa su COBIT®, e vi aggiunge le *best practice* per misurare, monitorare e massimizzare, in modo chiaro, il ritorno economico degli investimenti IT. Val IT completa dunque COBIT® dal punto di vista del business, in una prospettiva finanziaria ed è un aiuto per chi è interessato ad analizzare il *"value delivery*" che proviene dall'IT.

3. Information Technology Infrastructure Library (ITIL)

ITIL è un insieme di linee guida ispirate dalla pratica nella gestione dei servizi IT (*IT Service Management*) e consiste in una serie di pubblicazioni che forniscono indicazioni sull'erogazione di servizi IT di qualità e sui processi e mezzi necessari a supportarli.

ITIL è stato pubblicato in una serie di libri che seguono un approccio basato sul ciclo di vita del servizio. Il contenuto di questi libri è protetto da diritto d'autore (*Crown Copyright*[3]).

Il primo giugno 2007, l'OGC ha rilasciato un aggiornamento di ITIL, noto come ITIL v3. La pubblicazione iniziale di ITIL v3 è composta da cinque testi principali denominati *Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement* consolidando così molte delle pratiche della versione v2 attraverso il ciclo di vita del servizio (*service lifecycle*). A luglio 2011 è stata pubblicata una revisione di ITIL denominata versione 3.1.

Uno dei principali benefici dichiarato da coloro che supportano ITIL all'interno della comunità IT è la fornitura di un comune vocabolario (il cosiddetto esperanto IT), consistente di un glossario di concetti strettamente definiti e ampiamente concordati.

[2] cfr. ad es. Gazzetta Ufficiale dell'Unione Europea L077 pag. 6, 23 marzo 2005.
[3] il materiale protetto da *Crown copyright* può essere riprodotto a titolo gratuito utilizzando qualsiasi formato o mezzo di distribuzione senza la necessità di richiedere una autorizzazione specifica. L'autorizzazione all'utilizzo è concessa a condizione che quanto riprodotto venga duplicato in maniera fedele e non venga utilizzato in forma denigratoria o in un contesto fuorviante. L'origine del materiale e l'indicazione del titolare del diritto di autore devono essere riportati.

4. ISO/IEC 38500:2008 - Corporate governance of information technology

Il 2008 ha visto la pubblicazione di una importante norma, la ISO/IEC 38500:2008, che segna il riconoscimento internazionale della *IT Governace* e della necessità di arrivare ad una "formalizzazione" della sua adozione.
La norma stabilisce le definizioni, i principi e un modello di *governante informatica sulla base di sei principi fondamentali, necessari per guidare il processo decisionale:*

- *responsabilità*
- *strategia*
- *acquisizione*
- *esecuzione*
- *conformità*
- *comportamento*

La ISO/IEC 38500:2008 si applica al governo dei processi (e decisioni) gestionali relativi ai servizi di informazione e comunicazione utilizzati dall'organizzazione. Questi processi potrebbero essere controllati da specialisti informatici all'interno dell'organizzazione o da fornitori di servizio esterni, o da altre unità d'affari all'interno dell'organizzazione. La norma non è destinata ai fini della certificazione.

5. ISO 31000 - *Risk management*

Le norme sul sulla gestione del rischio (*risk management)* pubblicate dall'ISO sono attualmente due:

- ISO 31000:2009 Principi e linee guida
- ISO/IEC 31010:2009 Tecniche di valutazione del rischio

E' ormai risaputo che una buona *governance IT* non può prescindere da un'attenta conduzione dell'organizzazione verso una continua analisi e approccio al rischio, anche in proiezione futura.

Le organizzazioni ormai utilizzano una metodologia più o meno formalizzata di gestione del rischio e, per fornire un *framework* comune per questa attività, nel 2009 l'ISO ha iniziato la pubblicazione della famiglia di standard ISO 31000, per stabilire i principi che, se soddisfatti, possono rendere più efficace il *risk management*.

Questa nuova famiglia di norme intende fornire i principi e le linee guida generali in materia di gestione dei rischi e può essere utilizzata da qualsiasi organizzazione pubblica o privata.
Da sottolineare comunque che le norme di questa famiglia attualmente non sono destinate ai fini della certificazione.

6. ISO 9001:2008 - Sistema di Gestione della Qualità (applicato al software e al mondo IT)

La UNI EN ISO 9001:2008 definisce i requisiti per la qualità delle organizzazioni ed è utilizzabile da ogni tipo di Azienda o Ente. Contiene i requisiti dei sistemi di gestione della qualità relativi ad aziende di produzione e di servizi; in particolare si sposa molto bene anche con aziende di produzione hardware.

Adattare la UNI EN ISO 9001:2008 ad un'organizzazione che sviluppa software e che comunque opera nel mondo IT può risultare problematico: il termine "software" va letto tra le righe dei vari requisiti. Ad aumentare le difficoltà di adattamento contribuisce anche il fatto che l'attività di sviluppo del prodotto software coincide con l'attività di produzione dello stesso.

La difficoltà di affrontare il processo di sviluppo software e adattarlo ad un Sistema di Gestione della Qualità sono state ben messe in evidenza già con la UNI EN ISO 9001:2000. Sulla spinta di questa richiesta è stata predisposta la guida UNI CEI ISO 90003:2005 (Guida per l'applicazione della ISO 9001:2000 sul software per elaboratore). Essa riporta le regole riguardanti la conduzione aziendale per la qualità ed è una semplice guida concepita esclusivamente per orientare le organizzazioni nella realizzazione del Sistema Qualità, interpretando i requisiti della UNI EN ISO 9001:2000 per lo sviluppo, la fornitura e la manutenzione del software (Tabella 1).
Altro importante ausilio è dato dalla ISO/IEC 12207:2008 (processi del ciclo di vita del software) in cui è definito uno schema di riferimento per i processi relativi al ciclo di vita del software e contiene processi, attività/compiti che possono essere applicati durante l'approvvigionamento di prodotti/servizi software e durante la fornitura, lo sviluppo, la conduzione operativa e la manutenzione di prodotti software.
Nel corso del 2011 è stata pubblicata la ISO/IEC 29110 TR (*Technical Report*) riguardante il ciclo di vita del *software engineering* nelle PMI. E' ormai riconosciuta l'importanza del ruolo delle piccole aziende che svolgono, prevalentemente in subappalto, attività di sviluppo e manutenzione software. Le piccole aziende fungono da ammortizzatori produttivi cui è richiesta produttività alta, costi bassi e qualità del software prodotto.

7. ISO 20000 - Sistemi di Gestione dei Servizi IT

La famiglia ISO 20000[4] è gestita in ambito ISO a cura del comitato ISO/IEC JTC1 SC7 (*Systems and Software Engineering*) molto attivo in quanto sta implementando nuove norme ed ha già rivisto proprio quest'anno la ISO 20000-1.

4 Per una completa trattazione si veda l'articolo "ISO/IEC 20000: la norma per la qualità dell'erogazione dei Servizi IT", pubblicato su Mondo Digitale di marzo 2009.

Attualmente chi eroga servizi IT, ancora oggi dopo oltre sei anni di presenza di queste specifiche norme, per dimostrare la propria capacità, si certifica UNI EN ISO 9001:2008 settore EA 33 (IT), mentre ha una valida possibilità di dimostrare il controllo efficace e il miglioramento continuo dell'intero complesso di prestazioni con la norma ISO/IEC 20000-1:2011, che prevede i requisiti per l'implementazione di un **Sistema di Gestione dei Servizi IT** (SGSIT).

L'ISO/IEC 20000, infatti è una serie di norme dedicate alla valutazione delle organizzazioni che erogano servizi IT. Queste norme riconoscono l'importanza dei servizi IT, ne individuano le specificità e stabiliscono l'esigenza di una risposta adeguata ai problemi che le tecnologie dell'informazione comportano nella impostazione e nell'esercizio di un Sistema di Gestione del servizio.

Le norme della famiglia ISO/IEC 20000 sono applicabili a organizzazioni di tutte le dimensioni e il contenuto è comunque tale da poter supportare *framework* come ITIL o approcci simili come MOF *Microsoft Operational Framework* (Microsoft), HP ITSM *Reference Model* (Hewlett Packard).
La famiglia ISO/IEC 20000 si sta arricchendo di ulteriori norme o linee guida che hanno visto così anche per *l'IT Service Management* un particolare interesse (Tabella 2).

8. ISO 27001 - Sistemi di Gestione della Sicurezza delle Informazioni

La norma ISO/IEC 27001 pubblicata nel 2005 è la progenitrice della famiglia ISO 27000, una serie di norme relative all'*Information Security* curate dal comitato ISO/IEC JTC 1/SC27.

Principale obiettivo di un **Sistema di Gestione per la Sicurezza delle Informazioni** è la protezione delle Informazioni gestite da un'organizzazione[5]. Al giorno d'oggi diventa fondamentale individuare le informazioni gestite all'interno dell'organizzazione, i rischi a cui sono sottoposte e le misure di protezione che debbono essere messe in atto per una loro adeguata protezione. Oltre alle informazioni su supporto cartaceo o informatico, vanno gestite anche le infrastrutture (computer, reti aziendali, accessi esterni sia fisici che informatici) e il personale (senza dimenticare il *know how* posseduto dallo stesso).

Attualmente la famiglia ISO 27000 è costituita da nove specifiche norme (Tabella 3), mentre nel corso dei prossimi anni è prevista la pubblicazione di ulteriori norme, generali e anche specifiche, che trattano applicazioni settoriali o particolari aspetti tecnici (Tabella 5).

[5] Per una completa trattazione si veda l'articolo "La sicurezza delle informazioni e le Norme ISO 27000", pubblicato su Mondo Digitale di settembre 2008.

"La sicurezza è un processo, non un prodotto" è l'affermazione di Bruce Schneier, noto autore di libri sulla sicurezza informatica e sulla crittografia, che riassume la filosofia alla base degli standard ISO 27000.

9. BS 10012 - Sistemi di Gestione delle Informazioni Personali

La BS 10012:2009 è la più recente tra le norme innovative proposte dal British Standard Institute, l'ente normatore inglese.

La norma BS 10012 specifica i requisiti per un **Sistema di Gestione delle Informazioni Personali** (PIMS) che fornisce un'infrastruttura per mantenere e migliorare la conformità con il *Data Protection Act* (DPA) 1998, che a sua volta attua la direttiva europea 95/46/CE e si applica ai "dati personali", definiti come "informazioni relative a individui viventi". Può certamente adattarsi alla nostra legislazione e in particolare al D.Lgs 196/2003 sulla tutela dei dati personali.

La BS 10012 è stata sviluppata da un collegio di esperti, tra rappresentanti dell'industria, del governo, delle università e delle associazioni dei consumatori: un periodo di tre mesi di commenti pubblici ha prodotto un elevato numero di osservazioni confluite nella stesura dello standard. La BS 10012 fornisce il quadro che consente una gestione efficace e su misura dei dati personali: può essere utilizzata da organizzazioni pubbliche e private di qualsiasi dimensione e settore, per gestire le procedure in ambiti quali la formazione e la sensibilizzazione, la valutazione del rischio, la condivisione, la conservazione e lo smaltimento dei dati e la comunicazione a terzi.

L'introduzione della norma BS 10012 sottolinea come la protezione dei dati abbia assunto una rilevanza strategica in ogni business e fornisce un utile modello per le organizzazioni che desiderano migliorare le modalità di *governance* per la protezione dei dati nell'organizzazione.

10. BS 25999 - Sistemi di Gestione della *Business Continuity*

La BS 25999 è anche questa una delle norme "giovani" prese in analisi[6]. Attualmente è un *British Standard* ma vista la sua attuale notorietà potrebbe presto diventare una norma internazionale. L'ISO ha già messo in campo specifici gruppi di lavoro sull'argomento e potremmo a breve vedere pubblicata una specifica norma.

[6] Per una completa trattazione si veda l'articolo "Business Continuity: come prevenire i disastri applicando le normative", pubblicato su Mondo Digitale di settembre 2009.

E’ la prima norma al mondo per la **Gestione della Continuità Operativa** (*Business Continuity Management*) che è stata sviluppata per ridurre al minimo il rischio di interruzioni dell’attività di una organizzazione (in tabella 4 si evidenza una sintesi dei principali eventi che hanno caratterizzato l’evoluzione della normativa sul *Business Continuity Management*).

La norma è progettata per mantenere la continuità delle attività anche nelle circostanze più problematiche e impreviste, salvaguardando il personale e la reputazione dell'azienda, permettendole di continuare a produrre e ad essere operativa (continuità dell’operatività o business).

La BS 25999 è indicata per qualsiasi organizzazione, grande o piccola, di qualsiasi settore. È particolarmente raccomandabile per le organizzazioni che operano in contesti ad alto rischio, quali la Finanza (Banche ed Assicurazioni), le Telecomunicazioni, il Trasporto e la Pubblica Amministrazione, dove la capacità di assicurare la continuità delle operazioni è fondamentale per l'organizzazione stessa, per i suoi clienti e per le parti interessate.

La BS 25999 è articolata in due parti: il *Code of Practice*, che fornisce consigli pratici per attuare il *Business Continuity Management*, e la *Specifica*, che fornisce i requisiti per un Sistema di Gestione della *Business Continuity*. Questa ultima è la parte della norma da utilizzare per dimostrare la conformità, mediante il processo di valutazione e certificazione.

Conclusioni

L’utilizzo delle tecnologie IT per il trattamento delle informazioni nelle organizzazioni, può rappresentare un reale strumento di evoluzione del business e di ottimizzazione dei costi, ma questo non basta. Per la gestione dell’IT sono richieste appropriate strutture organizzative e di governo con ruoli e responsabilità ben chiare. È necessario che vi sia un preciso mandato da parte del *top management*, mandato che deve assegnare un chiaro controllo e una chiara responsabilità per le decisioni e i compiti più importanti. E’ quindi necessario adottare *frameworks* e modelli che possano corrispondere alle esigenze e all’ottimizzazione dei processi investendo in competenza, professionalità e formazione.
Per ultimo, non bisogna dimenticare che l’*Information Technology* non deve essere intesa come un centro di costo, ma un centro di valore.

Norma ISO	Titolo	Corrispondente documento UNI
ISO 9000:2005	Sistemi di gestione per la qualità - Fondamenti e vocabolario	UNI EN ISO 9000:2005
ISO 9001:2008	Sistemi di gestione per la qualità - Requisiti	UNI EN ISO 9001:2008
ISO 9004:2009	Gestire un'organizzazione per il successo durevole - L'approccio della gestione per la qualità	UNI EN ISO 9004:2009
ISO/IEC 90003:2004	Ingegneria del software e di sistema - Guida per l'applicazione della ISO 9001:2000 al software per elaboratore	UNI CEI ISO/IEC 90003:2005
ISO/IEC 12207:2008	Systems and software engineering - Software life cycle processes	==
ISO/IEC TR ISO/IEC TR29110:2011	Software engineering - life cycle profiles for Very Small Entities (VSEs)	==

Tabella 1
Norme per implementare un Sistema di Gestione della Qualità
(APPLICATE AL SOFTWARE E AL MONDO IT)

Norma ISO	Titolo
ISO/IEC 20000-1:2011	Information technology — Service Management — Part 1: Requirements (Stabilisce i requisiti del sistema di gestione)
ISO/IEC 20000-2:2012	Information technology — Service Management — Part 2: Guidance on the application of service management systems (Raccomanda buone pratiche per la gestione)
ISO/IEC TR 20000-3:2009	Information technology — Service Management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
ISO/IEC TR 20000-4:2010	Information Technology – Service Management — Part 4: Process Reference Model
ISO/IEC TR 20000-5:2010	Information technology — Service Management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1
ISO/IEC 20000-7	Information technology — Service Management — Part 7: Guidance on the application of ISO/IEC 20000-1 to the Cloud
ISO/IEC TR 20000-10	Information technology — Service Management — Part 10: Concepts and terminology
ISO/IEC TR 20000-11	Information technology — Service Management — Part 11: Guidance on the relationship between ISO/IEC 20000-1 and related framework

- Un gruppo di lavoro ISO congiunto (WG 25 - WG24 “Software Life Cicles for Very small Enterprises”) ha avviato uno studio per definire le linee guida di applicazione di ISO/IEC 20000 alle VSE (piccole organizzazioni con meno di 25 persone).
- Il gruppo di lavoro ISO WG23 “System Quality Management” sta lavorando per produrre un draft della futura ISO/IEC 90006 che fornirà le linee guida per l’applicazione della ISO 9001 all’IT Service Management.

Tabella 2
Norme della famiglia ISO 20000 IT Service Management

Norma ISO	Titolo
ISO/IEC 27000:2009	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27002:2005	Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 27003:2010	Information technology -- Security techniques -- Information security management system implementation guidance
ISO/IEC 27004:2009	Information technology -- Security techniques -- Information security management -- Measurement
ISO/IEC 27005:2011	Information technology -- Security techniques -- Information security risk management
ISO/IEC 27006:2011	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2011	Information technology -- Security techniques -- Guidelines for information security management systems auditing
ISO/IEC TR 27008:2011	Information technology -- Security techniques -- Guidelines for auditors on information security controls

Tabella 3
Norme della famiglia ISO 27000
Security Management

Anno	Codice	Titolo
2002	BCI GPG 2002	Good Practice Guidelines. A framework for Business Continuity mgmt
2005	BCI GPG 2005	Good Practice Guidelines. A framework for Business Continuity mgmt
2003	BSI PAS 56:2003	Guide to Business Continuity Management
2006	BSI PAS 77:2006	IT Service Continuity Management. Code of Practice
2006	BSI BS 25999-1:2006	Business continuity management. Code of practice
2007	999-2:2007	Business continuity management. Specification
2008	BCI GPG 2008	Good Practice Guidelines. A framework for Business Continuity mgmt
2008	BSI BS 25777:2008	Information and communications technology continuity management. Code of practice
2010	BCI GPG 2010	Good Practice Guidelines. A framework for Business Continuity mgmt

Tabella 4
Sintesi dell'evoluzione della normativa sulla BCM

Norma ISO	Titolo
ISO/IEC 27010 FCD	Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2008	Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013 CD	Information technology -- Security techniques -- Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27015 WD *odice Norma ISO*	Proposal on an Information security management guidelines for financial and insurance services
ISO/IEC TR 27016 WD	Information technology -- Security techniques -- Information security management -- Organizational economics*Codice* ***Norma ISO***
ISO/IEC 27017	Information technology -- Security techniques -- Cloud computing security and privacy management system -- Security controls -- Part 2: Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002
ISO/IEC 27031:2011	Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032 FDC	Information technology -- Security techniques -- Guidelines for cybersecurity General Information
ISO/IEC 27033-1:2009	Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
ISO/IEC 27033-3:2010	Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
ISO/IEC 27034-1:2011	Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts
ISO/IEC 27035:2011	Information technology -- Security techniques -- Information security incident management
ISO/IEC 27036 WD	Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
ISO/IEC 27037 CD	Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038 WD	Information technology -- Security techniques -- Specification for Digital Redaction
ISO/IEC 27039 WD	Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems
ISO/IEC 27040 WD	Information technology -- Security techniques -- Storage security General Information
ISO 27799:2008	Health informatics -- Information security management in health using ISO/IEC 27002
ISO/IEC 24762:2008	Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

Tabella 5
Alcune nome settoriali o tecniche
previste o pubblicate nella famiglia ISO 27000

Bibliografia

[1]ISO/IEC 38500:2008 - Corporate governance of information technology.
[2] ISO 31000:2009 – Risk management – Principles and guidelines
[3] SO/IEC 31010:2009 Risk management - Risk assessment techniques
[4] COBIT® vers. 4.1. - VAL IT vers. 2.0 (www.isaca.org).
[5] COBIT® vers. 4.1 Framework (vers. Inglese e italiano).
[6] Foundations of ITSM basato su ITIL v3 Autore: Jan Van Bon Ed. Van Haren Publishing.
[7] UNI EN ISO 9001:2000 - Requisiti per un Sistema di Gestione della Qualità.
[8] UNI EN ISO 9001:2008 - Requisiti per un Sistema di Gestione della Qualità.
[9] UNI EN ISO/IEC 90003:2005 - Guida per l'applicazione della ISO 9001:2000 al software per elaboratore.
[10] ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes.
[11] ISO/IEC TR 29110:2011 Software engineering - Lifecycle profiles for Very Small Entities (VSEs).
[12] ISO/IEC 27001:2005 - Security techniques - Information security management systems - Requirements.
[13] ISO/IEC 27002:2005 - Information tecnology - Security tecniques - Code of practice for information security management.
[14] ISO/IEC 20000-1:2011 Information technology - Service management - Part 1: Service management system requirements.
[15] ISO/IEC 20000-2:2012 Information technology – Service management – Part 2: Guidance on the application of service management systems.
[16] ISO/IEC 20000-2:2005 Information technology - Service management - Part 2: Code of practice.
[17] BSI BS 25999-1:2006 Business continuity management. Code of practice.
[18] BSI BS 25999-2:2007 Business continuity management. Specification.
[19] BSi BS 10012:2009 – Data protection. Specification for a personal information management system.
[20] Business Continuity Institute - GPG 2010 Good Practice Guidelines.

Biografie

DAVID D'AGOSTINI avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

ANTONIO PIVA, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA. Presidente della Sezione Territoriale AICA del Nord Est.
E-mail: antonio@piva.mobi

ATTILIO RAMPAZZO, consulente di Sistemi Informativi e Sicurezza delle Informazioni. Ha maturato un'esperienza più che trentennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. E' Vice Presidente del Comitato AICQ "Qualità del Software e dei Servizi IT", Valutatore Sistemi di Sicurezza delle Informazioni R.G.V.I. (cert. AICQ_SICEV), certificato CISA, CRISC, LoCSi e ITIL v.3 foundation, socio AICQ, ISACA Venice chapter, AIPSI, AICA; ASSOVAL, FederPrivacy
E-mail: attilio.rampazzo@gmail.com