UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Edizione italiana a cura di ALSI e Tecnoteca
http://upgrade.tecnoteca.it

L'Auditing dei Sistemi Informativi dei piani di Business Continuity

di Agatino Grillo

Versione italiana, a cura dell'autore, dell'articolo
" Information Systems Auditing of Business Continuity Plans "
pubblicato sul vol. IV, No. 6, December 2003 della rivista online UPGrade, a cura del CEPIS

Riassunto
Il Business continuity management è una responsabilità del top management. L'audit del BCP diventa così un elemento fondamentale dell' IT Governance in quanto rappresenta un assessment indipendente i cui risultati possono essere condivisi e comunicati anche al di fuori dei sistemi IT, ad esempio agli stakeholder, alle autorità di controllo o ai business-partner. Per le istituzioni finanziarie, in particolare, l' auditing dei piani di BC un obbligo normativo. E' necessario adottare allora una metodologia di BCP ben strutturata e verificabile. L'articolo introduce le problematiche generali dell'Information Systems Auditing (ISA) e presenta l'approccio di audit al BCP basato su COBIT, un framework generale sviluppato da ISACA (Information Systems Audit and Control Association).
.

Parole chiave*:* Piano di continuità dei servizi, IS Auditing, ISACA, COBIT, IT Governance

1. IS Auditing

L'Information Systems Auditing (ISA) analizza e verifica le risorse IT aziendali (*IT Asset*) con l'obiettivo di misurare il grado di controllo esistente, rilevando le potenziali criticità o aree di rischio e proponendo, se necessario, le misure o *best-practices* per il ripristino del livello desiderato.

Le attività consistono sia nella valutazione e verifica dei controlli IT di tipo generale che dei controlli di tipo applicativo; tra i primi rientra l'IS Auditing del Business Continuity Plan (BCP) aziendale.

L' ISA dei piani di BC è una necessità aziendale in quanto assicurare la continuità dei servizi è una necessità primaria del business ed anche un requisito normativo.

Organizzazioni quali le istituzioni finanziarie o le pubbliche amministrazioni devono confrontarsi, infatti, con nuovi adempimenti legali che riguardano anche la business continuity.

In Italia, per esempio, il primo gennaio 2004 entrerà in vigore il nuovo "Codice in materia di protezione dei dati personali"; esso richiede una maggiore attenzione e protezione dei dati anche per le problematiche relative alla business continuity ed al disaster recovery[1].

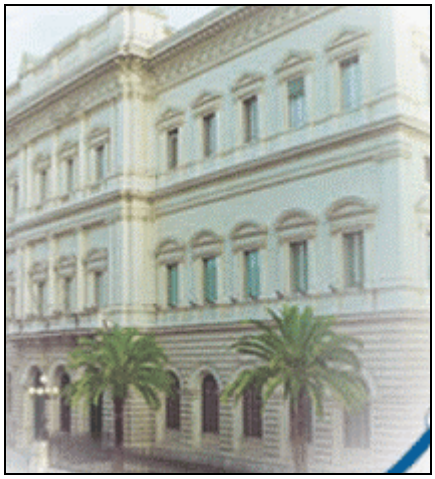
[1] Il Codice riepiloga ed ordina tutte le precedenti norme sulla protezione dei dati personali In Italia; si noti che le misure di protezione richieste a tutte le entità coinvolte nei trattamenti di dati sono state rese più precise e severe in conformità con la politica seguita alla promulgazione della legge sulla Privacy (legge numero 675/1996). Il Codice introduce, inoltre, nella legislazione italiana la Direttiva comunitaria 2002/58. Per quanto riguarda specificatamente la business

Nel seguito dell'articolo, saranno indicati i requisiti per il BCP nelle istituzioni finanziarie e proposto, successivamente, un approccio per l'audit del BCP.

2. BCP ed Istituzioni finanziarie

In linea con gli indirizzi emersi in ambito internazionale a seguito degli eventi dell'11 settembre 2001, la Banca d'Italia[2], ha avviato un complesso di iniziative, d'intesa tra le funzioni preposte al controllo degli intermediari, dei mercati e dei sistemi di pagamento, volte a verificare il livello di preparazione del sistema finanziario italiano a fronteggiare eventi catastrofici, a sanare le situazioni ritenute non adeguate, a elevare il grado di sicurezza operativa dei principali intermediari finanziari, delle infrastrutture dei mercati e del sistema dei pagamenti.

La Vigilanza ha provveduto, da un lato, a richiedere agli intermediari che mostravano carenze l'avvio, in tempi ragionevoli, dei necessari interventi di adeguamento, dall'altro, ha sottoposto all'attenzione degli operatori, per la discussione, un documento che definisce i requisiti minimi che dovrebbero essere rispettati da tutti gli intermediari e gli standard più elevati a cui dovrebbero attenersi i soggetti aventi rilevanza sistemica[3].



Palazzo Koch, Roma, sede centrale della Banca D'Italia

Nel luglio 2003, il "Sistema europeo di banche centrali (SEBC)"[4] ed il "Committee of European Securities Regulators" (CESR)[5] hanno pubblicato un documento intitolato "*Standards for*

continuity, il Codice recita: "*I trattamenti di dati personali con mezzi elettronici sono ammessi solo se sono adottate le relative misure minime di sicurezza al fine di assicurare (tra l'altro) l'esistenza di copie di sicurezza e la capacità di ripristino dei dati e dei sistemi*". Si noti che misure di sicurezza ulteriori devono essere adottate, in caso di trattamento di dati sensibili o giudiziari, per garantire la disponibilità delle informazioni

[2] La Banca D'Italia è l'organo di vigilanza per i mercati finanziarie ed il rappresentante italiano del sistema europeo delle banche centrali (European System of Central Banks - ESCB).

[3] Banca D'Italia, "Assemblea Generale Ordinaria Dei Partecipanti", maggio 2003 disponibile in: http://www.bancaditalia.it/pubblicazioni/ricec/relann/rel02/rel02it/rel02ita.zip

[4] Il Sistema europeo di banche centrali (SEBC) è composto dalle Banche centrali nazionali (BCN) degli Stati membri dell'Unione europea e dalla Banca centrale europea (BCE). L'Eurosistema è costituito dalle BCN dei paesi che hanno adottato l'euro, tra cui l'Italia, e dalla BCE.

securities clearing and settlement systems in the European Union" che contiene una serie di raccomandazioni anche relativamente al BCP nelle istituzioni finanziarie. Ad esempio si dice che i piani di business continuity ed i programmi di backup dovrebbero garantire, con un ragionevole grado di fiducia, il ripristino delle procedure in tempi in grado di preservare il business e con garanzia di integrità dei dati; i piani di business continuity e disaster recovery dovrebbero inoltre essere testati regolarmente ed anche dopo significativi cambiamenti al sistema; dovrebbero infine essere predisposti adeguate strutture per la gestione delle crisi nonché liste di contatto per le emergenze (sia a livello periferico che centrale) e ciò al fine di poter gestire in maniera efficiente e puntuale le cadute dei processi IT ed evitare il propagarsi della indisponibilità dei sistemi.

Infine, nel Luglio 2003 il "Comitato di Basilea" [6] della Banca dei Regolamenti Internazionali ha reso pubblici i propri principi di controllo per l'electronic banking; il principio numero 13 dichiara: "*Le banche dovrebbero possedere piani di business continuity e contingencyal fine di assicurare la disponibilità dei sistemi e servizi di e-banking*"[7]; il Comitato sottolinea anche che le banche dovrebbero effettuare degli audit (interni o esterni) periodici ed indipendenti sulla propria business continuity e contingency planning.

3. Un approccio strutturato e verificabile

Come visto la "Business Continuity" è una componente critica di ogni organizzazione finanziaria.

Nuove leggi, le aspettative degli azionisti, i requisiti degli investitori richiedono perciò un solido piano di continuità del servizio integrato con gli altri processi aziendali.

E' necessario adottare allora una metodologia di BCP ben strutturata e verificabile; al momento sono disponibili un elevato numero di standard: i più importanti sono stati sviluppati dal "Disaster Recovery International Institute" (DRI), dal "Business Continuity Institute" (BCI), dal

[5] CESR è un comitato indipendente che raggruppa i rappresentanti delle autorità nazionali competenti per il controllo del mercato mobiliare; il rappresentante italiano nel CESR è la "Commissione Nazionale per le Societa e la Borsa" (CONSOB)

[6] Il Comitato di Basilea, creato dai governatori delle banche centrali del gruppo dei Dieci alla fine del 1974, definisce standard e linee guida per la supervisione e la vigilanza delle istituzioni finanziarie.

[7] "*Risk management principles for electronic banking*", Basel Committee Publications No. 98, Luglio 2003, disponibile in: http://www.bis.org/publ/bcbs98.pdf

"National Institute of Standards and Technology" (NIST) e dalla "Information Systems Audit and Control Association" (ISACA)[8].

Tutte queste organizzazioni concordano sulla presenza del seguente set minimo di best practices quando si disegna e realizza un piano di business continuity:

- deve essere approvato un budget per il BCP da parte del top management;
- deve essere identificato una struttura che in caso di disastro o di interruzione del servizio coordini la strategia di ripristino;
- deve essere previsto un sistema per la gestione degli incidenti o comunque un processo per controllare la situazione ed operare il ripristino;
- il piano deve essere periodicamente rivisto ed occorre fare dei benchmark relativi ai regolamenti di mercato ed ai processi analoghi in altre organizzazioni.

Nelle pagine che seguono sarà illustrato l'approccio di audit al BCP di ISACA; esso si basa su COBIT, un framework generale applicabile alla IT Governance.

4. ISACA

L'*Information Systems Audit and Control Association* (ISACA) è stata fondata negli USA nel 1967 e raggruppa più di 28.000 professionisti nelle aree dell' IS Auditing ed IT Security.

L'ISACA redige gli standard di IS auditing, pubblica una rivista dedicata ai controlli IT (Information Systems Control Journal) ed organizza una serie di conferenze internazionali focalizzate su aspetti sia tecnici che manageriali dell' IS assurance, dei controlli, della sicurezza e della IT governance.

L'associazione è presente in circa 60 paesi; in Italia esistono due capitoli locali: Milano e Roma.

Last but not least, ISACA gestisce due certificazioni professionali: CISA (*Certified Information Systems Auditor*) e CISM (*Certified Information Security Manager*).

5. COBIT

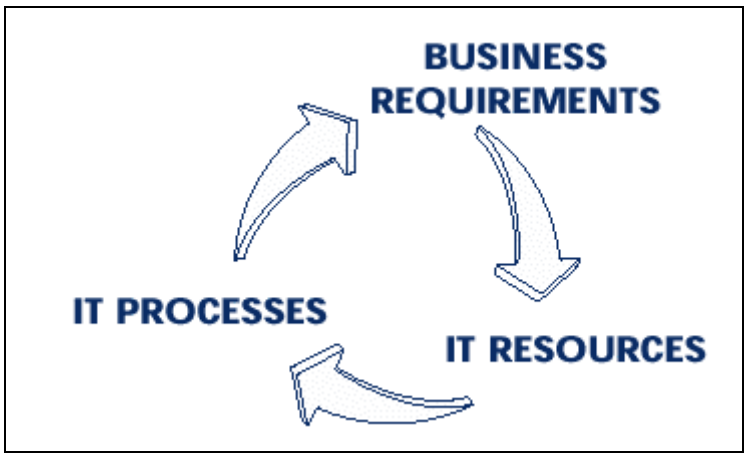
"Control Objectives for Information and related Technology" (COBIT), giunto alla terza edizione, è un framework sviluppato da ISACA che aiuta le organizzazioni a gestire i rischi IT e ad assicurare che i processi IT siano coerenti con le necessità di business.

La missione di COBIT è: ricercare, sviluppare e rendere pubblico un set internazionale di obiettivi di controllo generalmente accettati e che possano essere utilizzati non solo dai tecnici ma anche dai manager e dagli auditor.

La maggior parte delle componenti di COBIT sono liberamente utilizzabili e possono essere scaricate dal sito ISACA.

[8] Un confronto completo dei principali approcci di BCP è disponibile in "*Business Continuity Management Standards—A Side-by-side Comparison*" by Brian Zawada and Jared Schwartz in *Information Systems Control Journal*, Volume 2, 2003

Il framework COBIT identifica 34 principali processi di Information Technology, raggruppati in 4 domini e supportati da 318 obiettivi di controllo dettagliati. Ciascuno dei 34 processi individua le risorse IT coinvolte ed i requisiti di qualità, fiducia e di sicurezza richiesti.



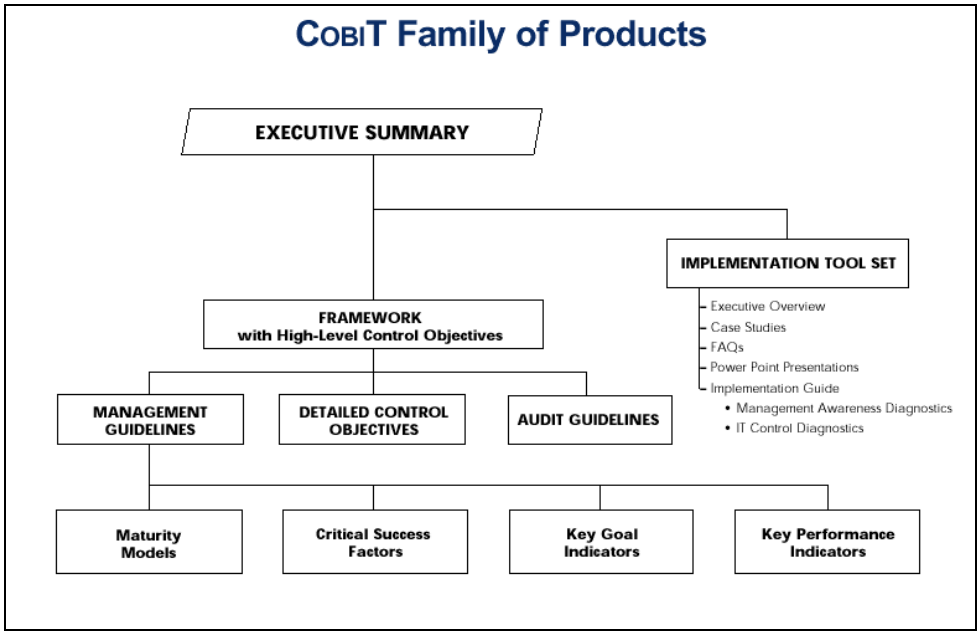
Si noti che le linee guida di COBIT sono generiche ed orientati ai processi allo scopo di indirizzare le seguenti necessità del management che si occupa di controlli:

misurazione delle performance – quali sono i migliori indicatori di performance?

IT control profiling – cosa è veramente importante? Quali sono i fattori critici per il successo dei controlli?

Consapevolezza – quali sono i rischi che potrebbero impedirci di raggiungere i nostri obiettivi?

Benchmarking – cosa fanno gli altri? Come possiamo misurare e confrontare i nostri risultati?

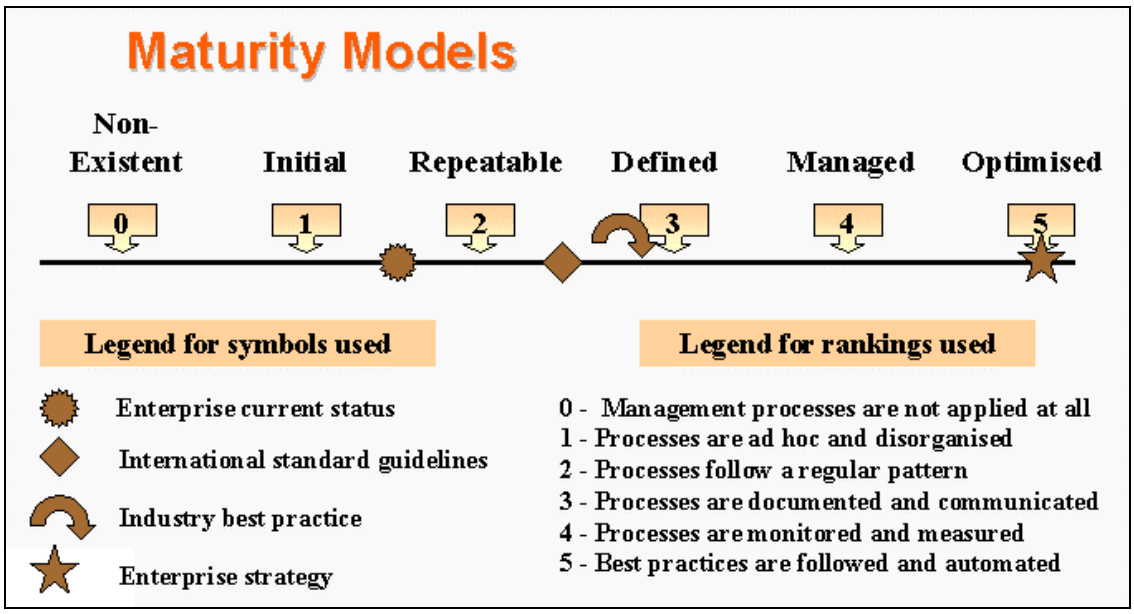


6. Il Maturity model

Per ciascuno dei 34 processi COBIT, è previsto di adottare una scala di misurazione basata su un rating che varia fra "0" e "5"; la scala è associata con un modello di maturità che varia dal "Non Esistente" a "Ottimizzato", modello mutuato dal “Capability Maturity Models®” del Software Engineering Institute - SEI[9].

Carnegie Mellon
Software Engineering Institute

Si noti che la scala di valutazione è volutamente non troppo granulare al fine di rendere il sistema semplice da usare; viceversa è opportuno concentrasi sui livelli qualitativi di maturità del processo analizzato utilizzando una serie di condizioni non ambigue.



Per ciascuno dei 34 processi CobiT è così possibile mappare sulla base del livello qualitativo indicato:

- lo stato corrente dell’organizzazione – dove è oggi l’organizzazione;
- lo stato corrente (best-in-class in) dell’industry di riferimento – il confronto;
- lo stato corrente come indicato dagli standard internazionali – il benchmarking;
- la strategia dell’organizzazione per operare il miglioramento – dove l’organizzazione vuole posizionarsi nel futuro.

Di seguito sono riepilogati i 34 Obiettivi di controllo di alto livello di COBIT (traduzione italiana a cura dell’autore).

[9] Il Software Engineering Institute (SEI) è un centro di ricerca statunitense finanziato dal Dipartimento della Difesa

Organizzazione e pianificazione	PO1	Definizione di un piano IT strategico	*Define a strategic IT plan*
	PO2	Definizione delle architecture informatiche	*Define the information architecture*
	PO3	Determinazione delle direzioni tecnologiche	*Determine technological direction*
	PO4	Definizione dell'organizzazione IT	*Define the IT organisation and relationships*
	PO5	Gestione degli investmenti IT	*Manage the IT investment*
	PO6	Comunicazione al management degli obiettivi strategici	*Communicate management aims and direction*
	PO7	Gestione delle risorse umane	*Manage human resources*
	PO8	Assicurare il rispetto dei requisiti esterni	*Ensure compliance with external requirements*
	PO9	Risk Assessment	*Assess risks*
	PO10	Project Management	*Manage projects*
	PO11	Gestione della qualità	*Manage quality*
Acquisizione e realizzazione	AI1	Identificazione delle soluzioni automatizzate	*Identify automated solutions*
	AI2	Acquisizione e manutenzione delle applicazioni software	*Acquire and maintain application software*
	AI3	Acquisizione e manutenzione della infrastruttura tecnologica	*Acquire and maintain technology infrastructure*
	AI4	Sviluppo e manutenzione delle procedure	*Develop and maintain procedures*
	AI5	Installazione e certificazione dei sistemi	*Install and accredit systems*
	AI6	Ch'ange Management	*Manage changes*
Erogazione del servizio e assistenza	DS1	Definizione e gestione dei Service Level Agreement (SLA)	*Define and manage service levels*
	DS2	Gestione delle terze parti	*Manage third-party services*
	DS3	Gestione delle performance e capacità	*Manage performance and capacity*
	DS4	Assicurare la continuità del servizio	*Ensure continuous service*
	DS5	Assicurare la sicurezza dei sistemi	*Ensure systems security*
	DS6	Identificare ed attribuire i costi	*Identify and allocate costs*
	DS7	Training e formazione degli utenti	*Educate and train users*
	DS8	Assistenza e informazione dei clienti	*Assist and advise customers*
	DS9	Gestione delle configurazioni	*Manage the configuration*
	DS10	Gestione degli incidenti	*Manage problems and incidents*
	DS11	Gestione dei dati	*Manage data*
	DS12	Gestione delle facility	*Manage facilities*
	DS13	Gestione delle operazioni	*Manage operations*
Monitoraggio	M1	Monitoraggio dei processi	*Monitor the processes*
	M2	Assessment dell'adeguatezza dei controlli interni	*Assess internal control adequacy*
	M3	Ottenere una assurance indipendente	*Obtain independent assurance*
	M4	Fornire un audit indipendente	*Provide for independent audit*

Uno dei 34 obiettivi di controlli di alto livello è specificatamente indirizzato alle problematiche del BCP. L'obiettivo è assicurare la continuità del servizio, previa analisi dei requisiti di business, al fine di ridurre al minimo gli impatti in seguito ad eventi disastrosi o incidenti significativi. E' richiesto pertanto un IT Continuity Plan operativo e periodicamente sottoposto a verifica che comprenda come elementi fondamentali:

- la classificazione delle possibili criticità;
- le procedure alternative in caso di incidente o disastro;
- le procedure di back-up e recovery;

- un piano sistematico di testing e formazione;
- processi di monitoring ed escalation;
- la definizione chiara delle responsabilità (interne ed esterne) organizzative;
- i piani per l'attivazione della business continuity, il fallback ed il ripristino;
- le attività di risk management;
- l'individuazione e valutazione dei possibili singoli punti di debolezza e di guasto potenziale;
- problem management;
- monitoring.

Tale obiettivo di controllo di tipo generale viene infine "tradotto" in 13 controlli specifici per il Piano di continuità IT (traduzione a cura dell'autore).

1.	Esistenza di un framework generale per la continuità del servizio	*IT Continuity Framework*
2.	Strategia e filosofia dell'IT Continuity Plan	*IT Continuity Plan Strategy and Philosophy*
3.	Contenuti del piano di IT Continuity	*IT Continuity Plan Contents*
4.	Requisiti minimi per la IT Continuity	*Minimising IT Continuity Requirements*
5.	Manutenzione del piano di IT Continuity	*Maintaining the IT Continuity Plan*
6.	Collaudo del piano di IT Continuity	*Testing the IT Continuity Plan*
7.	Formazione relativa al piano di IT Continuity	*IT Continuity Plan Training*
8.	Comunicazione del piano di IT Continuity	*IT Continuity Plan Distribution*
9.	Procedure alternative di back-up per gli utilizzatori	*User Department Alternative Processing Back-up Procedures*
10.	Classificazione delle risorse IT critiche	*Critical IT Resources*
11.	Procedure di back-up del sito e dell'hardware	*Back-up Site and Hardware*
12.	Conservazione dei supporti di back-up in località remota	*Off-site Back-up Storage*
13.	Procedure finali	*Wrap-up Procedures*

Ad esempio per quanto riguarda i primi due punti, si richiede di valutare quanto segue:

- Esistenza di un framework generale per la continuità del servizio: il Management IT, in collaborazione con i "proprietari" degli processi di business, dovrebbe definire un framework che definisca ruoli, responsabilità e la metodologia (*risk-based*) da adottare al fine di permettere sia la documentazione del BCP che l'esistenza di un processo coerente di verifica ed approvazione dello stesso;
- Strategia e filosofia dell'IT Continuity Plan: il management dovrebbe assicurare che le componenti IT del BCP siano in linea con il piano di continuità generale dell'azienda; analogamente l'IT Continuity Plan deve tener conto dei piani generali IT a medio e lungo termine.

L'elenco completo dei controlli richiesti può essere consultato (in inglese) nel documento COBIT *Control Objectives* disponibile, come detto, sul sito ISACA.[10].

7. Conclusioni

Il Business continuity management è una responsabilità del top management.

Ciò è importante perché una organizzazione deve per prima cosa definire gli obiettivi ed il piano della propria business continuity. L'audit del BCP diventa così un elemento fondamentale dell' IT Governance in quanto rappresenta un assessment indipendente i cui risultati possono essere

[10] https://www.isaca.org/TemplateRedirect.cfm?Template=/MembersOnly.cfm&ContentFileID=1398 solo per utenti registrati

condivisi e comunicati anche al di fuori dei sistemi IT, ad esempio agli *stakeholder*, alle autorità di controllo o ai business-partner.

8. Links

Garante per la protezione dei dati personali:
http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
Il Codice in materia di protezione dei dati personali:
http://www.garanteprivacy.it/garante/document?ID=228213
Banca D'Italia: http://www.bancaditalia.it
ABI – Associazione Bancaria Italiana: www.abi.it
ESCB - The European System of Central Banks: http://www.ecb.int/about/escb.htm
CESR - Committee of European Securities Regulators: http://www.europefesco.org/v2/default.asp
CONSOB - Commissione Nazionale per le Società e la Borsa: http://www.consob.it
Il Comitato di Basilea: http://www.bis.org/bcbs/aboutbcbs.htm
BCI - The Business Continuity Institute: http://www.thebci.org/
DRJ -Disaster Recovery Journal www.drj.com
ISACA - Information Systems Audit and Control Association: http://www.isaca.org
NIST - National Institute of Standards and Technology: http://www.nist.gov/
ISACA capitolo di Milano: www.aiea.it
ISACA capitolo di Roma: www.isacaroma.it .
SEI - Software Engineering Institute: http://www.sei.cmu.edu

Bibliografia

Ken Doughty, *Business Continuity: A Business Survival Strategy*, Information Systems Control Journal, Volume 1, 2002

Yusufali F. Musaji, *Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans*, Information Systems Control Journal, Volume 1, 2002

Brian Zawada and Jared Schwartz, *Business Continuity Management Standards— A Side-by-side Comparison*, Information Systems Control Journal, Volume 2, 2003

L'autore

Agatino Grillo, CISA, CISSP. E' il responsabile della practice e-security di Euros Consulting. Precedentemente ha lavorato in Ernst & Young ed Arthur Andersen come IS auditor e IT Security consultant. Ha più di dieci anni di esperienza come consulente nell'IT. E' docente e relatore sui temi dell'e-business e della sicurezza per diverse organizzazioni e business school. Ha pubblicato numerosi articoli e white papers sui temi dell' IS Auditing e della IT Security, disponibili in: www.agatinogrillo.it. Email: agatino.grillo AT libero.it