Giovanni Oldani

IBM Consultant

Lo Standard BS25999

Roma, 9 luglio 2008

AGENDA

Contesto normativo

Business Continuity vs Disaster Recovery ICT

Contenuti della norma

CONTESTO NORMATIVO

La crescente dipendenza dei processi di business dai servizi IT ha fatto evolvere per importanza e per estensione le discipline preposte al controllo ed alla mitigazione dei rischi.

"Business resilience is the ability to rapidly adapt and respond to risks, as well as opportunities, in order to maintain continuous business operations, be a more trusted partner, and enable growth". ***IBM***

BUSINESS RESILIENCY

GESTIONE E CONTROLLO DEL RISCHIO OPERATIVO

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events…" ***Basilea II***

"Business continuity is strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level" ***BS25999.***

BUSINESS CONTINUITY

SECURITY ICT

"Information security is preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved". ***ISO27001***

DISASTER RECOVERY ICT

"(sono di) disaster recovery le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e servizi di comunicazione." ***CNIPA***

Basel II Capital Accord - Operational Risk Management

"*Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events…*"

Le tipologie di eventi di perdita che devono essere considerate nella valutazione delle esposizioni al rischio operativo forniscono una mappa dei rischi applicabile a qualsiasi segmento di industria.

- **Frode interna** – esempi: alterazione intenzionale di dati, sottrazione di beni e valori, operazioni in proprio basate su informazioni riservate.
- **Frode esterna** – esempi: furto, contraffazione, falsificazione, emissioni di assegni a vuoto, pirateria informatica.
- **Rapporto di impiego e sicurezza sul posto di lavoro** – esempi: risarcimenti richiesti da dipendenti, violazione delle norme a tutela della salute e sicurezza personale, attività sindacale, pratiche discriminatorie, responsabilità civile.
- **Pratiche connesse con la clientela, i prodotti e l'attività** – esempi: violazione del rapporto fiduciario, abuso di informazioni confidenziali, transazioni indebite effettuate per conto della banca, riciclaggio di denaro di provenienza illecita, vendita di prodotti non autorizzati.
- **Danni a beni materiali** – esempi: atti di terrorismo e vandalismo, terremoti, incendi, inondazioni.
- **Disfunzioni e avarie di natura tecnica** – esempi: anomalie di infrastrutture e applicazioni informatiche, problemi di telecomunicazione, interruzione nell'erogazione di utenze.
- **Conformità esecutiva e procedurale** – esempi: errata immissione dei dati, gestione inadeguata delle garanzie, documentazione legale incompleta, indebito accesso consentito a conti di clienti, inadempimenti di controparti non clienti, controversie legali con fornitori.

ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements

"Information security is preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved".

Lo standard definisce 11 categorie di security control;

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- *Information Security Incident Management*
- *Business Continuity Management*
- Compliance

CONTESTO NORMATIVO
BUSINESS CONTINUITY

BS25999 - "Business continuity is strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level".

BS25999 - Part 1 – Code of Practice for Business Continuity Management .

- Definisce i processi di BCM (Business Continuity Management), principi, e la terminologia (es. Incident Management Plan, Business Continuity Plan);
- Stabilisce criteri condivisi per disegnare, sviluppare e realizzare la continuità operativa nell'ambito di un'azienda, al di là delle dimensioni e del settore di appartenenza;
- Fornisce una metodologia completa basata sulle best practices di BCM e sull'intero ciclo di vita del BCM.
- È basata sui processi di business

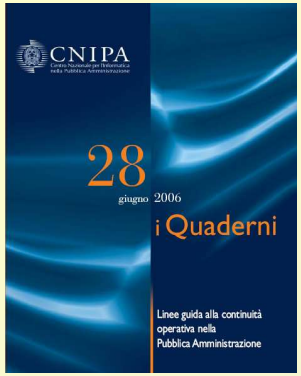
BS25999 - Part 2 – Specification

- Formalizza i requisiti (verificabili) per definire, realizzare, esercire, monitorare/controllare, mantenere nel tempo e adattare un sistema documentato per la BC (Business Continuity Management System) nell'ambito dei rischi in cui un'organizzazione può incorrere.
- Formalizza i requisiti per definire e implementare i controlli di continuità operativa adattati alle necessità di una singola organizzazione.
- È auditabile, ossia prevede registrazioni, audit interni e audit di terze parti.

CONTESTO NORMATIVO

DISASTER RECOVERY ICT

CNIPA Linee Guida alla Continuità Operativa nella PA: "(sono di) disaster recovery le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e servizi di comunicazione"



Linee guida alla continuità operativa nella PA
"i Quaderni" n. 28" - giugno 2006
Aspetti metodologici, analisi dei costi e dei benefici, problematiche organizzative e giuridiche, tecnologie disponibili: il documento costituisce un'efficace guida per tutte quelle amministrazioni che intendano affrontare in modo sistematico il tema della continuità operativa dei servizi, attraverso la realizzazione di soluzioni adeguate a specifiche esigenze.

La continuità operativa nella P.A. - Casi di studio
"i Quaderni n. 35" - febbraio 2008

Piano triennale per l'ICT della Pubblica Amministrazione Centrale 2008 – 2010
Razionalizzazione della spesa ICT:
... razionalizzato l'utilizzo delle infrastrutture IT (anche condividendo siti di disaster recovery) ...
Investire nella sicurezza:
... Il CNIPA, insieme alle amministrazioni, intende individuare un blocco di regole comuni scritte in base a un modello condiviso in grado di garantire un livello base di sicurezza. Inoltre il CNIPA, come già è avvenuto nel caso del Centro unico di backup degli Enti, può promuovere iniziative congiunte tra le amministrazioni, creando economie di scala e messa a fattor comune di best practice.

AGENDA

Contesto normativo

Business Continuity vs Disaster Recovery

Contenuti della norma

BC vs DR

Il Piano di Disaster Recovery ICT è parte del Piano di Business Continuity dell'azienda e assicura la ripartenza dei servizi informativi a sostegno delle attività di business critiche dell'azienda stessa .

Single Local Event

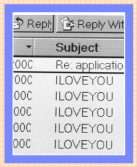
Fire

Wide Area Event

Hurricane
Quake

Flood

Logical Threat



Viruses

Hacking

Systemic Threat

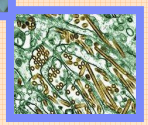
Terrorism

Black out

Global Threat (Pandemic)

SARS

Avian
Flue



Disaster Recovery

Central IT

IT Server Farms

Business Continuity

WorkPlaces

Call Centers

Trading Rooms

Devices

Operational Risks

1960 ***1970*** ***1980*** ***1990*** ***2000*** ***2010***

weeks

days

hours

minutes

Business Recovery

Business Resilience

Transparent recovery

Glass House
Mainframe

Departimental
Midrange

Client Server
Personal Computers

Internet e-business
Laptops

Mobile
Pervasive Computing

Grid Computing
Virtual

Supercomputing

AGENDA

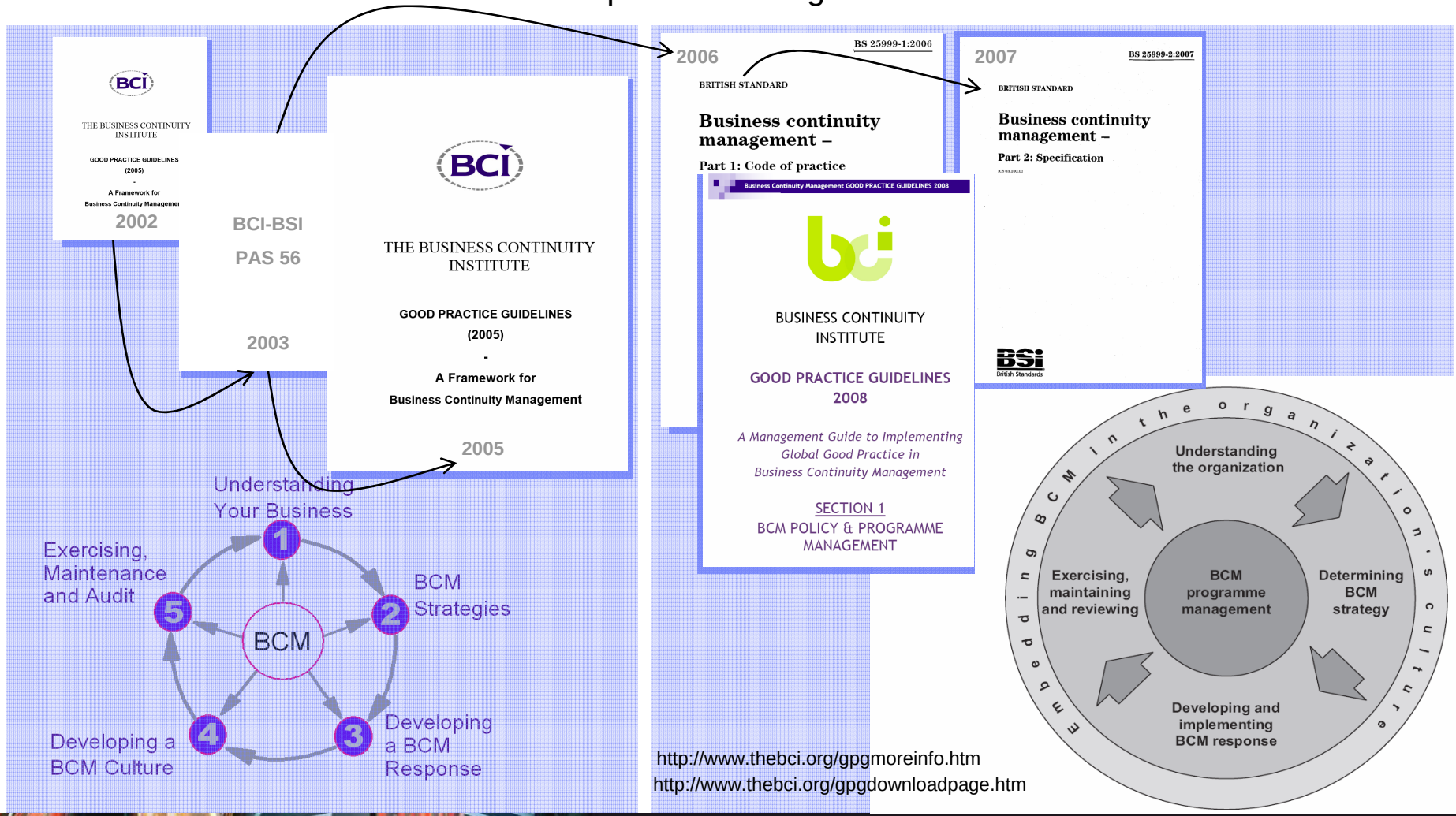
Contesto normativo

Business Continuity vs Disaster Recovery ICT

Contenuti della norma

CONTENUTI DELLA NORMA
STORIA

La versione del 2008 di "*Business Continuity Institute - Good Practice Guidelines*" riformula la versione del 2005 riflettendo la stessa impostazione e glossario della BS25999.



http://www.thebci.org/gpgmoreinfo.htm
http://www.thebci.org/gpgdownloadpage.htm

CONTENUTI DELLA NORMA
PRIMA PARTE

La prima parte del British Standard definisce i processi, i principi e la terminologia per la gestione della continuità operativa, fornendo una base comune per comprendere, disegnare, realizzare e mantenere nel tempo la continuità del business di una organizzazione, di qualunque dimensione, settore, tipologia o ubicazione.

.

Un sistema di gestione della continuità operativa (BCMS) secondo il BS25999 - Part 1 – Code of Practice for Business Continuity Management:

- **assicura la capacità di un'azienda di affrontare situazioni di emergenza anche molto grave, mantenendo attive le proprie operazioni vitali nell'ambito delle propria missione;**
- **fornisce un metodo verificabile della capacità che un'azienda ha di ripristinare i propri servizi e prodotti nel rispetto di livelli di servizio condivisi;**
- **dimostra la capacità dell'azienda di saper gestire qualunque situazione di emergenza grave a garanzia della propria reputazione e dei propri clienti / utenti.**

CONTENTI DELLA NORMA
SECONDA PARTE

La seconda parte del British Standard formalizza i requisiti (verificabili) di un sistema documentato per la Business Continuity (BCMS) nell'ambito dei rischi in cui un'organizzazione può incorrere.

.

- **La seconda parte della normativa specifica i requisiti minimi richiesti per disegnare, realizzare, rendere operativo, controllare, rivedere, verificare e testare, mantenere efficiente ed adeguato nel tempo (ciclo PDCA) il sistema di gestione della continuità operativa.**
- **I requisiti della norma sono generali e possono essere applicati a tutte le organizzazioni.**
- **Le fasi di disegno e realizzazione di ciascun sistema di gestione della continuità operativa devono necessariamente tener conto delle regole e delle norme vigenti, della tipologia di clienti / utenti dell'azienda, delle dimensioni e della tipologia di business.**
- **La parte 2 dello standard può essere utilizzata da parti interne o terze all'azienda, compresi gli enti certificatori, per verificare la capacità dell'azienda di mantenere continua la propria operatività, anche nel rispetto di requisiti contrattuali, legali e normativi in genere.**

CONTENUTI DELLA NORMA

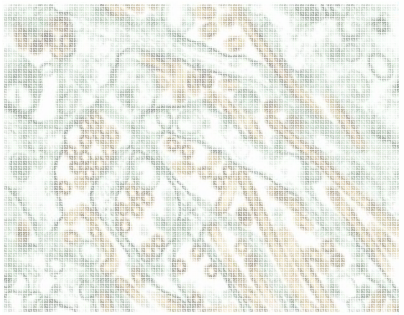
In generale un sistema di gestione della business continuity è ben definito se risultano....

- **Definiti l'ambito e gli obiettivi del sistema di gestione della continuità operativa.**
- **Stabilita la politica del BCMS.**
- **Disponibili le risorse.**
- **Personale coinvolto addestrato e competente.**
- **Eseguita la business impact analysis e risk assessment**
- **Stabilita la strategia di continuità operativa**
- **Definito il sistema di incident response**
- **Steso il piano di continuità operativa e piano di gestione degli incidenti.**
- **Effettuati i test continuità operativa.**
- **Avviato il piano di mantenimento e aggiornamento del BCMS**
- **Applicate le contromisure correttive e preventive del BCMS**
- **Condotti gli audit interni**
- **Coinvolto il management aziendale**
- **Avviato il ciclo di adeguamento del sistema di gestione**

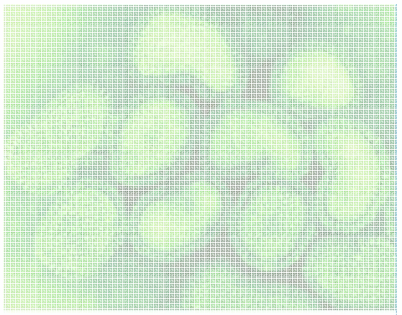
CONTENTI DELLA NORMA

... in definitiva un efficace sistema di gestione della continuità operativa (BCMS) permette all'azienda il raggiungimento dei seguenti risultati:

- **I servizi e i prodotti dell'azienda sono noti, protetti e forniti con continuità.**
- **L'azienda è in grado di rispondere in modo appropriato in caso di incidente rilevante.**
- **L'azienda è a conoscenza di quanto è essenziale per la propria missione la disponibilità delle altre organizzazioni (es. fornitori, autorità pubbliche, enti regolatori).**
- **In caso di situazioni di emergenza grave il personale dell'azienda è in grado di reagire in modo appropriato, preparato e informato su quanto deve essere fatto e sta accadendo.**
- **Il management dell'azienda è responsabilizzato al raggiungimento degli obiettivi di continuità.**
- **Le esigenze degli utenti sono ben note e l'azienda può assicurarne il mantenimento in ogni momento.**
- **La catena dei fornitori è messa in sicurezza e garantita.**
- **La reputazione è garantita nel tempo e l'azienda risulta conforme ai requisiti di legge e alle regole di settore.**



H5N1: a virus with proven pandemic potential
(Source: CDC Public Health Image Library).



Influenza viruses are highly unstable, genetically labile, and well adapted to elude host defences.

GRAZIE

Giovanni Oldani, IBM Consultant

Business Continuity and Resiliency Services

IBM Italia SpA

Circonvallazione Idroscalo

20090 Segrate (MI)

giovanni_oldani@it.bm.com

+390259620459, +393357368685