SwissBanking

Agosto 2013

Raccomandazioni per il Business Continuity Management (BCM)

Indice

1 Premessa e obiettivi 2
2 Basi 3
3 Ambito di applicazione e fattori di pericolo 4
4 Raccomandazioni 6
4.1 Definizione ed estensione 6
4.2 Responsabilità 7
4.3 Analisi dei rischi 7
4.4 Business Continuity Management Strategy (standard minimo obbligatorio) 8
4.5 Componenti del Business Continuity Management 8
4.5.1 Business Impact Analysis (standard minimo obbligatorio) 8
4.5.2 Business Recovery Options (standard minimo obbligatorio) 9
4.5.3 Business Recovery Planning 10
4.5.4 Business Continuity Review 10
4.5.5 Business Continuity Tests 10
4.6 Gestione delle crisi 11
4.7 Reportistica, comunicazione, formazione 11
4.7.1 Reportistica 11
4.7.2 Comunicazione 12
4.7.3 Formazione e sensibilizzazione 12
5 Entrata in vigore 13
Appendice A – Glossario 14
Appendice B – Scala di gravità degli eventi 18
Appendice C – Andamento di una crisi 19
Appendice D – Fonti di approfondimento 20

1 Premessa e obiettivi

Molti degli avvenimenti accaduti negli ultimi anni, in particolare gli atti terroristici, le pandemie e le catastrofi naturali, hanno messo in evidenza la vulnerabilità degli operatori e dei sistemi dei mercati finanziari. Di pari passo, si è acuita l'attenzione verso eventi del genere e le loro possibili conseguenze.

A livello internazionale e in molti paesi sono state emanate direttive e raccomandazioni nell'ambito del Business Continuity Management (BCM) con precise esigenze poste agli operatori dei mercati finanziari e alle autorità di vigilanza.

L'Autorità federale di vigilanza sui mercati finanziari (FINMA) considera un valido Business Continuity Management uno dei requisiti indispensabili per il rilascio dell'autorizzazione per svolgere l'attività bancaria, conformemente a quanto disposto all'art. 3 della Legge sulle banche, e in questo senso sostiene l'adozione di un codice di autodisciplina da parte dell'Associazione svizzera dei banchieri (ASB).

La presente autoregolamentazione dell'Associazione svizzera dei banchieri, destinata ai suoi membri, contiene una serie di raccomandazioni («best practice») per l'allestimento di un BCM in ogni istituto che tenga conto dei relativi aspetti specifici, soprattutto per quanto concerne la situazione di rischio e la rilevanza sistemica dei singoli istituti.

Tre paragrafi delle presenti raccomandazioni sono considerati dalla FINMA «Norme di autoregolamentazione riconosciute come standard minimo» in base alla Circolare 2008/10 e fungono da standard minimo in materia di vigilanza, la cui ottemperanza viene verificata dalle società di audit. La definizione di una strategia di Business Continuity Management (paragrafo 4.4), l'attuazione di Business Impact Analysis (paragrafo 4.5.1) e la determinazione di Business Recovery Options (paragrafo 4.5.2) hanno carattere vincolante.

L'ambito di applicazione delle presenti raccomandazioni si estende a tutte le banche e tutti i commercianti di valori mobiliari (in seguito «istituti»). Non sono contemplati gli effetti delle raccomandazioni sul rapporto di diritto civile fra l'istituto e i propri clienti.

2 Basi

Le presenti raccomandazioni si rifanno a diversi standard analoghi (vedi anche le fonti di approfondimento riportate nell'appendice D). In particolare si rifanno alle seguenti norme:

- «High-Level Principles for Business Continuity» formulati dal Joint Forum e dal Comitato di Basilea per la vigilanza bancaria[1],
- «British Standard for Business Continuity Management BS 25999»[2] o ISO 22301[3].

Gli «High-Level Principles» menzionati contengono le raccomandazioni qui elencate.

1. Gli operatori dei mercati finanziari e le autorità di vigilanza devono disporre di un Business Continuity Management completo ed efficiente. La responsabilità della Business Continuity compete al consiglio di amministrazione (Board of Director) e alla direzione (Senior Management).
2. Nel loro Business Continuity Management gli operatori dei mercati finanziari e le autorità di vigilanza devono considerare l'eventualità che possano verificarsi gravi disfunzioni operative.
3. Gli operatori dei mercati finanziari sono tenuti a sviluppare degli obiettivi di recovery (Recovery Time Objectives, RTO) che tengano conto della loro rilevanza sistemica e del rischio che essi rappresentano per l'intero sistema finanziario.
4. I piani di Business Continuity degli operatori dei mercati finanziari e delle autorità di vigilanza devono definire delle misure atte a garantire la comunicazione interna ed esterna in caso di lunghe interruzioni dell'attività aziendale.
5. Qualora le interruzioni prolungate dell'attività aziendale comportino implicazioni internazionali, occorre che i piani informativi

[1] Basel Committee on Banking Supervision, Bank for International Settlements, agosto 2006, www.bis.org.

[2] British Standards Institution, settembre 2008, www.bsigroup.com.

[3] International Organization for Standardization (ISO), maggio 2012, www.iso.org.

prevedano anche le comunicazioni con le autorità di vigilanza estere.

6. Gli operatori dei mercati finanziari e le autorità di vigilanza devono sottoporre i loro piani di Business Continuity a test periodici per valutarne l'efficacia ed eventualmente adeguare di conseguenza il Business Continuity Management.
7. Si raccomanda alle autorità di vigilanza di valutare, nel quadro di un monitoraggio costante, il Business Continuity Management degli istituti sottoposti alla loro sorveglianza.

È opportuno inoltre tenere in debito conto il lavoro svolto dal gruppo «BCP Piazza finanziaria svizzera» che, sotto la guida della Banca Nazionale Svizzera (BNS), ha identificato due processi critici: «pagamenti di grossi importi tramite SIC» e «approvvigionamento di liquidità mediante operazioni Repo»[4].

3 Ambito di applicazione e fattori di pericolo

Gli istituti devono considerare tutti i principali fattori di potenziale pericolo che possono portare l'azienda a una crisi. Per «crisi» si intende una situazione di emergenza che richiede decisioni straordinarie e che non può essere gestita con gli strumenti di direzione e le competenze decisionali ordinari. In questa accezione, la rimozione delle «incidenti» non è oggetto dichiarato delle presenti raccomandazioni («Availability Management», vedi definizione dei termini nelle appendici A e B). Esempi di situazioni di crisi:

- eventi «accidentali» come incendi o esplosioni,
- atti di matrice terroristica, sabotaggi,
- catastrofi naturali come inondazioni o terremoti.

A titolo di «best practice» si consiglia di concentrarsi, nell'impostazione del Business Continuity Management, sulle conse-

[4] Banca nazionale svizzera (BNS), Business Continuity nel settore finanziario svizzero, 2006 e 2009, www.snb.ch.

guenze e non sulle cause delle crisi. Per il ripristino di processi operativi e attività aziendali ad alta criticità dopo un'interruzione devono essere vagliati gli effetti delle varie opzioni di Business Recovery in funzione degli obiettivi fissati di recovery (vedi paragrafo 4.5.2).

Gli istituti devono individuare, nel ambito del BCM, i pericoli rilevanti, definendoli e valutandoli in base all'impatto che possono avere (scala di gravità).

Questi eventi possono comportare in particolare l'indisponibilità totale o parziale di collaboratori e/o di elementi infrastrutturali (soprattutto edifici, postazioni di lavoro, strutture di direzione, telecomunicazioni) per lo svolgimento di processi operativi critici. È possibile inoltre che tali processi non possano più avere luogo a causa di problemi dei fornitori di servizi informatici o di infrastrutture.

Per quanto riguarda le pandemie, occorre considerare gli scenari di danno e le raccomandazioni dell'Ufficio federale della sanità pubblica (UFSP). Nei piani pandemici è necessario tener conto del fatto che, in termini di durata e imprevedibilità del fenomeno, le ripercussioni di un contagio su larga scala si differenziano notevolmente dalle situazioni di crisi BCM.

Una situazione di crisi BCM…

- subentra improvvisamente e in tempi rapidi provoca profonde conseguenze sull'attività aziendale e
- la pianificazione si focalizza sul rapido ripristino della capacità operativa,

mentre una pandemia…

- prevede un lungo periodo di incubazione prima di raggiungere il picco dei casi di malattia e
- richiede una pianificazione per salvaguardare i processi operativi di maggiore criticità e sospendere quelli di minore criticità.

Si raccomanda di redigere un piano pandemico almeno a livello di istituto. Informazioni aggiornate al riguardo sono consultabili sul sito dell'UFSP[5].

In molti processi operativi alcune prestazioni, che potrebbero essere interrotte senza preavviso, vengono erogate da fornitori esterni. Nel caso in cui ci si avvalga di fornitori esterni in processi operativi critici occorre verificare in maniera adeguata la loro « BCM maturity. »

Nel ambito delle opzioni di Business Recovery (paragrafo 4.5.2) si può analizzare tra l'altro la possibilità di passaggio da fornitori esterni a fornitori interni. Oltre a ciò si possono incaricare preventivamente fornitori supplementari o alternativi a quelli esistenti.

A complemento della Circolare FINMA 2008/7 «Outsourcing – banche, appalto di campi di attività – banche» si consiglia a titolo di «best practice» di prevedere sempre delle soluzioni alternative per il caso in cui i fornitori esterni interrompano i loro servizi.

Il BCM deve garantire, nel modo migliore possibile, l'osservanza delle disposizioni legali, regolamentari, contrattuali e interne anche in caso di crisi.

4 Raccomandazioni

4.1 Definizione ed estensione

Con l'espressione «Business Continuity Management (BCM)» si designa un approccio su scala aziendale in grado di assicurare che, al verificarsi di un evento straordinario interno o esterno di vasta portata, i processi operativi critici possano continuare a funzionare. Tra i suoi scopi il BCM mira a minimizzare i danni finanziari, legali o di reputazione conseguenti a tali eventi.
Nel suo complesso il BCM deve garantire la continuità – in una misura prestabilita – o la ripresa tempestiva dell'attività aziendale nelle situa-

[5] Ufficio federale della sanità pubblica (UFSP), Piano pandemico svizzero Influenza, gennaio 2009, www.bag.admin.ch.

zioni di crisi. Il BCM concerne quindi, in generale, tutti i settori operativi e organizzativi di un'azienda. A questo proposito occorre fare una distinzione tra le misure di pianificazione del BCM a monte e la gestione delle crisi (conduzione in situazioni di crisi) in caso di messa in atto.

4.2 Responsabilità

La responsabilità per il Business Continuity Management compete al consiglio di amministrazione e alla direzione di ogni singolo istituto (vedi anche la Circolare FINMA 2008/24 «Sorveglianza e controllo interno nel settore bancario»).

Il consiglio di amministrazione è responsabile di verificare il rispetto della strategia BCM documentata in forma scritta. La direzione provvede a realizzarla e definisce le altre responsabilità, competenze e flussi informativi mediante direttive e regolamenti interni. In particolare regola (su autorizzazione del consiglio di amministrazione) i propri rapporti con l'organizzazione di crisi (unità di crisi).

4.3 Analisi dei rischi

Nell'ambito del Business Continuity Management può essere effettuata un'analisi dei rischi che possono pregiudicare le risorse critiche. È possibile anche riferirsi ad analisi dei rischi condotte in altre unità aziendali (ad es. gestione dei rischi). L'analisi dei rischi svolta nel BCM serve a individuare i fattori suscettibili di compromettere il funzionamento dei processi operativi, partendo dal presupposto che tali fattori possano verificarsi effettivamente. Anche se non è sempre possibile identificare tutti i rischi, l'analisi permette comunque di rilevare e valutare le potenziali fonti di pericolo. Attraverso misure mirate, peraltro, si può ridurre a un livello accettabile la probabilità di accadimento di uno scenario di crisi.

4.4 Business Continuity Management Strategy (standard minimo obbligatorio)

Nella Business Continuity Management Strategy l'istituto stabilisce le linee di base che intende seguire per impostare il Business Continuity Management.

La Business Continuity Management Strategy può essere integrata nella strategia aziendale dell'istituto o avere una sua fisionomia separata. Nel caso in cui si vogliano assumere consapevolmente singoli rischi residui, è obbligatorio fornire nella strategia esplicite informazioni al riguardo. Le decisioni in merito devono essere documentate in forma scritta.

Nella BCM Strategy occorre regolare i seguenti aspetti:

- definizione e delimitazione del perimetro di pertinenza del BCM (scope),
- integrazione del BCM nell'organizzazione aziendale,
- creazione di una struttura di governance adeguata all'organizzazione aziendale,
- determinazione dei ruoli e delle responsabilità relative al BCM,
- individuazione dei fattori di pericolo e delle loro ripercussioni sulle risorse dell'azienda (base di pianificazione),
- indicazione della periodicità delle review e dei test concernenti i piani e le misure previste,
- modalità di reportistica, comunicazione, formazione.

4.5 Componenti del Business Continuity Management

4.5.1 Business Impact Analysis (standard minimo obbligatorio)

La Business Impact Analysis (BIA) fornisce le informazioni necessarie sia sui processi operativi critici che sulle risorse critiche. Per quanto attiene ai processi operativi critici vengono valutate, nell'ambito del BCM, le conseguenze specifiche di una perdita totale o parziale delle singole risorse. Ogni settore operativo deve determinare i propri processi critici e le proprie risorse critiche.

La valutazione comprende anche i rapporti di dipendenza reciproca tra settori operativi (la cosiddetta «process dependency») e dai provider e fornitori esterni (outsourcing).

I risultati di questa analisi, da cui si ricavano gli obiettivi di recovery, devono indicare almeno:

- il periodo definito di tempo necessario per il ripristino dei processi operativi critici (Recovery Time Objective, RTO),
- il grado auspicato di ripristino dei processi operativi critici entro l'RTO fissato,
- la consistenza minima di risorse (sostitutive), in termini di edifici, collaboratori, IT/dati, e fornitori esterni che in caso di crisi devono essere disponibili per raggiungere il grado auspicato di ripristino.

La BIA va verificata annualmente; i metodi e la portata dei controlli dipendono dalla situazione di rischio specifica dell'istituto.

4.5.2 Business Recovery Options (standard minimo obbligatorio)

Le opzioni di Business Recovery fissano i principi operativi di base con i quali l'azienda intende raggiungere – nei settori indicati al paragrafo 4.5.1 – i propri obiettivi di recovery definiti nella Business Impact Analysis per i fattori di pericolo individuati e le relative ripercussioni sulle risorse. Gli obiettivi di recovery devono essere documentati in forma scritta e contenere le opzioni di Business Recovery scelte per le risorse critiche. Nel testo devono essere menzionate almeno le opzioni di Business Recovery che in linea di massima sono praticabili in caso di indisponibilità di

- personale,
- edifici,
- sistemi o infrastrutture IT (incl. sistemi di comunicazione),
- fornitori esterni (outsourcing), ad es. provider di informazione.

Le suddette opzioni di Business Recovery devono essere specificate in termini concreti nei rispettivi piani di Business Recovery. L'assunzione

di un rischio residuo può rappresentare un'opzione di Business Recovery e come tale deve essere selezionata e formulata per iscritto, come descritto in precedenza.

4.5.3 Business Recovery Planning

I piani di Business Recovery descrivono le procedure necessarie per la continuazione (continuity) o il ripristino (recovery) dei processi operativi critici (inclusa l'osservanza delle disposizioni legali, regolamentari, contrattuali e interne), le soluzioni alternative e le risorse sostitutive minime per realizzarle. I piani devono contenere almeno la descrizione degli eventi per cui sono applicabili (fattori scatenanti), le procedure e il repertorio delle misure con le rispettive priorità e le risorse sostitutive necessarie.

I piani di Business Recovery devono essere verificati almeno una volta all'anno per controllarne l'aggiornamento e, se necessario, adeguati di conseguenza. Eventuali cambiamenti sostanziali nell'attività aziendale (riassetti organizzativi, apertura di un nuovo comparto ecc.) possono rendere necessaria una rielaborazione dei piani.

4.5.4 Business Continuity Review

Le Business Continuity Review contengono un inventario della documentazione BCM allestita dai singoli settori operativi e una valutazione della sua conformità ai criteri di esame stabiliti. È consigliabile definire criteri di esame coerenti e un chiaro processo per il monitoraggio e l'evasione dei punti in sospeso.

4.5.5 Business Continuity Tests

I test di Business Continuity servono a esaminare e verificare l'implementazione dei piani di Business Recovery e IT Disaster Recovery e l'efficacia dell'organizzazione della gestione delle crisi. Il contenuto e la frequenza dei singoli test devono essere decisi in funzione della valutazione di criticità (vedi Business Impact Analysis). L'aggregazione dei risultati dei test condotti contemporaneamente in

singole unità organizzative permette di giudicare la capacità dell'intero istituto di far fronte alle situazioni di crisi.

Si raccomanda di coordinare le singole attività di test inserendole in un piano sistematico, di prevedere una reportistica unitaria e di definire un processo di monitoraggio e rimozione delle carenze.

La pianificazione deve essere effettuata in modo tale da prevedere almeno una volta all'anno la verifica delle misure principali (incl. l'organizzazione di crisi) mediante prove pratiche o test.

4.6 Gestione delle crisi

L'obiettivo è la definizione di una struttura di gestione delle crisi che consenta all'azienda di affrontare e risolvere con efficacia le situazioni di emergenza. Nelle circostanze in cui si impongono decisioni critiche o misure e competenze decisionali che vanno oltre la normale amministrazione si ricorre all'istituzione di un'unità di crisi che assume il compito di gestire la crisi fino al ripristino della normale operatività.

È consigliabile regolare preventivamente in modo chiaro le modalità di attivazione, le responsabilità e le competenze dell'unità di crisi, adattando l'organizzazione della gestione delle crisi all'attività aziendale e alla struttura geografica dell'istituto. Occorre prestare particolare attenzione a garantire in modo ottimale la reperibilità dei responsabili designati, anche nelle situazioni di emergenza.

4.7 Reportistica, comunicazione, formazione

4.7.1 Reportistica

Le attività del BCM e lo stato degli interventi preliminari per far fronte alle crisi devono essere oggetto di rapporti redatti a cadenza periodica ai vari livelli, destinati al consiglio di amministrazione e alla direzione. In essi devono essere riportati nello specifico i risultati delle Business Continuity Review e dei test di Business Continuity.

4.7.2 Comunicazione

La comunicazione ricopre un ruolo essenziale nella gestione delle crisi. L'approntamento sistematico e accurato di modelli concettuali e piani di comunicazione (verso l'interno e verso l'esterno) nei casi di crisi esige quindi la massima cura. Occorre in special modo mantenere un grado elevato di professionalità nei confronti degli stakeholder e salvaguardare la credibilità e la fiducia nell'istituto.

I piani di comunicazione devono indicare le persone di contatto in caso di crisi (elenco con nomi e numeri di telefono di autorità di vigilanza, collaboratori, media, clienti, controparti, provider ecc.). Se la crisi assume dimensioni internazionali, è necessario che la comunicazione venga adeguata con misure speciali.

L'autorità di vigilanza deve essere debitamente informata su un'eventuale situazione di crisi o sull'istituzione di un'unità di crisi.

4.7.3 Formazione e sensibilizzazione

Deve essere garantita un'adeguata istruzione dei collaboratori, in modo che conoscano i propri compiti e le proprie responsabilità e competenze nell'ambito delle attività BCM. Occorre quindi provvedere a una formazione ad hoc dei nuovi assunti e ad aggiornamenti periodici delle conoscenze dei collaboratori in servizio. Un'attenzione particolare deve essere dedicata alla formazione dei membri dell'organizzazione di crisi.

È necessario inoltre far sì che, con l'aiuto di una costante campagna di informazione, i collaboratori vecchi e nuovi siano costantemente sensibilizzati sull'importanza del BCM.

5 Entrata in vigore

Le presenti raccomandazioni sono state emanate dal Consiglio di amministrazione dell'ASB con decisione del 24 giugno 2013 e approvate dalla FINMA in data 12 luglio 2013. Entrano in vigore il 1° ottobre 2013 e devono essere attuate entro il 30 settembre 2014. Esse sostituiscono le direttive con lo stesso titolo entrate in vigore il 1° gennaio 2008.

Basilea, 29 agosto 2013

Appendice A – Glossario

Availability Management

Procedura comprendente la definizione, l'analisi, la pianificazione, la misurazione e l'ottimizzazione di tutti gli aspetti che influiscono sulla disponibilità dei servizi informatici. L'Availability Management garantisce che l'infrastruttura IT nel suo complesso, tutti i processi, tool e compiti ecc. in ambito informatico, corrispondano ai requisiti stabiliti nei Service Level Agreement per quanto riguarda la disponibilità. Gli eventi che pregiudicano tale disponibilità possono essere controllati mediante le usuali procedure gestionali e le normali competenze decisionali.

Business Continuity Management (BCM)

Approccio gestionale su scala aziendale (policy e standard) in grado di assicurare che, al verificarsi di un evento straordinario (interno o esterno), i processi operativi critici continuino a essere svolti o vengano ripristinati tempestivamente. Il BCM comprende le fasi di pianificazione, implementazione e controlling e si estende all'intero ambito di pertinenza (settori, processi, tecniche) necessario per garantire, dopo un simile evento, la continuità dei processi operativi critici o la ripresa entro un periodo di tempo predefinito.

Business Continuity Management Strategy

Nella Business Continuity Management Strategy l'istituto stabilisce le linee di base che intende seguire per impostare il Business Continuity Management. In questo ambito rientrano anche la determinazione di un organo preposto al BCM, dei ruoli e delle responsabilità e del perimetro di pertinenza (scope) delle attività BCM.

Le decisioni in merito devono essere documentate in forma scritta.

Business Continuity Reporting

Reportistica (anche all'attenzione del consiglio di amministrazione e della direzione) sulle attività svolte nell'ambito del BCM e, in particolare, sullo stato degli interventi preliminari per far fronte alle crisi. Nel Business Continuity Reporting devono essere riportati nello specifico i risultati delle Business Continuity Review e dei Business Continuity Test.

Business Continuity Tests

Verifica sistematica a intervalli periodici dei piani di Business Continuity, soprattutto sotto il profilo della loro implementazione, efficacia e attualità.

Qualora l'azienda abbia un'organizzazione IT al suo interno è necessario testare ovviamente con regolarità anche i piani di IT Disaster Recovery.

Business Impact Analysis (BIA)

Procedura di identificazione e di misurazione (quantitativa e qualitativa) delle ripercussioni di eventuali interruzioni dell'attività aziendale o di singole risorse o singoli processi. La BIA comprende in particolare l'individuazione di processi operativi critici e delle risorse indispensabili per il Business Recovery, sulla scorta di un'analisi dei rapporti di interdipendenza e delle conseguenze di eventuali interruzioni dei processi, unita a una valutazione e classificazione dei potenziali danni.

Business Recovery

Ripristino fino a un grado prestabilito di specifici processi operativi e attività aziendali dopo un'interruzione o misure da adottare dopo un evento dannoso (vedi piani di Business Recovery). Ciò può essere realizzato in varie tappe fino alla normalizzazione dell'attività aziendale o al recupero della piena operatività.

Business Recovery Options

Definizione dei principi operativi di base per il mantenimento della normale operatività aziendale, ad esempio in caso di perdita di risorse critiche (incl. determinazione del limite di accettazione del rischio, analisi delle possibilità di azione e delle decisioni di base per la messa a disposizione di risorse sostitutive). Le Business Recovery Options si basano sulla Business Impact Analysis e costituiscono il fondamento per i piani di Business Recovery.

Business Recovery Planning

Piano preventivo circostanziato di tutte le misure (incl. check list e strumenti ausiliari) atto a garantire la continuazione dell'attività aziendale, o la ripresa tempestiva e ordinata dei processi operativi critici in caso di crisi.

Crisi

Situazione di emergenza che richiede decisioni straordinarie e che non può essere gestita con gli strumenti di direzione e le competenze decisionali ordinari.

Incidente

Evento che causa un'interruzione di comparti dell'attività aziendale, una perdita e/o una limitazione della qualità dei servizi erogati. A differenza della crisi, l'incidente può essere gestito nel ambito del processo di Availability Management.

Processi operativi critici

Processi di un'azienda la cui interruzione compromette fortemente o rende impossibile la continuazione dell'erogazione dei servizi alla clientela, l'osservanza degli obblighi legali dell'azienda e/o la gestione delle posizioni di rischio, causando un danno critico (diretto o indiretto).

Recovery Point Objective (RPO)

Periodo massimo accettabile di perdita di dati in caso di crisi.

Recovery Time Objective (RTO)

Periodo definito entro il quale i processi operativi critici e/o i servizi IT devono essere ripristinati.

Risorse critiche

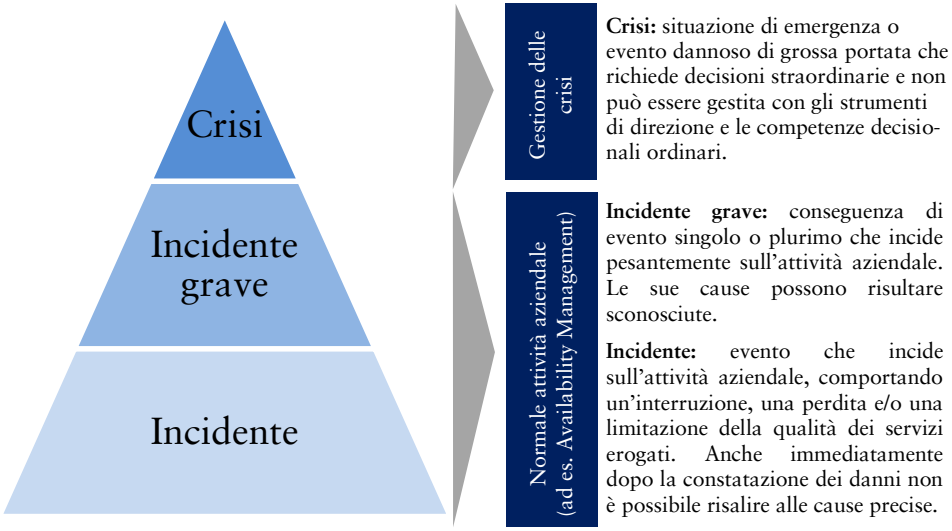
Risorse di un'azienda (personale, edifici, IT/dati, provider e fornitori esterni ecc.) che, nel caso in cui non siano più disponibili, possono comportare l'interruzione o l'arresto definitivo di processi operativi (critici). Le risorse critiche vengono identificate nel ambito della Business Impact Analysis.

Unità di crisi (detta anche Crisis Management Team (CMT) o organizzazione per la gestione delle emergenze)

Team a cui viene affidata la responsabilità di far fronte a una crisi fino al ripristino della normalità (minimizzazione dei danni economici e dei rischi di immagine).

Appendice B – Scala di gravità degli eventi

A seconda della gravità delle conseguenze risultanti da uno o più eventi, si distingue tra incidente corrente, incidente grave o crisi. Il Business Continuity Management concerne esclusivamente la prevenzione e la gestione delle crisi.



Crisi: situazione di emergenza o evento dannoso di grossa portata che richiede decisioni straordinarie e non può essere gestita con gli strumenti di direzione e le competenze decisionali ordinari.

Incidente grave: conseguenza di evento singolo o plurimo che incide pesantemente sull'attività aziendale. Le sue cause possono risultare sconosciute.

Incidente: evento che incide sull'attività aziendale, comportando un'interruzione, una perdita e/o una limitazione della qualità dei servizi erogati. Anche immediatamente dopo la constatazione dei danni non è possibile risalire alle cause precise.

Appendice C – Andamento di una crisi

Andamento di una crisi in caso di impatto del tipo «Perdita di IT/dati»

Appendice D – Fonti di approfondimento

Nell'implementazione di un Business Continuity Management interno all'azienda è possibile fare riferimento tra l'altro agli standard qui riportati. L'elenco non è esaustivo.

Australian Prudential Regulatory Authority (APRA), Prudential Standard APS 232 «Business Continuity Management» e Guidance Note 232,
www.apra.gov.au

Banca nazionale svizzera (BNS), Business Continuity nel settore finanziario svizzero, gennaio 2006 e settembre 2009,
www.snb.ch/de/iabout/finstab/id/finstab_bcp

Basel Committee on Banking Supervision (BCBS), High-Level Principles for Business Continuity, Bank for International Settlements, agosto 2006,
www.bis.org/publ/joint17.htm

British Standards Organisation, Business Continuity Management Standard, BS 25999-2:2007,
www.bsigroup.com/en/Standards-and-Publications/

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Ufficio federale tedesco per la sicurezza informatica), BSI-Standard 100-4 – Notfallmanagement (Gestione delle emergenze), 2008,
www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Business Continuity Institute, The BCI Good Practice Guidelines 2008 e 2010,
www.thebci.org/

Federal Reserve System (Fed), Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003,
www.federalreserve.gov

Financial Services Authority (FSA), Business Continuity Management Practice Guide, novembre 2006,
www.fsa.gov.uk/pubs/other/bcm_guide.pdf

Information Security Forum, Aligning Business Continuity and Information Security, marzo 2006,
www.securityforum.org

International Organization for Standardization (ISO), ISO/IEC 27031:2011: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity,
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44374

International Organization for Standardization (ISO), ISO 22301:2012: Societal security – Business continuity management systems – Requirements,
www.iso.org/iso/catalogue_detail?csnumber=50038

Ufficio federale della protezione della popolazione UFPP, analisi dei rischi e dei pericoli nell'ambito della protezione della popolazione, marzo 2011,
www.bevoelkerungsschutz.admin.ch/internet/bs/it/home/dokumente/Unterlagen_Risiken.html

Ufficio federale della sanità pubblica (UFSP), Piano pandemico – Manuale per la preparazione aziendale, novembre 2007,
www.bag.admin.ch/influenza/01120/01134/03058/04319/index.html?lang=it

Associazione Svizzera dei Banchieri
Aeschenplatz 7
Casella postale 4182
CH-4002 Basilea
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org