KeyClient Cards & Solutions
Direzione ICT

Manuale
Business Continuity Management

Versione 1.2

Pagina lasciata intenzionalmente in bianco

Indice

1 Introduzione

L'esistenza della possibilità di accadimento di eventi che potrebbero compromettere l'incolumità fisica delle persone o di eventi che, pur non compromettendo l'incolumità fisica delle persone possono causare l'interruzione dell'attività lavorativa, la complessità attuale del Business che necessita di un adeguato supporto tecnologico ed operativo, le nuove disposizioni del Comitato di Basilea sul Rischio Operativo Bancario, le disposizioni emanate da Banca d'Italia e non da ultimo, gli aspetti di sicurezza legati agli eventi accaduti negli ultimi anni, hanno dato un contributo determinante per l'avvio di un processo di verifica e adeguamento delle contromisure in essere relative a questi temi.

Key Client Cards & Solutions (Key Client) ed Help Phone si sono impegnati a sviluppare un processo articolato di Business Continuity Management (BCM) al fine di assicurare la continuità operativa dei processi essenziali.

Gli obiettivi primari del presente manuale sono :

- Definire i principi di Business Continuity Management (BCM), da cui derivano tutte le definizioni e le implementazioni trattate in tutti i manuali/documenti di Disaster Recovery (DR) e Business Continuity (BC).
- Stabilire chiare definizioni per il BC ed il DR, quali elementi costitutivi del BCM.
- Stabilire chiare definizioni per la Gestione della Crisi.
- Definire i rischi coperti dal BCM realizzato o in fase di realizzazione per l'Azienda (intesa come l'insieme delle società Key Client ed Help Phone)
- Definire una struttura che permetta a Key Client ed Help Phone di gestire la normale operatività del BCM.
- Definire una struttura che permetta a Key Client ed Help Phone di gestire incidenti non previsti.
- Definire all'interno di Key Client ed Help Phone i ruoli e le responsabilità in ambito BC e DR.
- Definire i processi di attuazione del BCM.

2 Ambito di applicabilita’

Questo manuale così come ogni altro Standard o Linee Guida collegati, sono applicabili a tutte le Direzioni o Funzioni di Key Client ed Help Phone.

E’ obbligatorio che tutti coloro che fanno parte di Key Client e di Help Phone, sia come dipendenti che consulenti, seguano le disposizioni di questo manuale così come di ogni altro Ordine di Servizio, Standard o Manuali collegati.

In aggiunta, i contenuti di questo manuale, così come di ogni Ordine di Servizio, Standard o Manuali collegati, devono essere conosciuti ed applicati da tutte le Direzioni o Funzioni di Key Client ed Help Phone nell’ambito di ogni relazione con:

- tutti i Fornitori Esterni, che forniscono a Key Client ed Help Phone, beni o servizi di qualunque natura;
- tutti i partner di Business che partecipano unitamente a Key Client ed Help Phone nella produzione ed erogazione di beni o servizi per la nostra clientela.

3 Perimetro del BCM

Il perimetro del Business Continuity Management, così come definito ed approvato negli Steering Committee BCM del 13/4/07 e del 3/9/07 prevede i seguenti scenari:

Scenari di crisi gestiti : indisponibilità di un edificio, indisponibilità del personale di un ufficio

Scenari di crisi NON gestiti : indisponibilità di entrambi (2) gli edifici di Key Client e di Help Phone, totale indisponibilità del personale di più di un ufficio

Agli scenari di BC si affiancano gli scenari di Disaster Recovery (DR)

Scenari di crisi gestiti : indisponibilità di una o più infrastrutture nei siti primari

Scenari di crisi NON gestiti : indisponibilità di entrambi le infrastrutture nei siti primari e nei siti di Recovery

La combinazione degli scenari di BC e di DR è di difficile applicabilità essendo i siti ospitanti le infrastrutture tecnologiche, diversi dagli edifici ospitanti il personale di Key Client ed Help Phone. La probabilità dell'accadimento di tale scenario è riscontrabile solo nel caso di un evento di proporzioni Continentali (Europa continentale).

Tale evento, pur essendo di scarsissima probabilità, non impatta il servizio più critico erogato da Key Client e cioè l'autorizzazione alla spesa delle carte dei titolari gestiti. Questo è possibile grazie alla possibilità di delegare detta funzionalità ai Circuiti Internazionali, (VISA, MasterCard).

4 I principi di BCM

4.1 Business Continuity Management

Per **Business Continuity Management** si intendono le azioni poste in essere dall'Azienda (intese come l'insieme delle società Key Client ed Help Phone) per garantire la continuità delle attività essenziali allo svolgimento del proprio Business, a fronte di qualunque evento che ne renda indisponibili le strutture o i servizi (edifici, impianti, attrezzature, sistemi informativi, ecc.) per un periodo di tempo prolungato.
Gli eventi che possono causare l'indisponibilità delle strutture e/o servizi e che sono contemplati in questo manuale, ricadono nelle seguenti casistiche:

- Naturali (terremoti, inondazioni, incendi, etc).
- Sociali (guerre, terrorismo, atti vandalici, etc).
- Tecnologici (servizi di fornitura elettrica, acqua, gas, infrastruttura tecnologica, immobili, etc).

Non sono quindi contemplati in questo manuale e nella pratica di Key Client e di Help Phone gli eventi che causano indisponibilità del servizio dovuti alla normale operatività quotidiana, risolvibile tramite le ordinarie procedure di ripristino (es. danni minori agli immobili ed alle infrastrutture correlate, guasti ordinari alle apparecchiature tecnologiche informatiche o alle applicazioni informatiche, etc).

Principi di base che ispirano la realizzazione del Business Continuity Management sono:

- Valutazione dei rischi operativi, allo scopo di definire la criticità dei processi correlati
- Sviluppo della resilienza delle infrastrutture, dei processi, degli stabili e delle persone a scapito di soluzioni basate sul ripristino degli stessi
- Definizione di opportune procedure per il riavvio dei processi essenziali
- Condivisione e partecipazione allo sviluppo di procedure/processi di riavvio del servizio dei Fornitori critici dell'Azienda
- Promozione e sviluppo di una cultura di BCM proattiva che:
  - faccia crescere la consapevolezza e la conoscenza del BCM in tutti i dipendenti dell'Azienda
  - assicuri il costante mantenimento e miglioramento del programma di BC e DR dell'Azienda

Requisiti minimi del Business Continuity Management sono:

- Assicurare l'adempimento delle obbligazioni contrattuali e normative relative all'esecuzione, al regolamento ed al riscontro di tutte le operazioni concluse fino al momento della crisi
- Assicurare la capacità di gestire i rischi di mercato
- Riprendere le normali attività, per i Business Critici e le funzioni di supporto entro il giorno lavorativo seguente, se non prima
- Riprendere e mantenere il più vicino possibile alla situazione di normale operatività, tutte le attività e le funzioni di supporto nel modo più veloce ed appropriato possibile

- Ristabilire la comunicazione con clienti sia interni che esterni e con le autorità di vigilanza in conformità alle prassi di mercato ed alle regole locali
- Continuare le attività di Business, così come definite dai requisiti minimi del BCM, da un'altra sede (ad esempio un altro ufficio dell'Azienda, una sede di recovery dedicata od altre sedi ove sia possibile il collegamento di tipo remoto).
- Assegnare la responsabilità ad ogni Direzione la quale deve occuparsi della riattivazione della propria operatività front to back e deve coordinarsi con ogni back office o funzione di supporto necessaria alla continuità delle attività di front office.
- Assicurare che sia definita e realizzata nelle strutture di back office e nelle funzioni di supporto una strategia appropriata, che rifletta le necessità del front office; inoltre si deve assicurare che somme adeguate siano incluse nel budget e rese disponibili per eseguire queste strategie front to back.
- Pianificare le azioni da intraprendere nel caso di perdita di una sede di uffici
- Prevedere le azioni da intraprendere nel caso di impossibilità di viaggiare in aereo ed in treno.
- Prevedere le azioni da intraprendere nel caso di blocco degli accessi stradali, nel raggio di un miglio[1] dalle zone in cui si trovano gli uffici dell'Azienda
- Separare siti di recovery ed uffici lavorativi: le centrali dati e le sedi degli uffici non devono avere la stessa rete elettrica dei siti di recovery e devono essere ad una distanza ragionevole l'una dall'altra.

Il BCM comprende sia le attività di preparazione ad eventi che possono rendere inutilizzabili le strutture o i servizi (BC e DR), che la vera e propria gestione dell' evento disastroso (Crisis Management) mediante la messa in opera delle attività precedentemente preparate.

4.2 Business Continuity

Per **Business Continuity (BC)** s'intende la predisposizione d'azioni e/o misure che assicurino la capacità di portare a termine attività essenziali di Business senza interruzioni significative, durante un periodo di indisponibilità di persone, servizi o infrastrutture di supporto quali ad esempio mancanza d'energia elettrica oppure indisponibilità di un edificio e/o persone.

4.2.1 Analisi dei processi aziendali e dei possibili impatti in caso di eventi disastrosi

La compilazione delle **Business Impact Analysis** (BIA) da parte di ogni Direzione, ha permesso di analizzare i processi di lavoro coinvolti direttamente nella gestione del cliente e del Business, individuando quelli a rischio per l'Azienda in termini di danno economico e di immagine (pagamento penali, perdita valuta, perdita di Business, insorgenza frodi, ecc.); per ognuno di questi è stato stabilito il "tempo massimo tollerabile di indisponibilità", cioè l'intervallo di tempo entro cui l'attività deve essere ripristinata per evitare l'insorgenza del danno.

[1] Pari a 1.6093 KM

La BIA analizza il rischio delle attività svolte dalle varie aree attraverso la valutazione degli impatti generati da eventi dannosi sui processi in carico ad ogni Direzione; tale esercizio permette di individuare i processi essenziali e quelli non essenziali.
La BIA contiene una stima della perdita massima che potrebbe teoricamente generarsi, una volta scaduto il tempo massimo tollerabile d'indisponibilità del servizio (a partire dal momento della dichiarazione della crisi indicato come RTO[2]), aggiungendo così ulteriori informazioni di carattere economico all'analisi di rischio.

4.2.2 Strategia della ripresa del servizio

Il concetto adottato dall'Azienda di ***mutual backup*** presso gli stabili di Direzione Generale di Key Client e di Help Phone, consente alle persone coinvolte in attività essenziali di continuare ad operare, in caso di evento straordinario, spostandosi temporaneamente sulle postazioni lasciate libere dai colleghi non coinvolti in attività/processi essenziali.
Tale soluzione, che si basa sul fatto che un evento straordinario non avvenga contemporaneamente in tutte e due gli stabili, permette di contenere i costi logistici necessari alla costituzione e alla manutenzione di postazioni di lavoro dedicate che sarebbero quindi utilizzate solo in caso d'emergenza.

4.2.3 Business Continuity Plan

Dalla definizione dei rischi da coprire, dall'analisi degli impatti economici sui processi di Business e dalla definizione della strategia di ripresa del servizio, discende il **Business Continuity Plan** (Piano di Continuità del Business) di seguito BCP. La gestione del BC è supportata dall'attuazione dell'insieme di procedure operative che sono appunto denominate **Business Continuity Plan** (il piano di sostituzione delle persone indisponibili per l'effetto di eventi quali ad esempio, malattie, rapimenti, isolamento di zone, atti terroristici, è parte integrante della gestione della BC).

I piani di BC contengono tutte le informazioni necessarie alla gestione delle conseguenze di tali eventi all'interno delle linee di Business di riferimento, usando misure, applicazioni e/o siti di recovery alternativi.

La documentazione del BCP è divisa in due parti:
- una descrittiva in cui sono indicati le linee guida, i ruoli e le regole per l'attuazione del BCP); i principali argomenti trattati sono:
  - continuità dei processi essenziali
  - ruoli coinvolti nel piano di continuità del Business
  - tipologie di situazioni lavorative
  - attuazione del BCP (comportamento e procedure organizzative di ripartenza dell'attività lavorativa) in caso di crisi

[2] **RTO**: Recovery Time Objective; è' il requisito di "tempo massimo d'indisponibilità" di un servizio/processo, intendendosi l'intervallo di tempo limite, a partire dalla dichiarazione di crisi a seguito dell'evento dannoso, oltrepassato il quale si incorre in un grave danno economico o di immagine per l'Azienda.

- una numerica-nominativa in cui sono riportati il piano operativo di mutual backup del personale dell'Azienda con i valori quantitativi (es: uffici per edificio, n.ro di risorse per ufficio, task force minima con cui ripartire, uffici di backup, ecc.) e le liste nominative dei team di persone con specifici compiti nel BCP.

Il BCP **non si sostituisce** ai Piani d'Evacuazione, ma ne è strettamente correlato;
Il piano d'evacuazione, infatti, indica le modalità di abbandono degli uffici in caso di emergenza[3], mentre il piano di BC definisce tempi e modalità di ripartenza delle attività lavorative, e quindi indica il comportamento da assumere in caso di inagibilità delle strutture del edificio in cui viene svolta l'attività lavorativa.

Fanno parte del piano di Business Continuità anche i Fornitori esterni dell'Azienda, per i quali devono essere valutate le capacità di ripristino del servizio in caso di eventi disastrosi che affliggono la propria struttura nonché la capacità di seguire il BCM dell'Azienda in caso d'evento disastroso che affligga quest'ultima.

4.3 Disaster Recovery

Il **Disaster Recovery (DR)** è definito come la capacità di far ripartire funzioni essenziali di Business in seguito alla perdita o all'indisponibilità di un servizio di tipo tecnico (es. Rete di telecomunicazione, Calcolatore centrale – mainframe- o periferici –midrange, infrastruttura di edificio – energia elettrica, impianti principali- o di edificio)

Il DR discende direttamente dalle definizioni espresse nella BIA di riferimento, rispetto al RTO(Recovery Time Objective) di ogni processo.

L'RTO è l'obiettivo in termini di tempo che ci si prefigge di rispettare per il ripristino di un processo interrotto per cause derivanti da un evento disastroso.

L'RTO parte dal momento in cui viene dichiarata la crisi e quindi dall'acclarata necessità di attivare la procedura di Disaster Recovery.

L'RTO e definito sia nella BIA che nella Ramm (Key Client risk assessment management methodology. Cfr sezione Deliverable). Nella Ramm l'RTO è definito nel parametro AI11 del foglio BCQ availability.

Nella Ramm è espresso anche il tempo di ripristino dell'applicazione in situazioni di operatività quotidiana (parametro AI3 del foglio BCQ availability) che però nulla ha a che vedere con il Disaster Recovery.

Attraverso la compilazione del parametro RTO nella BIA, le Direzioni responsabili del processo, esprimono una specifica richiesta alla Direzione ICT e/o alla Funzione Servizi Generali Immobili e Logistica (SGIL) della Direzione Amministrativa per l'implementazione di una soluzione di DR congruente con quanto richiesto.

[3] Le **procedure di evacuazione** sono predisposte ed aggiornate dalla Funzione Servizi Generali, Immobili e Logistica (SGIL) della Direzione Amministrativa, nell'ambito delle competenze ad esso attribuite in materia di sicurezza e di salute sul luogo di lavoro (D. Lgs. N. 626/94)

E' compito della Direzione ICT e/o della Funzione Servizi Generali, Immobili e Logistica (SGIL) definire e proporre alle Direzioni una soluzione in linea con quanto richiesto. Le Direzioni dovranno approvare la proposta e fornire le risorse necessarie a consentire il completamento dell'implementazione.

La gestione del DR è supportata dall'attuazione dell'insieme di procedure operative che sono denominate Disaster Recovery Plan (Piano di ripristino dal disastro), di seguito DRP.

Il DRP definisce le azioni che devono essere intraprese dalla Direzione ICT e/o dalla SGIL o dai Fornitori Esterni al fine di garantire la capacità di riavvio del servizio dell'Azienda in situazioni critiche dovute a problemi di tipo tecnico od infrastrutturale. I DRP contengono tutte le informazioni necessarie a gestire il riavvio dei servizi di tipo tecnico, p.e. sistemi informativi utilizzati dalle Direzioni, elementi di infrastrutture tecniche ed attrezzature immobiliari, sia mediante duplicazione, o con altri mezzi, nel caso di indisponibilità di un servizio primario o di una sede.

Ogni infrastruttura o insieme omogeneo d'infrastrutture sia tecnologiche che immobili, ha un DRP associato.

Il DRP contiene una serie di soluzioni che garantiscono la possibilità di utilizzare componenti ed applicazioni IT in modo alternativo in caso di incidenti, o di utilizzare infrastrutture immobili(intese come edificio ospitante le persone dell'Azienda) o tecnologiche alternative in caso di inagibilità. I DRP inoltre contengono le procedure da attuare per il ripristino della situazione normale precedente l'emergenza.

Per la trattazione specifica dei temi riguardanti le modalità di attivazione dei DRP della loro esecuzione e della loro manutenzione, si rimanda agli specifici manuali riportati nel sito intranet di Key Client

4.4 Gestione della Crisi

La predisposizione delle azioni e delle misure per garantire la capacità di portare a termine attività essenziali di Business senza interruzione significative durante un periodo di indisponibilità di servizi o infrastrutture definite nei BCP e nei DRP, trovano attuazione durante un evento disastroso, definito di crisi.

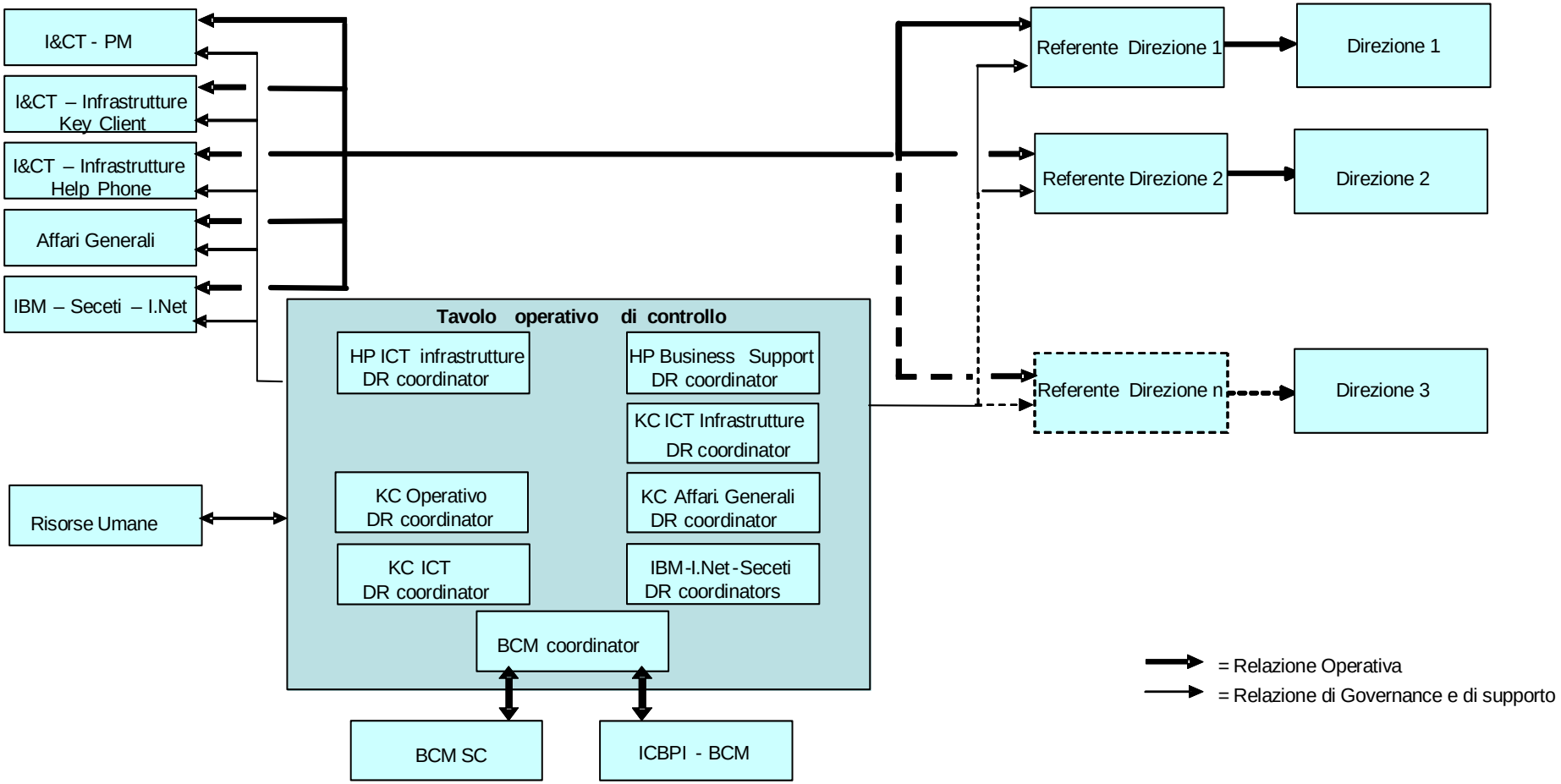
Sono previsti approcci di gestione differenziati per la crisi di Key Client e per la crisi di Help Phone.

Si rimanda al manuale specifico di gestione della crisi di Key Client e di Help Phone per tutti i dettagli.

5 Struttura organizzativa della gestione quotidiana del BCM

I ruoli e le responsabilità dei soggetti descritti nello schema sotto riportato, sono ampiamente definiti nel capitolo successivo.

Lo schema non riporta tutti i ruoli coinvolti nel BCM, ma si focalizza su quelli maggiormente coinvolti. Il capitolo successivo descrive in maniera esaustiva tutti i ruoli coinvolti e le loro responsabilità.


I&CT - PM
I&CT – Infrastrutture Key Client
I&CT – Infrastrutture Help Phone
Affari Generali
IBM – Seceti – I.Net
Risorse Umane
Tavolo operativo di controllo
HP ICT infrastrutture DR coordinator
HP Business Support DR coordinator
KC ICT Infrastrutture DR coordinator
KC Operativo DR coordinator
KC Affari Generali DR coordinator
KC ICT DR coordinator
IBM-I.Net-Seceti DR coordinators
BCM coordinator
BCM SC
ICBPI - BCM
Referente Direzione 1
Direzione 1
Referente Direzione 2
Direzione 2
Referente Direzione n
Direzione 3
= Relazione Operativa
= Relazione di Governance e di supporto

6 Ruoli

La gestione operativa del processo di BCM prevede tre categorie principali di ruoli, ognuno con specifiche responsabilità.

6.1 Governo e coordinamento

A questa categoria appartengono i ruoli che concorrono alla definizione delle policies e degli standard di BCM, alla loro divulgazione ed alla verifica della loro applicazione costante e continua.

I ruoli appartenenti a questa categoria sono :

Ruolo	**Descrizione**
Senior Managers	Direttori Generali di Key Client ed Help Phone. Direttori delle Direzioni di Key Client
BCM Steering Committee	Comitato guida BCM – costituito dai Direttori delle Direzioni
BCM Manager	Responsabile BCM
S.G. DR co-ordinator	Direzione Amministrativa - rappresentante dei Servizi Generali con conoscenze degli Immobili dell'azienda e delle infrastrutture correlate
KC ICT DR co-ordinator	Direzione ICT – rappresentante dell'ICT con sufficienti conoscenze dell'intero parco applicativo informatico
KC ICT Infrastrutture DR co-ordinator	Direzione ICT – rappresentante dell'ICT con sufficienti conoscenze dell'intera infrastruttura informatica
Fornitore DR co-ordinator	Rappresentanti dei principali Fornitori di servizi Infrastrutturali con conoscenze della propria infrastruttura
KC Operativo DR co-ordinator	Direzione Operativa - rappresentante con conoscenze dei principali processi Aziendali di Key Client
HP B.S. DR co-ordinator	Help Phone Business Support - rappresentante con conoscenze dei principali processi Aziendali di Help Phone
HP Infrastrutture DR co-ordinator	Help Phone ICT – rappresentante dell'ICT con sufficienti conoscenze dell'intero parco applicativo ed infrastrutturale di Help Phone

T.O.C.	Tavolo Operativo Continuità costituito dai DR co-ordinators e dal BCM Manager. I DR co-ordinators dei Fornitori sono chiamati a partecipare al Tavolo quando necessario

6.2 Realizzazione e Manutenzione

A questa categoria appartengono i ruoli che concorrono alla realizzazione "sul campo" degli standard e delle policies di BCM ed alla loro manutenzione costante e continua.

I ruoli appartenenti a questa categoria sono :

Ruolo	**Descrizione**
Referente di Direzione	Referente BCM per ogni Direzione di Key Client e di Help Phone
BCP Owner	Business Continuity Plan Owner
Referente Per Edificio	Referente di edificio di Key Client e di Help Phone
KC ICT PM	Information Technology Product Manager
KC ICT Infrastrutture	Information Technology Infrastructure Product Manager
Servizi Generali - Immobili	Referente dei Servizi Generali con competenze sulla gestione degli Immobili

A questi si aggiungono, con funzioni di supporto i seguenti principali ruoli[4]

Ruolo	**Descrizione**
RU	Risorse Umane
Servizi Generali - Logistica	Settore dei Servizi Generali con competenze sulla gestione degli Acquisti

[4] Altre funzioni possono essere coinvolte in base a specifiche esigenze.

6.3 Esecuzione

In questa categoria rientrano tutti i dipendenti di Key Client e di Help Phone e quindi le diverse strutture organizzative, in quanto esecutori dei BCP e dei DRP al verificarsi di eventi che causano l'interruzione dell'attività lavorativa.
A questi si aggiungono gli altri ruoli delle tipologie di "Governo e Coordinamento", di "Realizzazione e Manutenzione".

Le attività di competenza di questi ruoli in caso d'emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone"

7 Responsabilità

La gestione operativa del processo di BCM prevede specifiche responsabilità per ogni ruolo allo scopo di garantire sia la continuità delle attività essenziali dell'Azienda in caso di specifica emergenza, sia il costante aggiornamento delle procedure (revisione/inserimento di attività essenziali, spostamenti di personale, aggiornamento dei nominativi, ecc.).

7.1 Governo e Coordinamento

A questa categoria appartengono i ruoli di seguito descritti. Per ogni ruolo sono riportate le principali responsabilità assegnate

7.1.1 Senior Managers

I Senior Managers sono i Direttori Generali di Key Client ed Help Phone ed i Direttori delle Direzioni Key Client.

Le responsabilità specifiche dei Senior Managers prevedono:

- assicurare la continuità delle operazioni e la disponibilità delle funzioni di Business;
- assicurare che il BCM sia implementato e finanziato in modo adeguato al fine di gestire e ridurre il rischio operativo del Gruppo, inclusa la minimizzazione di conseguenti effetti negativi sulla posizione legale del gruppo;
- assicurare il rispetto delle disposizioni regolamentari riferite al BCM;
- delegare allo Steering Committee BCM il ruolo di organo di governo interno.

7.1.2 BCM Steering Committee

Le principali responsabilità del BCM Steering Committee sono:

- verificare l'implementazione locale della Policy di BCM con le relative procedure e standard di supporto;
- facilitare l'attivazione del BCM e identificare i necessari finanziamenti;
- valutare la fattibilità di iniziative/programmi del BCM e richiedere azioni correttive o miglioramenti ove necessario;
- assicurare la nomina dei Crisis Managers, che sono autorizzati ad agire in caso di dichiarazione di stato di crisi;
- riportare ai Senior Managers lo stato e gli eventuali problemi più importanti in materia di BCM

Il BCM Steering Committee è parte è composto dai Direttori delle Direzioni di Key Client e di Help Phone, o da loro delegati con appropriato potere decisionale;

7.1.3 Business Continuity Manager

L'obiettivo principale del BCM Manager è quello di assistere le Direzioni nel garantire la continuità delle attività essenziali della Azienda assicurando la costante applicazione del Business Continuity Plan.
Il BCM Manager riporta gerarchicamente alla Direzione ICT

Le principali responsabilità del B.C.M. Manager durante la gestione quotidiana sono:

- assicurare la conformità con la Policy di BCM e con gli standard e linee guida collegati;
- mantenere aggiornato il Business Continuity Plan interagendo sia con i Referenti delle Direzioni, sia con i referenti dei Servizi Generali competenti in materia di gestione Immobili ed Acquisti, nonché con il Referente della gestione Risorse Umane
- verificare periodicamente la bontà delle procedure di Business Continuity e di Disaster Recovery richiedendo alle varie Direzioni di completare i test e le simulazioni come previsto dal piano predisposto;
- definire e comunicare le Policies, le Linee Guida e gli Standard
- verificare lo stato di avanzamento delle attività (scorecards), tenendo informato l'ufficio BCM della CapoGruppo
- co-ordinare le interdipendenze cross-Business;
- controllare l'esecuzione dei test;
- coordinare la revisione continua del BCM e il regolare aggiornamento del sito intranet;
- coinvolgere il personale in specifiche attività di formazione e di simulazione;
- sviluppare sistemi di misurazione del rischio e meccanismi di raccolta dei dati;
- fornire indicazioni alle Direzioni ed alle Funzioni che gestiscono le infrastrutture per lo sviluppo ed implementazione delle proprie strategie.
- riportare periodicamente al BCM Steering Committee sullo stato e sulle iniziative necessarie per adeguare il programma alle Policy / Standard

Le attività di competenza del BCM Manager in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.1.4 Disaster Recovery co-ordinators (DRC)

I DR co-ordinators vengono nominati dalle proprie Direzioni per operare sia durante la gestione quotidiana del BCM che in caso d'emergenza.

La Direzione KC ICT nomina i DR co-ordinators ICT ed Infrastrutture
La Direzione Operativa nomina il DR co-ordinator Operativo
La Direzione di Help Phone nomina i DR co-ordinators Infrastrutture e Business Support

Le principali responsabilità dei DR co-ordinators durante la gestione quotidiana del BCM sono:

- presidiare, nell'ambito del Disaster Recovery, le Policy di Gruppo e le normative emesse da Banca d'Italia e derivanti da Basilea 2 e da tutti gli altri enti di controllo normativo di riferimento curandone l'applicazione in ambito locale anche mediante l'emanazione di procedure;
- verificare la validità e congruenza dei DRP predisposti dall'IT Product Manager dell'ICT e dai Servizi Generali Immobili
- gestire le richieste di esecuzione di attività di tipo progettuale;
- coordinare i Test di DR;
- comunicare regolarmente con le corrispondenti strutture globali per verificare la congruenza delle procedure in essere con le disposizioni emanate centralmente.

Le attività di competenza dei DR co-ordinators in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.1.4.1 KC ICT DR co-ordinator

Oltre alle già citate responsabilità, le altre principali specifiche responsabilità del KC DR co-ordinator ICT durante la gestione quotidiana del BCM sono:

- supportare gli ICT PM nell'identificazione e mitigazione di qualsiasi rischio di tipo applicativo che possa ostacolare il recovery;
- assieme agli ICT PM ed alle Direzioni, creare e mantenere un archivio centrale delle applicazioni che evidenzi le criticità, le priorità di recovery ed il tempo di recovery, se testato o documentato;
- assieme all'ICT DR co-ordinator fornire gli indirizzi strategici agli ICT PM ed ai DR co-ordinators dei Fornitori, per quanto riguarda gli aspetti di infrastruttura IT delle diverse opzioni riguardanti il Disaster Recovery.

7.1.4.2 KC ed HP ICT Infrastrutture DR co-ordinators

Oltre alle già citate responsabilità, le altre principali specifiche responsabilità dei KC ed HP ICT Infrastrutture DR co-ordinators durante la gestione quotidiana del BCM sono:

- supportare i Referenti DR dei Fornitori nell'identificazione e mitigazione di qualsiasi rischio di tipo infrastrutturale IT che possa ostacolare il recovery;
- assieme ai Referenti DR dei Fornitori, agli ICT PM ed ai Referenti delle Direzioni, creare e mantenere un archivio centrale delle infrastrutture IT che evidenzi le criticità, le priorità di recovery ed il tempo di recovery, se testato o documentato;
- assieme al KC DR co-ordinator ICT fornire gli indirizzi strategici agli ICT PM ed ai Referenti DR dei Fornitori, per quanto riguarda gli aspetti di infrastruttura IT delle diverse opzioni riguardanti il Disaster Recovery;
- fornire indirizzo strategico ed eseguire analisi costi/benefici assieme al KC DR co-ordinator Servizi Generali, per quanto riguarda gli aspetti di infrastruttura IT delle diverse opzioni riguardanti i siti di mutual backup;

- gestire l'infrastruttura IT, provvedere e fornire un costante mantenimento dei siti di mutual backup in linea con le mutevoli esigenze del Business.

7.1.4.3 Fornitori DR co-ordinators

Le principali responsabilità dei DR co-ordinators dei Fornitori durante la gestione quotidiana del BCM sono:

- supportare i Referenti DR di KC ed HP nell'identificazione e mitigazione di qualsiasi rischio di tipo infrastrutturale IT che possa ostacolare il recovery;
- assieme ai Referenti DR di KC ed HP, agli ICT PM, creare e mantenere un archivio centrale delle infrastrutture IT che evidenzi le criticità, le priorità di recovery ed il tempo di recovery, se testato o documentato;
- ricevere gli indirizzi strategici dai referenti DR KC ed HP , per quanto riguarda gli aspetti di infrastruttura IT delle diverse opzioni riguardanti il Disaster Recovery;
- partecipare all'analisi costi/benefici per quanto riguarda gli aspetti di infrastruttura IT delle diverse opzioni riguardanti i siti di mutual backup;
- gestire l'infrastruttura IT, provvedere e fornire un costante mantenimento dei siti di mutual backup in linea con le mutevoli esigenze del Business, secondo le specifiche e gli accordi presi con Key Client ed Help Phone.
- Supportare l'esecuzione dei test di DR

7.1.4.4 KC DR co-ordinator Servizi Generali

Oltre alle già citate responsabilità, le altre principali specifiche responsabilità del DR co-ordinator dei Servizi Generali – Immobili durante la gestione quotidiana del BCM sono:

- supportare la Direzione Amministrativa nel definire le linee guida strategiche e nell'eseguire analisi costi/benefici per quanto riguarda gli aspetti di propria competenza, delle diverse di opzioni riguardanti il sito di mutual backup;
- supportare la Direzione Amministrativa nella gestione delle infrastrutture degli edifici e la fornitura di servizi e nel provvedere al costante mantenimento del sito di recovery;
- supportare la Direzione Amministrativa nell'identificazione di ogni rischio relativo alle infrastrutture ed ai servizi degli edifici che possa impedire il recovery informando, ove opportuno, le strutture interessate.

7.1.4.5 KC DR co-ordinator Operativo

Le principali responsabilità del KC DR co-ordinator Operativo durante la gestione quotidiana del BCM sono:

- comunicare al BCM Manager ogni variazione della documentazione e nell'organizzazione di Key Client;
- Coordinare l'esecuzione del test di DR delle Direzioni KC.

7.1.4.6 HP DR co-ordinator Business Support

Le principali responsabilità dell'HP DR co-ordinator Business Support durante la gestione quotidiana del BCM sono:

- comunicare al BCM Manager ogni variazione della documentazione e nell'organizzazione di Help Phone;
- Coordinare l'esecuzione del test di DR di Help Phone.

7.1.5 Tavolo Operativo della Continuità (DR co-ordinators e BCM Manager)

Il Tavolo Operativo della Continuità è composto dai DR co-ordinators KC ICT, ICT Infrastrutture, Operativo, Servizi Generali, HP ICT Infrastrutture, HP Business Support e dal BCM Manager. In relazione alle strutture interessate, possono partecipare al Tavolo Operativo di Controllo anche i citati DR co-ordinator dei Fornitori, nonché i rappresentanti delle Risorse Umane e dei Servizi Generali Acquisti. Le responsabilità del Tavolo Operativo di Controllo sono il risultato del raggruppamento delle responsabilità di ogni DR co-ordinator, con l'obiettivo di :

- presidiare le Policy eventualmente emanate dalla CapoGruppo;
- presidiare le normative emesse da Banca d'Italia e derivanti da Basilea 2 e da tutti gli altri enti di controllo normativo di riferimento;
- traslare le Policy e le normative in ambito locale;
- emanare regole e procedure da seguire mediante circolari o altri mezzi di comunicazione appropriati (e-mail);
- gestire le richieste di esecuzione di attività di tipo progettuale;
- controllare la corretta applicazione delle eventuali Policy e delle Normative emesse dalla CapoGruppo e da enti esterni (es VISA, MasterCard)
- facilitare e stimolare l'esecuzione periodica dei test.

Le attività di competenza del TOC in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.2 Esecuzione e Manutenzione

A questa categoria appartengono i ruoli di seguito descritti. Per ogni ruolo sono riportate le principali responsabilità assegnate.

7.2.1 Direzioni

Le principali responsabilità delle Direzioni durante la gestione quotidiana del BCM sono:

- nominare un Referente del Business continuity ;
- assicurare la disponibilità degli strumenti e dei piani di Business continuity per le proprie linee di Business/funzioni “front to back”;
- definire la strategia e le esigenze di recovery, inclusa la definizione e l’assegnazione di priorità dei processi essenziali, delle applicazioni e dei dati per il proprio Business/funzioni “front to back”;
- assicurare che tutto ciò sia implementato con documentazione, definizione dei requisiti IT, effettuazione dei test ed attività di reporting;
- mantenere la prontezza di intervento al mutare delle esigenze del Business;
- assicurare che ogni cambiamento nelle esigenze del Business sia comunicato ali BCM Manager, perché questi possa attivarsi per la propria parte di competenza;
- assicurare che i fondi necessari siano inclusi nel budget e siano messi a disposizione di tutte le strutture, sia di front office che di back office e da ogni funzione di supporto, per garantire la conformità con questa Policy e con gli standard di Disaster Recovery, così come ogni altro standard o linee guida collegati;
- assicurare che per ogni nuovo processo da sviluppare all’interno della propria area venga eseguita la Business Impact Analysis a seguito della quale, se del caso, vengano richieste/attivate le opportune implementazioni di BCP e DRP.

Le attività di competenza delle Direzioni in caso di emergenza sono descritte nel “Manuale di Gestione della Crisi per Key Client e per Help Phone”.

7.2.2 Referente di Direzione

È previsto che ogni Direzione abbia un referente per il BCP, con la responsabilità della definizione e della manutenzione delle informazioni relative alla propria area di Business (processi essenziali, task force minima con cui ripartire, tempi di ripartenza, liste nominative, ecc.). Le principali responsabilità del Referente di Direzione durante la gestione quotidiana del BCM sono:

- revisionare periodicamente le informazioni contenute nelle BIA ed i relativi Piani di Business Continuity (BCP) della propria area di Business (processi essenziali, task force minima con cui ripartire, tempi di ripartenza, liste nominative, ecc.);
- Fornire chiari requisiti ed informazioni agli ICT PM ed ai Servizi Generali in termini di BCM e Disaster Recovery per lo sviluppo di nuovi progetti/funzioni e per il loro mantenimento.

- interagire con il BCM Manager per segnalare qualunque variazione nella propria area di competenza;
- organizzare e svolgere il test del BCM per le aree di propria competenza e provvedere o farsi promotore delle correzioni delle eventuali non aderenze rilevate;
- assicurare che per ogni nuovo processo da sviluppare all'interno della propria area venga eseguita la Business Impact Analysis a seguito della quale, se del caso, vengano richieste/attivate le opportune implementazioni di BCP e DRP.

L'elenco dei Referenti di Direzione è riportato in allegato A.

Le attività di competenza del Referente di Direzione in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.2.3 Servizi Generali - Immobili

Le principali responsabilità della Funzione Servizi Generali – Immobili durante la gestione quotidiana del BCM sono:

- identificare e mitigare qualsiasi rischio legato alle facilities (Immobili ed infrastrutture correlate) di Key Client e di Help Phone che possa ostacolare il recovery e riferire tali rischi al KC DR co-ordinator Servizi Generali per la definizione delle necessarie attività di rimedio, ed al BCM Manager;
- fornire indirizzo strategico ed eseguire analisi costi/benefici assieme agli ICT PM, per quanto riguarda gli aspetti legati alle facilities dei i siti di mutual backup;
- eseguire i test di DR delle facilities;
- assicurare che l'archivio dei dati sugli stabili e sulle facilities sia aggiornato con tutte le informazioni rilevanti.

Le attività di competenza del Referente di Direzione in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.2.4 Information & Communication Technology Product Manager (ICT PM)

Le principali responsabilità dell'Information & Communication Technology Product Manager durante la gestione quotidiana del BCM sono:

- assistere le Direzioni nell'identificare e nello stabilire i tempi ed i costi di recovery di tutte le applicazioni critiche;
- assicurare che tutte le applicazioni critiche siano recuperabili entro i tempi richiesti dalle Direzioni;
- implementare, testare e mantenere i piani di recovery in accordo con le esigenze delle Direzioni, mantenendoli in linea con l'ambiente di produzione normale e le mutevoli esigenze delle Direzioni;
- assicurare che l'archivio delle applicazioni sia aggiornato con tutte le informazioni rilevanti;

- identificare e ridurre qualsiasi rischio di recovery delle applicazioni e riportare tali rischi alle Direzioni di riferimento per la definizione delle necessarie attività di rimedio;
- eseguire i test di DR delle Infrastrutture IT.

Le attività di competenza dell' ICT PM in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone" .

7.2.5 Business Continuity Plan Owner (B.C.P. Owner)

Viene nominato per ogni ufficio/Funzione in cui è divisa ogni Direzione; nel caso in cui l'ufficio/Funzione sia dislocata in differenti piani dello stesso edificio, o in differenti edifici, viene nominato un BCP Owner per ogni piano/edificio.

Le principali responsabilità del BCP Owner durante la gestione quotidiana del BCM sono:

- svolgere il test del BCM per le aree di propria competenza;
- riportare al Referenti di Direzione le eventuali non aderenze riscontrate durante il Test per le opportune successive correzioni.

Le attività di competenza del Referente di Direzione in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

L'elenco dei BCP Owners e BCP Owners Deputy è riportato in allegato B.

7.2.6 Referente per edificio

Viene nominato un Referente per l'edificio di Key Client ed uno per quello di Help Phone

Le principali responsabilità del Referente per l'Edificio durante la gestione quotidiana del BCM sono:

- svolgere il test del BCM per le aree di propria competenza;
- riportare al KC Servizi Generali DR co-ordinator ed al BCM Manager le eventuali non aderenze riscontrate durante il Test per le opportune successive correzioni.

Le attività di competenza del Referente per l'Edificio in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

L'elenco dei Referenti per Edificio e dei relativi Deputy è riportato in allegato C.

7.2.7 Servizi Generali - Acquisti

Le principali responsabilità della Funzione Servizi Generali - Acquisti durante la gestione quotidiana del BCM sono:

- assicurare che ogni negoziazione con fornitori esterni avvenga in conformità con gli obiettivi di questa policy o di qualsiasi altro standard o linee guida collegati e che, ove possibile, sia inserito in ogni contratto o SLA;
- predisporre la disponibilità dei dati relativi ai fornitori critici;
- pianificare la collaborazione con i fornitori critici in preparazione dei casi d'emergenza.

Le attività di in carico al Referente di Direzione in caso di emergenza sono descritte nel "Manuale di Gestione della Crisi per Key Client e per Help Phone".

7.2.8 Comunicazioni con la Stampa

In caso di dichiarazione dello stato di crisi i mezzi d'informazione potrebbero essere coinvolti nell'aggiornamento dell'opinione pubblica sugli accadimenti.

Sarà cura esclusiva del Top Management dell'Azienda, mantenere i rapporti con la stampa e dare le informazioni necessarie ad assicurare la clientela sul superamento del momento di crisi.

Il personale deve quindi astenersi dal rilasciare dichiarazioni alla stampa, invitando i giornalisti a rivolgersi agli organi competenti.

7.2.9 Risorse Umane

Le Risorse Umane collaborano col il BCM Manager e con il TOC durante durante la gestione quotidiana del BCM per:

- predisporre la disponibilità dei dati relativi ai dipendenti e ove disponibili dei familiari, al fine di facilitarne il contatto;
- pianificare la predisposizione di una helpline/ ufficio informazioni per i dipendenti ed i familiari;
- pianificare la collaborazione con i servizi d'emergenza nei casi di irreperibilità di dipendenti;
- pianificare la disponibilità di forze lavorative nel caso di indisponibilità dei dipendenti;
- pianificare la disponibilità di adeguati livelli di assistenza al personale

7.2.10 Tutti i dipendenti dell'Azienda

Sono tenuti ad attenersi alle disposizioni del Business Continuity Management ed a conoscere (rilevandolo dal manuale di Business Continuity Plan riportato nell'apposito sito intranet) :

- se l'ufficio di appartenenza svolge o meno attività essenziali alla continuità del Business;
- il nominativo di riferimento (B.C.P. Owner/B.C.P. Owner Deputy) in caso di dichiarazione dello stato di crisi del proprio ufficio;
- il numero di persone minimo e i tempi di ripartenza necessari per riattivare le attività nell'edificio di backup;
- l'edificio di backup per il proprio ufficio;
- le procedure di evacuazione del proprio edificio.

8 Gestione operativa del BCM

La gestione del processo di BCM si svolge in tre momenti distinti:

- Realizzazione del processo
- Manutenzione continua del processo
- Gestione dello stato di crisi

A tali momenti corrispondono attività e responsabilità, di seguito meglio specificate, diversificate tra Business Continuity e Disaster Recovery.

Il BCM Manager garantisce in quest'ambito il coordinamento generale del progetto al fine di garantire unità di intenti e razionalità nell'esecuzione del progetto.

8.1 Realizzazione del BCM

La fase di realizzazione del BCM prevede tre diversi livelli operativi con diversi attori coinvolti, a seconda che si tratti di attività di BC o di DR.

1) Governance

L'attività di Governance (primo livello) è in capo al BCM Steering Committee; i cui compiti primari, come riportato precedentemente, sono relativi alla valutazione delle soluzioni proposte, definizione delle priorità di intervento, approvazione delle proposte presentate.

2) Coordinamento Operativo

La Gestione Operativa del Progetto del BCM è in capo ai Referenti delle Direzioni per quanto riguarda il BC (supportati dal BCM Manager), mentre per quanto riguarda il DR è in capo agli ICT PM ed ai Fornitori coadiuvati dall' ICT DR co-ordinator e dall' ICT DR co-ordinator Infrastrutture..

3) Esecuzione

Business Continuity e Disaster Recovery danno origine ad una serie di prodotti differenti.

8.1.1 Business Continuity

Le attività connesse al Business Continuity sono svolte dalle Direzioni; i Referenti di Direzione hanno il compito di fornire al BCM Manager le **BIA** complete per il/i Business di cui sono referenti; le BIA sono poi utilizzate dal BCM Manager per redigere i **Piani di Business Continuity** (Business Continuity Plan) che poi vengono pubblicati sul sito intranet BCM.

In aggiunta, i Referenti di Direzione devono segnalare qualunque variazione dell'attività lavorativa per revisionare periodicamente le informazioni contenute nelle BIA e nei BCP della

propria area di Business (processi essenziali, task force minima con cui ripartire, tempi di ripartenza, liste nominative, ecc.).

Questa attività è di fondamentale importanza, in quanto una BIA ed un BCP aggiornati consentono all'ufficio di operare ed eseguire le attività giudicate essenziali in caso di emergenza. In mancanza di BIA e BCP aggiornati vi è il rischio da parte dell'ufficio di non poter ripartire in modo corretto; la responsabilità di BIA e Piani di Business Continuity aggiornati è in capo alle Direzioni.

8.1.2 Disaster Recovery

La definizione ed implementazione dei piani di DR sono in carico agli ICT PM ed ai Fornitori, ed è coordinata dai Disaster Recovery co-ordinators ICT ed ICT Infrastrutture

Il tipo d'implementazione di DR è dipendente dal requisito di ripartenza (RTO) espresso nella BIA.

E' compito degli ICT PM supportati dei Fornitori, fornire ai Referenti di Direzione la proposta di soluzione più aderente possibile alla richiesta.

Sarà compito del Referente di Direzione accettare o meno la proposta.

Nei casi in cui la soluzione di DR da implementare non sia aderente alla richiesta o non venga implementata alcuna soluzione di Disaster Recovery su specifica richiesta del Referente di Direzione, questi deve produrre una Risk Acceptance.

I DR co-ordinators devono assicurare la coerenza e correttezza dei piani che devono contenere tutte le informazioni ed indicazioni necessarie per garantire il riavvio di servizi essenziali di tipo tecnico ed infrastrutturale.

I piani di DR dovranno essere sempre aggiornati; in particolare in caso di modifiche sostanziali di tipo tecnico ed infrastrutturale, dovranno essere modificati per assicurare una costante copertura di eventi che possono fermare funzioni essenziali di Business a causa dell'indisponibilità di servizi di tipo tecnico/infrastrutturale.

8.1.3 Deliverables

I deliverables del BCM sono:

BIA (Business Impact Analysis): ogni Direzione redige la BIA relativa ai processi gestiti. La BIA è un documento che riporta la mappatura Ufficio / Immobile / Processo / Applicazione / Infrastruttura Tecnologica.
Per ogni Ufficio è indicato l'Immobile in cui questo opera ed i Processi gestiti.
Ogni Processo è valutato essenziale o non essenziale in funzione del potenziale danno economico in cui si incorrerebbe in caso di evento disastroso (che coinvolga persone, tecnologia, immobili) fino al suo riavvio.

In caso d'indisponibilità dell'immobile, è stabilito il numero di persone da ricollocare nella nuova sede entro un intervallo di tempo definito. E' individuata anche l'ubicazione dove le persone devono essere ricollocate (Mutual Backup).
In caso d'indisponibilità delle persone, è stabilito il numero minimo di persone con cui far ripartire il processo.
Per i casi di cui sopra e per il caso d'indisponibilità tecnologica è indicato il tempo massimo d'indisponibilità del processo oltre il quale potrebbe manifestarsi un danno economico. Questo tempo è denominato Recovery Time Objective (RTO) ed è l'elemento che discrimina se e quale tipo di Recovery deve essere implementato.
Per ogni processo sono definite le applicazioni informatiche a questo correlate.
Per ogni applicazione è riportata la piattaforma tecnologica su cui questa opera.

Il Referente di Direzione è responsabile della redazione, manutenzione ed aggiornamento della BIA.

BCP Business Continuity Plans: riportano nel dettaglio le persone, gli uffici, gli immobili (in emergenza ed ospitanti) ed i diversi responsabili coinvolti nelle procedure di recovery per casi d'indisponibilità degli immobili, dei servizi correlati agli immobili.
Il BCP è la realizzazione pratica di quanto definito nella BIA.

Il BCM Manager è responsabile della redazione, manutenzione ed aggiornamento del BCP.

Ramm (Risk assessment management methodology): E' lo strumento utilizzato congiuntamente dalle Direzioni per la rilevazione dei livelli di sicurezza logica e fisica delle applicazioni informatiche.
Un parametro del documento Ramm è la massima indisponibilità del servizio tollerata dalle Direzioni (parametro AI11 del foglio BCQ availability. della Ramm è espresso anche il tempo di ripristino dell'applicazione in situazioni di operatività quotidiana (parametro AI3 del foglio BCQ availability) che però nulla ha anche vedere con il Disaster Recovery).

Il dato deve essere congruente con quanto espresso nella BIA per il processo correlato.
Il tempo massimo d'indisponibilità dell'applicazione determina il tipo di soluzione di DR (DR strategy) che si dovrebbe implementare.
In caso di più processi che utilizzano la stessa applicazione l'RTO della Ramm deve adeguarsi al valore più basso tra quelli espressi nelle varie BIA.

Il Referente di Direzione è responsabile della redazione, manutenzione ed aggiornamento dell'informazione della massima indisponibilità contenuta nella Ramm.

DR Strategy: è un documento che riporta la soluzione di DR per gli immobili e per l'infrastruttura tecnologica, implementata in ottemperanza ai criteri espressi nella BIA e nella Ramm.

Gli ICT PM in collaborazione con l'ICT DR co-ordinator, e l'ICT Infrastrutture DR co-ordinator, sono responsabili della redazione, manutenzione ed aggiornamento del DR Strategy.

DR Plan: è un documento prodotto dal gestore della piattaforma tecnologica e/o dell'immobile, condivisa con tutti gli utilizzatori, allo scopo di definire e riportare nel dettaglio tutti i passi per il ripristino dell'immobile e/o dell'infrastruttura tecnologica secondo i tempi definiti nella BIA e nella Ramm (solo per l'infrastruttura tecnologica) e riportati nel documento di DR Strategy.

I Fornitori sono responsabili della redazione, manutenzione ed aggiornamento del DR Plan, coadiuvati dall' ICT PM, dall' ICT DR co-ordinator e dall' ICT DR co-ordinator Infrastrutture.

Soluzione di DR: è l'implementazione di DR vera e propria realizzata in ottemperanza al DR Strategy ed al DR Plan.

I Fornitori, coadiuvati dall' ICT PM, dall' ICT DR co-ordinator e dall' ICT DR co-ordinator Infrastrutture, sono responsabili della realizzazione, e manutenzione della soluzione di DR.

BCM Test: i test di Business Continuity Management previsti dalle policies sono:

Call Tree Test: verifica della catena di comunicazione. Due volte l'anno ogni Direzione devono eseguire un test di verifica della catena di comunicazione.

Si tratta di un test della lista di contatti telefonici di ogni ufficio/linea di Business, che include le indicazioni da fornire a tutte le persone chiave coinvolte.

I Referenti di Direzione sono responsabili assieme ai BCP Owner della redazione, manutenzione ed esecuzione del Call Tree Test.
Le eventuali anomalie o mancanze devono essere riportate al BCM Manager ed il Referente di Direzione deve pianificare il ripristino.

Walk Through Test: una volta l'anno ogni Direzione devono ripercorrere "a tavolino" i passi previsti dal BCP.

Tale test prevede la revisione dei piani e delle procedure di BCM e dovrebbe includere la revisione delle liste dei contatti, dei punti di ritrovo, delle indicazioni relative ai siti di back-up ed ogni altra informazione rilevante ai fini del recovery della propria linea di Business.

I Referenti di Direzione sono responsabili assieme ai BCP Owner della predisposizione ed esecuzione del Walk Through Test.
Le eventuali anomalie o mancanze devono essere riportate al BCM Manager ed il Referente di Direzione deve pianificare il ripristino.

Recovery Site Test: una volta l'anno ogni Direzione deve eseguire un test in cui le persone definite essenziali si recano presso l'ufficio ospitante e verificano la disponibilità delle applicazioni essenziali per la ripartenza del processo gestito.

I Referenti di Direzione sono responsabili assieme ai BCP Owner della predisposizione ed esecuzione del Recovery Site Test con il coordinamento e supporto del TOC.
Le eventuali anomalie o mancanze devono essere riportate al BCM Manager. Il Referente di Direzione, con il supporto dei DR co-ordinators, deve pianificare il ripristino.

DR Test: una volta l'anno ogni Direzione, in collaborazione con la Direzione ICT, responsabile dell'infrastruttura tecnologica ed i Servizi Generali Immobili, responsabile degli immobili, eseguono il test di DR degli edifici di Key Client e di Help Phone ed inoltre supportano i Fornitori nell'esecuzione del DR dei Data Centres (centro elaborazione dati).

Gli ICT PM ed i fornitori sono responsabili della predisposizione ed esecuzione del DR Test con il coordinamento e supporto del TOC.
La richiesta di esecuzione del DR Test parte dal Referenti di Direzione, che dovrà aver fatto predisporre opportuno budget per la sua esecuzione.
Le eventuali anomalie o mancanze devono essere riportate al BCM Manager; agli ICT PM ed al fornitore, che con il supporto dei DR co-ordinators devono pianificare il ripristino.

Documenti di Test di DR: sono i documenti che definiscono i casi prova da eseguire ed i risultati ottenuti.

Sono evidenziati eventuali anomalie o inadempienze il cui ripristino deve essere in seguito definito e pianificato.

Gli ICT PM ed i fornitori sono responsabili della redazione e manutenzione dei documenti di test del DR .

Assets: la corretta esecuzione dei piani di BC e di DR è basata anche su un preciso censimento dei dati elementari costituenti il modello di BCM.
Per questo motivo sono censiti tutti gli Assets dell'Azienda (es. Applicazioni, Infrastrutture tecnologiche, Palazzi, Connessioni interne ed esterne, Fornitori critici, Clienti critici, etc.).
I DR co-ordinators con il supporto degli ICT PM, e dei Referenti di Direzione sono responsabili della redazione, manutenzione ed aggiornamento dei documenti che si riferiscono agli Assets dell'Azienda.

8.2 Manutenzione del processo di BCM

La manutenzione del Processo di BCM si realizza attraverso il regolare aggiornamento delle BIA, dei BCP e dei DR Plan, ogni qualvolta cambiamenti alla struttura, alle attività ed ai processi aziendali lo rendano necessario.

L'intero processo di BCM funziona solo se i vari piani di BCP e DR sono aggiornati ed in linea con le esigenze delle Direzioni, pertanto sarà compito dei Referenti di Direzione mantenere aggiornati i piani di BC fornendo le necessarie informazioni al BCM Manager.

Allo stesso tempo, gli ICT PM, in collaborazione con i DR co-ordinators, provvedono al costante aggiornamento dei piani di DR.

In aggiunta, al fine di verificare la validità dei piani, devono essere eseguiti regolarmente dei test come elencato di seguito.

8.2.1 Test di Disaster Recovery

Ogni infrastruttura IT per la quale è stato realizzato il DR deve sostenere un Test almeno una volta l'anno.
In caso di rilevanti variazioni, il Test deve essere eseguito a valle del completamento della variazione.

Ogni Facility (Ascensori, Generatori Ausiliari di corrente, etc) deve sostenere almeno annualmente un test di recovery.

Almeno una volta l'anno deve essere eseguito il test dell'indisponibilità di uno dei due Data Centre di ogni fornitore.

Tutti i test devono essere accompagnati da documentazione che dettaglia lo scopo ed il risultato del test, approvato dai diversi livelli di responsabili delle Direzioni in funzione dl tipo di test, e fornire dettagli per ogni eventuale azione di rimedio in un formato approvato dal TOC.

I test delle infrastrutture tecnologiche di basso / medio profilo (server, network, Generatori ausiliari di corrente, etc) devono essere approvati dai Referenti di Direzione, dal DR co-ordinator ICT, dal DR co-ordinator ICT Infrastrutture e dal DR co-ordinator Servizi Generali .

I Test delle infrastrutture tecnologiche più complesse (Mainframe) o del Data Centre devono essere approvati dal BCM Steering Committee.

Il test dovrebbe includere anche le interfacce critiche, tranne nei casi in cui ciò può causare un inaccettabile rischio di tipo operativo all'ambiente di produzione normale.

I test devono essere documentati ed approvati dai suddetti diversi livelli delle Direzioni.

8.3 Gestione della crisi

Rappresenta il momento in cui al verificarsi di uno stato di crisi, che può essere causato da eventi di diversa tipologia, i ruoli preposti intervengono per garantire la continuità delle attività essenziali.

La trattazione di quest'argomento è rinviata al "Manuale di Gestione della Crisi per Key Client e per Help Phone".

9 Allegato A – Elenco dei Referenti di Direzione

Pagina lasciata intenzionalmente in bianco

10 Allegato B – Elenco dei BCP Owner

Pagina lasciata intenzionalmente in bianco

11 Allegato C – Elenco dei referenti per Edificio

Pagina lasciata intenzionalmente in bianco