



Seminario: L'attuazione del piano operativo di business continuity. Problematiche realizzative, di aggiornamento e di auditing.

Da luglio 2005 a Dicembre 2006: cosa ci attende? Che priorità? Che rischi di progetto?

Anthony Cecil Wright
Responsabile Progetto Continuità Operativa del Gruppo BNL
Presidente ANSSAIF

Monte dei Paschi di Siena,
Centro Formazione di Gruppo,
Siena, 8 luglio 2005

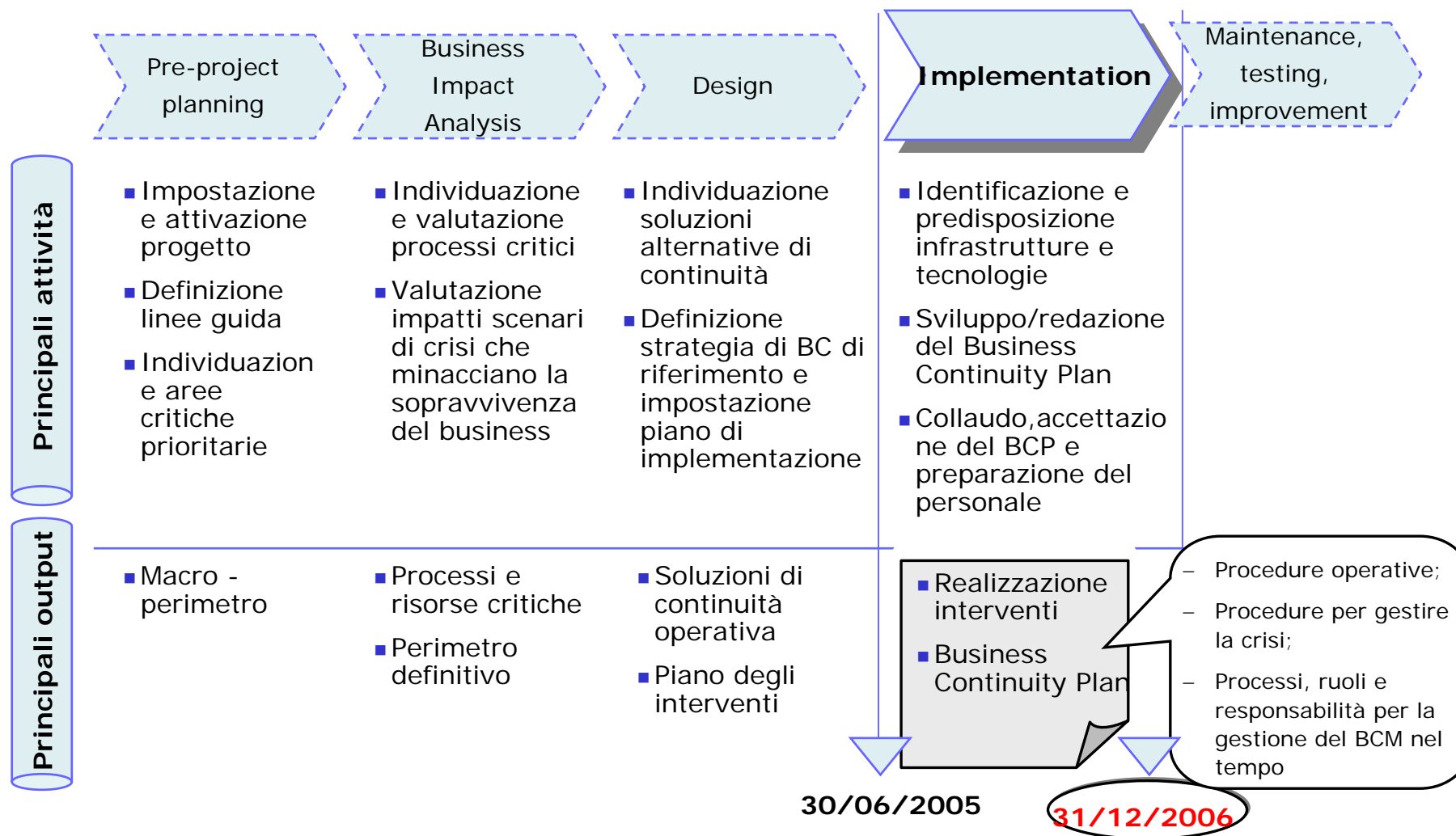
Indice

- La “fase 2”
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

Indice

- La "fase 2"
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

La "fase 2"



La "fase 2"

- Entro il 2006 si deve realizzare quanto previsto nel piano operativo presentato al Vertice aziendale ed inviato in Banca d'Italia.
- Il tutto ha un obiettivo oramai ampiamente memorizzato: "ridurre ad un livello ritenuto accettabile i danni conseguenti a incidenti e catastrofi che colpiscono direttamente o indirettamente un'azienda." Ciò mediante misure preventive, misure di gestione dell'emergenza e di rientro nella normalità.
- Si scriveranno dei manuali che dovranno contenere istruzioni concrete, attuabili, verificate, aggiornate tempestivamente e conosciute a tutti gli opportuni livelli.

Che rischi di progetto vi sono?

Indice

- La "fase 2"
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

Rischi di progetto

- Mancato completamento di quanto previsto entro la data stabilita.
 - Possibili cause:
 - ✓ Omissione di alcuni processi critici
 - ✓ Omissione di alcune tipologie di eventi
 - ✓ Assenza di certificazione di alcune verifiche di funzionamento dei piani
 - ✓ Incompleta conoscenza delle procedure da parte del personale
- Superamento del budget previsto.
 - Possibili cause:
 - ✓ Maggiori oneri per rispettare i tempi
 - ✓ Budget richiesto inferiore all'effettiva necessità

Rischi di progetto (2)

- Problemi derivanti da “incomprensioni” o “resistenze” da parte del personale.
 - Possibili cause:
 - ✓ Alcuni importanti fattori sono stati trascurati o sottovalutati (es: emotività; “paure”).
 - ✓ Richieste non accettate dalle rappresentanze sindacali (es: rintracciabilità vs. reperibilità).

Rischi di progetto (3)

- Procedure di Gestione dell'Emergenza (PGE) da scrivere:

$$\text{PGE} = \text{n.processi critici} \times \text{possibili eventi} \times \text{n.siti}$$

- Persone da coinvolgere / intervistare (PI) per ogni processo / evento:

$$\text{PI} = 2 \text{ (BCM settoriale + process owner)} + \text{esperti (Risorse Umane; Org.ne; Sistemi Inform. /DR; sic. ICT; sic. Fisica)} + \text{Responsabile U.O.} = 8 \text{ (minimo)}$$

- Interviste / consultazioni per raccolta informazioni per la redazione del piano:

$$\text{Tot.Int.} = \text{PGE} \times \text{PI}$$

Esempio: processi critici: 62; eventi: 6; siti per processo: 1; 8 esperti

$$\text{Tot. Inf.} : 62 \times 6 \times 1 \times 8 = 2.976$$

Rischi di progetto (4)

- Le interrelazioni fra persone (BCM, BCM settoriali, process owner, responsabile di struttura, eventuale funzione centrale, ed esperti dell'area Organizzazione, S.I., Sicurezza, Risorse Umane, Legale, Comunicazione, ecc.) per la raccolta di pareri di coerenza, fattibilità, ecc., rappresentano un'attività che può essere fortemente "time consuming".
- Un moltiplicatore è anche rappresentato dal numero dei processi definiti critici.
- Maggiore è il numero di processi definiti critici per il Gruppo, maggiore è l'impegno richiesto, più complesse sono le verifiche, e più grande è il rischio di non completare il progetto entro la scadenza.

Rischi di progetto (5): possibili soluzioni

1. Realizzare le procedure gradualmente, concentrandosi, per la nota scadenza del 2006, principalmente sui processi vitali di sistema.
2. Ridurre al massimo le tipologie di eventi; per esempio, prenderne in esame una in grado di rappresentare più casistiche altrettanto probabili.
3. Condurre le attività di stesura dei manuali con il responsabile di processo ed il BCM e, solo al termine, raccogliere le opinioni degli esperti e delle altre Funzioni Aziendali.
4. Adottare tutte e tre le soluzioni anzidette.

Rischi di progetto (6): valutazione delle ipotesi

1. Una riduzione nel numero dei processi critici da mitigare non appare possibile, specialmente se il Vertice ha già approvato il piano operativo.
2. Una sola tipologia di evento potrebbe essere possibile. Ragionando in termini di probabilità di accadimento, l'indisponibilità del sito ove si svolge il processo critico è tra gli eventi più probabili. Tra l'altro, un piano di ricollocazione delle risorse in altro luogo coprirebbe anche casi quali: incidenti parziali nell'edificio; interruzione nelle *public utilities*; evacuazione della zona; ecc.
3. Un coinvolgimento delle Funzioni Centrali solo al termine della stesura di un manuale potrebbe comportare "ricicli" piuttosto "time consuming".

Rischi di progetto (7)

- Quello rappresentato è un possibile esempio, ma altri possono essere fatti:
 - Manuale delle procedure da seguire per allocare le risorse entro il “time frame” prefissato (RTO) vs. manuale delle procedure operative - del processo critico - da seguire in caso di disastro: sono due cose diverse; li redige entrambi il BCM? E l'Organizzazione?
 - Stesura ed aggiornamento del piano: esistono tools che agevolano / assistono il BCM? O sono tools per redigere disaster recovery plans? Che manualità richiede? Quanto inciderà sui tempi di progetto?
 - Impatti sul personale dell'Azienda (cfr.prossima slide): si sente molto parlare di hardware, software, telecomunicazioni ... e le risorse umane? Rintracciabili, disponibili, “committed” sul processo, con “cloni” pronti ad intervenire se mangiano funghi tutti assieme...

Rischi di progetto (8): impatti sul personale

- Scarsa cultura di sicurezza
- Doverosa attenzione alla prevenzione ed alla tutela dei colleghi (stiamo o no parlando di incidenti o catastrofi anche estese?)
- Doverose riflessioni sui possibili impatti sulle famiglie dei lavoratori
- Perdita di persone "chiave": tema molto delicato, per tanti possibili risvolti.
- Rintracciabilità / reperibilità: vi è una necessità reale di formalizzazione? Possibili risvolti non immediatamente positivi.

Indice

- La "fase 2"
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

I controlli interni

- “L’approccio alla continuità operativa e il piano di emergenza sono regolarmente controllati dalla funzione di revisione interna (internal auditing). Gli auditor prendono visione dei programmi di verifica, assistono alle prove e ne controllano i risultati, propongono modifiche al piano sulla base delle mancanze riscontrate. (...)”.
- “Le verifiche delle misure di emergenza sono correlate ai rischi; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. (...)”.
- “Il consiglio di amministrazione (...) approva il piano; viene informato, con frequenza almeno annuale, sulla adeguatezza dello stesso.”.

I controlli interni (2)

■ Domande:

- È l'auditing perfettamente in grado di affermare che le verifiche eseguite sono coerenti con i possibili rischi?
- E' stato formalmente definito il "risk appetite" di Gruppo?
- C'è qualche standard a cui poter fare riferimento?
- Non esistono incomprensioni fra Sistemi Informativi / BC /DR ed Auditing? (ad esempio, con la dizione "processo" si intende la stessa cosa? L'approccio per sito / U.O./ Processo è condiviso?).

Indice

- La "fase 2"
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

Il caso BNL: L'implementazione della strategia di continuità operativa

- In rispetto della normativa, il Gruppo BNL dovrà realizzare, entro il **31 dicembre 2006** un piano di gestione della **continuità operativa**
- Il piano degli interventi predisposto da BNL è articolato nei seguenti filoni progettuali:

Avvio della struttura di Business Continuity Management (BCM) e dell'Unità di Crisi

- Ordini di servizio, disposizioni interne e procedure operative

Implementazione delle soluzioni di continuità individuate

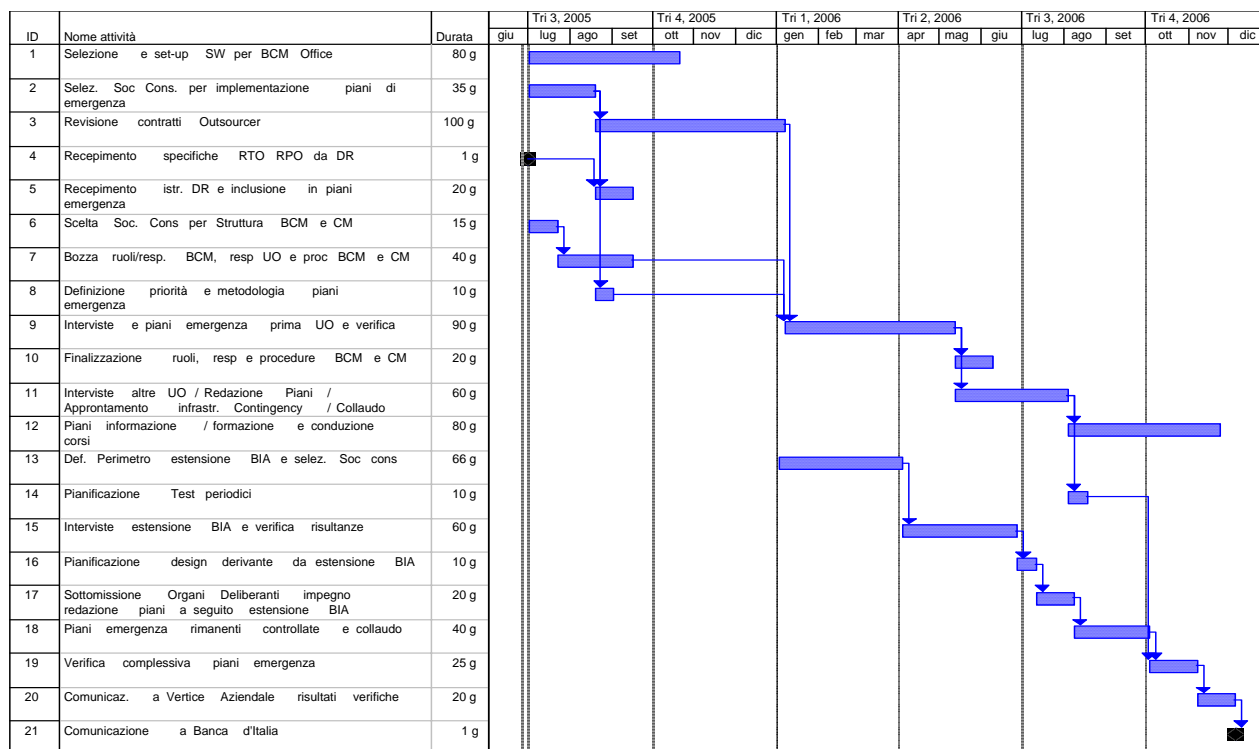
- Realizzazione degli interventi necessari ad **abilitare le soluzioni di continuità identificate**. Gli interventi potranno essere sia di **carattere strutturale** (ad esempio: predisposizione ambienti di backup, adeguamento impianti, ecc.) che di **carattere organizzativo** (ad esempio: stesura procedure organizzative, formazione utenti, ecc.)

Estensione delle analisi BIA

- Predisposizione del piano di continuità operativa (**Business Continuity Plan**)*
- Ampliamento del perimetro dei processi della Banca e delle società del Gruppo da sottoporre alla **Business Impact Analysis**

(*) Il Piano di Continuità Operativa "formalizza i principi, fissa gli obiettivi e descrive le procedure per la gestione della continuità operativa dei processi aziendali critici" (Banca d'Italia – 20.07.2004)

Il caso BNL: Il piano degli interventi



Alla base della pianificazione, onde avere la ragionevole certezza di rispettare i tempi e la qualità attesa, vi sono diverse ipotesi che sarebbe bene poter condividere fra banche di pari dimensione e complessità.

Indice

- La "fase 2"
- Rischi di progetto
- I controlli interni
- Il caso BNL
- Conclusione

Conclusione

E' quindi doveroso ora, prima che la seconda fase sia pienamente operativa, verificare assieme all'ABI quali possano essere i rischi da affrontare, ed iniziare ad individuare possibili approcci.

Ciò anche con l'aiuto di esperti di Società Multinazionali, con lunga esperienza maturata in Paesi ove alcune tematiche sono già state avviate da tempo.

Conclusione (2)

Appare quindi chiaro perché ci troviamo oggi qui, assieme a chi è impegnato nell'auditing della BC, e con la importante presenza dell'ABI.

Questo di oggi mi auguro sia il primo di una serie di incontri sulle tematiche che ci occupano, che ci consentano di avere, in tempi possibilmente brevi, condivise ipotesi di approccio da sottoporre alla valutazione delle banche e della Banca d'Italia.

The end.

Grazie per l'attenzione.