

PREVENZIONE ITALIA 2005

Roma, 16 giugno 2005

Business continuity e approccio integrato alla gestione della sicurezza

Vincenzo Mirko Carlone

Settore Tecnologie e Sicurezza, ABI

Settore Ricerca, ABI Lab

v.carlone@consulenti.abi.it

Le attività sulla continuità operativa nel sistema finanziario italiano

- Lo scenario
- Il Sistema Italia
- La risposta delle banche
- Le continuità operativa
- Le attività svolte sulla continuità operativa
- I servizi infrastrutturali e le utilities
- Il piano di Sistema
- Le istruzioni di vigilanza sulla continuità operativa
- Gli elementi normativi per la gestione della BC
- La Metodologia ABI Lab
- Le crescenti necessità delle banche verso gli outsourcer

Costi e rischio operativo in ottica Basilea II

Il nuovo approccio integrato alla sicurezza

I cambiamenti e le evoluzioni del contesto economico e sociale hanno **modificato** il **profilo dei rischi** che le imprese devono affrontare.



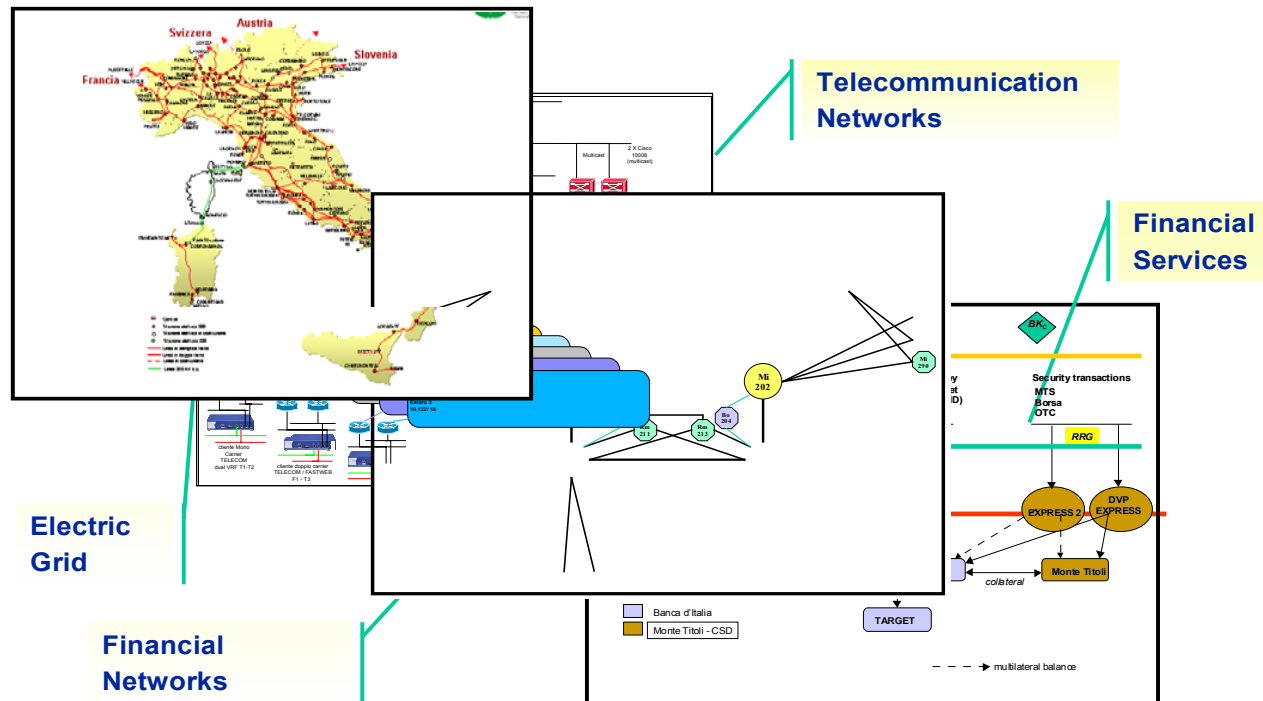
- **nuovi metodi di valutazione del contesto**
- **approccio integrato** alla gestione della sicurezza
- misure di sicurezza, anche organizzative, a **presidio di tutte le risorse**

Sistema Paese

- Sicurezza per i cittadini e le imprese
- disponibilità servizi vitali

Sistema bancario

- Funzionamento servizio bancario
- funzionamento dei mercati



E' stata avviata da tutti i principali attori del sistema paese un'azione di presidio su le infrastrutture critiche

La risposta delle banche

Priorità di investimento in ICT per il 2004 delle banche italiane.



Fonte: Assinform 2004 - Campione di 114 banche

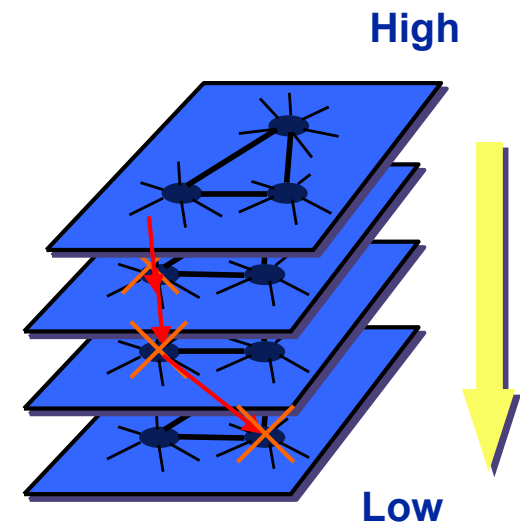
Costi/Rischio e Business Continuity

La **continuità operativa** è definita come “l'insieme di tutte le iniziative volte a **ridurre a un livello** ritenuto **accettabile i danni conseguenti a incidenti e catastrofi** che colpiscono direttamente o indirettamente un'azienda”.

Bollettino di vigilanza Bdl, luglio 2004.

- **Interdipendenza delle infrastrutture**
- **necessari differenti “livelli” di analisi:**

- *core financial services*
- *financial network*
- *telecommunications*
- *utilities*



In seguito agli eventi disastrosi dell'11 settembre le **Banche Centrali** hanno avviato un processo di **definizione delle misure** da adottare **per garantire la continuità** di esercizio sia a livello di sistema che di singolo operatore.



Le attività di Banca d'Italia

Primavera 2002: avvio iniziative di coordinamento

Luglio 2004: normativa "*Gestione della continuità operativa*" per le banche;

Novembre 2004: "*Linee guida per la continuità di servizio delle infrastrutture qualificate dei sistemi di pagamento*".



Il cammino dell'ABI

Partecipazione alle attività coordinate da Banca d'Italia;

Metodologia per la realizzazione del piano di continuità operativa;

Coinvolgimento terze parti e infrastrutture critiche.



Le iniziative dell'ABI in merito ai servizi infrastrutturali e le utilities

ABI

L'ABI ha intrapreso numerose iniziative al fine di supportare le banche nell'analisi della **continuità offerta sui servizi infrastrutturali e le utilities** dagli operatori del sistema Paese

Infrastrutture critiche



Approfondimento della “**Protezione delle infrastrutture critiche informatizzate**” promosso dalla *Presidenza del Consiglio dei Ministri*

Telecomunicazioni



Adesione al **GdL Infrastrutture critiche di telecomunicazione** promosso da *Ministero delle Comunicazioni*.

Partecipazione ai sotto-gruppi di approfondimento:

Servizi e Sicurezza

analisi dei rapporti di outsourcing instaurati o instaurabili dalle infrastrutture critiche

Gestione delle emergenze e degli incidenti

analisi della gestione delle emergenze ICT “locali”



Avvio dell'approfondimento sulla tematica con i distributori di energia e il GRTN attraverso il consorzio costituito **ABI Energia**

Banca d'Italia sta approfondendo le **modalità di gestione del piano di continuità di sistema** con gli operatori e le banche di rilevanza sistemica

BANCA D'ITALIA 
INDICAZIONE DEI SERVIZI VITALI
INDISPONIBILI IN CASO DI
DISASTRO

“Linee guida per la continuità di servizio delle infrastrutture qualificate dei sistemi di pagamento”

Dialogo diretto con la Vigilanza

BANCA D'ITALIA	BORSA ITALIANA	CCG	e-MID	IAAI	ICCREA	MONTE TITOLI	MTS	SECETI	SIA	SSB	BNL	CAPITALIA	INTESA BCI	MPS	SAN PAOLO	UNICREDITO
----------------	----------------	-----	-------	------	--------	--------------	-----	--------	-----	-----	-----	-----------	------------	-----	-----------	------------

Servizi Vitali in corso di approfondimento

- Compensazione e regolamento: BI-REL, Target, Clearing e regolamento (Express II), Gestione conti in titoli (CSD), Servizi di controparte centrale (CCP), RRG)
- Mercati monetari e finanziari: Mercato Interbancario dei depositi (e-MID), Operazioni di politica monetaria (Aste BCE), Pronti controtermine su MTS
- Procedure interbancarie retail: Bancomat

Approccio normativo flessibile, basato sulla **responsabilizzazione delle banche che agiscono nel rispetto di raccomandazioni ed orientamenti**, focalizzando gli interventi prioritariamente sui propri **processi critici autonomamente definiti**

**Normativa Banca d'Italia sulla
"Gestione della continuità
operativa" Bollettino di
Vigilanza luglio 2004**

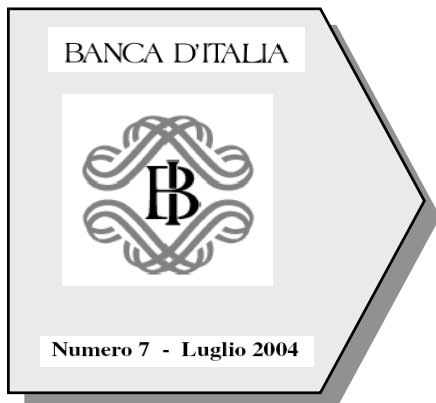
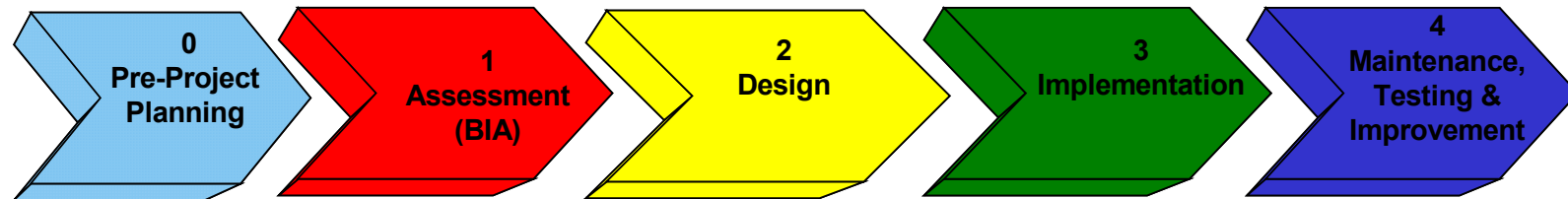


Scadenze per le banche

- **Gruppi bancari con attivo consolidato > 5 mld €:**
 - Stato Avanzamento Lavori entro marzo 2005
 - pianificazione BC entro giugno 2005
 - adeguamento DR entro giugno 2005
- **Altre Banche:**
 - piano di continuità entro 2006

Gli elementi normativi per la gestione della business continuity

percorso strutturato sulla base degli **elementi previsti dalla normativa** Banca d'Italia del 15 Luglio 2004 sulla "Gestione della continuità operativa"



4.1 Ruolo dei vertici aziendali
4.3 Responsabilità del piano

3. Ambito del piano di continuità operativa
3.1 Correlazione ai rischi
4.2 Processi critici
5. Requisiti particolari

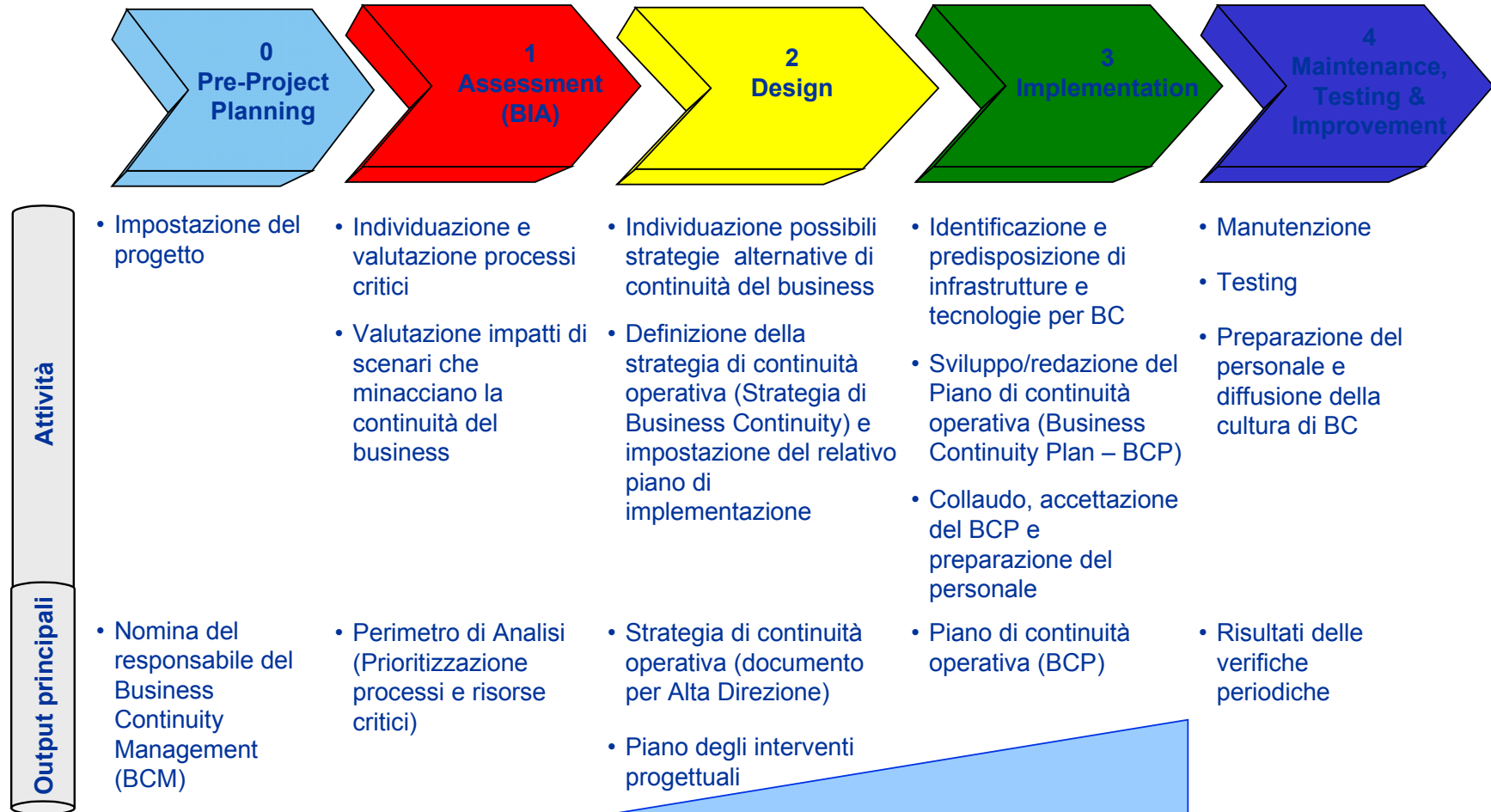
4.7 Esternalizzazione delle attività critiche
4.8 Infrastrutture e controparti rilevanti

4.4 Contenuto del piano
4.6 Risorse umane
4.10 Comunicazioni alla Banca d'Italia

4.5 Verifiche
4.9 Controlli interni

La Metodologia ABI di BC: gli obiettivi e gli output

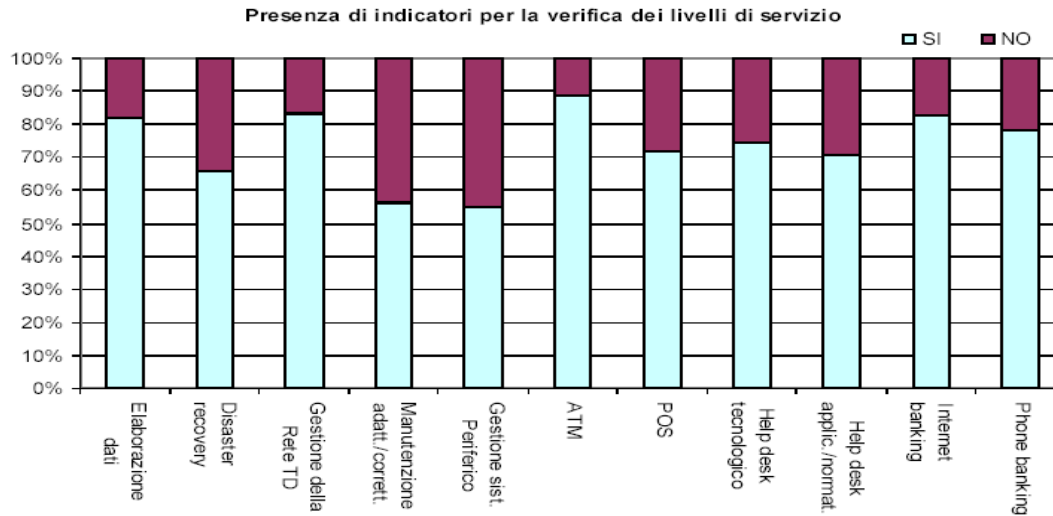
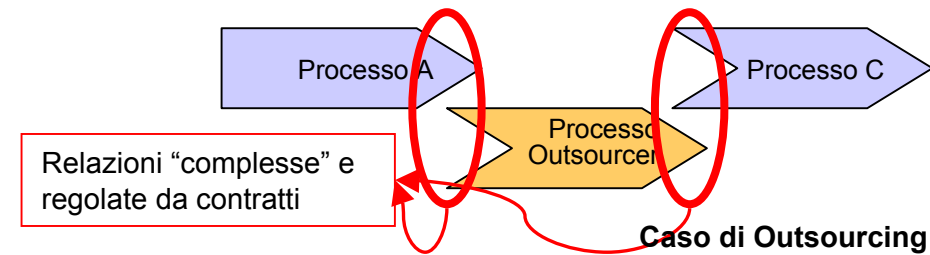
Metodologia per la realizzazione del Piano di Continuità Operativa



Dicembre 2006

Le crescenti necessità delle banche verso gli outsourcer

La **continuità** delle attività critiche in outsourcing, in base alla nuova **normativa**, rende necessaria una maggiore **responsabilizzazione** dell'outsourcer sulla **qualità** del servizio offerto e sulla **continuità**



Si denota una sempre maggiore attenzione alla definizione di **livelli di servizio contrattuali** dettagliati per tipologia di servizio

□ Le attività sulla continuità operativa nel sistema finanziario italiano

📄 Costi e rischio operativo in ottica Basilea II

- Le fasi metodologiche: la sicurezza e i rischi secondo Basilea II
- Le fasi metodologiche: l'approccio unitario dei rischi operativi
- Le prossime attività dell'ABI in merito alla business continuity
- Le azioni cooperative dell'ABI per supportare il sistema bancario

□ Il nuovo approccio integrato alla sicurezza

Il percorso sulla *Business Continuity*, che le banche devono sviluppare per il 2006, **presenta numerosi punti di contatto con l'approccio sui rischi operativi** indicato dagli accordi di Basilea.



- individuazione dei **processi critici**
- soluzioni di **mitigazione dei rischi**
- **analisi costi/benefici** per il contenimento dei costi operativi

Le fasi metodologiche: la sicurezza e i rischi secondo Basilea II

I rischi operativi insistono trasversalmente sui processi della banca creando una stretta **relazione tra la gestione dei rischi e l'analisi degli impatti legati alla Business Continuity.**

FRODI INTERNE	FRODI ESTERNE	CONTRATTO DI LAVORO E SICUREZZA DEL POSTO DI LAV.	CLIENTI, PRODOTTI E PRATICHE DI BUSINESS	DANNI O PERDITA DI BENI MATERIALI	IT E APPLICATIVI	GESTIONE DEL PROCESSO
Attività non autorizzate	Furti e frodi	Relazioni sindacali	Fiducia, privacy e relazioni con il cliente	Disastri naturali o altri eventi	Sistemi	Avvio, esec. e completamento delle transazioni
Furti e frodi	Crimini informatici	Sicurezza sul lavoro	Pratiche di business o di mercato improprie			Monitoraggio e reporting
		Discriminazioni	Vizi di prodotto			Acquisizione dei clienti e relativa documentaz.
			Selezione, spons. e limiti di esposizione			Gestione dei conti dei clienti
			Attività di consul. informativa			Controparti commerciali
						Gestione Fornitori

Categorie di rischio individuate da Basilea II

Principali tipologie di rischi operativi connessi alla BC

L'ABI ha individuato l'opportunità di proseguire nell'approfondimento delle logiche di gestione della business continuity con l'ausilio di Gruppi di lavoro banche e aziende ICT

Business Continuity



PERCORSI FORMATIVI

- ❑ Erogazione di un sistema info/formativo per l'acquisizione di competenze trasversali metodologiche sulla realizzazione del piano di continuità operativa
- ❑ Definizione di soluzioni cooperative e standard in autoregolamentazione
- ❑ **Approfondimenti** con il GdL ABI di **tematiche di interesse** tra cui:
 - ❑ Modello di correlazione tra capitale di garanzia della banca e investimenti in BC

Approfondimento e **definizione di azioni cooperative e standard in autoregolamentazione** come previsto tra le attività delle associazioni di categoria nella normativa di Banca d'Italia.

Analisi e individuazione delle soluzioni di continuità sui processi critici

Obiettivo

Identificare possibili soluzioni cooperative e di continuità su processi critici, con particolare attenzione all'area finanza

Realizzazione di un Osservatorio sulle soluzioni di DR

Obiettivo

Identificare soluzioni di DR coerenti con livelli di investimento e assetti organizzativi-operativi sostenibili

❑ **Le attività sulla continuità operativa nel sistema finanziario italiano**

❑ **Costi e rischio operativo in ottica Basilea II**

 **Il nuovo approccio integrato alla sicurezza**

- Le nuove esigenze emergenti: la gestione integrata della sicurezza
- Oneri di gestione della sicurezza nelle banche
- Il nuovo modello integrato di sicurezza
- Un modello di *governance* integrato della sicurezza in banca

Le nuove esigenze emergenti: la gestione integrata della sicurezza

Sicurezza Aziendale

Sicurezza dei **beni materiali ed immateriali** (immagine aziendale)

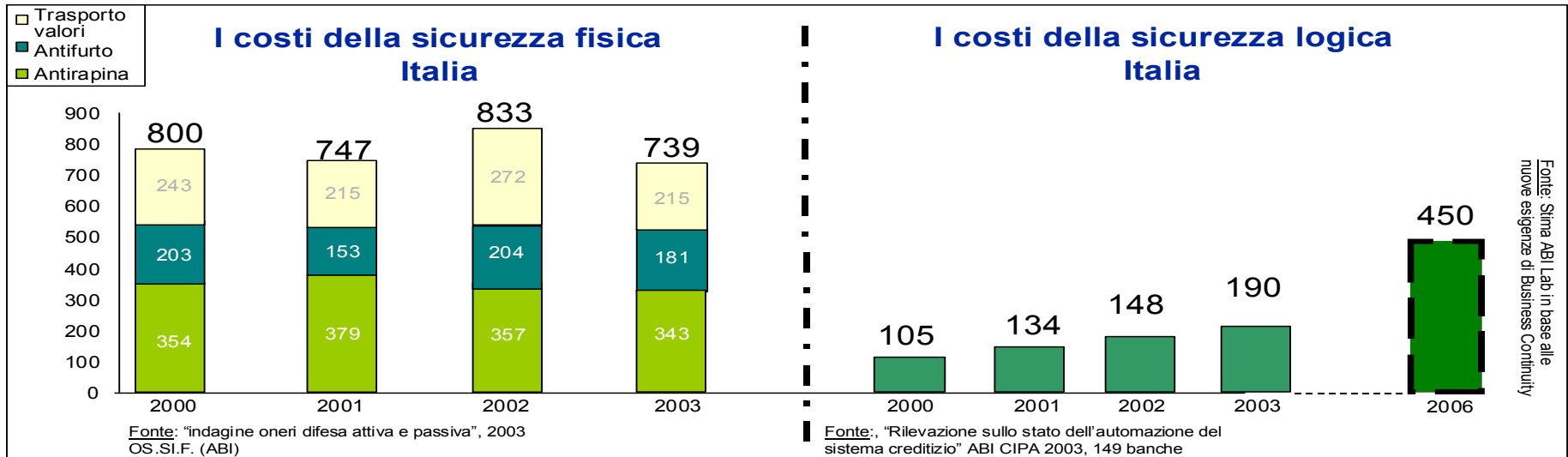
Sicurezza delle **persone e tutela ambientale**

Sicurezza dell'**informazione**

Sicurezza **informatica**

Sicurezza del **sistema informativo non automatizzato** (informazione e know-how)





La continua ricerca delle scelte e delle tecnologie comuni a tutti gli ambiti della sicurezza è un punto di partenza per l'accrescimento dei livelli di sicurezza e l'ottimizzazione dei costi

L'ottimizzazione dei "costi di sicurezza" impone l'analisi delle opportunità di condivisione dell'esistente e l'aggregazione delle necessità di acquisto

Le nuove opportunità di cambiamento nella gestione del rischio operativo offrono spazi per un'analisi sistematica dei rischi, degli impatti e delle contromisure

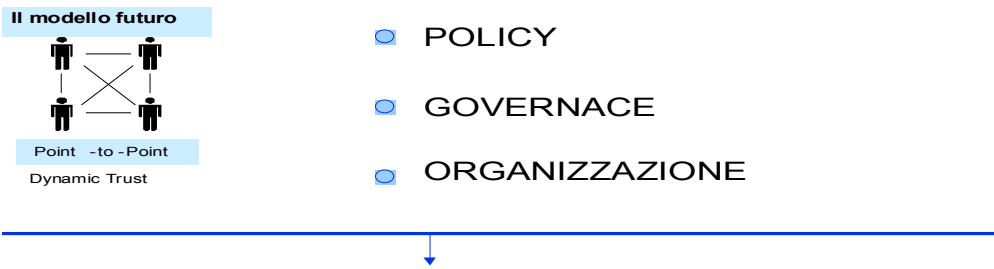
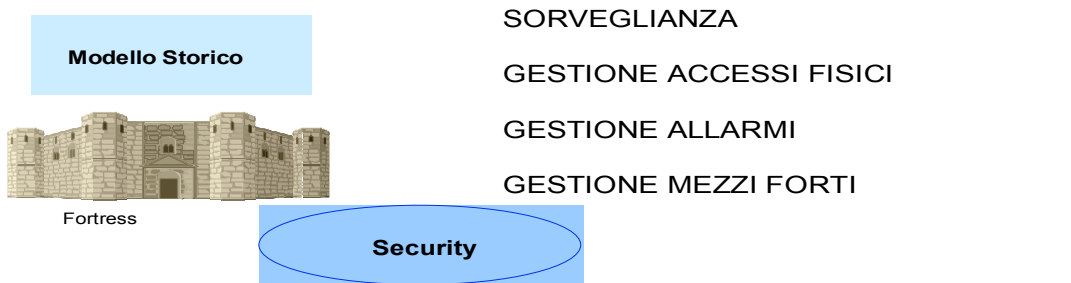
I driver emergenti indirizzano alla realizzazione di un **nuovo modello** della sicurezza in banca che risulti **trasversale ai processi gestionali e integrato in termini di infrastrutture**

LINEE GUIDA

- *Integrazione fisico-logica*
- *Controllo integrato*
- *Modularità, riusabilità e sostituibilità*
- *Scalabilità tecnico economica*

M
O
D
E
L
L
O
I
N
T
E
G
R
A
T
O

Un modello di *governance* integrato della sicurezza in banca



GESTIONE INTEGRATA DEI RISCHI

SECURITY EVOLUTION

Dalla
sicurezza perimetrale
alla
gestione integrata
dei rischi

Obiettivi del progetto:

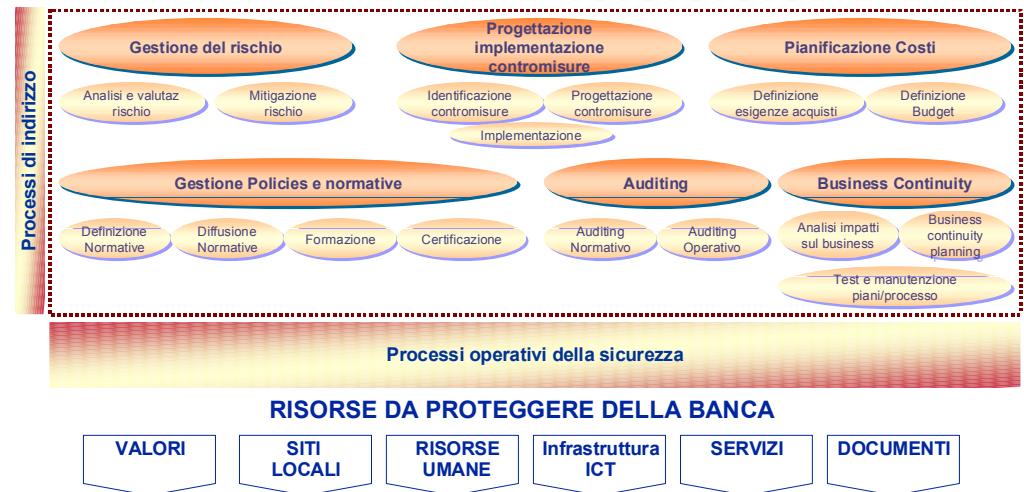
Contribuire allo sviluppo di un modello standard di **governance** della sicurezza che consenta un confronto rapido e omogeneo tra la propria azienda

- Realizzazione di uno studio per l'**analisi e sistematizzazione** del quadro regolamentare, degli indirizzi e delle direttive dei principali **standard internazionali**

- Analisi del contesto attraverso interviste mirate e **benchmarking con banche e partner ICT**
- Definizione e gestione di un insieme di **indicatori sui costi e sugli investimenti di sicurezza**

- Realizzazione di una **metodologia operativa** per la “Governance e organizzazione della sicurezza”

Prime risultanze dello studio di fattibilità



- Costituzione di un **osservatorio permanente** in grado di sviluppare/aggiornare i contenuti di sicurezza sulla base degli impulsi generati dall'evoluzione normativa, dagli standard e dalla tecnologia.