



ANSAIF
Associazione Nazionale Specialisti Sicurezza
in Aziende di Intermediazione Finanziaria



Sicurezza Logica e le altre funzioni di sicurezza - sinergie, conflitti, opportunità - benchmarking con altre importanti realtà bancarie e non

Stefano Cabianca

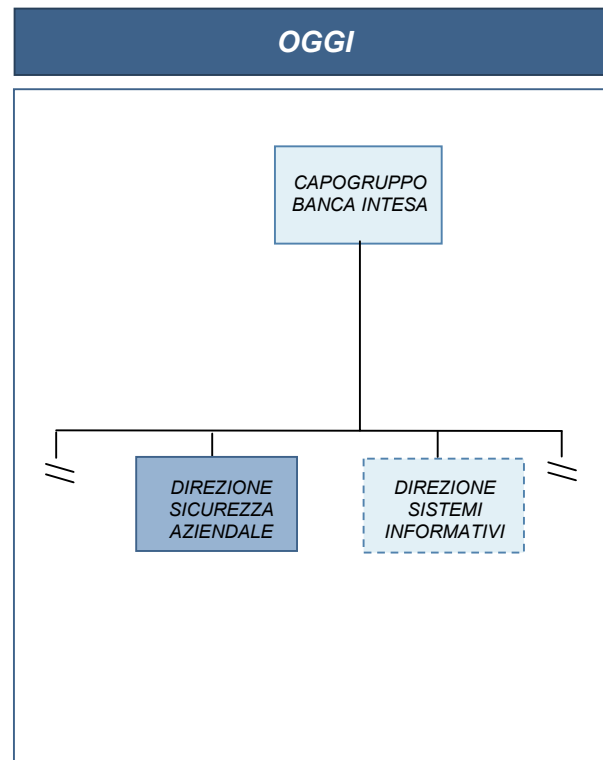
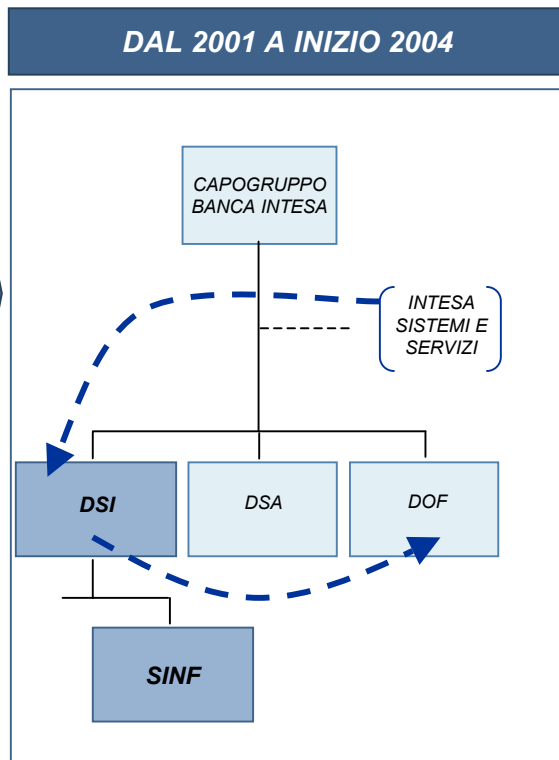
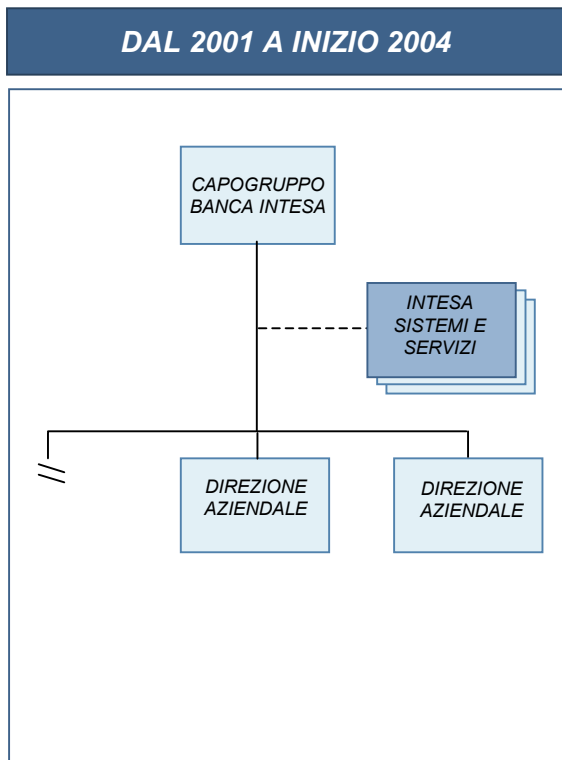
Responsabile Servizio Gestione Sicurezza Informatica

Roma, 16 giugno 2005

■ L'evoluzione della Sicurezza all'interno del Gruppo Intesa

- Il modello di governo della Sicurezza integrata
- Le prossime sfide in Banca Intesa
- Considerazioni finali

Il ruolo della Sicurezza Logica è radicalmente evoluto nel Gruppo



*Sin dalla nascita del Gruppo Intesa, la sicurezza informatica è stata posizionata come servizio dedicato nella **società IT del Gruppo**, ...*

... dopo il riassorbimento di ISS, la sicurezza informatica rispondeva alla Direzione Sistemi Informativi ...

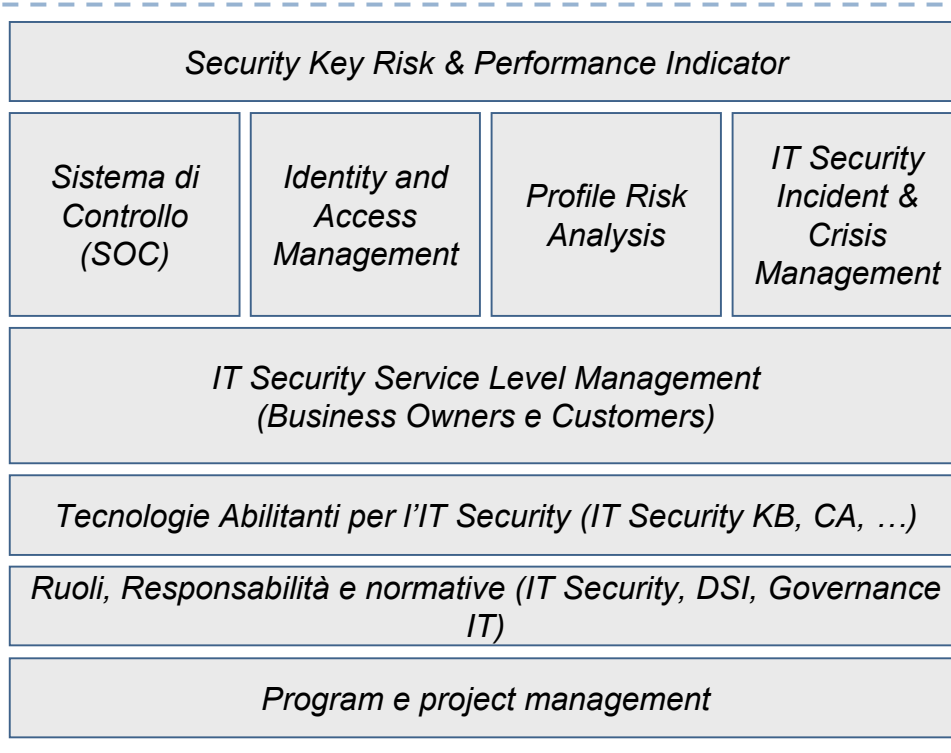
*... adesso compete ad una **direzione** che ha come mission la **Security Governance** all'interno di un Gruppo integrato*

Partendo da un approccio di tipo operativo e bottom-up ...

I PRINCIPALI TEMI DI PRESIDIO OPERATIVO ...

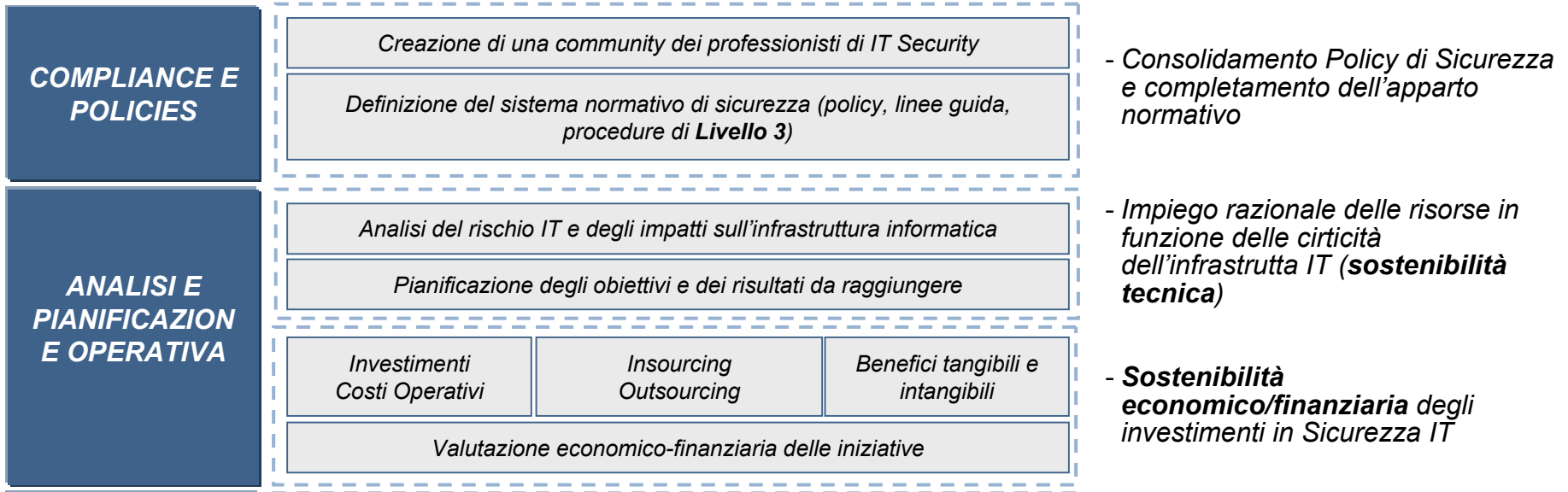
... PER OTTENERE OBIETTIVI TATTICI

GESTIONE E CONTROLLO DI PROCESSI E STRUMENTI DI SICUREZZA IT



- **Controllo delle performance e dei rischi** di Sicurezza IT basato su misurazioni quantitative (indicatori)
- Gestione delle situazioni e di **eventi di carattere ordinario** (incidenti) e **straordinario** (crisi)
- **Controllo delle tematiche di Identity Management**
- Integrazione della **Sicurezza IT nelle linee di business** (sicurezza dei servizi offerti alla clientela e come fattore differenziante nell'offerta) e **sui nuovi canali** (mobile, Internet, telefono, ...)
- **Governo e controllo del cambiamento**

... il modello di riferimento è stato poi esteso fino ad affrontare temi di governo della sicurezza a livello aziendale



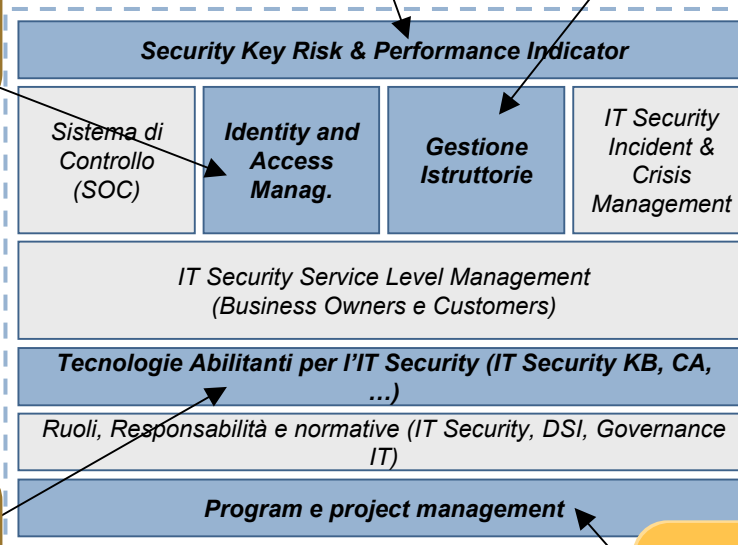
Alcune evidenze sulla complessità operativa dell'ambiente gestito

- Oltre 50.000 utenti interni (dipendenti)
- 10.000 utenti esterni (consulenti)
- Circa 1,5 Mln clienti finali sui canali diretti

- Circa 50 Indicatori (KPI) direzionali sulle performance e sui rischi di sicurezza a livello aziendale costantemente monitorati

- Circa 300 istruttorie rilasciate nell'ultimo anno
- Tempo medio di risoluzione inferiore alla settimana

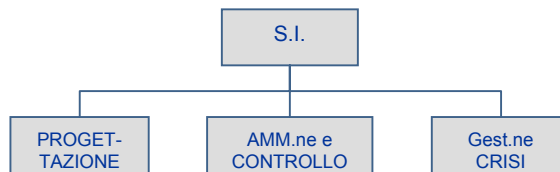
GESTIONE E CONTROLLO DI PROCESSI E STRUMENTI DI SICUREZZA IT



- 15 MAINFRAME
- OLTRE 70 DOMINI MICROSOFT
- CIRCA 9000 SERVER
- OLTRE 35.000 CLIENT
- 60.000 CASELLE DI POSTA ELETTRONICA
- ...

- Razionalizzazione delle infrastrutture di sicurezza (RA unica)
- Tecnologie crittografiche
- Tecnologie per sicurezza perimetrale
- ...

- 10 "grandi" progetti l'anno
- Altre iniziative
- ...



OLTRE 130 FTE INTERAMENTE DEDICATI AL PRESIDIO DELLA SICUREZZA

Banca Intesa ha progressivamente integrato gli ambiti di competenza presso le proprie strutture centrali, attivando da fine 2003 specifiche funzioni di governo ed indirizzo della Sicurezza

- Si è partiti da un modello organizzativo che prevedeva la funzione di **Sicurezza Fisica** all'interno della **Direzione Centrale Immobili e Acquisti di Banca Intesa** e la funzione di **Sicurezza Logica** presso la Società di Servizi **ISS**
- A fine 2003 è stata istituita, presso la Direzione Centrale Risorse Umane ed Organizzazione, il **Servizio Sicurezza e Continuità Operativa** a presidio di:

- Continuità Operativa;
- Sicurezza del patrimonio Informativo;
- Sicurezza Fisica ed Organizzativa;

mantenendo il presidio della gestione della Sicurezza Informatica in ISS

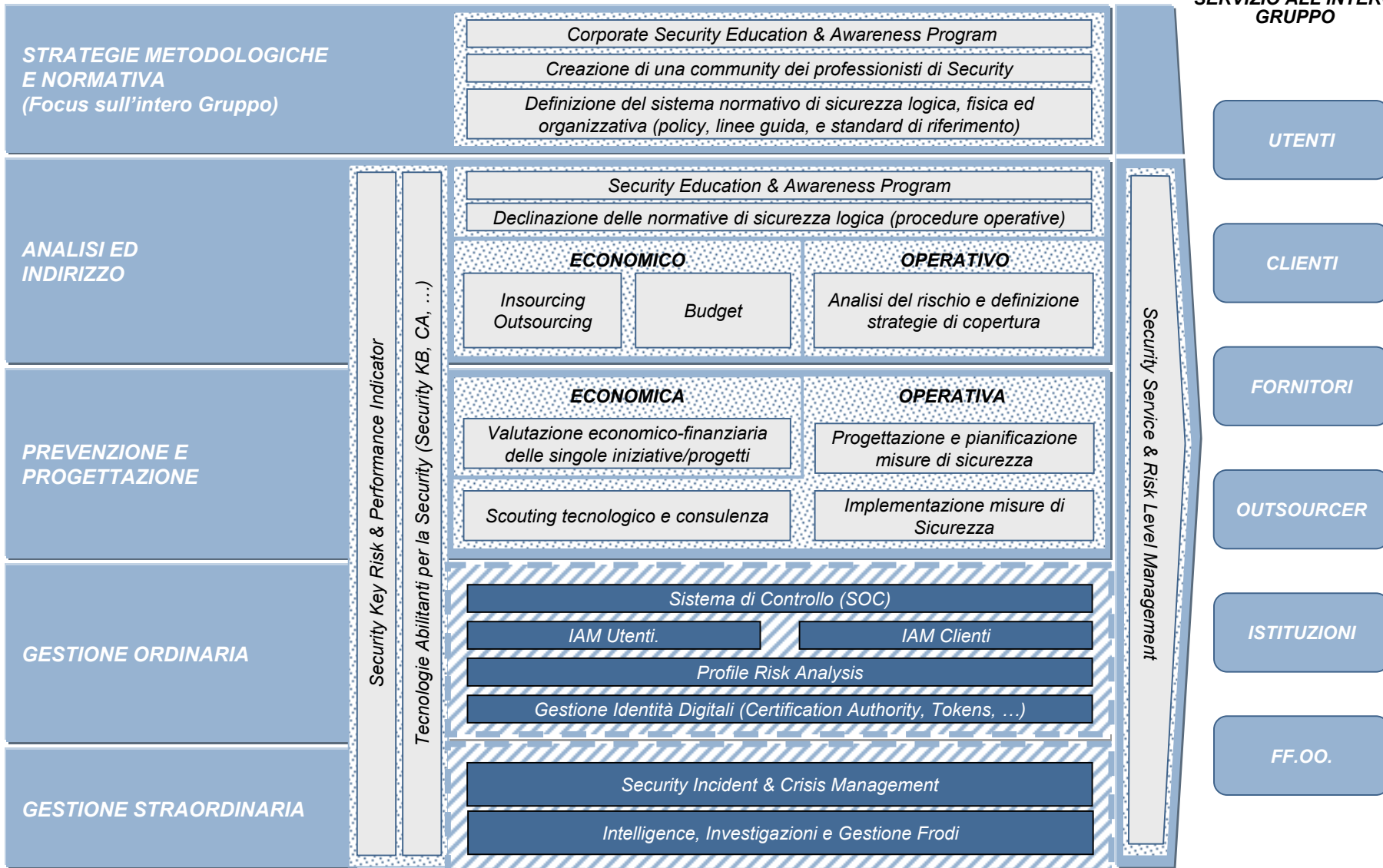
- Ad inizio 2005 è stata poi costituita la **Direzione Centrale Sicurezza di Banca Intesa**, per l'indirizzo e la gestione di:
 - Continuità Operativa;
 - Sicurezza Patrimonio Informativo;
 - Sicurezza Fisica ed Organizzativa;
 - Sicurezza Informatica.

... e la necessità di un modello di governo della Sicurezza integrata

IL MODELLO FUNZIONALE DI GESTIONE DELLA SICUREZZA ...

... DEVE ESSERE DECLINATO NEI PRINCIPALI TEMI STRATEGICI DI SICUREZZA LOGICA ...

... PER GARANTIRE I LIVELLI DI RISCHIO E SERVIZIO ALL'INTERO GRUPPO



- L'evoluzione della Sicurezza all'interno del Gruppo Intesa

- **Il modello di governo della Sicurezza integrata**

- Le prossime sfide in Banca Intesa

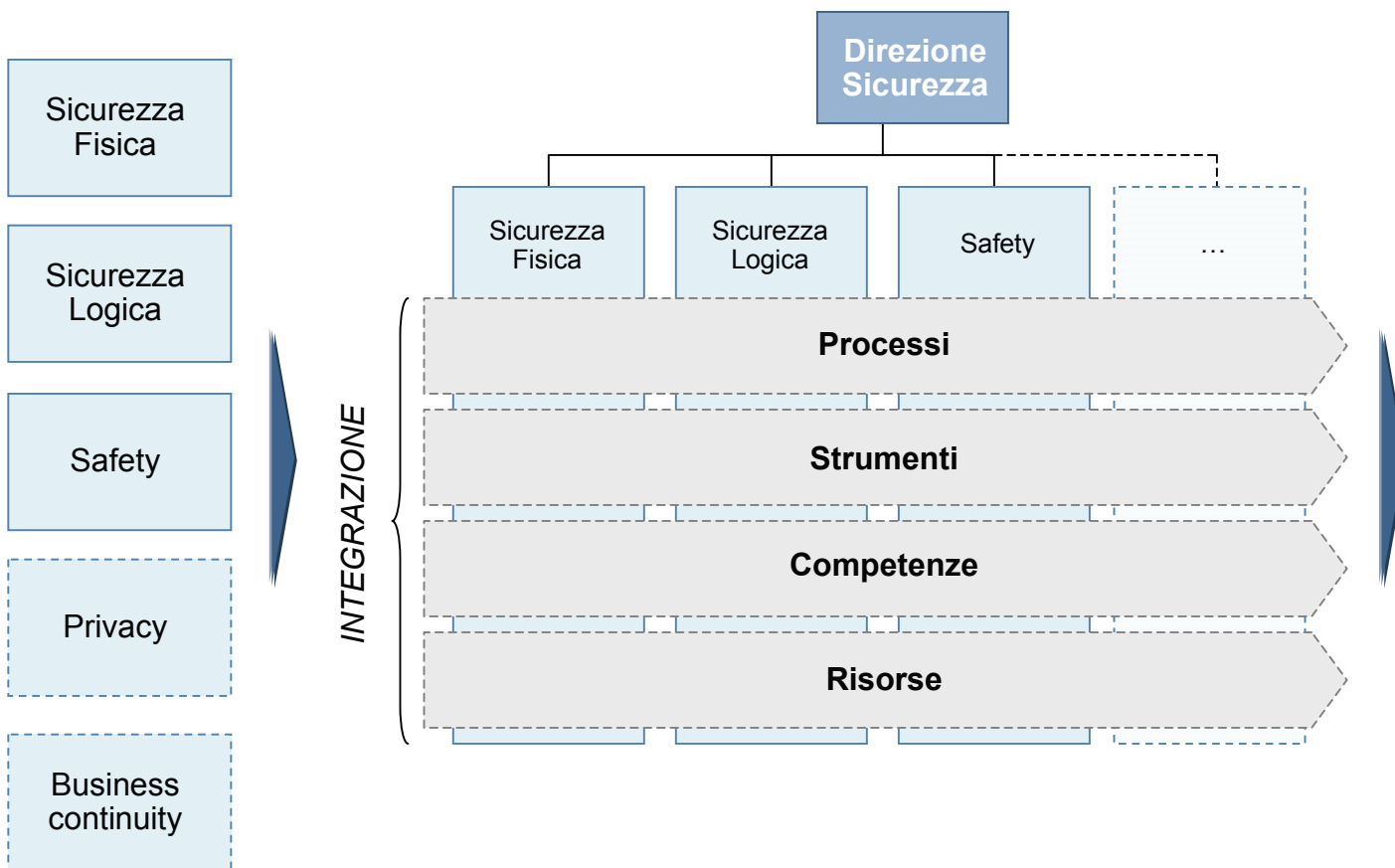
- Considerazioni finali

E' importante sviluppare una visione d'insieme e trovare soluzioni organizzative capaci d'interpretare le varie esigenze di sicurezza

Dalla gestione separata delle funzioni di security ...

... all'integrazione entro una direzione Centrale a dipendenza dal CEO ...

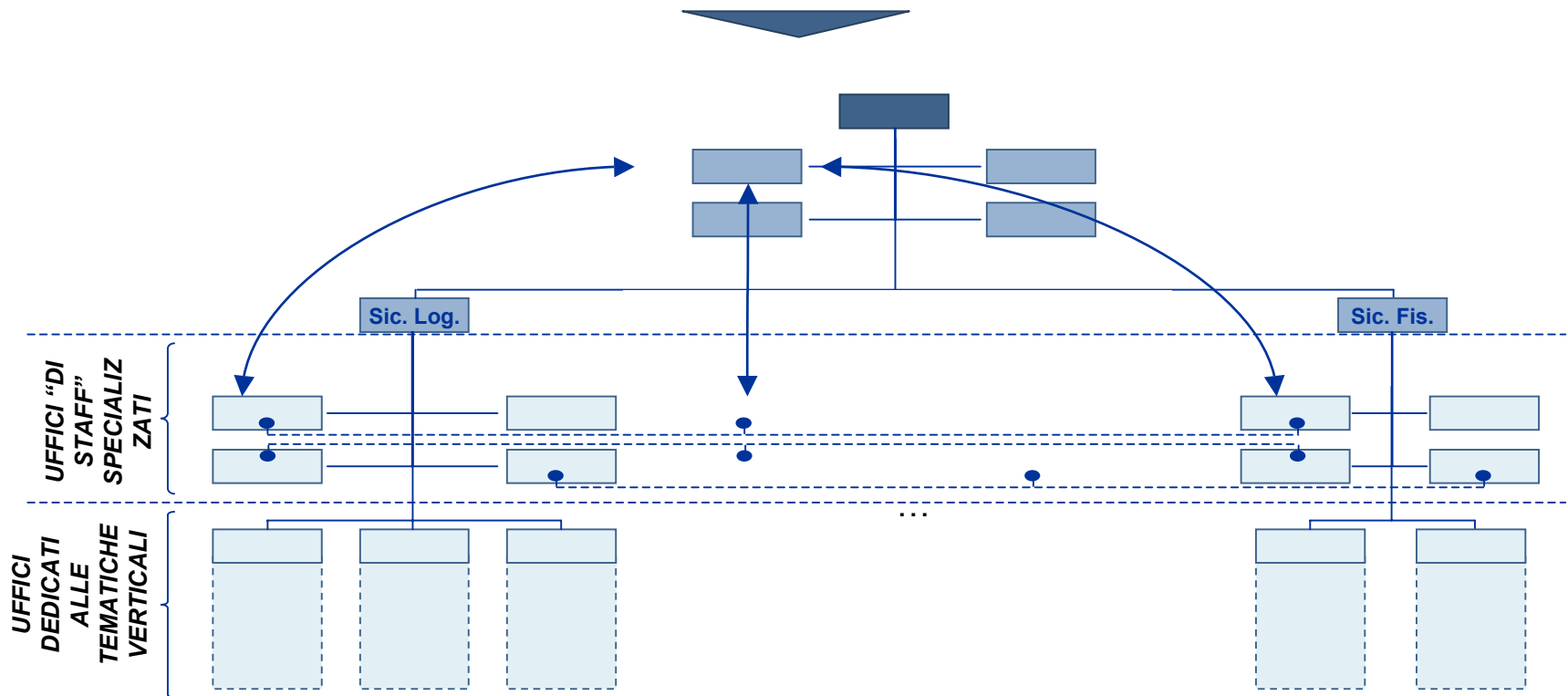
... al fine di creare sinergie e integrazioni



- **Integrazione** a livello di una **Direzione Centrale** di processi/strumenti per
 - **Pianificazione e controllo** della strategia di **gestione del rischio** e del **piano integrato** di Sicurezza
 - **Comunicazione di risultati e obiettivi** di Sicurezza verso il **top management** e le altre **direzioni aziendali**

E' necessaria una struttura organizzativa che consenta la gestione comune di alcune tematiche pur permettendo una forte autonomia gestionale

NELLE GRANDI AZIENDE L'ORGANIZZAZIONE DI SICUREZZA, PUR MANTENENDO DISTINTE LE DIVERSE AREE DI INTERVENTO, METTE A FATTOR COMUNE LA GESTIONE DI QUELLE TEMATICHE OVE RISULTA PREMIANTE LA VISIONE UNITARIA O LA SINERGIA DEI COSTI



DIREZIONE
SERVIZIO
UFFICIO



COORDINAMENTO GERARCHICO
COORDINAMENTO ORIZZONTALE

L'importanza di specifiche competenze per il raggiungimento degli obiettivi del modello

La realizzazione del modello di Sicurezza integrato nella Banca richiede l'utilizzo di diversificate competenze di natura specialistica, organizzativa, di processo e tecnica

- **Conoscenza di Standard e Metodologie di Sicurezza:**
 - Metodologie ABI;
 - ISO 17799 / BS7799:2 2002;
 - Norme UNI;
 - ...
- **Conoscenza delle tecnologie di sicurezza fisica ed informatica**
- **Conoscenza dei processi della Banca e capacità di re-engineering**
- **Capacità di governare budget e costi**
- **Capacità di gestire progetti multidisciplinari**
- **Capacità di relazionarsi con gli uomini di business**

Nelle realtà internazionali, e soprattutto in quelle Americane, anche a seguito della riforma del diritto societario, si osserva:

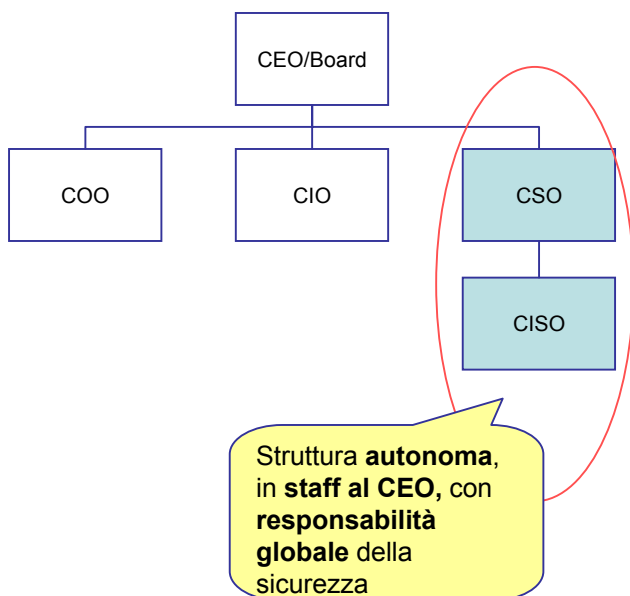
- Il riconoscimento che la sicurezza è legata tanto alla tecnologia quanto al business, in quanto gestore di una parte dei rischi operativi
- Un progressivo allargamento dell'ambito gestito dalle strutture di sicurezza, che, alla gestione delle tematiche di sicurezza logica, fisica e protezione degli asset, aggiungono prima le tematiche relative al copyright ed alla Business Continuity e, in alcuni casi, anche il presidio del rapporto con la clientela

Dal punto di vista organizzativo si osservano tre modelli di riferimento:

- La costituzione di una struttura organizzativa ad hoc dipendente direttamente dal CEO e/o dal BoD, presieduta da un Chief Security Officer (CSO), chiamato anche Global Security Officer, che ha la responsabilità globale della sicurezza (interna, esterna, fisica, logica, personale), sia per la componente strategica/di governo che operativa
- La gestione della sicurezza logica all'interno strutture IT, con la costituzione di un Chief Information Security Officer (CISO), dipendente direttamente dal CIO, che ha la responsabilità della protezione delle informazioni e, eventualmente, di altri aspetti strettamente correlati, quali, ad esempio, la sicurezza fisica, la pianificazione e sviluppo delle architetture di sicurezza, gli incidenti informatici
- La centralizzazione delle funzioni di controllo strategico della sicurezza in una struttura esistente in staff al CEO (ad esempio nella struttura di Risk Management, ove questa è preposta al governo dei rischi) responsabile della definizione delle policy, delle priorità e delle linee guida per tutto il Gruppo, con la costituzione di un Comitato di controllo cui è demandata la responsabilità sul rischio, delegando la parte di governo operativo al CISO, per la parte IT, oppure ad altre strutture operative (ad esempio la Logistica) preposte al presidio delle diverse tipologie di rischio

Vi è la tendenza a creare una struttura autonoma, con responsabilità globale della sicurezza, budget proprio e riporto diretto al CEO/BoD

— Modello di riferimento —



— Considerazioni —

- Si osserva come tendenzialmente tutte le aziende certificate BS7799 abbiano la funzione sicurezza dipendente da un CSO, che riporta direttamente al CEO/BoD, e che tale modello organizzativo è stato adottato principalmente dalle aziende USA e UK
- Il CSO ha la responsabilità globale della sicurezza (interna, esterna, fisica, logica, personale) e di tutti i suoi aspetti (strategia, governo, controllo e implementazione)
- Il CSO ha alle sue dipendenze:
 - un CISO, che ha la responsabilità della protezione delle informazioni e da cui dipendono:
 - ▶ IT Security Manager (sicurezza informatica)
 - ▶ IT Security Architect (risponde all'IT Security Manager e si occupa della pianificazione e sviluppo delle architetture di sicurezza)
 - ▶ IT Security Incident Manager (incidenti Informatici)
 - un Physical Security Officer (PSO), che gestisce la sicurezza fisica della struttura, incluse le eventuali norme di personal safety degli impiegati
- La parte investigativa, ove presente, è composta dal:
 - Capo dell'internal auditing, paritetico al CSO risponde come quest'ultimo al CEO
 - Chief Investigation Officer, che si occupa delle investigazioni interne e riporta al capo internal auditing. Il Chief Investigation Officer ha, inoltre, una serie di Senior Investigators, che si occupano di frodi/illeciti/violazioni delle politiche, anche di tipo AUP/Information Security. Si avvale dello staff di IT security per le operazioni di incident response e digital forensic

— Referenze —

Swiss Bank Corporation
HSBC
The Royal Bank of Scotland
Dresdner Bank
Citigroup
Republic National Bank New York
Standard Chartered Bank

Fidelity Investments
State Street Global Advisors
ING
Eurobank
Imperial Chemical Industries
DuPont

Nike Inc.
Thomson Corporation
Hershey Foods Corporation
Google
eBay
ENI
FIAT
Pirelli

In alcune realtà la funzione di Sicurezza è ancora posizionata nella componente IT, con il CISO che riporta al CIO

— Modello di riferimento —

— Considerazioni —



- Si osserva che tale modello organizzativo è ancora prevalentemente adottato nelle realtà bancarie italiane ed europee
- Il CISO dipende direttamente dal CIO ed è responsabile della pianificazione, del controllo e dell'implementazione del sistema di protezione delle informazioni e dell'architettura di sicurezza
- Il CISO si occupa prevalentemente della sicurezza logica e, in alcuni casi, di quella fisica, mentre il tema della Business Continuity viene ridotto alla definizione delle infrastrutture di Disaster Recovery nell'ambito delle attività di IT- Facility Management

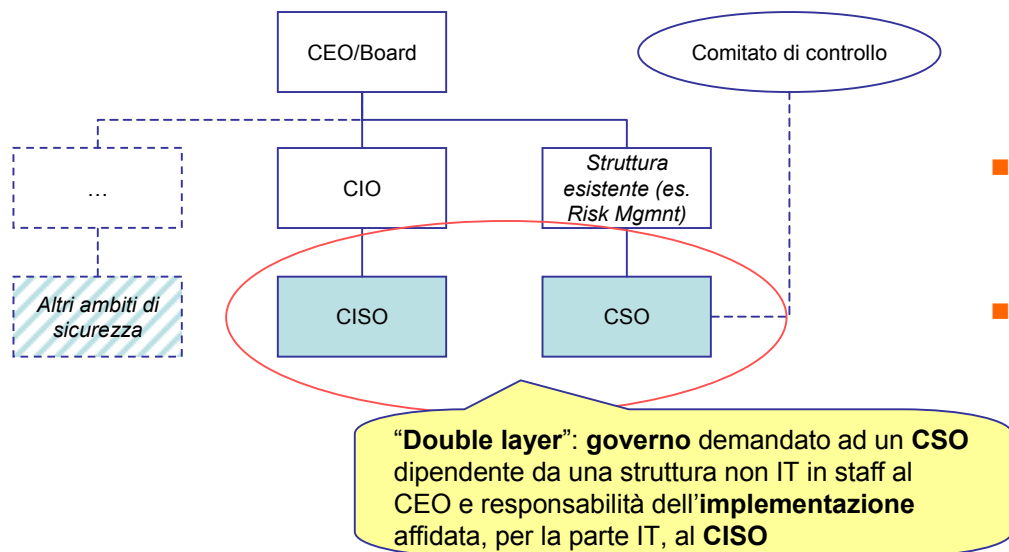
— Referenze —

Merrill Lynch
Bank of America
American Express
ABN Amro
National Bank Of Belgium
Crédit Agricole Indosuez

Banco Santander Central Hispano Americano
Banco Bilbao Vizcaya Argentaria
Capitalia
Solvay
Carnival Group

Vi è anche un modello “double layer”, in cui il CSO riporta ad una struttura di staff, mentre il CISO riporta al CIO

— Modello di riferimento —



— Considerazioni —

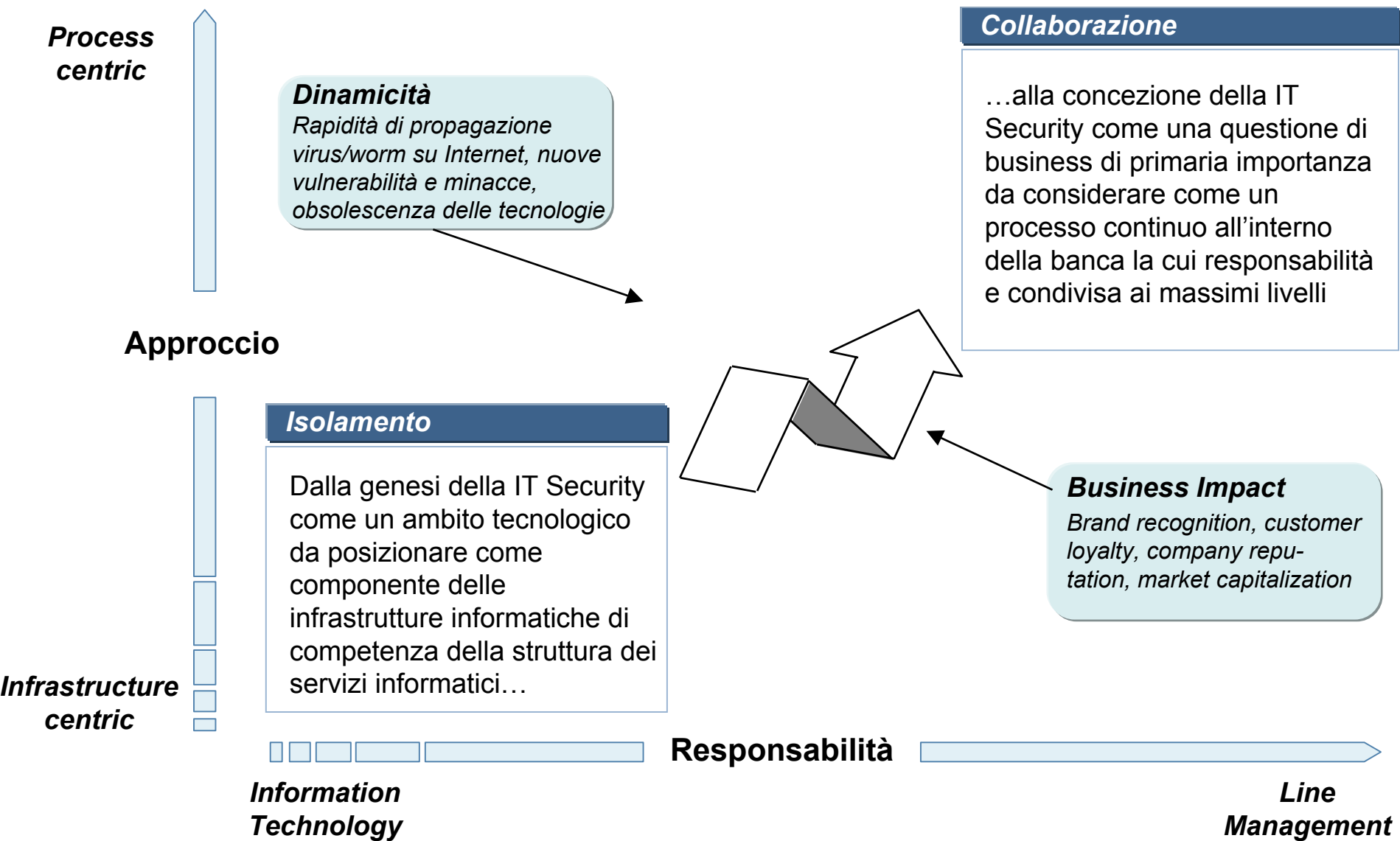
- Il CSO dipende da una struttura esistente di staff al CEO ed ha la responsabilità di definire le linee guida e gli obiettivi strategici e di controllarne l’effettivo rispetto; la responsabilità del rischio viene affidata ad un Comitato di controllo appositamente costituito
- L’applicazione delle strategie è demandata al CISO, per la parte IT, oppure ad altre strutture operative (ad esempio la Logistica) preposte al presidio delle diverse tipologie di rischio
- Il CISO risponde direttamente al CIO ed ha le seguenti responsabilità:
 - Protezione delle informazioni
 - Pianificazione e sviluppo delle architetture di sicurezza
 - Incidenti informatici

— Referenze —

JP Morgan Chase
Deutsche Bank
Unicredit
San Paolo IMI
BNL

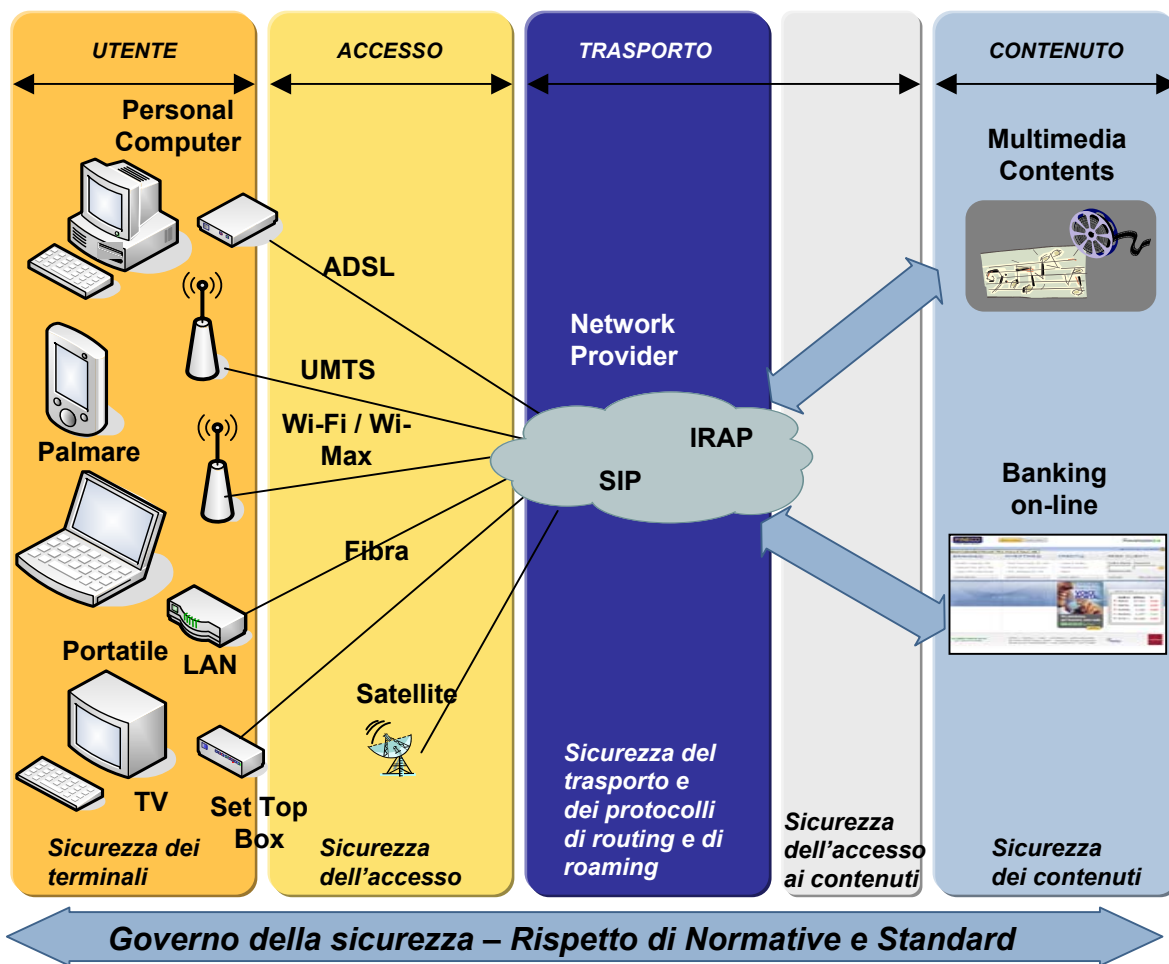
- L'evoluzione della Sicurezza all'interno del Gruppo Intesa
- Il modello di governo della Sicurezza integrata
- **Le prossime sfide in Banca Intesa**
- Considerazioni finali

La sicurezza assume un ruolo centrale verso gli altri processi e funzioni aziendali, erogando servizi ad alto valore aggiunto



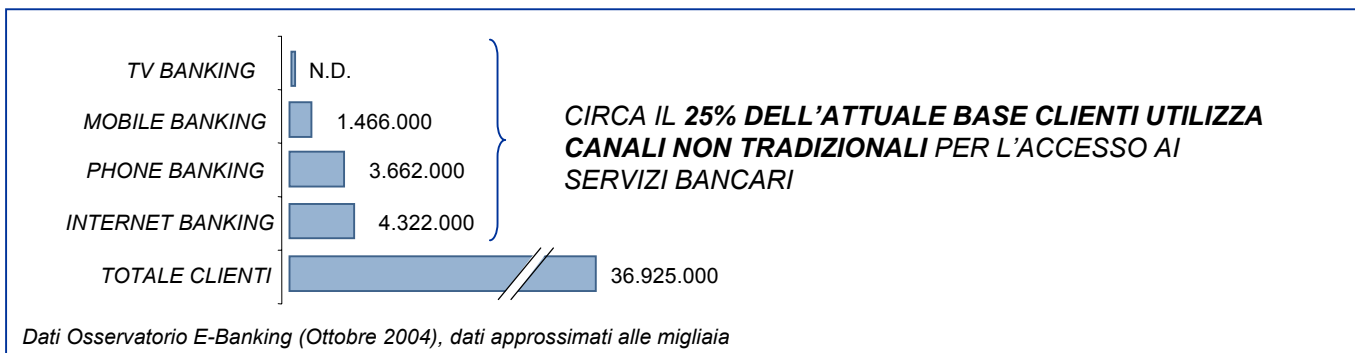
- Gestione unitaria del Business Continuity Management (sicurezza logica, fisica ed organizzativa)
- Gestione della clientela Canali Diretti
- Analisi dei rischi, definizione di un piano di sviluppo strategico e di allocazione del budget in ottica di servizio complessivo alla Banca vs. ottica di valorizzazione delle singole area di Sicurezza
- Gestione della tematica di “accessibilità” della persona a 360° (attraverso una gestione integrata degli accessi agli stabili, al sistema informativo, agli asset aziendali) vs. una gestione per singole aree di Sicurezza
- Monitoraggio complessivo degli eventi e gestione unitaria degli incidenti (attraverso un sistema di monitoraggio 24x7x365 che contempla sia gli eventi fisici che quelli logici) in ottica di massimizzare la capacità di analisi e la velocità di reazione vs. ...
- Univocità di indirizzo, massimizzazione dell’efficacia e minori costi attraverso la gestione unitaria di alcune attività quali, ad esempio, la Compliance e la Normativa, la Formazione, l’Intelligence e l’Investigation, la gestione delle relazioni con le Istituzioni

La tecnologia sta evolvendo rapidamente incidendo sulla sicurezza e sul modo di fare business (es. Internet e mobile banking)



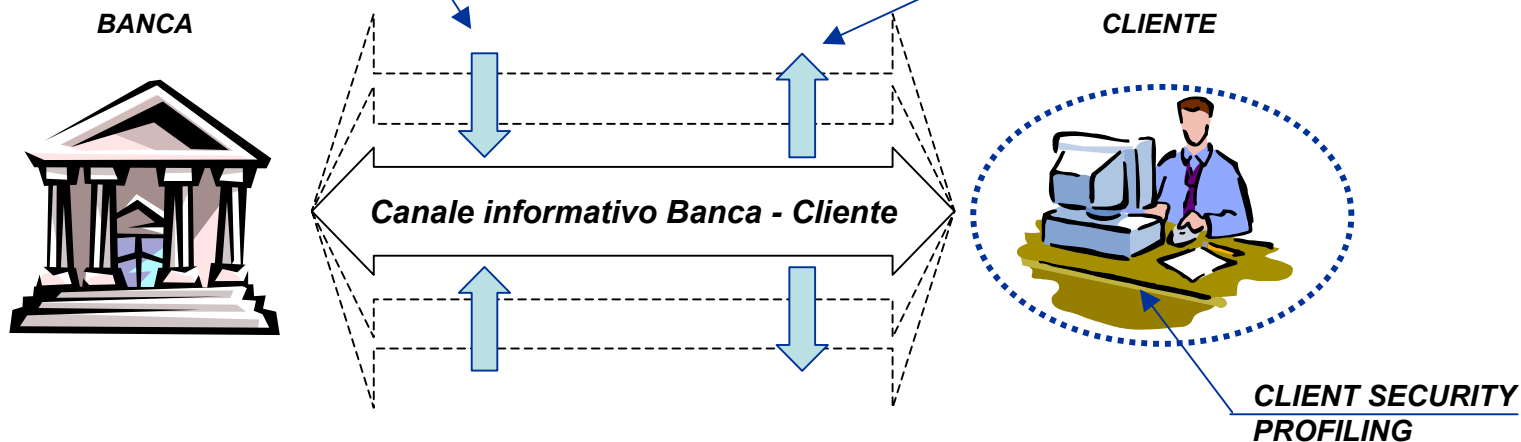
- Evoluzione Tecnologica**
 - Nuovi **Protocolli Accesso e Comunicazione** (WiMax, UMTS,...)
 - Evoluzione dei **terminali** (Open Source, maggiore capacità elaborativa, ...)
- Nuovi modelli di servizio**
 - **Integrazione** Fisso/Mobile
 - **Interworking** tra fornitori specializzati (Content/ Network Provider, ...)
- Centralità dei contenuti**
 - **Accesso ai contenuti (Identity Management)**
 - Gestione della **“proprietà” dei contenuti (DRM)**
- Governo end-to-end**
 - **Gestione operativa**
 - Rispetto di **normative e standard**
 - Gestione dei **livelli di servizio**

La sicurezza dei canali integrati come prima priorità di azione



La strategia di protezione del sistema Banca che impone una **segregazione di ambienti**, è in contrasto ...

... con una logica di Marketing che spinge per l'**apertura di servizi con modalità e canali differenti** e che persegue la facilità di fruizione degli stessi da parte dell'utente



- L'evoluzione della Sicurezza all'interno del Gruppo Intesa
- Il modello di governo della Sicurezza integrata
- Le prossime sfide in Banca Intesa
- **Considerazioni finali**

- Il percorso di evoluzione da funzione prettamente tecnica a funzione anche di governo ed indirizzo della Sicurezza richiede competenze e risorse adeguate al nuovo ruolo
- E'opportuno individuare ed attribuire responsabilità decisionali in posizione molto vicina la Vertice Aziendale
- Deve essere definito e progressivamente attivato un modello di funzionamento della Sicurezza integrata
- E'nessario comprendere che la costruzione di una funzione di governo non è solo un esercizio formale ma un percorso che deve essere sostenuto in tutte le sue fasi evolutive
- Per crescere, la funzione di Sicurezza integrata deve essere in grado di collaborare con le strutture di business nel perseguimento degli obiettivi di mercato integrando le logiche di Sicurezza con:
 - il rispetto delle logiche del time to market
 - la considerazione delle logiche competitive dei mercati
 - le priorità di indirizzo operativo
 - l'ottimizzazione ed il contenimento dei costi
- Per collaborare proficuamente con i business owner, la funzione deve dotarsi di adeguate competenze di processo che permettano per tempo di condividere soluzioni e non solo di evidenziare problemi
- E'nessario garantire la massima priorità alle iniziative realmente importanti per la tutela degli asset e degli ambito operativi della Banca.
- A tal fine è indispensabile attivare un processo efficace di pianificazione e realizzazione dell'analisi del rischio e definire i meccanismi e le regole volte all'approvazione del piano di Sicurezza



Sicurezza Logica e le altre funzioni di sicurezza - sinergie, conflitti, opportunità - benchmarking con altre importanti realtà bancarie e non

Stefano Cabianca
Responsabile Servizio Gestione Sicurezza Informatica

stefano.cabianca@bancaintesa.it

Roma, 16 giugno 2005