La valutazione del rischio informatico e gli impatti sul business

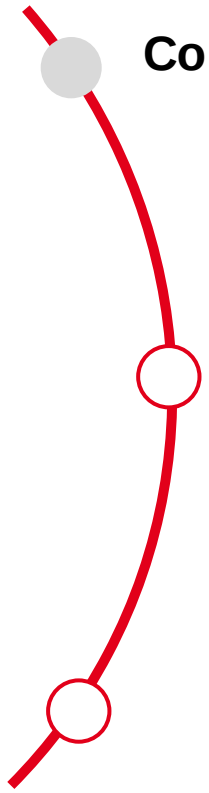
Convegno ABI: Basilea 3, Risk & Supervision 2014

Stefano Alberigo, Head of Group Operational & Reputational Risk Oversight di UniCredit

Nicasio Muscia, Manager della practice Finance & Risk di Accenture

Roma, Palazzo dei Congressi, 17 Giugno 2014

Agenda



Contesto normativo e trend di mercato

Possibili approcci alla valutazione del rischio ICT e impatti sul business

L'Integrazione con il Framework complessivo di gestione dei rischi operativi – Spunti di riflessione

Il contesto di riferimento

L'evoluzione del contesto regolamentare e nuovi modelli di *business* richiedono un approccio strutturato per la gestione del rischio informatico

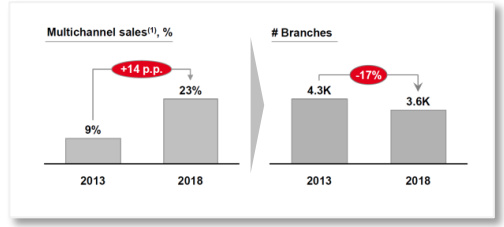
***Evoluzione normativa**: Nuovi requisiti Bankit*

- Definizione di un *«… quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico… e integrazione con i sistemi di misurazione e gestione dei rischi …» e della «… propensione al rischio informatico …»*

Fonte: 15° aggiornamento della Circolare n.263/2006, Banca d'Italia 2013

Strategia/ Investimenti: Investimenti in innovazione e digitalizzazione **per € 1 mld**

1. *Flexible branch formats*
2. *Integration of digital and physical network*
3. *Big Data analytics*
4. *Remote sales enablement*
5. *Process digitalization*
6. *Paperless banking services*



Fonte: Unicredit Group, Piano strategico 2013 - 2018

Evoluzione di mercato: Principali trend identificati nel mercato per i prossimi anni

A	**Business da fisico a digitale**	Stimati 212 miliardi $ di investimenti entro il 2020
B	**La nuova *supply chain* dei dati**	Solo 1/5 delle società sul mercato integrano i dati di tutta l'Azienda
C	**Il business delle applicazioni**	Entro il 2017, 1/4 delle società sul mercato disporranno di *App store*
D	**Architettura sempre più solida**	Crescente domanda di processi, servizi e sistemi non-stop (più resilienza e disponibilità)
…		

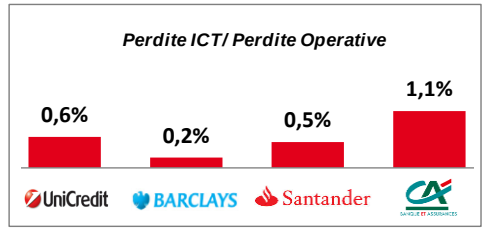
Fonte: Accenture Vision 2014, ogni business è digitale

Framework per la gestione dei Rischi ICT

Stato dell'arte ed evoluzioni future

I nuovi trend di mercato e regolamentari rendono necessaria una revisione/ integrazione dei pilastri utilizzati sino ad oggi per la gestione del rischio informatico

	SITUAZIONE ATTUALE	TEMI DA INDIRIZZARE
Valutazione dei Rischi ICT	▪ **Valutazione del Rischio Informatico** basata su dati di perdita economica	▪ Integrazione delle **perdite di reputazione** e di **quote di mercato** nella valutazione del Rischio Informatico
Eventi ICT rilevanti	▪ Presidi strutturati in essere per la mitigazione dei rischi **legati alle risorse fisiche** *(es. immobili, persone)* **ai fini della Continuità Operativa**	▪ Definizione/ rafforzamento dei presidi per la mitigazione dei rischi di **disfunzione/ interruzione delle Risorse ICT**
Governo dei Rischi ICT	▪ **Gestione a silos del Rischio Informatico** attraverso presidi specifici (e.g. OpRisk Mgmt, BCM, ICT Security, ICT Operation)	▪ Definizione di **meccanismi di coordinamento/ integrazione** delle attività in capo ai principali Attori coinvolti nella gestione del Rischio Informatico



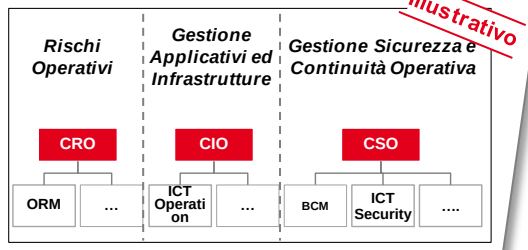
Fonte: Pillar III disclosure delle Banche selezionate

GRUPPO BPER ➢ *Terremoto in Emilia (05/2012): attivazione tempestiva delle procedure/ protocolli per la Continuità Operativa*

citi ➢ *Uragano Sandy (10/2012): riallocazione delle risorse nelle zone meno a rischio garantendo la continuità del servizio bancario*

Fonte: Il Sole 24 Ore, The Business Continuity Institute

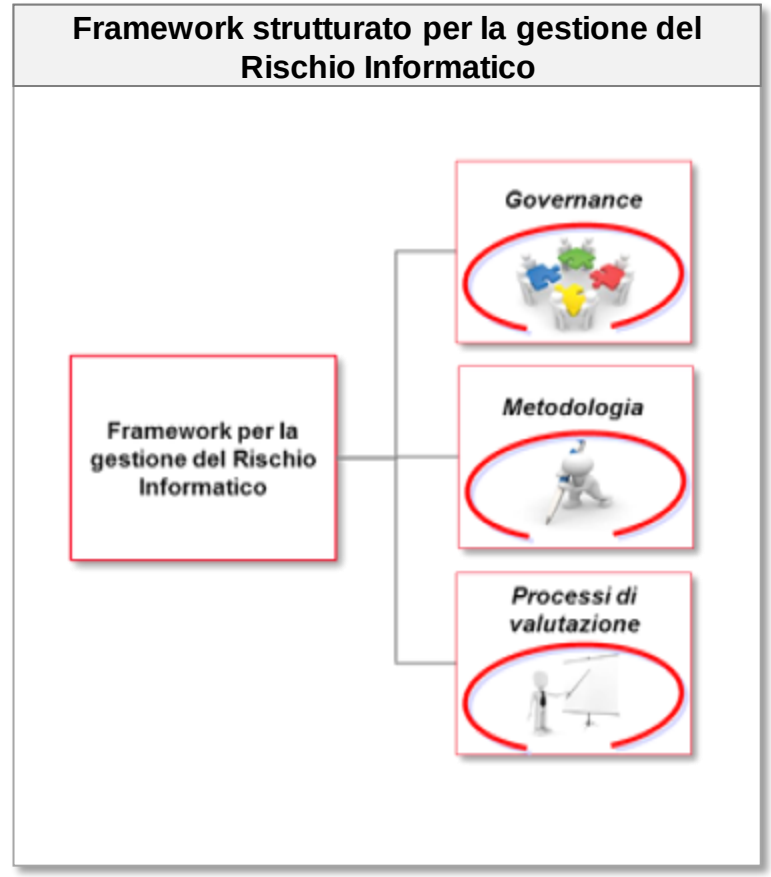
➢ *Attacco Informatico (03/ 2013): Indisponibilità dei servizi delle 3 principali banche Sudcoreane*



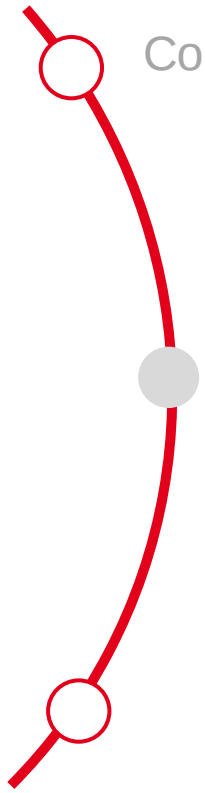
Framework per la gestione del Rischio Informatico

Per far fronte ad i temi aperti derivanti dai cambiamenti in atto è necessario che gli intermediari intervengano su 3 componenti: governo, metodologia, processi di valutazione

1. *Quali attori coinvolgere e quale modello relazionale definire?*
2. *Quale tassonomia dei rischi e degli Asset ICT adottare?*
3. *Quali metriche per la determinazione degli impatti?*
4. *Quale processo e chi identificare come Utente Responsabile?*



Agenda



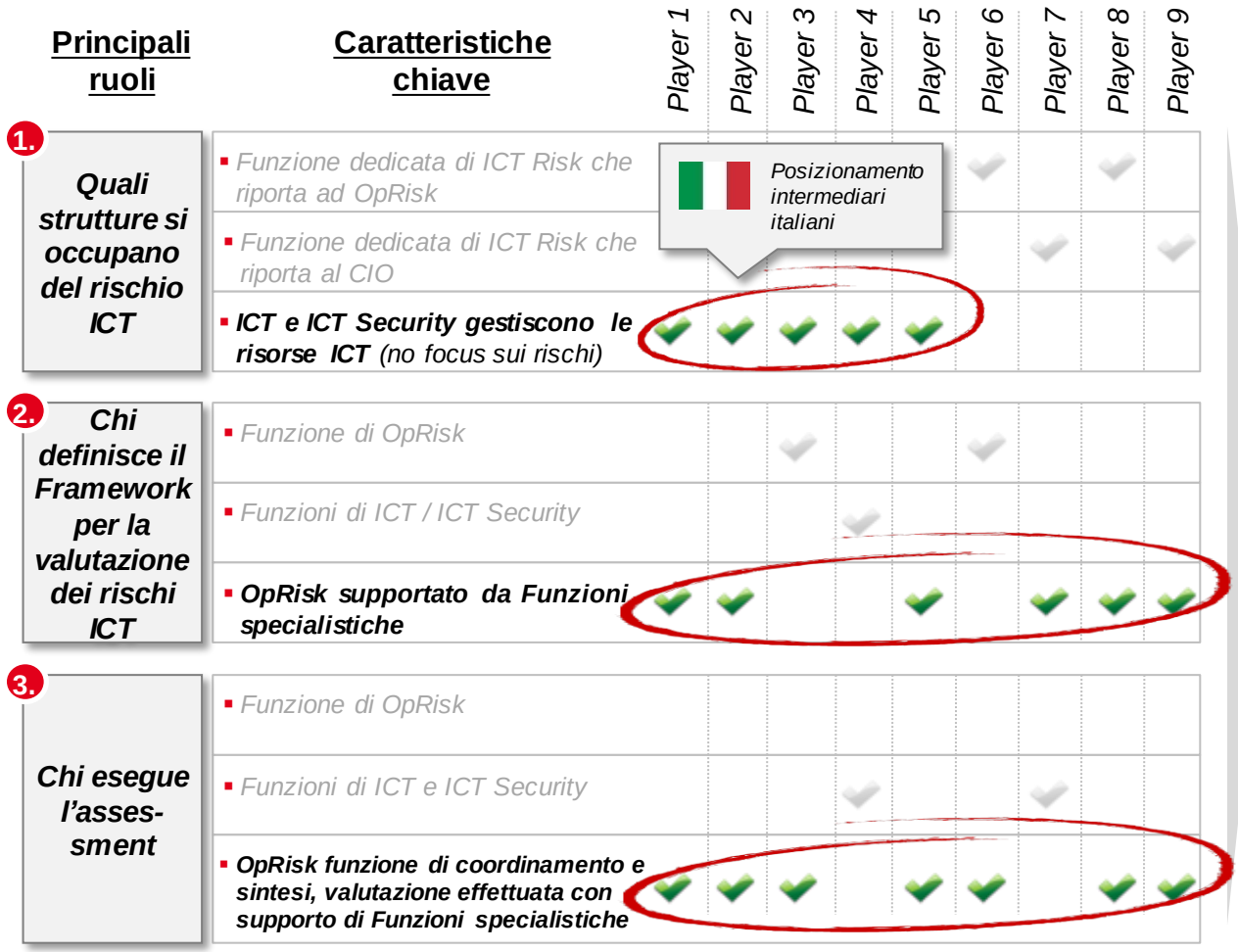
Contesto normativo e trend di mercato

Possibili approcci alla valutazione del rischio ICT e gli impatti sul business

L'Integrazione con il Framework complessivo di gestione dei rischi operativi – Spunti di riflessione

Il governo del rischio informatico

Diversi sono i modelli di governance per una adeguata gestione del rischio ICT che vedono il coinvolgimento dell'OpRIsk, ICT e ICT Security



- Ad oggi, nella maggior parte dei player in perimetro, **il Rischio Informatico è presidiato** da parte delle strutture specialistiche **con un approccio a «silos»**
- **OpRisk è fortemente coinvolto** nella fase di **definizione della metodologia**
- Inoltre, quest'ultimo svolge **il ruolo di coordinamento e sintesi** mentre la **valutazione del rischio è effettuata con il supporto di funzioni specialistiche** (ICT/ ICT Security)

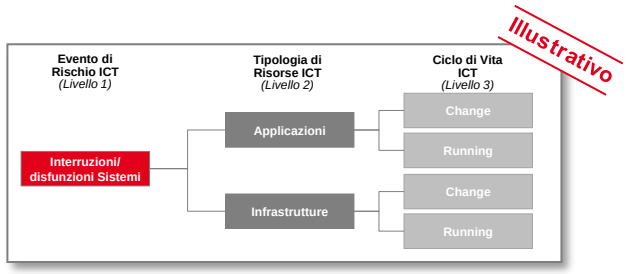
Fonte: *Benchmark Internazionale Accenture sulla Gestione del Rischio Informatico effettuato su un campione di 9 Intermediari internazionali (campione composto da: Barclays, RBS, BBVA, Goldman Sachs, JP Morgan, PNC BANK, State Street, Northern Trust, Unicredit Group)*

Gli elementi chiave della metodologia:Tassonomia dei rischi e classificazione degli Asset

La tassonomia dei rischi deve tener conto della tipologia di risorse ICT e del loro ciclo di vita mentre gli asset ICT devono essere classificati secondo le 3 dimensioni indicate da Bankit

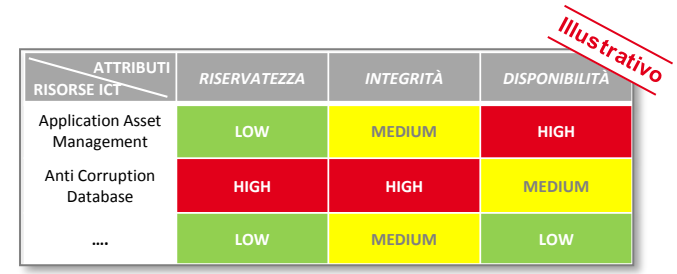
TASSONOMIA DEI RISCHI INFORMATICI

- Definizione delle categorie dei **Rischi ICT potenziali** sulla base di:
  - **Eventi di Rischio ICT** definiti dal Comitato di Basilea (Interruzioni/ disfunzioni Sistemi IT)
  - **Tipologia di Risorse ICT** (Applicativi, Infrastrutture, Sistemi di Sicurezza)
  - **Ciclo di vita delle Risorse ICT** *(Change, Running)*



CLASSIFICAZIONE DELLE RISORSE ICT

- Definizione della cartografia delle **Risorse ICT** in termini di ***Applicativi*** *e* ***Infrastrutture***
- **Mappatura dei Servizi ICT** e dei **Processi Bancari** supportati dalle Risorse ICT
- **Classificazione delle Risorse ICT** sulla base dei potenziali impatti di violazioni dei livelli di «Riservatezza», «Integrità» e «Disponibilità» stimati dagli Specialisti IT e dagli Utenti di Business adottando un «approccio qualitativo»



ATTRIBUTI / RISORSE ICT	RISERVATEZZA	INTEGRITÀ	DISPONIBILITÀ
Application Asset Management	LOW	MEDIUM	HIGH
Anti Corruption Database	HIGH	HIGH	MEDIUM
....	LOW	MEDIUM	LOW

Metriche per la valutazione del rischio informatico

Gli incidenti informatici costituiscono la metrica chiave per la valutazione degli impatti del rischio informatico

3

1. *DRIVER DI VALUTAZIONE DEL RISCHIO ICT*

INCIDENTI INFORMATICI

Illustrativo

- *Numero Incidenti = 50*
- *Percentuale (%) transazioni impattate*

Se opportunamente classificati, ***gli Incidenti Informatici esprimono la manifestazione del rischio*** *fornendo:*

- *indicazioni per la quantificazione delle metriche di impatto (es. facendo leva sulla durata dell'indisponibilità del servizio);*
- *elementi di back testing per verificare la coerenza con precedenti assessment qualitativi.*

2. *VALUTAZIONE DELLE METRICHE DI IMPATTO*

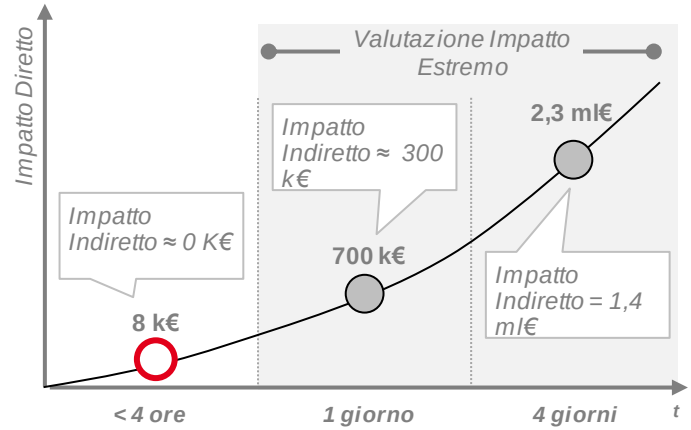
IMPATTO DIRETTO

- **Volumi di business**
- **Numero di clienti impattati**
- **Interesse per pagamenti in ritardo**
- **Sanzioni Regolamentari**
- **Spese per Contenziosi**

IMPATTO INDIRETTO

- **Perdita di Profitto (indice di customer satisfaction)**

3. *RISULTATI VALUTAZIONE DI IMPATTO*



Il processo di gestione del Rischio Informatico

Il processo di valutazione del rischio ICT è strutturato in 5 fasi mentre l'utente responsabile può essere individuato sia in strutture di Business che di Orga

FASI PRINCIPALI	ATTORI COINVOLTI
1. *Avvio e set up*	▪ Risk Management ▪ Organizzazione ▪ CIO
2. *Identificazione e valutazione*	▪ Risk Management ▪ CIO ▪ **Utente Responsabile** ▪ Altre Funzioni di supporto/ Organizzazione
3. *Analisi di coerenza*	▪ Risk Management
4. *Gestione e mitigazione del rischio*	▪ **Utente Responsabile** ▪ Risk Management ▪ CIO
5. *Monitoraggio e reporting*	▪ Risk Management

Chi è l'UTENTE RESPONSABILE?

Utente Responsabile ≡ Organizzazione

Utente Responsabile ≡ Business Owner

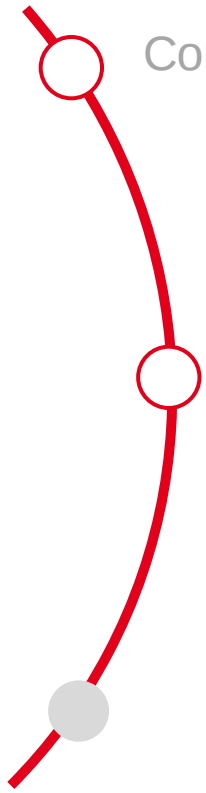
Pro

- *Possiede **una visione d'insieme***
- *Conoscenza approfondita **delle procedure IT***
- ***Coerenza con logiche RAF** e sinergie **con Framework ORM***
- *Conoscenza **approfondita degli impatti degli incidenti lato business***

Contro

- ***Poco coerente con le logiche RAF** e con il Framework ORM*
- ***Scarsa conoscenza** degli **impatti** degli incidenti **lato business***
- ***Identificazione onerosa***
- ***Limitata visione d'insieme***

Agenda



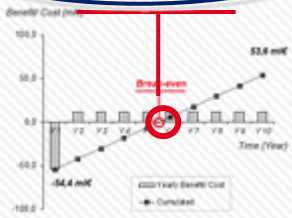
Contesto normativo e trend di mercato

Possibili approcci alla valutazione del rischio ICT e impatti sul business

L'Integrazione con il Framework complessivo di gestione dei rischi operativi – Spunti di riflessione

Integrazione del Rischio Informatico con il modello complessivo dei Rischi Operativi

Integrazione con il RAF e la valutazione dei progetti ICT sono 2 ulteriori sfide che devono essere affrontate per consentire una efficace gestione del rischio ICT

Ambito	Fattori critici di successo
A *L'accettazione del rischio e RAF* Fattori correzione $\frac{ExLosses}{Budget\ Costs}$ α β …	▪ **Stretto legame con tassonomia/linguaggio CFO** ▪ Utilizzo di **indicatori in grado di «catturare» fenomeni rilevanti** quali l'incidentalità attesa ▪ Identificazione di **fattori quali/quantitativi** che consentono l'introduzione di elementi prospettici ▪ **Indicatori *«actionable»*** che consentono di identificare interventi correttivi realizzabili
B *La valutazione dei progetti* $\frac{\Delta\ Risk}{\Delta\ Costs}$ 	▪ Definizione di un **approccio integrato con RAF** ▪ Valutazione basata su **criteri di rischio/rendimento** ▪ **Coerenza** con approccio per la valutazione dei **rischi ICT**

Framework complessivo della gestione dei rischi operativi

… oltre la *Compliance* regolamentare

Principali benefici di un Framework strutturato per la gestione del rischio informatico

PRINCIPALI BENEFICI

- **Scelte strategiche informate** «ICT *risk-based*» che contribuiscono al raggiungimento degli obiettivi strategici ed operativi;
- **Ottimizzazione degli investimenti** che tengono in considerazione il Rischio Informatico garantendo una migliore allocazione del capitale;
- **Gestione proattiva di potenziali minacce/ vulnerabilità** attraverso l'allineamento a standard Internazionali (es. COBIT, ISO) e miglioramento nel processo di gestione degli Incidenti Informatici;
- **Chiara definizione dei ruoli e delle responsabilità** degli attori coinvolti nella gestione dei Rischi Informatici.