Analisi e gestione del rischio informatico: metodologie, strumenti e best practice nel sistema bancario italiano

Dott. Marco Valsecchi
Responsabile Practice Sicurezza, Rischi e Controlli ICT OASI

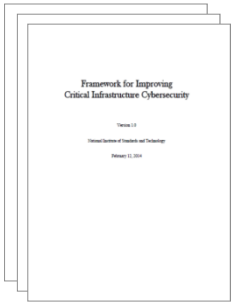
ABI Banche e Sicurezza 2015 – 5 Giugno 2015, Palazzo Altieri

Agenda del documento

1 ***Premessa: normative, framework e requisiti di riferimento per l'analisi del rischio informatico***

- Approccio metodologico per la definizione della strategia e dei piani operativi di sicurezza
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di analisi del rischio
- L'impegno di OASI a supporto delle banche in tema di gestione del rischio informatico

L'analisi del rischio informatico viene richiesta / suggerita da diverse normative / framework cui fanno riferimento gli attori del sistema bancario

Normative / framework		Contenuto	Perimetro di attuazione
Nuove disposizioni di vigilanza prudenziale per le banche *(Circolare n. 263 del 2 luglio 2013)*		L'analisi del rischio informatico costituisce uno strumento **a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT**, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario	Tutto il sistema informativo
Final guidelines on the security of internet payments *(EBA, 19 dicembre 2014)*		I Prestatori di Servizi di Pagamento devono condurre e documentare **i risk assessment relativi alla sicurezza dei pagamenti effettuati su internet** e ai servizi correlati	Sistemi IT coinvolti nell'erogazione dei servizi di pagamento
Framework for Improving Critical Infrastructure Cybersecurity *(National Institute of Standards and Technology)*		Il risk management è un **processo continuo per l'identificazione, la misurazione e la gestione del rischio**. Le organizzazioni devono verificare la probabilità di accadimento e l'impatto degli eventi e devono determinare la propria tolleranza al rischio	Sistemi IT esposti ai rischi di cybersecurity

I diversi requisiti relativi alla conduzione dell'analisi del rischio informatico generano una serie di tematiche da affrontare…

I Integrazione

- E' necessario definire **framework univoci** al fine di garantire la conduzione di valutazioni omogenee, evitare la duplicazione di processi di valutazione, introdurre vincoli operativi non utili rispetto alle esigenze di business e di protezione della banca

II Responsabilità

- E' necessario **incrementare la responsabilità e la consapevolezza** degli organi con funzioni di delibera fronte di un utilizzo sempre più pervasivo delle componenti IT nelle «macchine operative» delle banche

Per le banche che adottano componenti più o meno estese di outsourcing, il rischio permane in capo alla Banca, che può comunque in parte mitigarlo tramite vincoli contrattuali e processi di controllo dedicati

III Strutturazione

- E' necessario **valutare la connessione** tra la rilevanza dei processi di business, la tipologia di dati trattati e le misure di sicurezza implementate. A tal fine è necessario essere in grado di categorizzare il sistema informativo per fornire una valutazione chiara e mantenibile nel tempo delle relazioni Business – IT

IV Formalizzazione

- E' necessario **documentare le attività** di analisi svolte per incrementare ulteriormente la responsabilità degli organi e delle strutture coinvolte nella formulazione di assunzioni valutative e delle conseguenti decisioni in merito all'accettazione dei rischi residui

V Automazione

- E' necessario automatizzare il **processo di valutazione nel continuo** del rischio informatico per gestire la definizione / modifica di prodotti di business, l'introduzione o il cambiamento di infrastrutture tecnologiche, la rendicontazione dei rischi operativi e, in generale, dei rischi aziendali

Agenda del documento

- Premessa: normative, framework e requisiti di riferimento per l'analisi del rischio informatico

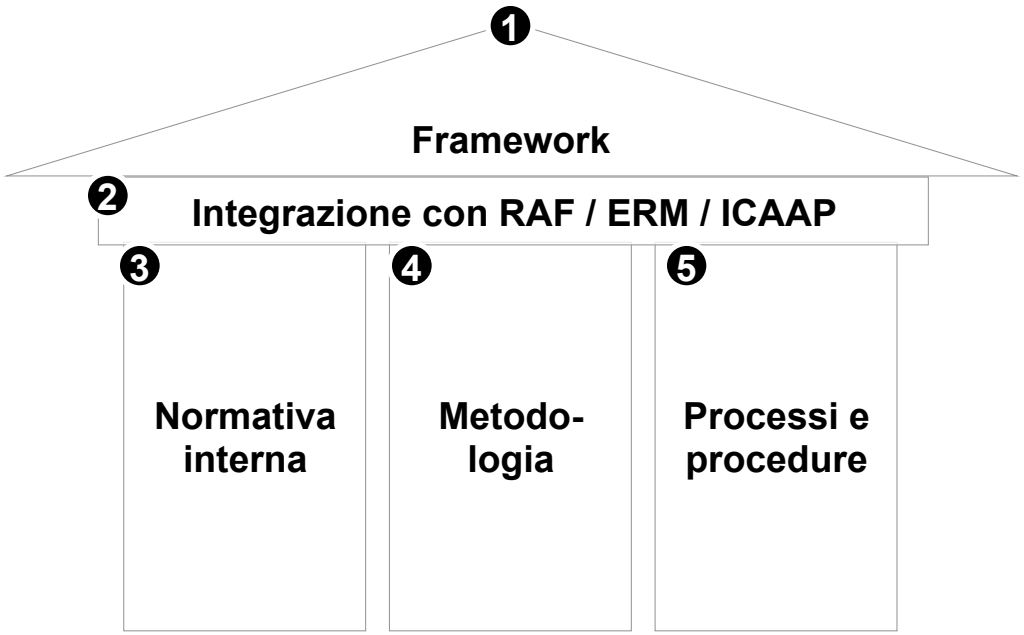
2 ***Approccio metodologico per la definizione della strategia e dei piani operativi di sicurezza***

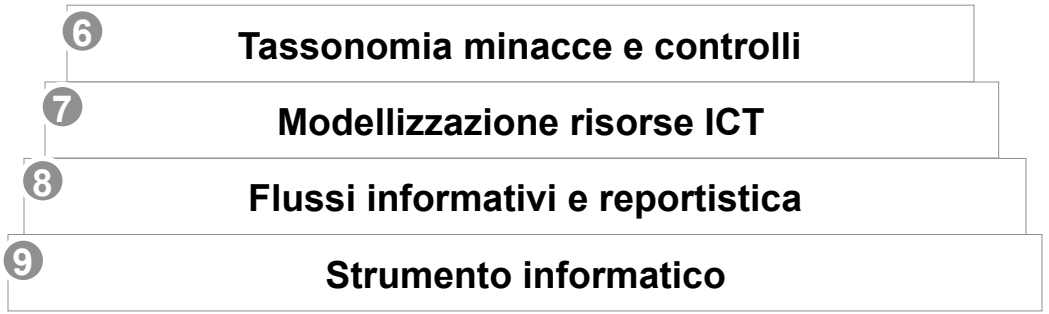
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di analisi del rischio

- L'impegno di OASI a supporto delle banche in tema di gestione del rischio informatico

E’ quindi necessario definire un framework univoco a livello aziendale che consenta di «abbracciare» le necessità specifiche in modalità univoca

Modello di riferimento





Elementi costituenti del modello

GOVERNO

1. Framework di riferimento a livello di Gruppo Bancario per il rischio informatico
2. Allineamento / integrazione del rischio informatico con il RAF e ERM
3. Normativa interna per la regolamentazione della gestione del rischio informatico
4. Metodologia per l’analisi e la gestione del rischio informatico
5. Processi / procedure per l’esecuzione delle attività necessarie alla gestione del rischio informatico

ESECUZIONE

6. Tassonomie driver / eventi di rischio informatico e relativi controlli / misure
7. Modellizzazione risorse informatiche e architetture del sistema informativo
8. Flussi informativi e reportistica verso gli Organi aziendali
9. Strumentazione operativa per lo svolgimento dell’analisi e la gestione del rischio informatico

La determinazione del rischio informatico si basa su elementi di valutazione che consentono di associare la «dimensione di business» alla «dimensione tecnologica»

Il rischio informatico associato (tramite criteri di valutazione qualitativi oppure quantitativi, ove possibile) ad una risorsa informatica adottata per l'erogazione di un processo / servizio di business erogato *dall'intermediario finanziario, è determinato dalla combinazione tra:*

I. i ***potenziali impatti negativi*** *che ne conseguirebbero per l'intermediario finanziario stesso;*

II. il ***livello di esposizione a un determinato scenario di rischio informatico*** *(valutato a sua volta come combinazione tra la probabilità di accadimento delle minacce che lo possono determinare e l'intensità dei controlli in essere);*

Gli elementi costitutivi di un rischio informatico sono quindi i seguenti:

Elementi costitutivi

1. **Processo / servizio di business** — Servizio / processo di business, basato sull'utilizzo di una o più piattaforme di Information Technology
2. **Risorsa informatica** — Elemento tecnologico che concorre alla ricezione, archiviazione, elaborazione e trasmissione di dati a supporto dei processi di business
3. **Scenario di rischio informatico** — Categoria di eventi che può concretizzarsi su una o più risorse informatiche, determinando un impatto sui processi di business

Elementi costitutivi

4. **Impatto** — Danno potenziale arrecato alla Banca in seguito al concretizzarsi di uno scenario di rischio informatico
5. **Minaccia** — Tipologia di evento, cui è potenzialmente esposta una risorsa informatica e che, nel caso in cui accadesse, produrrebbe il concretizzarsi di uno scenario di rischio
6. **Controlli** — Misura di tipo tecnico o organizzativo che può essere implementata al fine di mitigare il rischio informatico

La metodologia di valutazione deve garantire un approccio integrato tra Business Owner e IT / Security Manager

Pre-requisiti per l'implementazione di un modello di analisi efficace

- La banca deve disporre di un **catalogo dei processi / prodotti / servizi di business definito** in termini di strutture responsabili e di strutture utenti del sistema informativo
- La banca deve disporre di un **modello di enterprise architecture definito** che consenta di clusterizzare i componenti informatici in «filiere» omogenee in termini di tecnologie e di applicazioni supportate
- E' necessaria un'adeguata **sponsorship del vertice** per introdurre un approccio «risk based» e di medio-lungo periodo all'interno di processi finalizzati a garantire l'operatività «a breve» del sistema informatico

Alcuni ambiti specifici richiedono una modellizzazione dedicata per poter valorizzare un impianto unico di analisi del rischio informatico…

Ambito	Necessità	Modellizzazione
1 **Canali di erogazione**	Gli stessi processi aziendali sono tipicamente **erogati tramite diversi canali**: filiale / internet bkg / phone bkg / … A canali diversi corrispondono minacce, contromisure e componenti tecnologiche differenti, con valutazioni di rischio informatico differenti	Per ciascun processo sono analizzate le **applicazioni utilizzate su ciascun canale** di accesso e, di conseguenza, le relative filiere di riferimento. Il livello di rischio **è disponibile per ogni applicazione** utilizzata e per ogni canale di erogazione
2 **Cybercrime**	In aggiunta agli scenari «standard», introduce uno **scenario dedicato alla valutazione delle minacce che afferiscono la clientela**, che prevedono delle contromisure specifiche la cui responsabilità è, almeno parzialmente, in carico alla banca	Le componenti informatiche utilizzate per l'erogazione dei servizi on-line vengono **categorizzate in filiere specifiche**, valutate anche rispetto allo scenario di «violazione dei servizi on-line», cui sono applicate minacce e contromisure specifiche
3 **Outsourcer / Fornitori esterni**	Richiede la valutazione su servizi non gestiti direttamente in termini di infrastruttura e rispetto ai quali è necessario un contributo di terze parti di natura / dimensione eterogena	L'approccio proposto è **dimensionato all'impatto** previsto in caso di evento di rischio informatico: • Audit presso il fornitore • Questionario definito dalla banca • Integrazione valutazioni del fornitore • Autovalutazione referenti interni

Principali rischi informatici «potenziali» che richiedono valutazioni approfondite delle contromisure in essere e/o piani di trattamento specifici

Principali rischi informatici potenziali	Rilevanza
Divulgazione dei dati della clientela a seguito di accesso per campagne di mktg	
Divulgazione dei dati della clientela a seguito di accesso per assistenza clienti	
Scarsa qualità dei dati per la predisposizione bilancio	
Indisponibilità dei dati per la predisposizione bilancio nelle scadenze critiche	
Scarsa qualità dei dati per determinazione livello di rischio / accantonamenti	
Divulgazione dei dati dei dipendenti a seguito di utilizzo per gestione retribuzioni	
Disponibilità dei servizi informatici a supporto dei processi critici	
Divulgazione / alterazione dei dati dei bancari clienti relativi a movimenti e patrimonio	
Alterazione dei dati dispositivi relativi a mandati di incasso / pagamento	
Furto delle credenziali di accesso ai sistemi di pagamento multicanale	
Alterazione / indisponibilità dei servizi di accesso alla banca in modalità multicanale	
Divulgazione di documenti strategici per intrusione nei sistemi direzionali	
Interruzione dei servizi informatici per errori operativi nelle attività di manutenzione	

Alcune delle soluzioni di mitigazione adottate / in adozione per i principali scenari di rischio informatico

Ambito / soluzioni	Alterazione dati	Furto dati	Disponi-bilità dati	Non Conformità
1 Sistemi / DB				
• Mediazione per accesso a sistemi e basi dati	✓	✓		✓
• Gestione delle utenze impersonali	✓	✓		✓
• Funzionalità applicative di accesso ai dati	✓			✓
• Controlli su input / output dati dispositivi	✓			✓
• Back-up dei dati			✓	✓
• Cifratura dati critici di produzione		✓		✓
• Mascheramento dati in ambienti di collaudo		✓		✓
2 Rete tlc				
• Segregazione / segmentazione di rete	✓	✓	✓	✓
• Controllo accessi alla rete		✓	✓	✓
• Protezione rete dispositivi esterni	✓	✓	✓	✓
3 Traccia-menti				
• Log collection operazioni ICT (Gar. I)	✓	✓		✓
• Log collection operazioni utente (Gar. II)		✓		✓
• Tracciamento grafico operazioni critiche	✓	✓		✓
4 Controllo accessi				
• Gestione centralizzata delle identità	✓	✓		✓
• Gestione centralizzata delle abilitazioni	✓	✓		✓
• Gestione dei privilegi di accesso al SI	✓	✓	✓	✓
• Certificazione dei privilegi di accesso al SI	✓	✓		✓
5 Controparti / fornitori				
• Protezione dei flussi scambiati con controparti	✓	✓		✓
• Requisiti / vincoli di sicurezza con fornitori	✓	✓	✓	✓
• Censimento / governo di fornitori			✓	✓

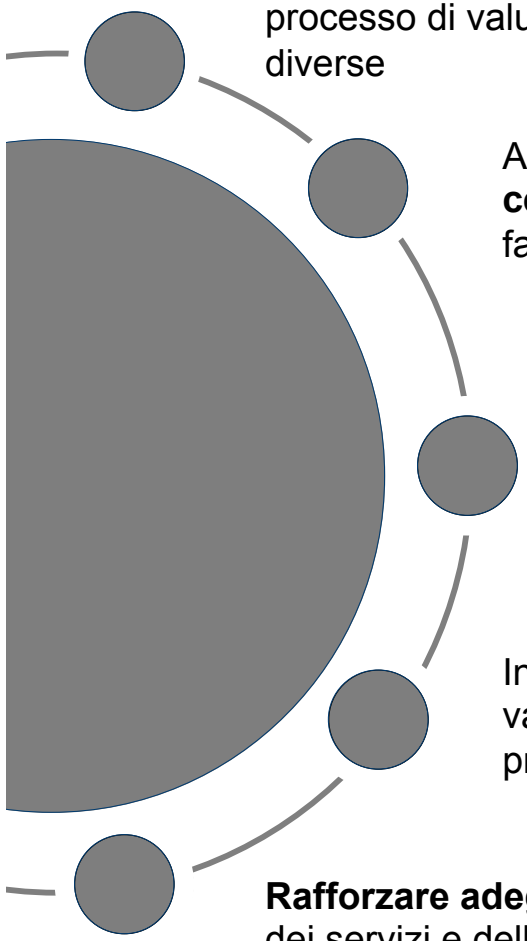
Agenda del documento

- Premessa: normative, framework e requisiti di riferimento per l'analisi del rischio informatico
- Approccio metodologico per la definizione della strategia e dei piani operativi di sicurezza

3 ***Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di analisi del rischio***

- L'impegno di OASI a supporto delle banche in tema di gestione del rischio informatico

Indicazioni metodologiche per l'attuazione di un processi di analisi del rischio adeguato alle necessità operative e ai requisiti normativi vigenti



Definire **un'unica metodologia di analisi del rischio informatico** da attuare per le diverse necessità di sicurezza e di conformità normativa: in tal modo si creano efficienze nel processo di valutazione e si garantisce l'univocità delle valutazioni condotte con finalità diverse

Adottare approcci di analisi che facciano riferimento a **framework definiti e certificati a livello nazionale** e conformi agli standard internazionali così da facilitare l'interlocuzione con centri servizi / fornitori esterni

Parlare un **linguaggio comprensibile dal business owner** in termini di tipologie di rischi coinvolti, livelli effettivi di rischio e tipologie di iniziative di trattamento da implementare. Nei modelli più maturi introdurre logiche di **analisi e valutazione di natura quantitativa**

Introdurre **strumenti che supportino l'IT Risk Manager** nella conduzione di valutazioni su una molteplicità di risorse informatiche e che introducano un processo strutturato, tracciato e conforme alla normativa esterna

Rafforzare adeguatamente le iniziative di IT Governance per la definizione dei processi, dei servizi e dell'architettura informatica in quanto costituiscono la base di partenza per lo sviluppo di un processo di analisi del rischio efficace

Agenda del documento

- Premessa: normative, framework e requisiti di riferimento per l'analisi del rischio informatico
- Approccio metodologico per la definizione della strategia e dei piani operativi di sicurezza
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di analisi del rischio

4 ***L'impegno di OASI a supporto delle banche in tema di gestione del rischio informatico***

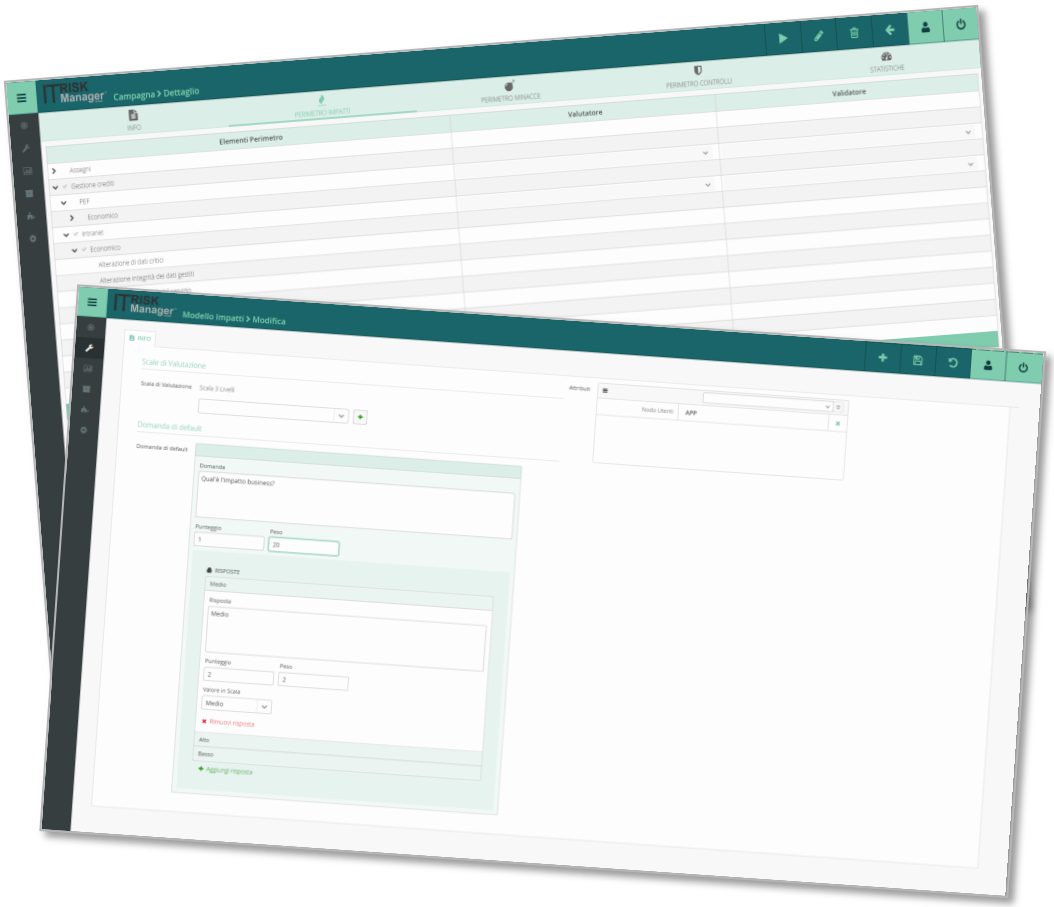
Oasi garantisce un'offerta completa e innovativa in tema di servizi e soluzioni in materia di sicurezza, rischi e compliance ICT

Ambito	Consulenza	Soluzioni	Servizi / outsourcing
Sicurezza informatica	- Policy e procedure - Gestione rischio informatico - Conformità Privacy - Certificazioni ISO 27001 - Adeguamenti Circ. 263/2006 - Assessment Cybersec. NIST - Revisione contrattualistica - IT auditing - Sistemi di reportistica	- Gestione dei log di sicurezza - Classificazione delle informazioni - Data Loss Prevention - Protezione degli endpoint - Prevenzione APT - Analisi del rischio informatico (IT Risk Manager™)	- Monitoraggio della sicurezza IT - Computer forensics - Vulnerability / penetration test - Revisione del codice sorgente
Antifrode e-payments	- Policy e procedure - Gestione rischio frode - Verifiche di conformità - Conformità Circ. 263/2006 - Conformità Racc. BCE / LG EBA	- Strong Authentication - Transaction monitoring	- Anti Phishing / Anti malware - Active Fraud Prevention - Monitoraggio canale CBI
Continuità Operativa	- Analisi degli impatti - Piani di Continuità Operativa - Piani di Disaster Recovery - Verifiche conformità - Certificazioni ISO 22301 - Revisione contrattualistica - Conformità Circ. 263/2006	← - SW per la gestione del piano di BC - SW per la gestione delle crisi →	
Trusted Services	- Policy e procedure - Modelli Organizzativi - Verifiche di conformità - Accreditamento	- Dematerializzazione - Identità Digitale	- Firme elettroniche - Marcatura temporale - Conservazione a norma

Focus on: la soluzione OASI *IT Risk Manager*™ a supporto del modello di gestione dei rischi informatici e di cybersecurity in conformità alla 263/2006

ILLUSTRATIVA

IT Risk Manager™



Benefici attesi

- **Conformità** con i requisiti della Nuove Disposizioni di Vigilanza Prudenziale per le Banche (Capitolo 8, aggiornamento n°15 Circ. BdI 263/2006), con flessibilità di estensione ad altri modelli requisiti specifici (e.g. analisi dei rischi CAI, analisi dei rischi ISO 27001, …)
- **Supervisione** da parte di un **Comitato degli Esperti** costituiti dagli IT Risk Manager di alcune delle principali banche italiane e organizzazione di user group periodici per lo scambio di best practice esperienze tra *peer*
- 4 moduli funzionali per la gestione di tutti i requisiti in materia di gestione del rischio informatico:
  - Modellistica del rischio ICT
  - Workflow processi / procedure
  - Reportistica
  - Amministrazione

Oasi
GRUPPO ICBPI

Grazie per l'attenzione

Marco Valsecchi
Responsabile Practice Sicurezza, Rischi e Compliance ICT

Oasi

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A.
Azienda del Gruppo Bancario Istituto Centrale delle Banche Popolari Italiane
Corso Europa, 18 - 20122 Milano - Tel. +39 02 77051
Cell.:**+39 335 1938328** Mail: m.valsecchi@oasi-servizi.it