Operational Risk vs Advanced IT RISK

Claudio Ruffini

24 Giugno 2015

LA FINANZA. INTERPRETATA A REGOLA D'ARTE.

Augeos

L'evoluzione normativa in tema di sicurezza informatica

Disposizioni di vigilanza prudenziale di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa

Valutazione del rischio informatico e correlazione con la gestione del rischio operativo

L'ottavo capitolo del 15 aggiornamento della **circolare 263** aggiorna la disciplina del sistema informativo per recepire le principali evoluzioni emerse a livello internazionale. Oltre a **disciplinare le modalità di governo del sistema informativo, di gestione del rischio informatico ed i requisiti per assicurare la sicurezza informatica**, le disposizioni recepiscono le raccomandazioni della BCE per la sicurezza delle transazioni bancarie tramite internet.

Un quadro normativo da interpretare

…. a regola d'arte

Augeos
Servizi e tecnologia per creare valore

IT Risk– Alcuni quesiti

- Come distinguere un Rischio IT diretto da un Fattore di Rischio IT indiretto in un processo bancario?
- Quale funzione deve valutare i fattori di rischio diretti o indiretti e con quale metrica?
- Come raccordare l'analisi delle minacce e delle vulnerabilità degli asset con la classificazione dei rischi operativi Basilea?
- Come ottimizzare i controlli tra le diverse funzioni ed evitare che ci siano sovrapposizioni di ambiti di controlli?
- Come monitorare tutte le informazioni di governance dell'IT e dei Rischi in un unico framework metodologico ed in un unico ambiente?

Chiavi di lettura del quadro normativo

- coinvolgimento vertici aziendali e approccio per Funzione
- visione integrata dei rischi
- efficienza ed efficacia dei controlli
- applicazione in funzione della dimensione e della complessità operativa

Migliorare la governance dei Rischi e Controlli della banca.

Approccio di governo del Rischio IT

Presidio Outsourcer

Ruoli e responsabilità

Metodologia di analisi

Monitoraggio

Governo del Rischio

Contesto Interno

- Assetto organizzativo
- Evoluzione offerta alla clientela
- Attività in outsourcing
- Sviluppo software

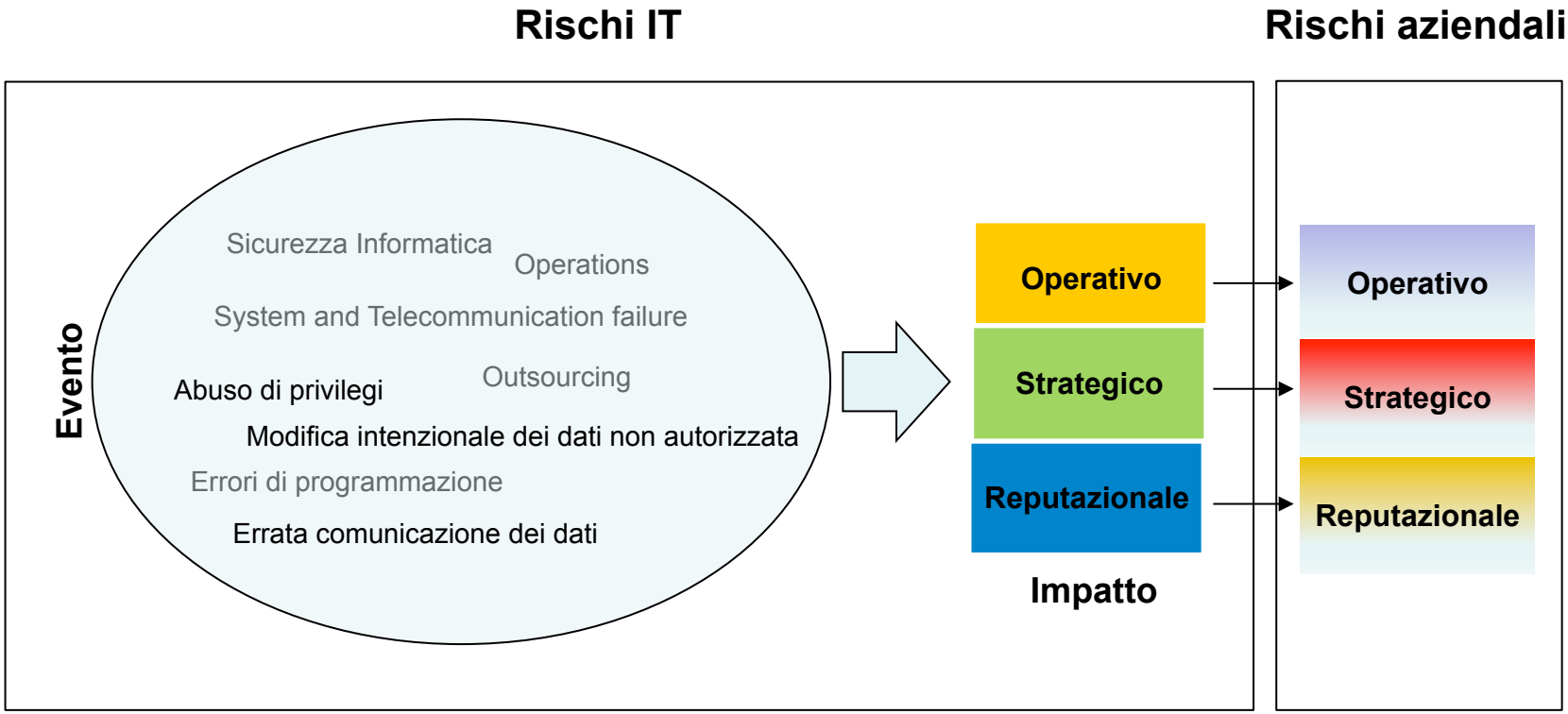
Contesto Esterno

- Evoluzione normativa
- Evoluzione minacce
- Evoluzione tecnologica
- Indicazioni di standard

Augeos
Servizi e tecnologia per creare valore

Il rischio informatico - Ambito

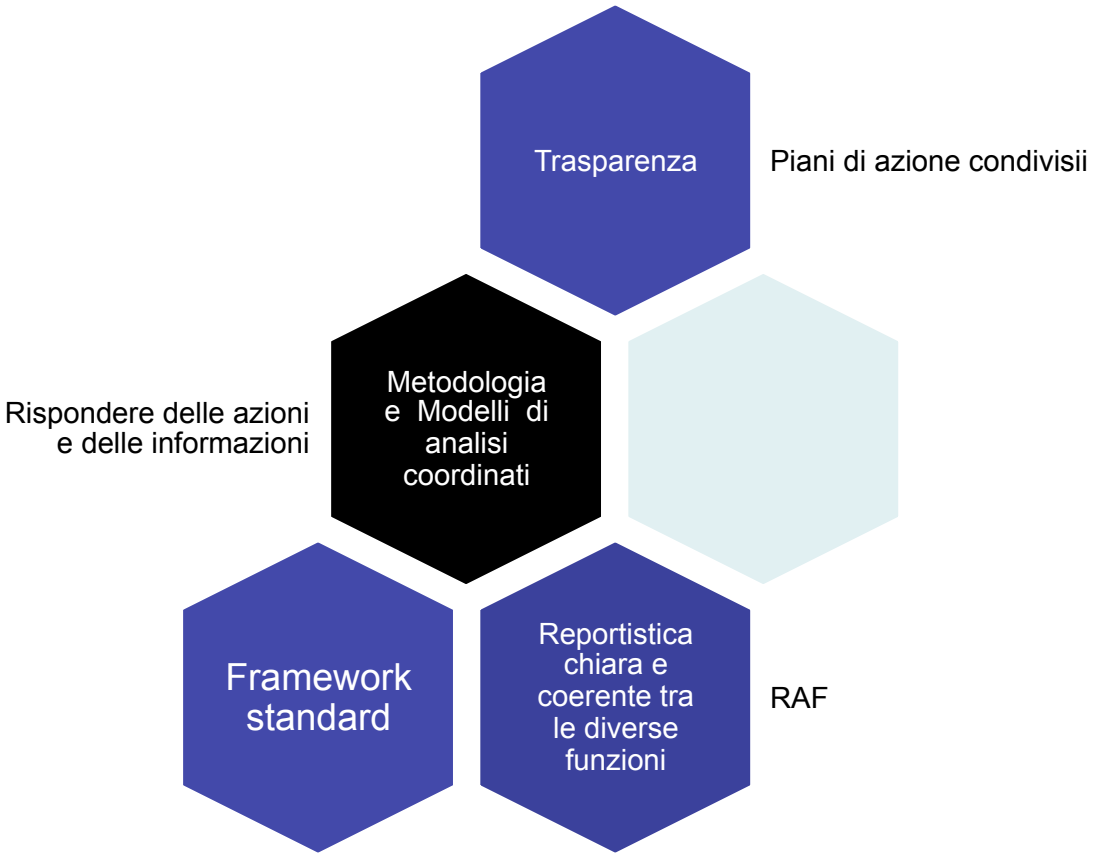
La valutazione dei singoli Rischi IT deve essere completata con la valutazione delle interrelazioni fra le diverse tipologie di rischio per una **visione aziendale dell'esposizione al rischio**



Augeos
Servizi e tecnologia per creare valore

Coinvolgimento vertici aziendali

Coinvolgere i vertici aziendali significa



Augeos
Servizi e tecnologia per creare valore

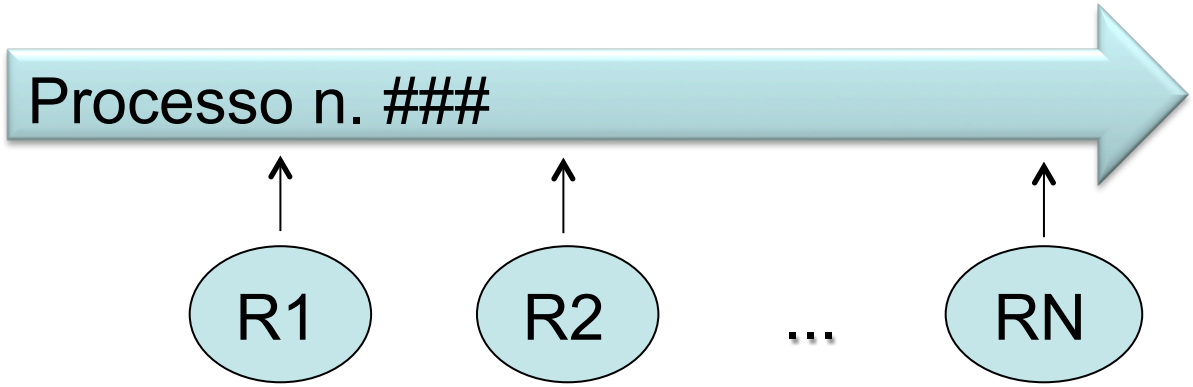
Operational Risk Mapping

Le categorie di rischio possono essere un semplice albero tassonomico a più livelli (Es. Tassonomia di Basilea 2). Ognuno degli incroci individua un particolare rischio nel singolo processo

	Risk Cat 1	Risk Cat 2	Risk Cat 3	...	Risk Cat N
Processo n. 1					x
Processo n. 2		x			
Processo n. 3	x		x		
...					
Processo n. N			x		

Augeos
Servizi e tecnologia per creare valore

Approccio per funzione



L'OR Management è orientato ai processi. Il rischio è definito dall'incrocio tra categoria di rischio potenziale e processo in cui questo si colloca.

Focalizzazione sui processi

Augeos
Servizi e tecnologia per creare valore

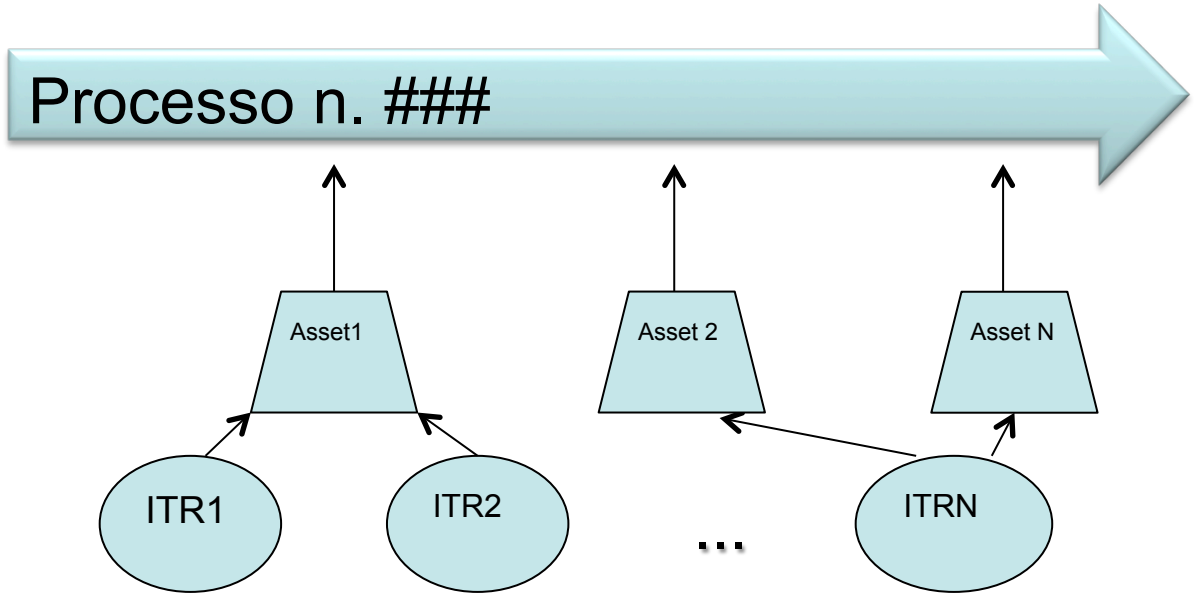
IT Risk Mapping

L'analisi del rischioIT è focalizzata sulle vulnerabilità degli asset informatici e le possibili minacce correlate per formare uno scenario di rischio potenziale;

	Threat cat 1	Threat Cat 2	Threat Cat 3	...	Threat Cat N
Asset n. 1					X
Asset n. 2		X			
Asset n. 3	X		X		
...					
Asset n. N			X		

Augeos
Servizi e tecnologia per creare valore

IT Risk Mapping



L'**IT Risk Management** è orientato quindi all'Asset IT. Il raccordo con i processi avviene identificando preventivamente gli Asset associati a ciascun processo.

Focalizzazione sugli Asset

Augeos
Servizi e tecnologia per creare valore

considerazioni

- L'IT Manager ottiene una mappa aggiornata e coerente in se stessa dei rischi IT della propria funzione.
- Il process owner viene sensibilizzato all'analisi dei rischi degli asset a lui collegabili.
- Ottengo una mappatura completa degli asset per processo aziendale a cui posso associare delle analisi di vulnerabilità

Augeos
Servizi e tecnologia per creare valore

Considerazioni

- Il process Owner viene intervistato più volte da persone diverse sui medesimi rischi
  - Operational Risk
  - IT Manager
  - Compliance
- Ogni funzione aziendale rischia di costruirsi la propria mappa dei rischi o addirittura la propria mappa dei processi
- Manca una visione univoca dei rischi ed è difficile realizzare una valutazione coerente dei rischi
- Si rischia di avere una duplicazione dei controlli o una de-responsabilizzazione

Augeos
Servizi e tecnologia per creare valore

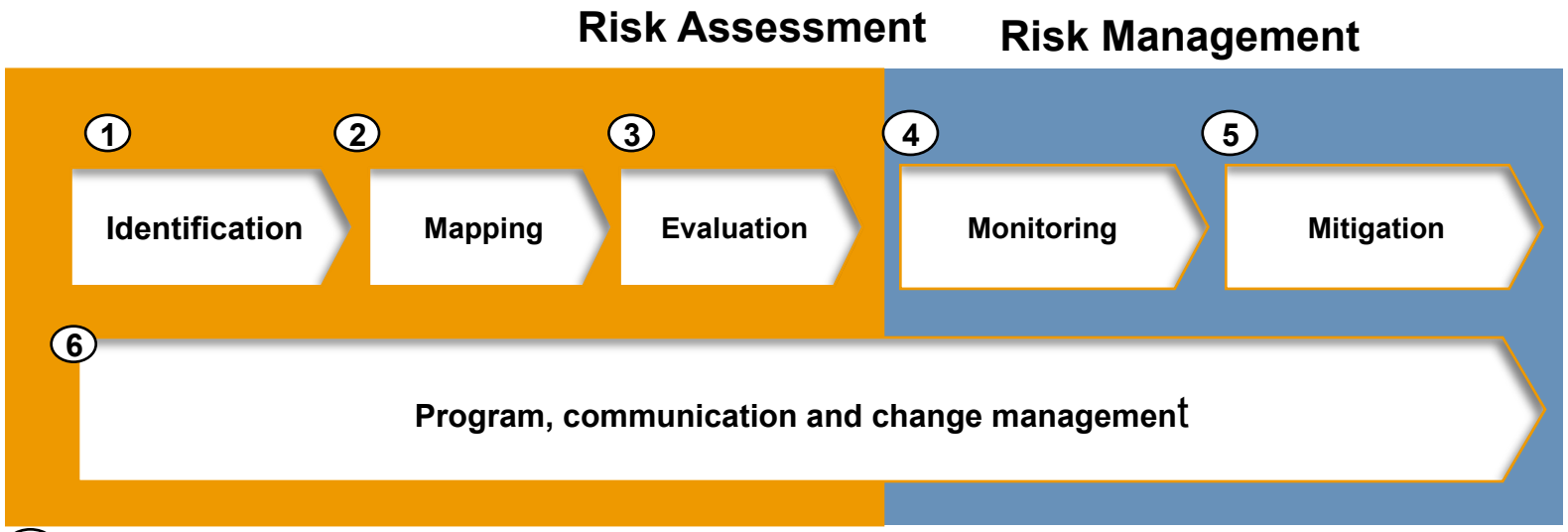
Chiavi di lettura del quadro normativo

- coinvolgimento vertici aziendali e approccio per Funzione
- visione integrata dei rischi
- efficienza ed efficacia dei controlli
- applicazione in funzione della dimensione e della complessità operativa

Migliorare la governance dei Rischi e Controlli della banca.

La Metodologia

Metodologia



1. **Identifica** i Rischi potenziali suddividendoli per tipologia o classificazioni. Questa fase, ha anche l'obiettivo di, selezionare i processi e le aree di rischio su cui intervenire.
2. **Attribuisce** in maniera strutturata i Rischi nei processi aziendali esplicitando dove questi si possono verificare..
3. **Valuta** i Rischi con metodologie ex-ante (Self Risk Assessment) e/o ex-post (analisi statistiche su eventi accaduti)
4. Configura **il sistema di monitoraggio** e le modalità di misurazione dei rischi identificati nella fase precedente anche con l'utilizzo di KRI
5. **Attua** azioni di mitigazione che operano sulle condizioni che determinano gli eventi per ridurre la probabilità di accadimento e annullarne gli effetti pianificando piani di intervento e verificandone l'esecuzione nel tempo
6. **Coordina le attività del progetto** e le attività nel rispetto degli obiettivi iniziali e sulla base del livello di maturità della gestione dei rischi

Augeos
Servizi e tecnologia per creare valore

Governo del Rischio – Metodologie di Analisi

Il modello di analisi utilizzato per l'identificazione dei **rischi IT** è adattabile alla tassonomia di Basilea II dei rischi operativi, della metodologia ABI e dei principali *standard* internazionali in materia (in particolare, **ISO:27001** e **COBIT5** for Risk).

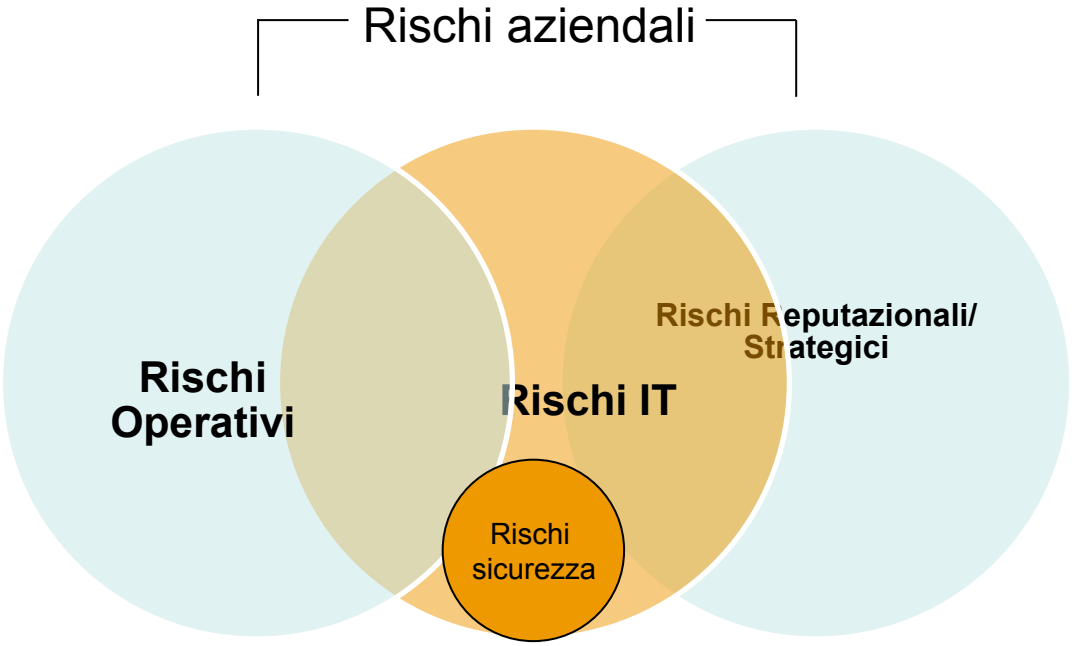
Il modello metodologico è supportato da un **framework** flessibile e adattabile ai vari contesti nel quale sono gestiti scenari di rischio, minacce, vulnerabilità, asset impattati, possibili contromisure e rischi operativi.
L'impostazione adottata segue un approccio top-down, combinando insieme i seguenti elementi:

- Scenari di rischio;
- Asset (secondo la metodologia ABI);
- Possibili contromisure (ex ISO:27001);
- Event Type (modello di Basilea II);
- Categorie di rischio di COBIT5.

Augeos
Servizi e tecnologia per creare valore

Visione integrata dei rischi

E’ necessario inquadrare il concetto di IT Risk in un approccio più ampio di rischio aziendale



Inoltre i rischi IT devono considerare sia le componenti IT interne sia le componenti IT in outsourcing

Augeos
Servizi e tecnologia per creare valore

- **Risk Factor:** sono quelle condizioni che influenzano la frequenza e/o l'impatto di uno scenario di rischio: si dividono in
  - External Context
  - Internal Context
  - Control and Risk Management Capabilities

Augeos
Servizi e tecnologia per creare valore

Augeos
Servizi e tecnologia per creare valore

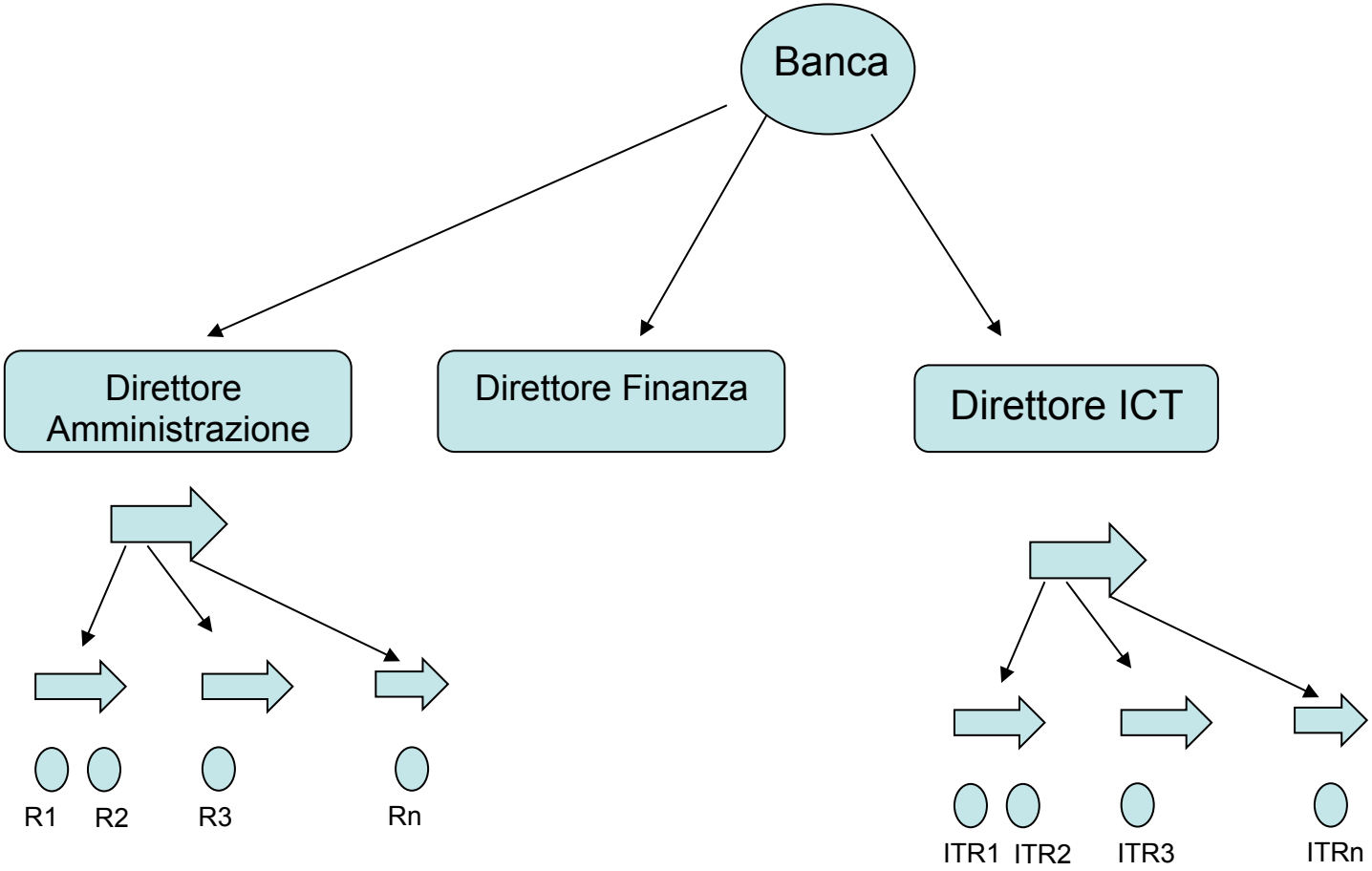
Esempi di IT come fattore di rischio diretto

- Interruzione totale o parziale dei servizi IT dovute a
  - «Bachi» nei programmi software: errori di codifica, attività di test non accurate
  - Rete di comunicazione: interruzione dei collegamenti per fattori intrinseci all'impiego di tecnologia (distorsioni elettromagnetiche, limitatezza di banda a fronte di punte di traffico, sw di rete non robusto
  - Apparati Hardware: sistemi di elaborazione, sistemi di rete che si rompono o si dannegiano
  - Prolemi dovuti ad erogazione di elettricità (interruzione o salti di tensione)
- Sistemi non progettati bene
  - la mancanza di qualche tassello nel sistema complessivo può causare un danno o una forte riduzione delle performance complessive del sistema
  - La ridondanza di sistemi o di dati può causare analogamente dei problemi. Si pensi alla ridondanza di dati su sistemi paralleli non perfettamente allineati.
  - Dimensionamenti sbagliati dei programmi, sistemi di elaborazione in funzione delle esigenze reali

Fattore di rischio indiretto

- Indirettamente i Sistemi informativi possono essere dei driver che facilitano l'evento di perdita dovuto ad altri fattori
  - Frode Interna: il personale interno approfitta di qualche situazione contingente per portare una frode o un furto tramite l'uso di tecnologie
  - Incapacità , scarsa preparazione, motivazione del personale addetto all'uso di certe tecnologie
  - Frode esterna: da parte di persone non dell'azienda attraverso l'uso di tecnologia
  - Disfunzioni organizzative che vengono amplificate dall'uso della potenza tecnologica
  - Cadute di immagine (reputazione) dovuta alla lentezza percepita dai clienti relativamente ai sistemi informativi

Augeos
Servizi e tecnologia per creare valore

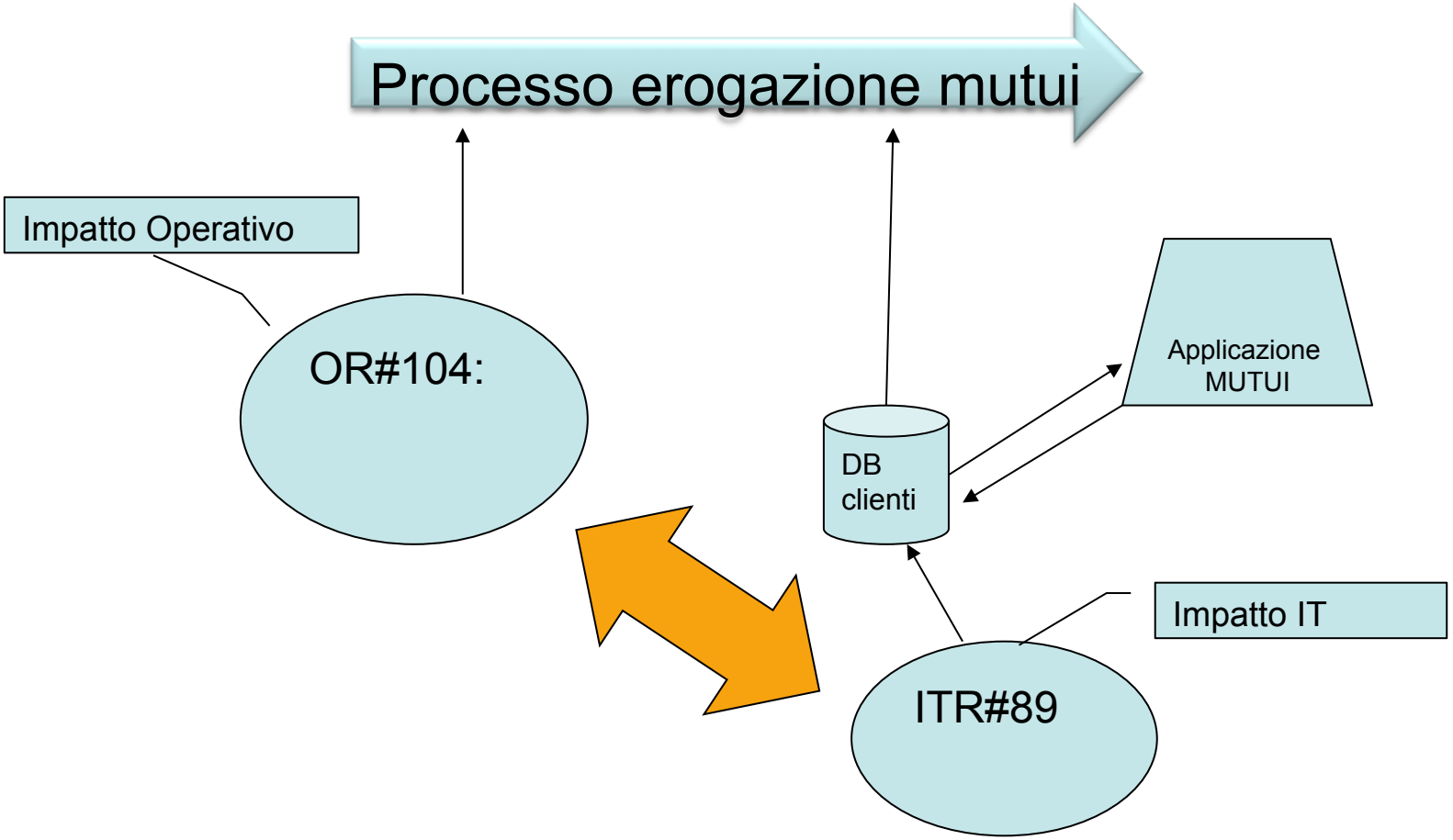


Augeos
Servizi e tecnologia per creare valore

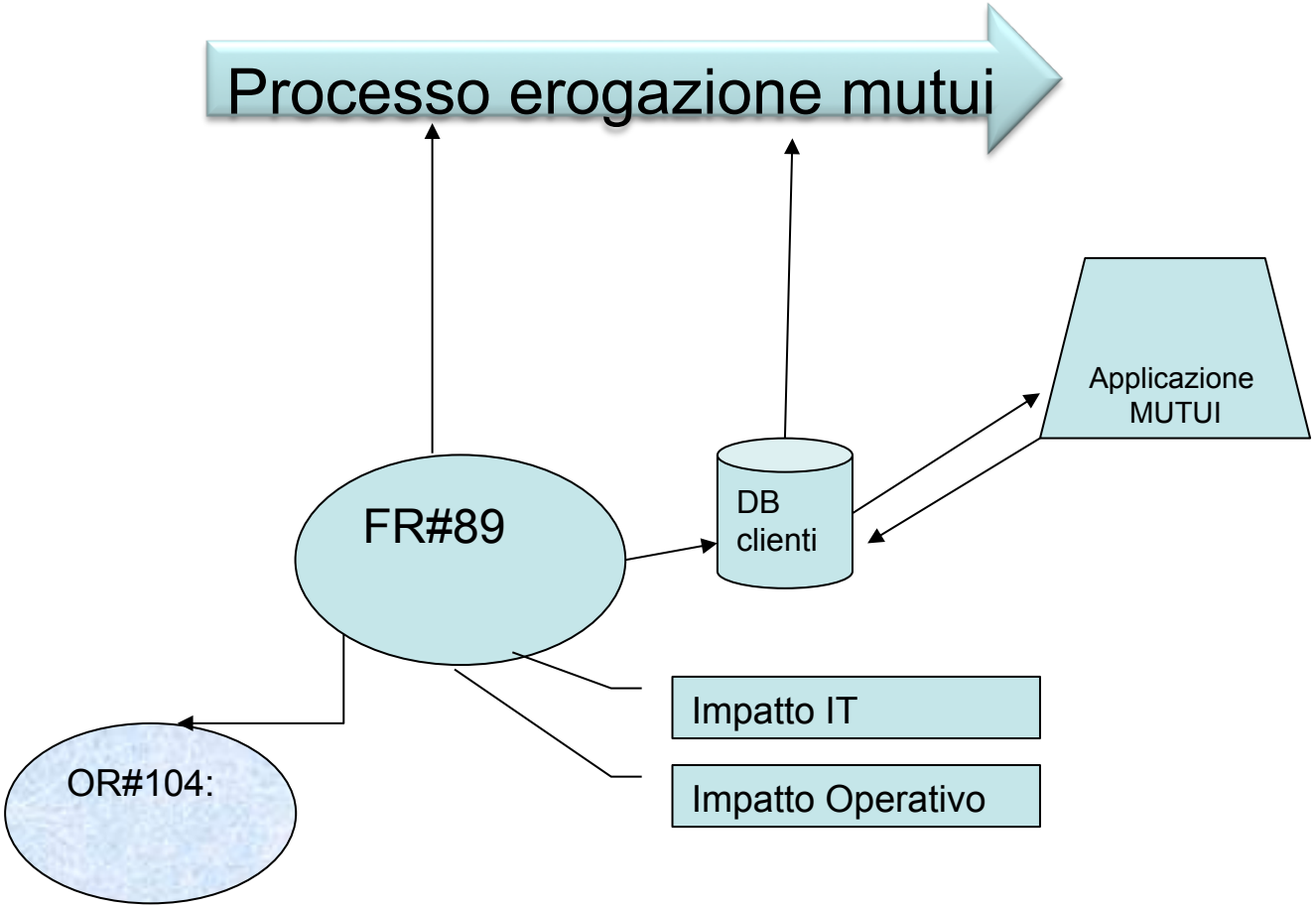
Es 1 Operational Risk vs IT Risk

- OR#104: Modifica non autorizzata dati nel processo erogazione mutuo;
  - Categoria di Basilea A1 con eventuale sottolivello
  - Impatto Operativo: valore residuo del mutuo
- ITR#89: Modifica non autorizzata della base dati anagrafica per applicazione mutui
  - minaccia: Modifica malevola dei dati in ambiente di produzione
  - Impatto IT: costo del ripristino del dato corretto

Augeos
Servizi e tecnologia per creare valore



Augeos
Servizi e tecnologia per creare valore

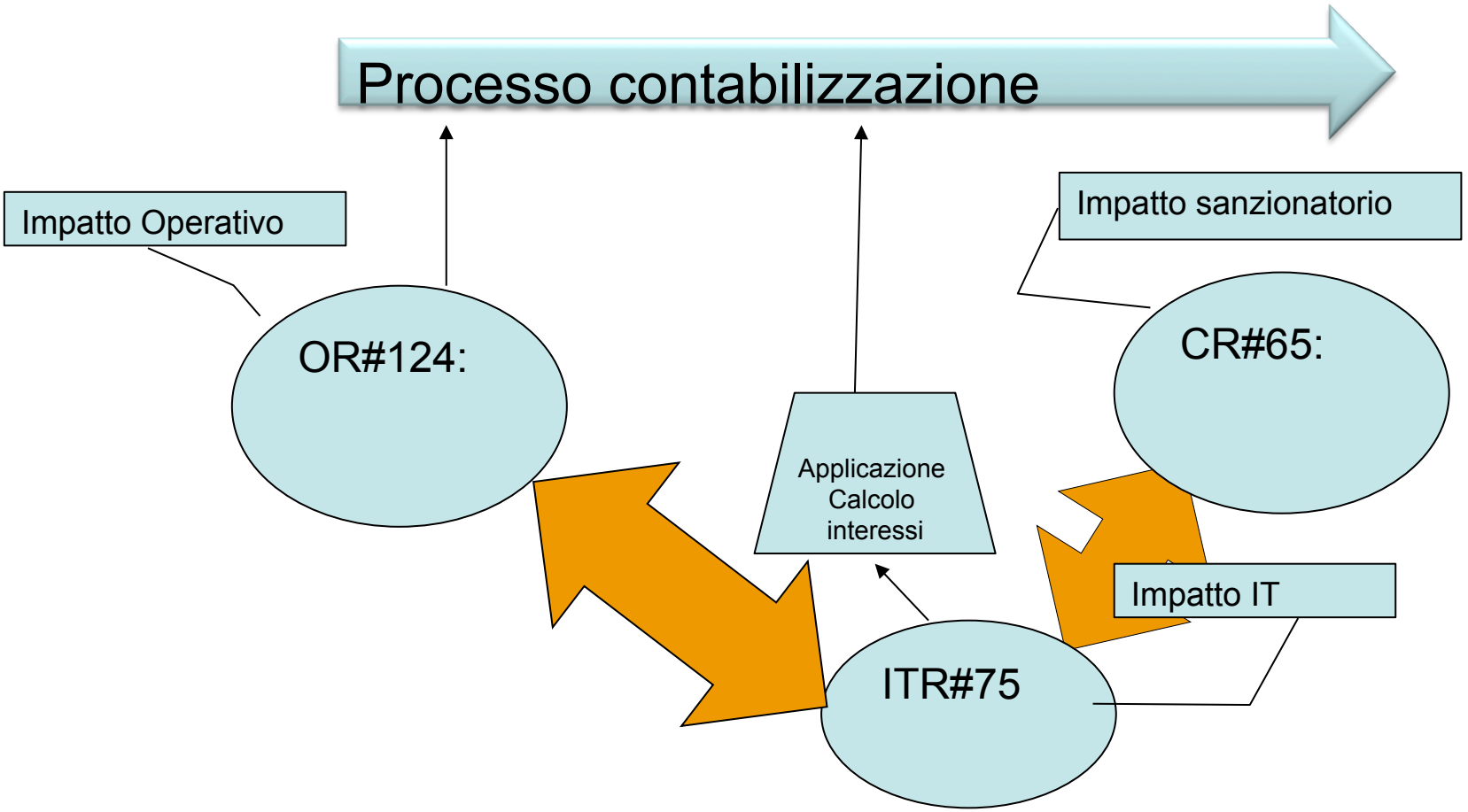


Augeos
Servizi e tecnologia per creare valore

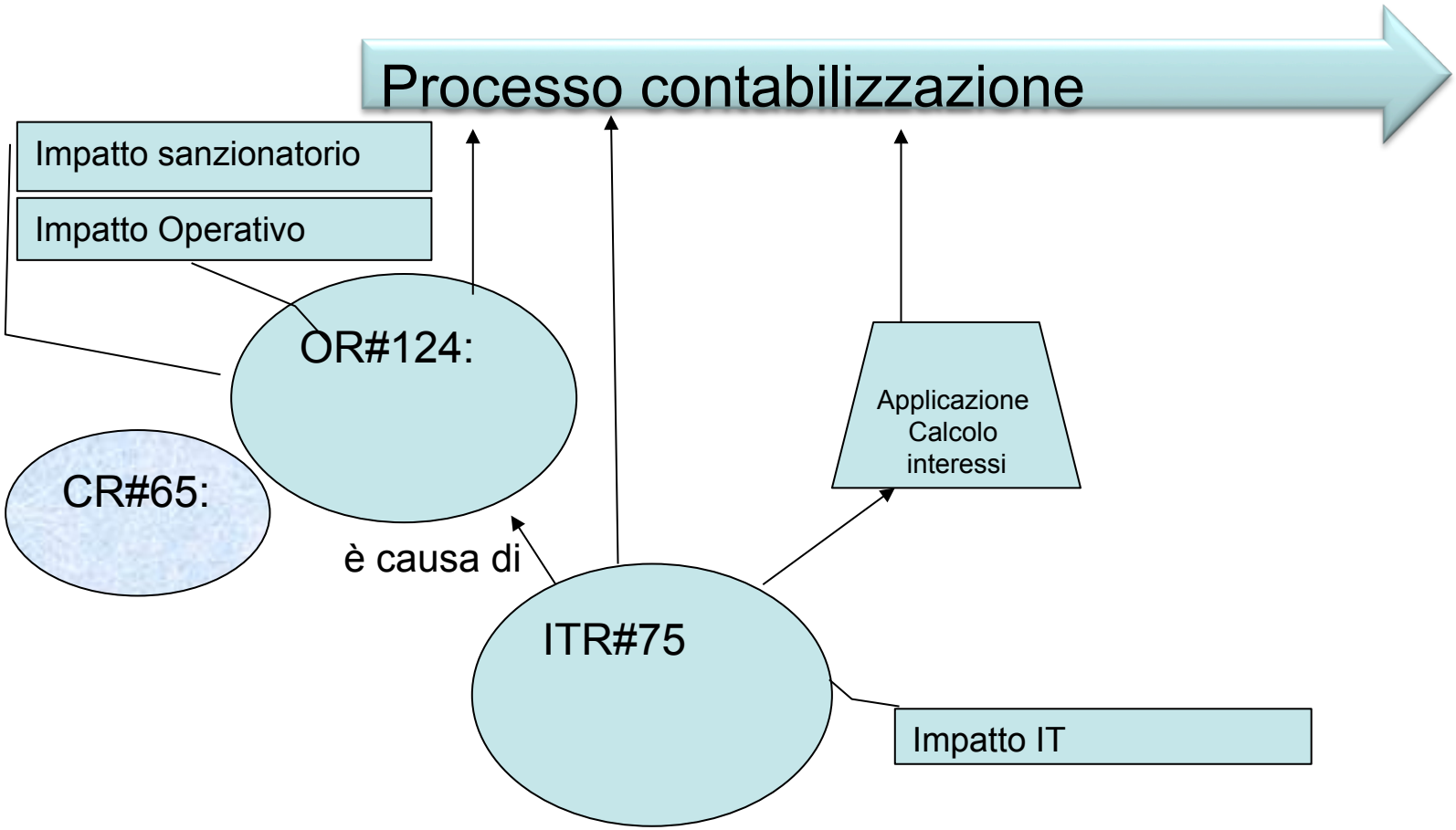
Es 2 Operational Risk vs IT Risk

- OR#124: errata contabilizzazione interessi ;
  - Categoria di Basilea G1 con eventuale sottolivello
  - Impatto Operativo: costo riparazione al danno effettuato
- ITR#75: Malfunzionamento nella procedura calcolo interessi
  - minaccia: Malfunzionamento SW
  - Impatto IT: costo della correzione e del nuovo rilascio di release
- CR#65: mantenere un comportamento corretto nei confronti del cliente
  - **Decreto legislativo 24 febbraio 1998, n. 58**
  - Sanzione: sanzione penale reclusione da 1 a tre mesi

Augeos
Servizi e tecnologia per creare valore



Augeos
Servizi e tecnologia per creare valore



Augeos
Servizi e tecnologia per creare valore

Unico Rischio

Diverse visioni

Augeos
Servizi e tecnologia per creare valore

Scenario di Rischio

Evento
- Interruzione
- Modifica
- Distruzione
- Furto
- Disclosure
- Ineffective design
- Ineffective execution
- Rules and regulations
- Uso inappropriato

Tipi di Minaccia:
- Maliziosa
- Accidentale
- Errore umano
- Failure
- Natura
- External requirement

Asset/Risorsa:
- Persone e competenze
- Struttura organizzativa
- Processi
- Infrastruttura
- Informazioni
- Applicazioni

Attori:
- Interni (staff o a contratto)
- Esterni: competitor, partner, regulator, market

Scenario di Rischio

Time:
- durata
- Occorrenza (criticao non critica)
- Detection
- Time lag

Augeos
Servizi e tecnologia per creare valore

- Costruire un set completo di scenari significa, in teoria, che ogni possibile valore di ogni componente dovrebbe essere combinato. Ogni combinazione dovrebbe essere valutata e se ritenuta possibile dovrebbe rientrare nella lista di rischi
- Il numero di scenari dovrebbe essere piccolo
- Gli scenari possono avere esempi negativi o positivi

Augeos
Servizi e tecnologia per creare valore

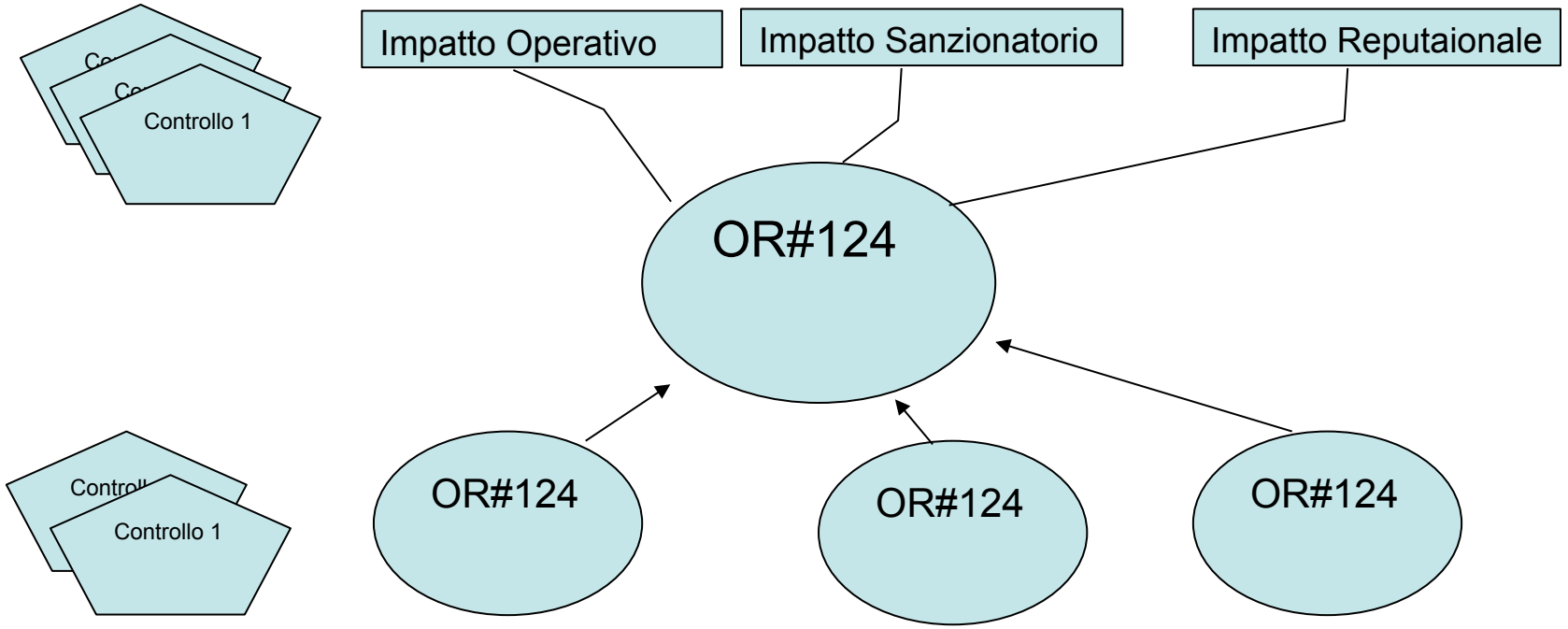
Chiavi di lettura della normativa

- coinvolgimento vertici aziendali e approccio per Funzione
- visione integrata dei rischi
- efficienza ed efficacia dei controlli
- applicazione in funzione della dimensione e della complessità operativa

Migliorare la governance dei Rischi e Controlli della banca.

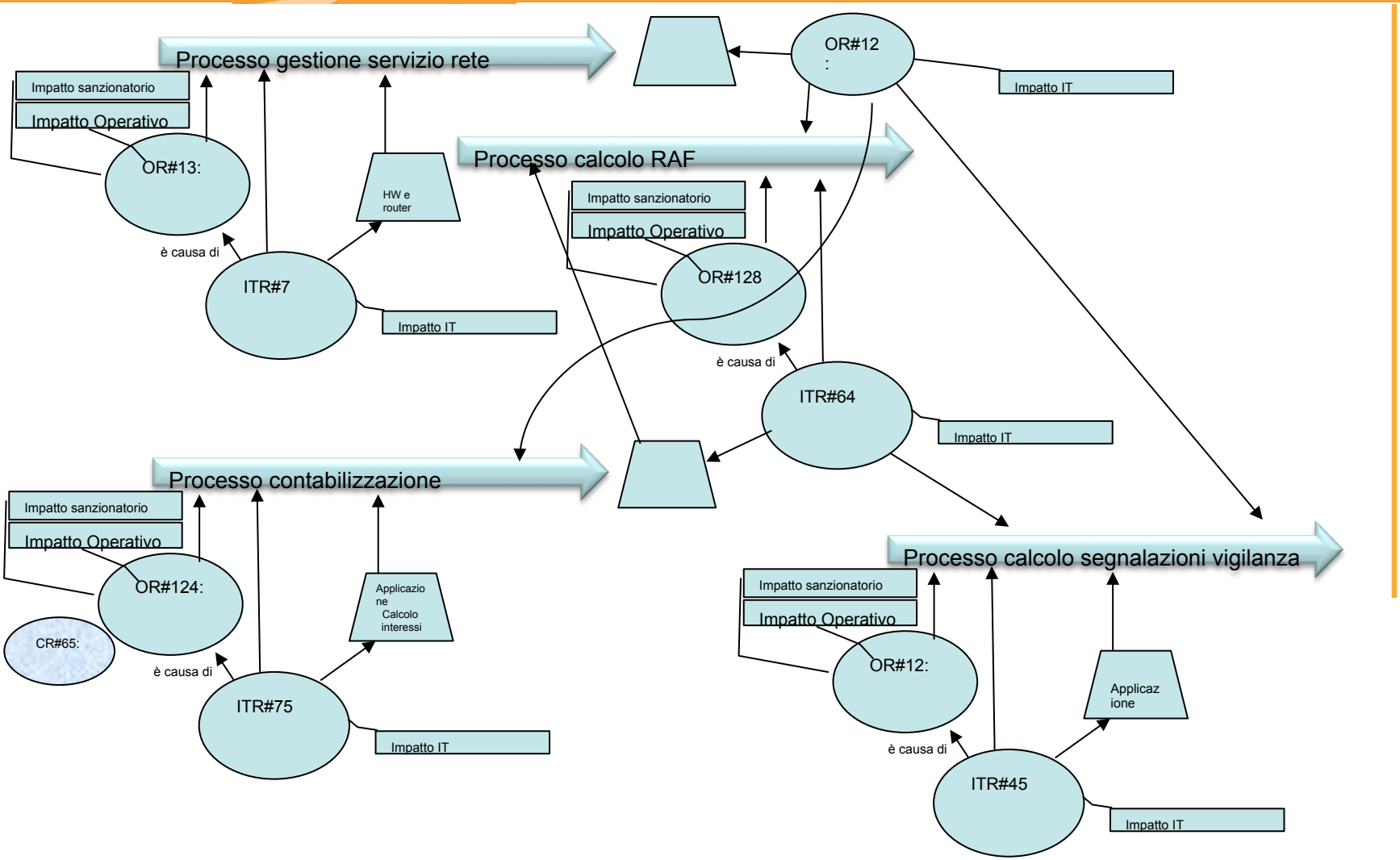
- Configurabilità e adattabilità del modello alle diverse realtà:
  - Workflow di approvazioni per funzioni
  - Presidi e controlli specifici di funzione
  - Verifica della completezza dei controlli in relazione al patrimonio informativo dei vari framework standard (Cobit, ISO27001, COSO, etc,,,)

Augeos
Servizi e tecnologia per creare valore



Augeos
Servizi e tecnologia per creare valore

Network Analysis Risk event



Augeos
Servizi e tecnologia per creare valore

Chiavi di lettura della normativa

- coinvolgimento vertici aziendali e approccio per Funzione
- visione integrata dei rischi
- efficienza ed efficacia dei controlli
- applicazione in funzione della dimensione e della complessità operativa

Migliorare la governance dei Rischi e Controlli della banca.

Governo del Rischio – Metodologie di Analisi

Analisi minacce di rischio informatico e correlazione con Rischio Operativo:

- Definizione tassonomia minacce
- Correlazione con Rischio Operativo

→ Approccio metodologico

Identification
Raccolta eventi e attacchi. Raccolta su informazioni di contesto (processi, asset, minacce, vulnerabilità, …). Raccolta attori coinvolti

Mapping
Individuazione dei rischi e dei fattori di rischio nei processi e riferiti ad asset.
Attribuzione dei ruoli degli attori coinvolti

Evaluation
Studio e valutazione degli impatti diretti ed indiretti anche considerando l'effetto dei presidi

Monitoring
Report di sintesi che aiutino le varie funzioni nel monitoraggio dei rischi e delle azioni di mitigazione

Mitigation
Attuazione delle contromisure per la mitigazione dei rischi e valutazione dell'avanzamento dei piani e dell'efficacia

Maturity Model Approach

Profondità di analisi in funzione del livello richiesto

- Risk Based Approach
- Functional Risk Approach
- Control in Action Approach

Augeos
Servizi e tecnologia per creare valore

Chiavi di lettura della normativa

- coinvolgimento vertici aziendali e approccio per Funzione
- visione integrata dei rischi
- efficienza ed efficacia dei controlli
- applicazione in funzione della dimensione e della complessità operativa

Migliorare la governance dei Rischi e Controlli della banca.

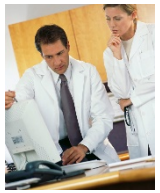
AUGEOS SOLUTION

Augeos
Servizi e tecnologia per creare valore

GRC Plus

Augeos
Servizi e tecnologia per creare valore

GRC Plus Approccio Modulare



Control In Action Approach	Normageos CIAA	RiskShelter CIAA	AIT Risk CIAA	Scenari di rischio
Functional Approach	Normageos	RiskShelter	AIT Risk	Controlli IT standard o personalizzati Minacce vulnerabilità standard o personalizzate
Risk Based Approach	Normageos RBA	RiskShelter RBA	AIT Risk RBA	Processi Standard Abilab Tassonomie standard Rischi

Augeos
Servizi e tecnologia per creare valore

Alcune innovazioni sono più incisive di altre