Unione Bancaria e Basilea 3
Risk & Supervision 2015

Valutazione dei rischi informatici

ai sensi del

15° aggiornamento della circolare di Banca d'Italia n° 263 del 27 dicembre 2006

Roma, 24 giugno 2015

UBI Banca

Agenda

- **Contesto di riferimento**
- Assetto Organizzativo
- Metodologia di Analisi
- Glossario

Contesto di riferimento

Premessa

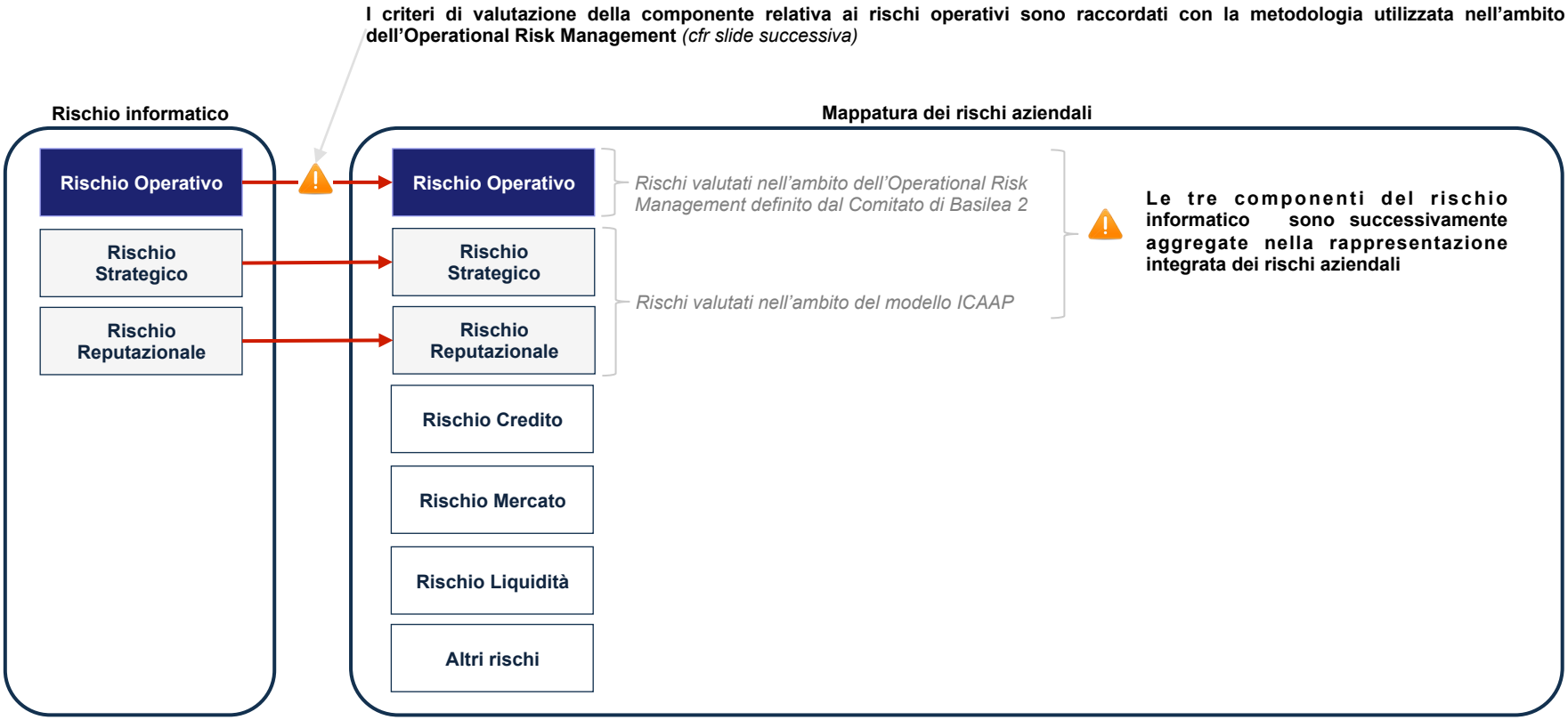
A seguito del 15° aggiornamento della circolare di Banca d'Italia n. 263 del 27 dicembre 2006, il Gruppo UBI Banca ha messo in atto una serie di interventi volti al potenziamento degli strumenti di governo e presidio del sistema ICT *(Information and Communication Technology)***, della gestione dei dati e del sistema di valutazione dei rischi informatici. Con riferimento a quest'ultima fattispecie di interventi, il nuovo contesto normativo ha definito specifici criteri per la valutazione del rischio basati su due principi fondamentali**

Principio	Criteri specifici
Valutazione del rischio potenziale cui sono esposte le risorse informatiche	La valutazione del rischio deve interessare: • le procedure in esercizio (al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione) • i nuovi progetti e/o le modifiche rilevanti del sistema informativo La valutazione del rischio deve prevedere la classificazione delle risorse ICT in termini di rischio informatico: • la classificazione deve essere raccordata con gli altri sistemi di valutazione dei rischi aziendali in modo da conseguire livelli di protezione uniformi indipendentemente dalle modalità di trattamento delle informazioni (informatico o manuale) • il rischio informatico deve essere valutato in funzione di un indicatore di criticità definito in relazione al danno potenziale derivante da possibili violazione dei requisiti di sicurezza e della probabilità che una minaccia possa sfruttare una delle vulnerabilità associate alla risorsa informatica
Gestione del Rischio residuo	La valutazione del rischio informatico deve essere svolta con il fine di individuare misure di attenuazione e/o di contenimento del rischio potenziale. In particolare, qualora il rischio residuo ecceda i livelli di propensione definiti dall'Organo di Supervisione Strategica, dovranno essere proposte ulteriori misure di attenuazione e/o contenimento del rischio e/o l'adozione di misure di trasferimento alternative. La definizione delle ulteriori misure di contenimento/ attenuazione del rischio deve prevedere il coinvolgimento della funzione di controllo dei rischi e sottoposta all'approvazione dell'organo con funzione di gestione.

Contesto di riferimento

Correlazione del rischio informatico con gli altri rischi aziendali

Il nuovo contesto normativo definisce il "Rischio informatico" come il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione. Pertanto, **nella rappresentazione integrata dei rischi aziendali tale tipologia di rischio è considerata secondo gli specifici aspetti dei rischi operativi** (componente valutata secondo la metodologia illustrata nel presente documento), **reputazionali e strategici** (componenti valutate nell'ambito del modello ICAAP).



Contesto di riferimento

Raccordo tra analisi del rischio informatico e valutazione del rischio operativo potenziale

- **La metodologia di analisi del rischio informatico è stata definita raccordando gli specifici criteri normativi con la metodologia già in uso per la valutazione dell'esposizione al rischio operativo potenziale definita nell'ambito del Risk Management**

- **Il fine ultimo perseguito è stato la definizione di un framework metodologico complessivo che garantisca la disponibilità di:**
  - **due differenti strumenti di analisi complementari tra loro**
  - **metriche di valutazione coerenti in modo da agevolare le verifiche di congruità e coerenza dei risultati ottenuti**

Operational Risk Management	ICT Risk	Valutazione Rischio informatico
Obiettivi principali Definizione delle politiche per l'identificazione, misurazione e controllo dei livelli di rischio complessivi		**Obiettivi principali** Garantire l'efficacia e l'efficienza delle misure di protezione delle risorse ICT in funzione della propensione al rischio.
Principali criteri metodologici 1. La quantificazione del rischio potenziale è determinata in funzione alle valutazioni effettuate dagli esperti di business 2. Le valutazioni degli esperti di business forniscono delle stime del rischio residuo (ai livelli di rischiosità medi rilevati storicamente sono applicati dei fattori correttivi valutati in funzione del contesto operativo e del sistema dei controlli interni) 3. Il livello di dettaglio dell'analisi è determinato dall'ambito di attività analizzato (processo aziendale) 4. L'analisi del rischio è effettuata in funzione di specifici scenari di rischio 5. La quantificazione del rischio è effettuata secondo tecniche attuariali che prevedono il modelling indipendente delle probabilità di accadimento degli eventi e degli impatti economici ad essi associati (Loss Distribution Approach definita dal Comitato di Basilea 2)		**Principali criteri metodologici** 1. La quantificazione del rischio potenziale è determinata in funzione alle valutazioni effettuate dagli Utenti Responsabili, dai System Owner e dall'unità specialistica di Sicurezza Logica e Continuità Operativa 2. Le valutazioni degli esperti di business forniscono delle stime del rischio potenziale e residuo 3. Il livello di dettaglio dell'analisi è determinato dalle Risorsa Informatiche utilizzate in ciascun ambito di attività analizzato 4. L'analisi del rischio è effettuata in funzione delle specifiche minacce informatiche (molto spesso le minacce informatiche coincidono con le cause sottostanti ad uno specifico scenario di rischio. In alcuni casi, invece, coincidono con gli scenari di rischio) 5. La quantificazione del rischio è effettuata in funzione del danno potenziale derivante da possibili violazione dei requisiti di integrità, riservatezza e disponibilità dei dati e della probabilità che una minaccia possa sfruttare una delle vulnerabilità associate alla risorsa informatica oggetto di analisi

Agenda

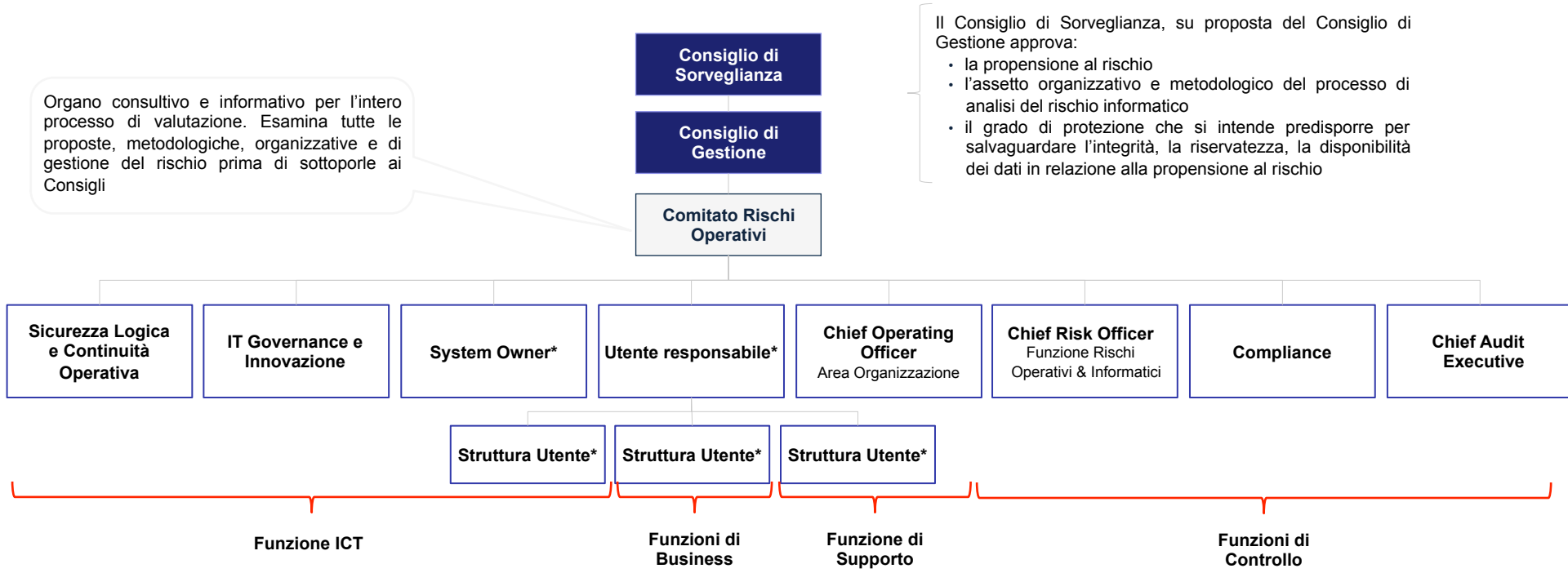
- Contesto di riferimento
- **Assetto Organizzativo**
- Metodologia di Analisi
- Glossario

Assetto Organizzativo

Modello organizzativo

- **Il processo di valutazione del rischio informatico si basa sulle valutazioni espresse dagli esperti di Business e di processo sul grado di esposizione al rischio e sull'efficacia delle contromisure in essere**

- **Come in tutti i processi aziendali, con il fine di garantire il regolare svolgimento delle attività che prevedono il coinvolgimento di diverse figure aziendali, anche per l'analisi del rischio informatico sono stati definiti ruoli e responsabilità demandate a ciascun ruolo coinvolto nel processo di analisi**

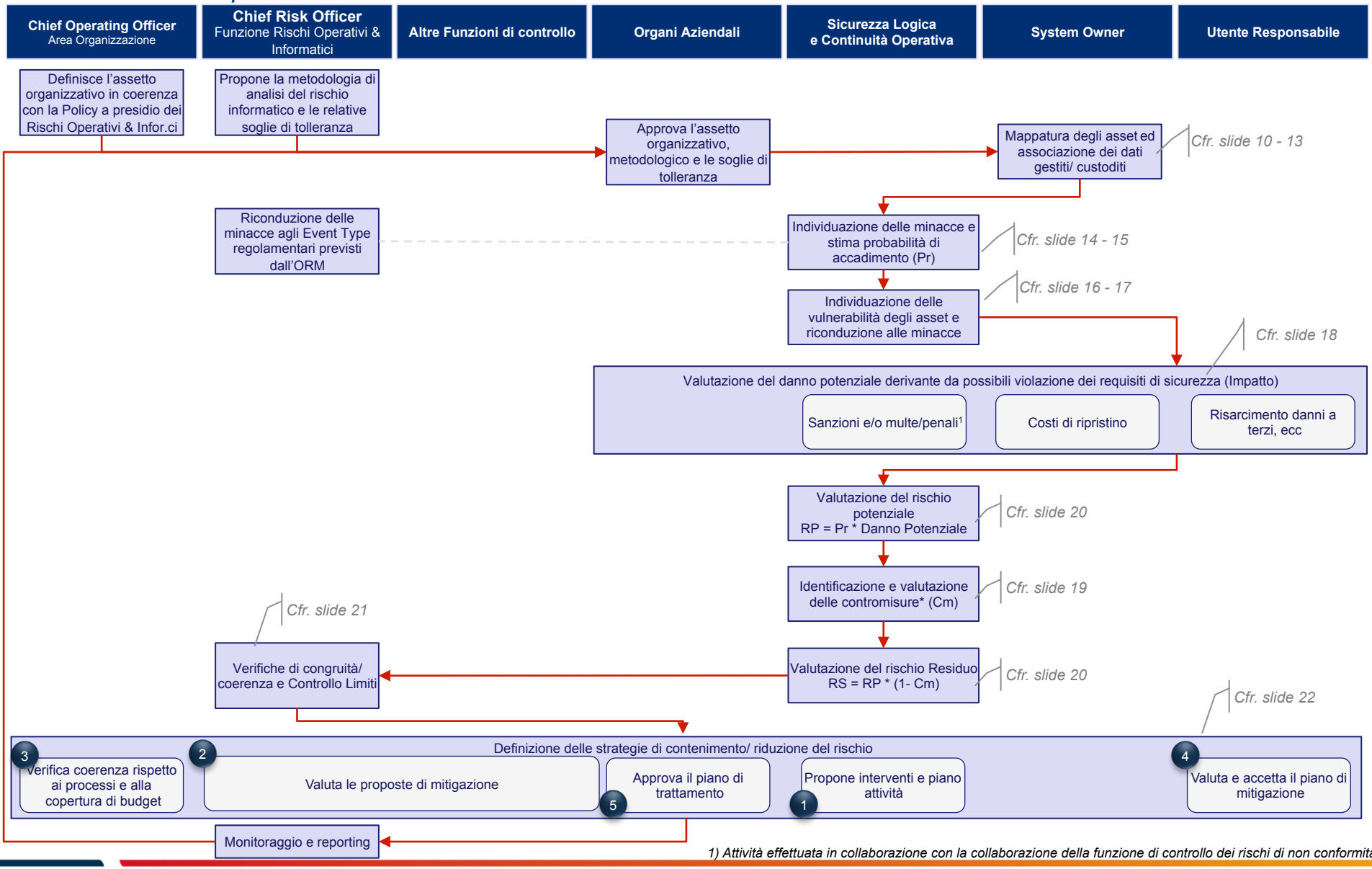


(*) Per ulteriori dettagli sul ruolo in oggetto si rimanda al glossario riportato in coda al documento

UBI Banca

Assetto Organizzativo

Flowchart del processo



1) Attività effettuata in collaborazione con la collaborazione della funzione di controllo dei rischi di non conformità

UBI Banca

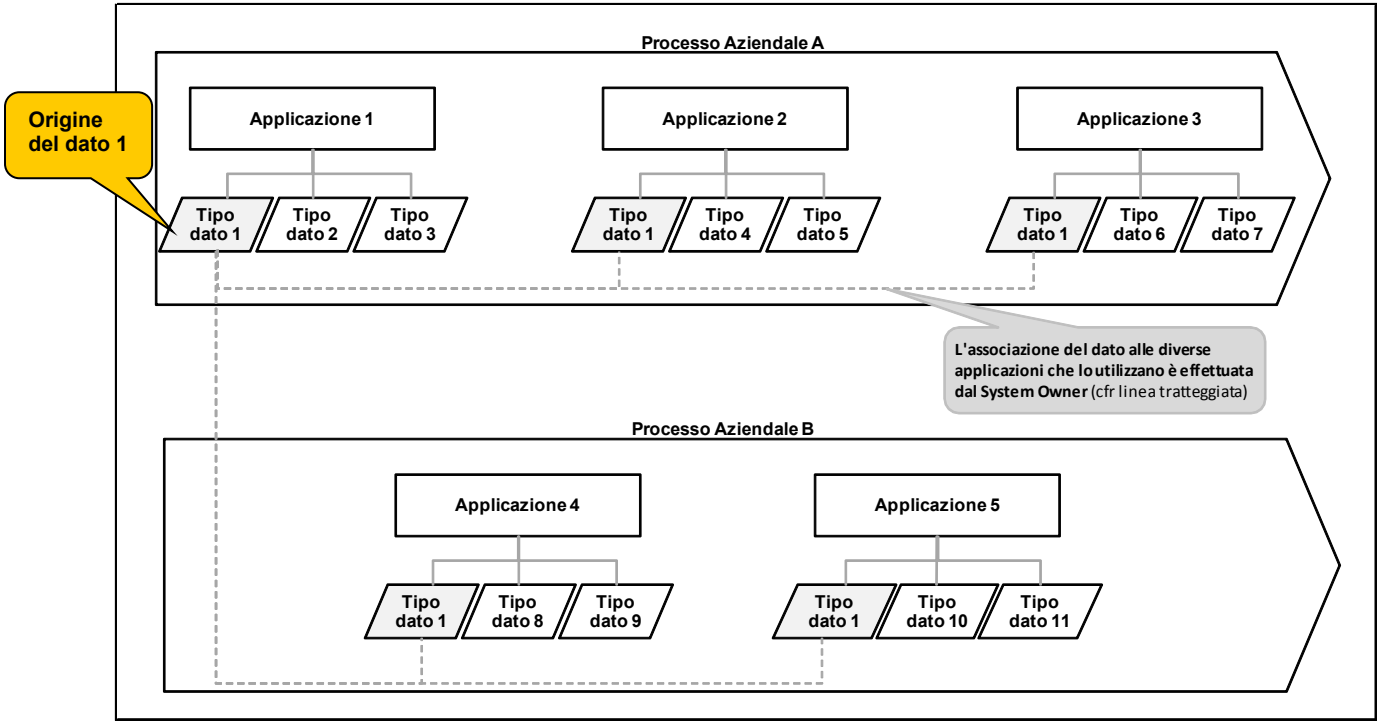
Agenda

- Contesto di riferimento
- Assetto Organizzativo
- **Metodologia di Analisi**
  - Mappatura degli asset aziendali
  - Identificazione e valutazione delle minacce
  - Identificazione delle vulnerabilità associate agli asset
  - Valutazione del danno potenziale
  - Identificazione e valutazione delle contromisure in essere
  - Valutazione del rischio
  - Verifiche di congruità e coerenza e controllo limiti
  - Strategie di gestione del rischio
- Glossario

Metodologia di analisi

Mappatura degli asset aziendali 1/4

La metodologia di analisi del rischio informatico è basata sul danno potenziale che potrebbe derivare dalla perdita di riservatezza, integrità e/o disponibilità[1] dei dati gestiti e/o custoditi da ciascun asset ICT[2] combinato con la valutazione delle probabilità di accadimento delle minacce e le vulnerabilità legate agli asset. Questi ultimi assumeranno un livello di criticità pari a quello dei dati gestiti (esempio: un server che gestisce dati sensibili è critico in quanto eredita il massimo livello di impatto dei dati trattati). **L'utilizzo di una metodologia basata sul "dato" consente di cogliere gli eventuali legami esistenti tra differenti asset aziendali**.



(1) Per ulteriori dettagli relativi alle definizioni di riservatezza, integrità e/o disponibilità dei dati si rimanda al glossario riportato in coda al documento
(2) Per asset ICT si intende un qualsiasi bene aziendale che consente la ricezione, elaborazione, trasmissione, fruizione archiviazione e custodia delle informazioni gestite informaticamente

Metodologia di analisi

Mappatura degli asset aziendali 2/4

Per evitare la sovrastima del rischio informatico associato a ciascuna applicazione, in fase di stima dell'impatto, l'Utente Responsabile deve riferire le proprie analisi ai soli dati originati/elaborati dalla risorsa informatica oggetto di analisi (nell'esempio: applicazione 1, 2, 3, ..) **non considerando i dati presi in input da altre procedure** (in quanto già valutati da altri Utenti Responsabili).

Riprendendo l'esempio riportato nella figura precedente, la valutazione del rischio potenziale relativo al processo aziendale A sarà determinata come segue:

$$Rischio\ Potenziale_{Processo\ A} = RP_{Applicazione\ 1} + RP_{Applicazione\ 2} + RP_{Applicazione\ 3}$$

Dove:

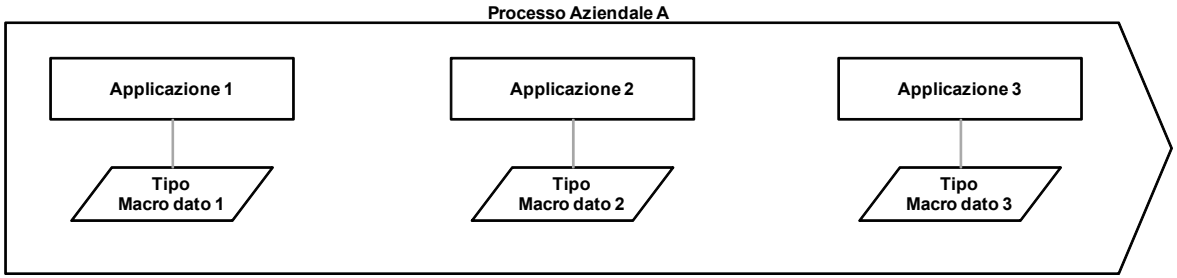
$$RP_{Applicazione\ 1} = RP_{Tipo\ Dato\ 1} + RP_{Tipo\ Dato\ 2} + RP_{Tipo\ Dato\ 3}$$
$$RP_{Applicazione\ 2} = RP_{Tipo\ Dato\ 4} + RP_{Tipo\ Dato\ 5}$$
$$RP_{Applicazione\ 3} = RP_{Tipo\ Dato\ 6} + RP_{Tipo\ Dato\ 7}$$
$$RP_{Tipo\ Dato\ 1} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 1\ effettuata\ nell'ambitodell'applicazione\ 1$$
$$RP_{Tipo\ Dato\ 2} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 2\ effettuata\ nell'ambitodell'applicazione\ 1$$
$$RP_{Tipo\ Dato\ 3} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 3\ effettuata\ nell'ambitodell'applicazione\ 1$$
$$RP_{Tipo\ Dato\ 4} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 4\ effettuata\ nell'ambitodell'applicazione\ 2$$
$$RP_{Tipo\ Dato\ 5} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 5\ effettuata\ nell'ambitodell'applicazione\ 2$$
$$RP_{Tipo\ Dato\ 6} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 6\ effettuata\ nell'ambitodell'applicazione\ 3$$
$$RP_{Tipo\ Dato\ 7} = Rischio\ potenziale\ relativo\ al\ tipo\ dato\ 7\ effettuata\ nell'ambitodell'applicazione\ 3$$

UBI Banca

Metodologia di analisi

Mappatura degli asset aziendali 3/4

Come prima applicazione dell'analisi del rischio informatico sarà utilizzato un criterio di approssimazione che prevede l'associazione di un *"macro dato"* in corrispondenza di ciascuna risorsa informatica analizzata.



Per consentire una rappresentazione della rischiosità su livelli di aggregazione via via decrescenti[1], ciascun dato è associato alla risorsa informatica di riferimento, la quale è associata all'Utente Responsabile, alla Struttura Utente, al processo aziendale di riferimento, alla tipologia di asset, al System Owner, ecc.

Area Funzionale ICT							Processi aziendali ARIS			
AREA	SOTTOAREA	APPLICAZIONE	SOTTOGRUPPO FUNZIONALE	REFERENTE INTERNO	RESPONSABILE	UNITA OPERATIVA	Responsabile di Processo	Area *(Liv. 1)*	Macro Ambito *(Liv. 2)*	Ambito *(Liv. 3)*
SUPPORTO	GESTIONE AMMINISTRATIVA	PERSONALE	PERSONALE - FORMAZIONE	Carlo Rossi	Roberto Bianchi	UBI.S-APP. RISORSE UMANE	Luigi Bra	AREA DI SUPPORTO	Risorse Umane	Formazione del personale
SUPPORTO	GESTIONE AMMINISTRATIVA	PERSONALE	PERSONALE - GESTIONE	Roberto Bianchi	Roberto Bianchi	UBI.S-APP. RISORSE UMANE	Luigi Bra	AREA DI SUPPORTO	Risorse Umane	Politiche gestionali risorse umane
SUPPORTO	GESTIONE AMMINISTRATIVA	PERSONALE	PERSONALE - GESTIONE	Roberto Bianchi	Roberto Bianchi	UBI.S-APP. RISORSE UMANE	Luigi Bra	AREA DI SUPPORTO	Risorse Umane	Politiche gestionali risorse umane

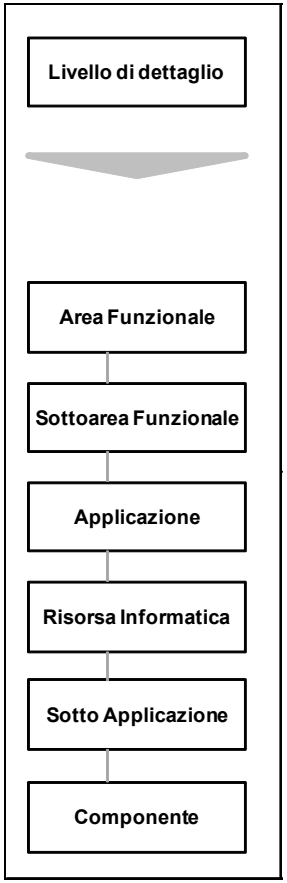
(1) Il livello di aggregazione con cui sono rappresentati gli esiti dell'analisi del rischio varia in funzione del destinatario del reporting

Metodologia di analisi

Mappatura degli asset aziendali 4/4

L'identificazione del livello applicativo su cui eseguire l'analisi del rischio informatico è effettuata in funzione del grado di omogeneità dei dati gestiti dalle risorse appartenenti ad uno specifico livello gerarchico. La metodologia prevede l'individuazione di un grado di dettaglio, denominato "Risorsa Informatica", definito come livello intermedio tra l'applicazione e la sotto-applicazione.

Il criterio seguito è il grado di omogeneità dei dati gestiti dalle singole applicazioni per le finalità di analisi. Nei casi in cui il livello "Applicativo" non risulti adeguato, la definizione della "Risorsa Informatica" è effettuata a livello delle "Sotto Applicazioni" e/o ad aggregazioni di queste *(individuazione effettuata sempre in funzione del grado di omogeneità e/o somiglianza dei dati da queste gestiti)*



Metodologia di analisi

Identificazione e valutazione delle minacce 1/2

- **Per minaccia si intende un'azione o un evento che, sfruttando una vulnerabilità del sistema, può pregiudicare la sicurezza del sistema stesso e rendere possibile il concretizzarsi di un rischio. In sostanza, la minaccia è un evento potenziale, accidentale o deliberato che può produrre un danno determinato dalla violazione di uno o più requisiti di sicurezza. Esistono minacce di tipo naturale** (es. alluvioni, terremoti, ecc)**, umane** (es. errori, diffusione di virus, ecc), **organizzative** (es. violazioni della normativa sulla privacy, ecc) **e tecnologiche** (es. malfunzionamenti dei sistemi)

- **La probabilità di accadimento di una minaccia è espressa in funzione del numero di accadimenti attesi annui** (se per uno specifico scenario ci si aspetta che accada 1 evento ogni 10 anni nella scheda di valutazione è indicato il valore 0,1 = 1/10)**, le stime di probabilità sono effettuate al lordo dell'efficacia delle contromisure in essere**

- **La stima del numero di eventi attesi annui dovrà essere coerente con le evidenze empiriche rilevate storicamente dal sistema di Loss Data Collection interno** (LDC) **e/o dalla procedura degli incidenti informatici** (il numero di accadimenti medio annuo rilevato da questi data base rappresenterà un *floor* al superamento del quale dovranno essere giustificati da riscontri oggettivi)

- **Indipendentemente dalla lista di minacce individuate è importante che esse siano:**
  - **legate ai parametri di riservatezza, integrità e disponibilità**
  - **raccordate con le classi di rischio previste dal sistema di gestione dei rischi operativi**
  - **legate alle risorse informatiche mediante l'associazione delle vulnerabilità di queste ultime alle minacce in oggetto**

Metodologia di analisi

Identificazione e valutazione delle minacce 2/2

Una minaccia non rappresenta un rischio se non esiste una vulnerabilità che possa essere "sfruttata"

Minacce Valutazione rischi informatici	Scenari di rischio Operational Risk Management	Event Type Basilea	Soglia di Tolleranza
Cancellazione/alterazione intenzionale di dati di sistema e/o diffusione di virus mediante accesso dall'esterno (es. rete internet, linee di tele comunicazione, dispositivi mobili, ecc)	Cancellazione/alterazione intenzionale di dati di sistema e/o diffusione di virus (ivi inclusa l'indisponibilità del sistema a causa di saturazione delle risorse) mediante accesso dalla rete internet o dalle linee di tele comunicazione	**Frode Esterna**	**542.316**
Saturazione intenzionale delle risorse da parte di terzi mediante accesso dall'esterno (es. rete internet, linee di tele comunicazione, dispositivi mobili, ecc)			
Furto di assets aziendali e/o della clientela da parte di personale interno (inclusi eventuali outsourcers)	Furto di denaro, valori in bianco o altri assets aziendali e/o della clientela da parte di personale interno (inclusi eventuali outsourcers)	**Frode Interna**	**573.026**
Cancellazione/alterazione intenzionale di dati di sistema e/o diffusione di virus da parte del personale interno (inclusi eventuali outsourcers)	Cancellazione/alterazione intenzionale di dati di sistema e/o diffusione di virus (ivi inclusa l'indisponibilità del sistema a causa di saturazione delle risorse) da parte del personale interno (inclusi eventuali outsourcers)	**Frode Interna**	**573.026**
Saturazione intenzionale delle risorse da parte del personale interno (inclusi eventuali outsourcers)			
Abuso di privilegio			
Furto di assets aziendali e/o della clientela da parte di terzi	Furto di denaro, valori in bianco o altri assets aziendali e/o della clientela da parte di soggetti esterni (escludere gli eventuali outsourcer)	**Frode Esterna**	**542.316**
Blocco o malfunzionamento softw are	Anomalie/ errori/ blocchi in fase di attivazione di nuove procedure, attivazione di nuove implementazioni e/o aggiornamenti, unificazione degli ambienti informatici e/o migrazione IT	**Interruzione e disfunzioni dei sistemi**	**101.917**
Distruzione/ danneggiamento di documentazione rilevante, locali, hardw are/ softw are determinati da disastri naturali (terremoti, alluvioni, incendi, etc.)	Distruzione/ danneggiamento di valori, documentazione rilevante, locali, arredi, hardw are/ softw are determinati da disastri naturali (alluvioni, incendi, etc.)	**Danni da eventi esterni**	**85.356**
Saturazione accidentale delle risorse	Blocchi dei sistemi IT e/o della rete e/o perdita dei dati dovuti alla distruzione/danneggiamento del centro elaborazione dati	**Interruzione dell'operatività e**	**101.917**
Guasto o malfunzionamento hardw are			
Frode informatica (appropriazione indebita di fondi aziendali e/o della clientela, sottrazione di dati, etc.) perpetrata da personale interno (inclusi eventuali outsourcers)	Frode informatica (appropriazione indebita di fondi aziendali e/o della clientela, sottrazione di dati, etc.) perpetrata da personale interno (inclusi eventuali outsourcers)	**Frode Interna**	**573.026**
Distruzione/ danneggiamento di documentazione rilevante, locali, hardw are/ softw are determinati da atti umani di origine esterna (terrorismo, vandalismo, danneggiamenti degli impianti, etc.)	Distruzione/ danneggiamento di valori, documentazione rilevante, locali, arredi, hardw are/ softw are determinati da atti umani di origine esterna (terrorismo, vandalismo, danneggiamenti degli impianti, etc.)	**Danni da eventi esterni**	**85.356**
Intercettazione delle comunicazioni (messaggi dati e pacchetti)			
Frode informatica (distrazione di fondi dai conti della clientela, sottrazione di informazioni riservate, etc.) perpetrata da parte di	Frode informatica (distrazione di fondi dai conti della clientela, sottrazione di informazioni riservate, etc.) perpetrata da parte di personale esterno mediante accesso dalla rete internet o dalle linee di	**Frode Esterna**	**542.316**
	zione non intenzionale dei dati	**Esecuzione e consegna dei processi**	**703.944**

In fase di identificazione della lista delle minacce informatiche si è fatto riferimento a:

- indicazioni fornite dal gruppo di lavoro dell'ABI
- modello di analisi dell'Operational Risk Management
- Best Practice di settore (es. Cobit, ISO27001)

UBI Banca

Metodologia di analisi

Identificazione delle vulnerabilità associate agli asset 1/2

Le vulnerabilità sono i punti di debolezza di un sistema, di un'apparecchiatura, di un processo di gestione o di qualunque altro elemento che concorra alla gestione delle informazioni, sfruttabili dalle minacce per ottenere accesso alle informazioni stesse

L'identificazione delle vulnerabilità è effettuata mediante l'analisi delle seguenti fonti informative:

- precedente documentazione disponibile relativa alla valutazione dei rischi informatici;
- esiti delle attività di verifica condotte dalle strutture di Internal Audit, Compliance, controllo rischi o altre strutture di controllo;
- esiti delle attività di verifica e test delle componenti ICT oggetto di change management;
- esiti delle attività di verifica condotte dalle strutture aziendali a cui sono demandati i presidi di sicurezza;
- corpo normativo interno (Policy, Regolamenti, Circolari, Manuali Operativi, ecc.) da cui è possibile individuare tutte le attività previste per ciascun macro-processo aziendale, nonché i ruoli e le responsabilità attribuite a ciascun organo coinvolto nell'iter di processo;
- normativa esterna, specialistica di settore e non (Leggi del Parlamento, Decreti del Governo, Circolari e/o Regolamenti degli Organi di Vigilanza, ecc.) da cui è possibile individuare i requisiti organizzativi minimi che l'Entità Giuridica è tenuta ad implementare e le eventuali sanzioni previste per ciascuna violazione alle norme. Per la corretta interpretazione di tale fonte di informazioni, l'analista può avvalersi del supporto delle unità specialistiche presenti all'interno delle diverse Entità Giuridiche del Gruppo;
- evidenze empiriche rilevate internamente dal sistema di Loss Data Collection e/o dalla procedura degli incidenti informatici e/o dal Data base Italiano delle Perdite Operative "DIPO". Tali tipologie di informazioni, se non sono direttamente disponibili, possono essere richieste alla Funzione di controllo dei Rischi Operativi della Capogruppo;
- altre fonti esterne (es. siti specializzati che identificano i bug di sistema e i difetti dei sistemi ICT, vulnerabilità pubblicate dai fornitori, ecc.);
- altre fonti alimentanti utili a verificare l'adozione o meno di alcuni requisiti di sicurezza.

Tipologia	Vulnerabilità
Infrastruttura	Mancanza di protezione fisica
	Mancanza di controllo degli accessi
	Linea elettrica instabile
	Locali soggetti ad allagamento
Hardware e impianti	Mancanza di sistemi di backup
	Suscettibilità a variazioni di tensione
	Suscettibilità a variazioni di temperatura
	Suscettibilità a radiazioni elettromagnetiche
	Programma di manutenzione insufficiente
Comunicazioni	Linee di comunicazione non protette
	Uso di password in chiaro
	Traffico wireless non cifrato
	Presenza di linee dial-up
	Libero accesso ai dispositivi di rete
Documentazione	Locali non protetti
	Carenza di precauzioni nell'eliminazione
	Assenza di controllo nella duplicazione
Software	Complessità interfaccia applicazioni
	Mancanza autenticazione utente
	Mancanza logging accessi
	Errori software noti
	Password non protette
	Cattiva gestione password
	Diritti di accesso scorretti
	Uso del software incontrollato
	Sessioni aperte senza presenza utente
	Assenza di backup
	Carenza nella dismissione dei supporti
Personale	Personale insufficiente
	Procedure reclutamento inadeguate
	Personale esterno incontrollato
	Addestramento di sicurezza inadeguato
	Uso improprio o scorretto hardware/software
	Carenza di monitoraggio

Metodologia di analisi

Identificazione delle vulnerabilità associate agli asset 2/2

Per ricavare una valutazione complessiva della probabilità che una minaccia possa "sfruttare" le vulnerabilità associate a ciascun asset è necessario che:

- **ogni minaccia sia correlata ad una o più vulnerabilità**
- **ogni vulnerabilità sia correlata a un asset**

Minaccia	Vulnerabilità	Tipologia di Asset Aziendale									
		Edificio	Locale Tecnico	Utente	Profilo Applicativo	Processo	Risorsa Informatica	Software	Hardware	Rete	Flusso dati
Blocco o malfunzionamento software	Errata definizione delle specifiche funzionali						X	X			
	Errato sviluppo software						X	X			
	Errati test funzionali						X	X			
	Errato rilascio/installazione						X	X	X		
	Errori nelle procedure di ripristino dei dati da backup						X	X	X		
	Inadeguatezza dei sistemi di protezione da software malevolo						X	X	X		
	Errata configurazione						X	X	X		
	Inadeguata valutazione di capacity planning						X	X	X		
	Mancanza delle linee di comunicazione dati e rete									X	
	Mancanza o inadeguatezza di un piano di disaster recovery						X	X	X		
Cancellazione e alterazione accidentale di dati	Errata attribuzione dei diritti di accesso				X						
	Errato sviluppo software						X	X	X		
	Mancanza di adeguata formazione			X							
	Utilizzo di software non autorizzati						X	X	X		
Cancellazione/alterazione intenzionale di dati di sistema e/o diffusione di virus da parte del personale interno (inclusi eventuali outsourcers)	Mancanza di adeguata formazione			X							
	Errata attribuzione dei diritti di accesso				X						
	Errato sviluppo software						X	X	X		
	Errati test funzionali						X	X	X		
	Errata configurazione						X	X	X	X	
	Utilizzo di software non certificati						X	X	X		
	Mancanza di tracciamento (log)						X	X	X	X	
	Inadeguatezza dei sistemi di autenticazione						X	X	X	X	
	Inadeguatezza delle policy di gestione delle credenziali (identificativo, password, terzo fattore)					X	X	X	X		
	Trasferimento in chiaro delle credenziali di autenticazione (identificativo, password, terzo fattore)						X	X	X	X	
	Errata gestione e custodia delle credenziali di autenticazione (identificativo, password, terzo fattore)					X					
	Mancanza aggiornamento software						X	X	X		
	Inadeguati strumenti e/o soluzioni di sicurezza informatica						X	X	X	X	

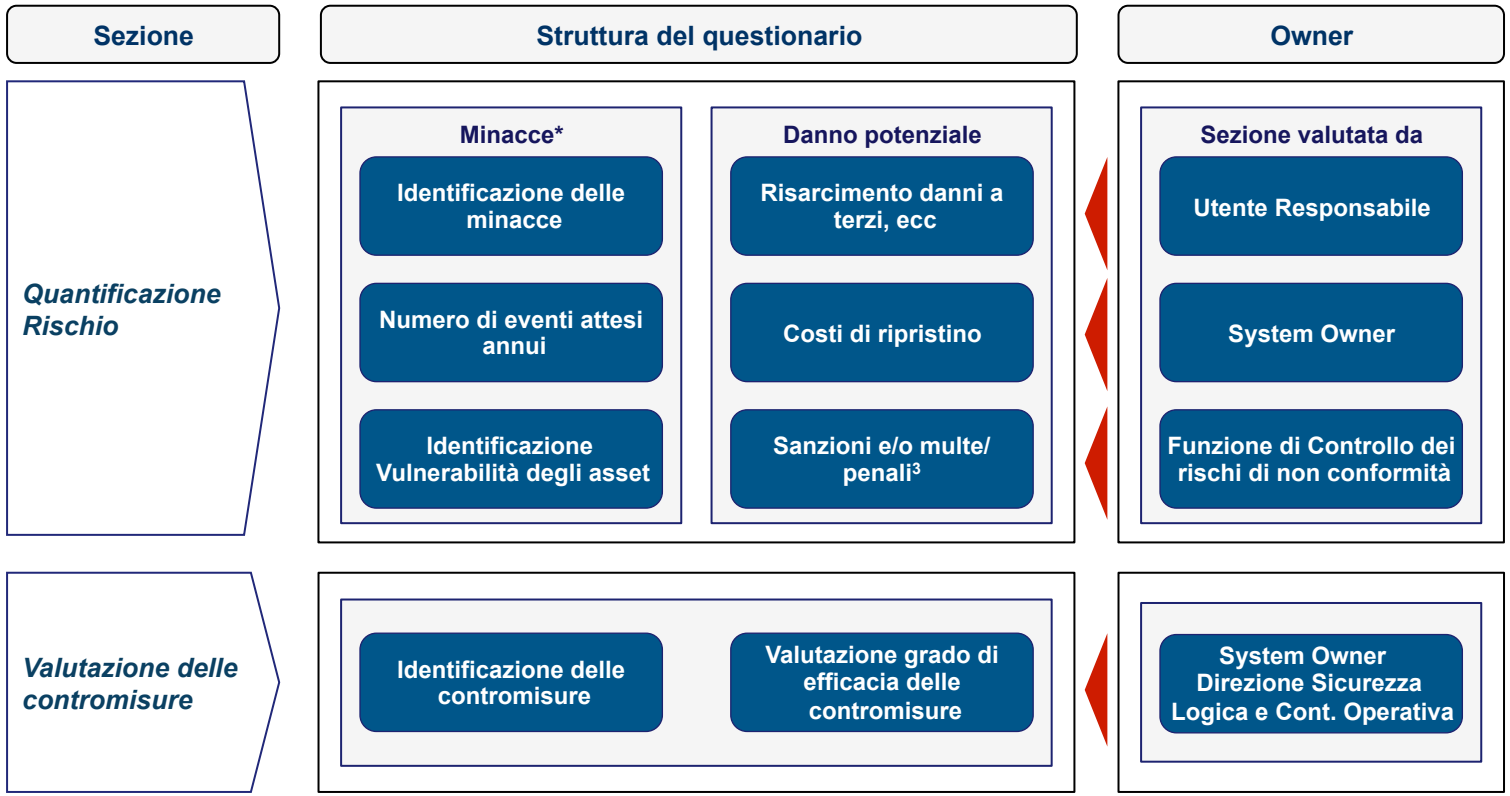
UBI Banca

Metodologia di analisi

Valutazione del danno potenziale

La valutazione del rischio è svolta con la compartecipazione di diversi attori previsti dal modello organizzativo. In particolare, ogni utente è chiamato a valutare particolari aspetti definiti in funzione delle specifiche competenze e degli ambiti di attività che gli sono stati attribuiti dall'Organigramma Aziendale

In termini operativi questo comporta la suddivisione del questionario in diverse sezioni di analisi, ciascuna compilata dall'utente competente in materia



(*) L'identificazione delle vulnerabilità a cui ciascun asset ICT è esposto e l'elenco delle possibili minacce che potrebbero sfruttare tale vulnerabilità (ivi inclusa la stima delle probabilità di accadimento delle stesse) è effettuata dalla struttura aziendale a cui è demandato il presidio della sicurezza logica e continuità operativa

UBI Banca

Metodologia di analisi

Identificazione e valutazione delle contromisure in essere

- **L'obiettivo di questa fase è quello di analizzare il sistema di contromisure ICT in essere e valutare la loro capacità di minimizzare e/o eliminare la probabilità che una minaccia possa "sfruttare" le vulnerabilità del sistema e/o contenere gli eventuali danni economici**
- **La valutazione è effettuata in funzione del livello di implementazione e dell'efficacia delle contromisure in essere**
- **Il livello di analisi è la singola componente della risorsa informatica: i risultati sono successivamente aggregati a livello di risorsa** (livello di analisi dell'utente responsabile)
- **In fase di valutazione si tiene anche conto dei seguenti fattori:**
  - **le misure di sicurezza devono trovare riscontro nella mappatura dei processi aziendali e/o nel corpo normativo in essere. Nel caso di mancato riscontro, esse non potranno essere valutate come contromisure in essere ma dovranno essere identificate come interventi di mitigazione proposti** (il fatto che tali contromisure non siano formalizzate è di per sé una criticità)
  - **le valutazioni devono riflettere le caratteristiche intrinsiche della contromisura. In particolare, la periodicità di esecuzione** (ex ante o ex post rispetto all'operazione), **il grado di automazione** (automatica o manuale)**, la frequenza di esecuzione rispetto all'operatività quotidiana** (es. controllo mensile su operatività giornaliera)

Metodologia di analisi

Valutazione del rischio

Il rischio è determinato dalla combinazione del danno potenziale derivante da possibili violazione dei requisiti di sicurezza con la probabilità che una minaccia possa sfruttare una delle vulnerabilità associate alla risorsa informatica

Rischio Potenziale

Si definisce "Rischio Potenziale" il livello di rischio identificato prima dell'applicazione delle contromisure in essere

Numero di eventi attesi annui		Danno potenziale
n° di eventi attesi annui per violazioni di Riservatezza dei dati	X	Danno derivante da violazioni di Riservatezza dei dati
n° di eventi attesi annui per violazioni di Integrità dei dati	X	Danno derivante da violazioni di Integrità dei dati
n° di eventi attesi annui per violazioni di Disponibilità dei dati	X	Danno derivante da violazioni di Disponibilità dei dati
n° di eventi attesi annui per violazioni di Riservatezza, Integrità e Disponibilità dei dati	X	Costi di ripristino dell'operatività a seguito di violazioni di Riservatezza, Integrità e Disponibilità dei dati
n° di sanzioni attese annue	X	Sanzione attesa annua per singolo evento, legata alle violazioni derivanti da perdita di riservatezza, integrità e disponibilità dei dati

Rischio Residuo

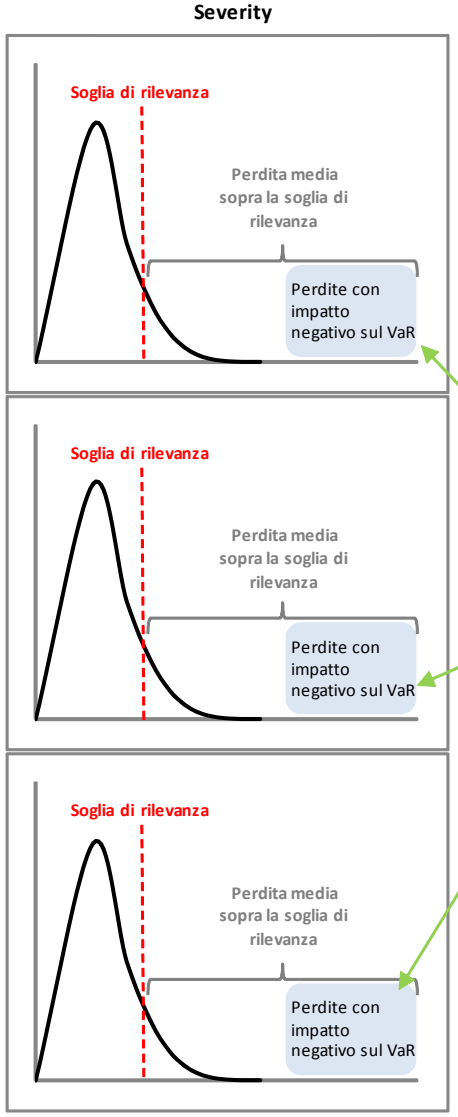
Applicando al rischio potenziale gli effetti di mitigazione derivanti dall'efficacia delle misure di sicurezza si ottiene il valore del rischio residuo

Rischio Potenziale × (1- efficacia delle misure di sicurezza)

UBI Banca

Metodologia di analisi

Verifiche di congruità e coerenza e controllo limiti



Perdite Esterne (DIPO)

Perdite Interne (LDC)

Perdite Potenziali (SRA)

Prima di procedere alla fase di gestione/ mitigazione del rischio informatico, i risultati dell'analisi sono sottoposti ad un controllo di congruità e coerenza da parte delle strutture del Chief Risk Officer:

- **identificazione e analisi di eventuali incoerenze esistenti tra l'analisi del rischio informatico e altre evidenze di rischio**
- **superamento della soglia di tolleranza al rischio**

Solgia di Tolleranza=
+ Perdita media sopra soglia LDC
+ Perdita media sopra soglia DIPO
+ Perdita potenziale media sopra soglia SRA
3

Soglia di tolleranza al rischio: è il danno potenziale massimo per singolo evento che il Gruppo ha deciso di accettare per salvaguardare i propri obiettivi strategici. Tale limite è identificato nella perdita media registrata oltre la soglia di rilevanza definita nell'ambito del modello di calcolo dell'Operational VaR

Tale limite, è differenziato per ciascuna risk class identificata per il modello di calcolo dell'Operational VaR e rappresenta i valore di perdita degli eventi che storicamente hanno avuto un impatto negativo sulla dotazione di capitale stimata per i rischi operativi

Nel caso in cui il rischio residuo ecceda la Soglia di Tolleranza, saranno valutate le più opportune strategie di gestione del rischio

Metodologia di analisi

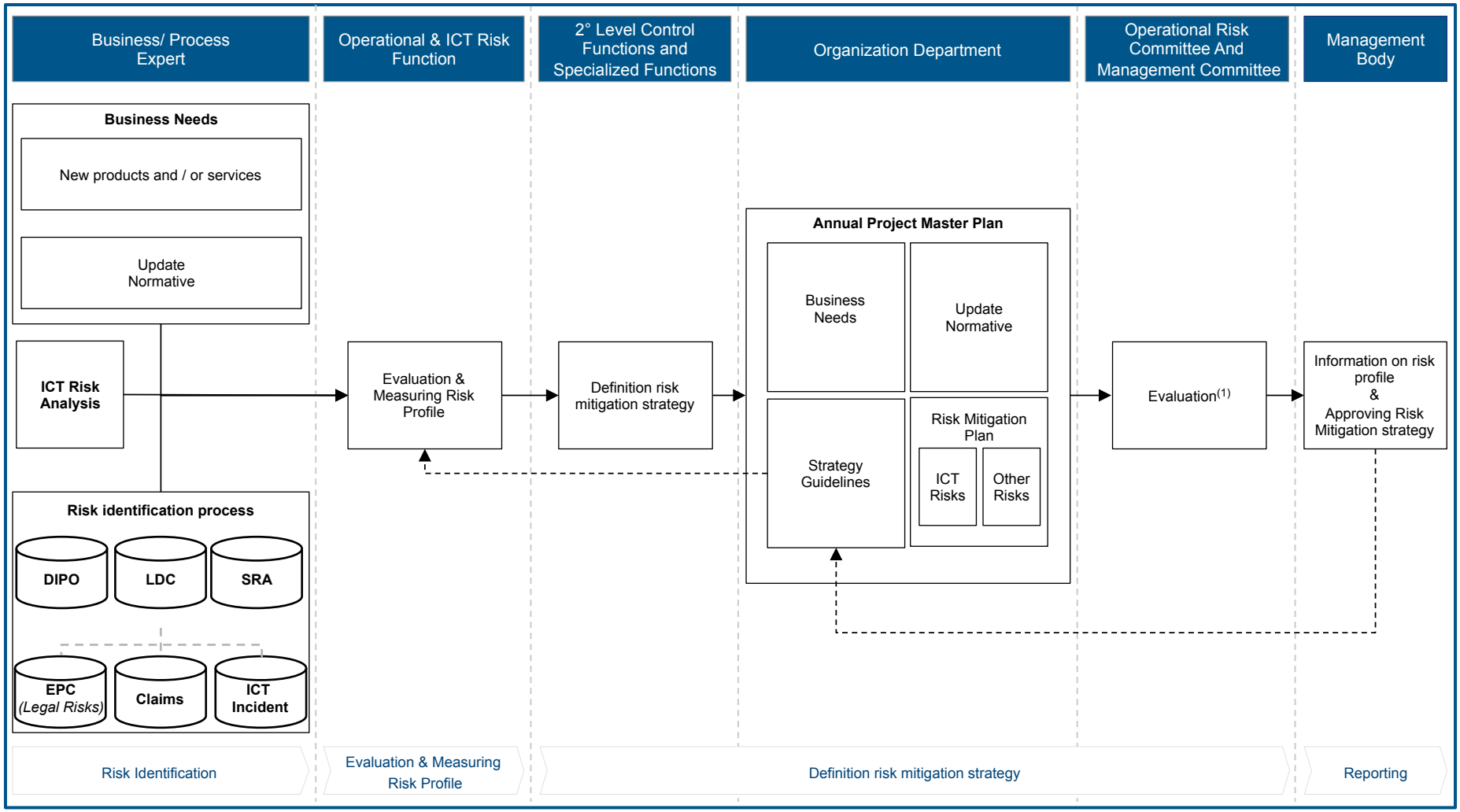
Strategie di gestione del rischio 1/2

- **Le strategie di gestione del rischio sono definite in funzione del tipo di rischio, della gravità delle conseguenze e dai costi ad esso associati**
- **La proposta della strategia di gestione del rischio** (piano di trattamento)**, è sottoposta alla valutazione preventiva del Comitato Rischi Operativi e successivamente all'approvazione degli Organi Aziendali**

Metodologia di analisi

Strategie di gestione del rischio 2/2

La definizione del master plan progetti annuale del Gruppo è effettuata anche in base alle evidenze delle attività di monitoraggio del profilo di rischio



(1) Analisi di tutte le proposte prima di essere sottoposte all'approvazione degli Organi Aziendali

Agenda

- Contesto di riferimento
- Assetto Organizzativo
- Metodologia di Analisi
- **Glossario**

Glossario 1/3

Rischio informatico: è il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT) .
Nella rappresentazione integrata dei rischi aziendali, tale tipologia di rischio è considerata secondo gli specifici aspetti dei rischi operativi, reputazionali e strategici. Le componenti relative ai rischi reputazionali e strategici sono valutate nell'ambito del modello ICAAP mentre la componente relativa ai rischi operativi è misurata secondo la metodologia di analisi dei rischi informatici illustrata nel presente documento

Incidente informatico: ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi di hacker, …) nonché i malfunzionamenti e i disservizi. Un incidente informatico si definisce grave qualora ne derivi almeno una delle seguenti conseguenze:

- perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità
- disservizi rilevanti sulla clientela e/o altri soggetti (ad es., intermediari o infrastrutture di pagamento). La valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio
- il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza

Componente critica: è il sistema/ applicazione per il quale un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni operative importanti aziendali (tra cui l'efficace espletamento dei compiti degli organi aziendali e delle funzioni di controllo)

Applicazioni sviluppate direttamente dalle unità operative e di controllo: sono le applicazioni sviluppate direttamente dalle unità operative e/o di controllo per lo svolgimento in modo automatico di attività standard e/o ripetitive. La stessa struttura utente è responsabile del sistema, ne autorizza le modifiche e/o le nuove implementazioni e/o le esegue direttamente. Ad essa è demandata inoltre la responsabilità di garantire gli stessi livelli di sicurezza, in termini di riservatezza, integrità e disponibilità dei dati, coerenti con quelli previsti dagli applicati sviluppati dalla Funzione ICT

Glossario 2/3

Riservatezza: consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate e si applica sia all'archiviazione sia alla comunicazione delle informazioni. Un'informazione è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione. Il nome e il numero di conto corrente di una persona, separati, non sono informazioni; è la combinazione dei due dati che costituisce l'informazione. La riservatezza dell'informazione può essere quindi garantita sia nascondendo l'intera informazione (per esempio con tecniche di crittografia) sia nascondendo la relazione tra i dati che la compongono. La riservatezza non dipende solo da strumenti hardware e software; il fattore umano gioca un ruolo chiave quando vengono ignorate le elementari regole di comportamento: tenere le password segrete, controllare gli accessi a reti e sistemi, rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione), cifrare i documenti e i messaggi riservati e così via.

Integrità: è il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche. Per l'hardware e i sistemi di comunicazione, l'integrità consiste di fattori come elaborazione corretta dei dati, livello adeguato di prestazioni e corretto instradamento dei dati. L'integrità del software riguarda fattori come la completezza e coerenza dei moduli del sistema operativo e delle applicazioni e la correttezza dei file critici di sistema e di configurazione. Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la coerenza tra dati in relazione tra loro (per esempio i record coinvolti in una transazione).

Disponibilità: è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono. Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili. Per impedire l'inaccessibilità delle informazioni, si deve preservare la disponibilità delle condizioni ambientali (energia, temperatura, umidità, atmosfera, ecc.) e delle risorse hardware e software a fronte sia di problemi interni (guasti, errori, blackout, disastri e altro), sia di attacchi esterni (per esempio provenienti da Internet), volti a impedire o a ridurre l'accessibilità ai sistemi e alle informazioni.

Glossario 3/3

Utente Responsabile: è la figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti, nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica. Normalmente, tale ruolo è assegnato ai responsabili di strutture a diretto riporto dell'Alta Direzione di Capogruppo nel caso di attività accentrate presso la Capogruppo e/o in service tecnologico presso UBI.S, ai responsabili di strutture a diretto riporto della Direzione Generale delle singole società controllate nel caso di attività non accentrate presso la Capogruppo e non in service presso UBI.S.

L'attribuzione del ruolo è automatica qualora corrisponda alla nomina a responsabile (anche se "ad interim") della struttura per la quale il sistema di gestione di valutazione del rischio informatico preveda il ruolo in esame. L'identificazione delle strutture e l'elenco dei nominativi che organizzativamente non risultano responsabili di unità organizzative cui assegnare il ruolo di Utente Responsabile è effettuata, in coerenza con le responsabilità e le modalità di esecuzione del Self Risk Assessment previsto dal sistema di gestione dei rischi operativi, dalla funzione di controllo dei rischi operativi di Capogruppo .

Ai fini gestionali l'Utente Responsabile identifica, fra le strutture a proprio riporto gerarchico, le Strutture Utenti cui delegare le attività maggiormente operative.

Struttura Utente: tale ruolo è identificato tra gli utenti esperti delle strutture organizzative a riporto gerarchico dell'Utente Responsabile ed ha il compito di supportare quest'ultimo nello svolgimento delle attività maggiormente operative ad egli demandate. Sono utenti che utilizzano quotidianamente l'applicazione informatica oggetto di analisi e ne definiscono le regole di funzionamento, certificano il corretto funzionamento nell'utilizzo quotidiano e/o la corretta implementazione degli eventuali interventi di adeguamento (mediante user test) in caso di change management e/o incidenti/ anomalie e ne certificano la conformità alle norme e alle esigenze di business.

System Owner: è il responsabile applicativo di una risorsa informatica all'interno della struttura della funzione ICT. Presidia la procedura informatica assicurandone lo sviluppo e la gestione tecnica secondo i processi standard condivisi a livello IT, garantendo l'allineamento delle procedure al disegno architetturale di riferimento e alle relative scelte tecnologiche. A tal fine riceve dall'Utente Responsabile, sia nel corso del processo di Demand Management sia durante la fase di gestione dei cambiamenti al sistema informativo , le richieste evolutive sui requisiti utente.