Deutsche Bank
Group Technology & Operations

Circolare Banca d'Italia "263"
Cap. 8 – *Il Rischio informatico*

"Un inquadramento metodologico per favorire l'integrazione del rischio informatico nella gestione del rischio operativo"

Passion to Perform

BANCHE E SICUREZZA 2014, 27-28 maggio

Content

Definizione di Rischio

Il R. viene solitamente definito e calcolato come prodotto dei fattori:

$$\mathbf{R = P \times I \times E}$$

dove:

P = probabilita' (della minaccia)	(alta per minacce molto probabili)
I = impatto (gravita' del danno / dell'effetto)	(alto per danni consistenti)
E = efficacia (dei controlli)	(alto per controlli poco efficaci)

In pratica il rischio viene definito come la probabilità che una minaccia sfrutti una vulnerabilità per generare un impatto nocivo (senza che esista una contromisura che lo impedisca).

Il valore determinato a valle dei primi due fattori e' il R. Potenziale, quello a valle dei tre fattori e' il R. residuo. La differenza tra R. potenziale e R. residuo viene solitamente calcolata valutando due momenti successivi: quello pre-controlli e quello post-controlli. In pratica:

$R.\ pot. = P_1 \times I_1$

$R.\ res. = P_2 \times I_2$

e ponendo l'efficacia dei controlli pari alla differenza dei due momenti.

Un Rischio, per essere descritto, deve essere sempre almeno associato ad una tripletta di informazioni: Minaccia, Vulnerabilita', Effetto.

Categorizzazione delle Minacce (1/2)

Una minaccia si puo' considerare come la causa che origina un evento nocivo. Per questo motivo, talvolta, viene anche chiamata "fattore di rischio". Una minaccia si considera un Fattore di Rischio per un evento quando ne costituisce la causa potenziale.

Le minacce possono insistere:

- sugli asset
- sui processi
- sui servizi / sugli output.

Le minacce, per essere efficaci, devono sfruttare una vulnerabilita', una carenza, una debolezza del sistema.

Una minaccia non ha una Probabilita' intrinseca associata ma gli viene attribuita in una certa circostanza (o scenario) quando contemporaneamente genera un impatto.

La probabilita' viene stimata sulla base di:

• un giudizio qualitativo	basata su un giudizio del tipo (Alto, Medio, Basso)
• una valutazione quali/quantitativa	basata su accadimenti stimati entro classi predefinite
• una stima quantitativa	basata sulle analisi storiche e su dati statistici

Categorizzazione delle Minacce (2/2)

Le minacce possono essere divise in:

Tipologia	Esempi
atti intenzionali	aggressioni, frodi
atti non intenzionali	errori involontari di tipo operativo
violazioni di clausole contrattuali / di normativa / di regole di mercato / di discipline	possono essere sia volontari sia involontari e sia verso clienti, sia verso terzi
atti di forza maggiore	disastri, eventi non controllabili
eventi tecnologici	malfunzionamenti, guasti

Categorizzazione delle Vulnerabilita’

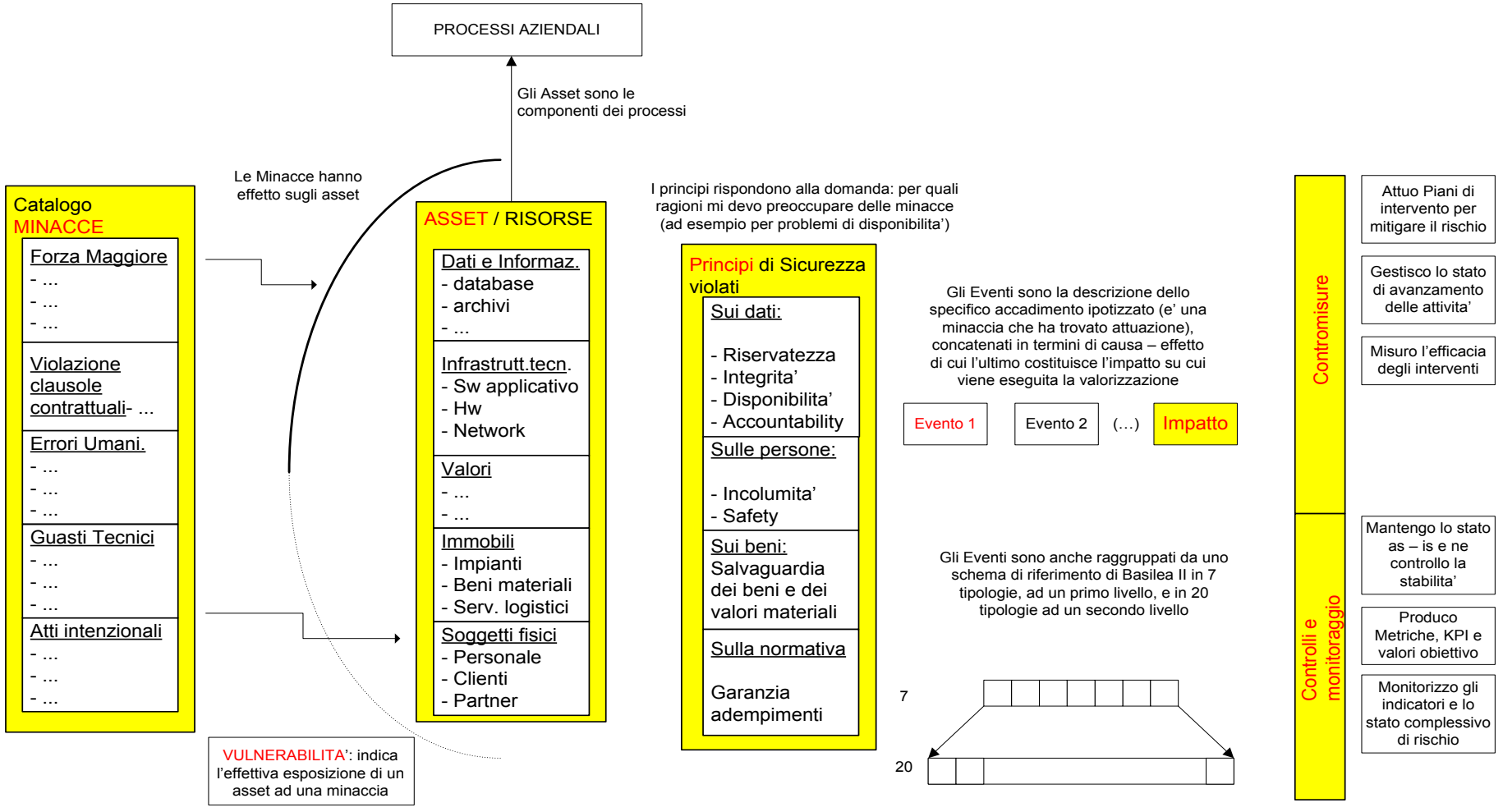
Le vulnerabilita’, invece, vanno distinte dalle cause origine, cioe’ dalle minacce, e sono riconoscibili per il fatto che rendono debole un sistema, cioe’ aggredibile dalle minacce. Sono una condizione necessaria ma da sole non implicano l’accadimento nocivo della minaccia, semplicemente ne favoriscono l’efficacia.

Le vulnerabilita’ possono essere individuate solitamente in :

Tipologia	Esempi
carenze procedurali	operativita’ manuale rispetto a processi automatici, carenze di formazione, inconsistenza documentale
carenze organizzative	carenza di risorse, di mezzi, fattori di stress
carenze di controlli	assenza di fasi di controllo, di monitoraggio
carenze manutentive / di misure preventive sui sistemi	attribuzione errata delle facolta’ agli utenti, impianti vetusti, sistemi non aggiornati

E’ utile la loro individuazione per analizzare come una minaccia si attiva e per individuare possibili misure di contenimento del rischio mediante mitigazioni preventive, che cioe’ riducono la probabilita’ di accadimento della minaccia.

Nomenclatura delle componenti dell'analisi



Il Rischio e' dato dal prodotto:

P (Evento) x G (Impatto) x E (Controllo)

dove P = Probabilita', G = Gravita', E = efficacia

Classificazione degli eventi

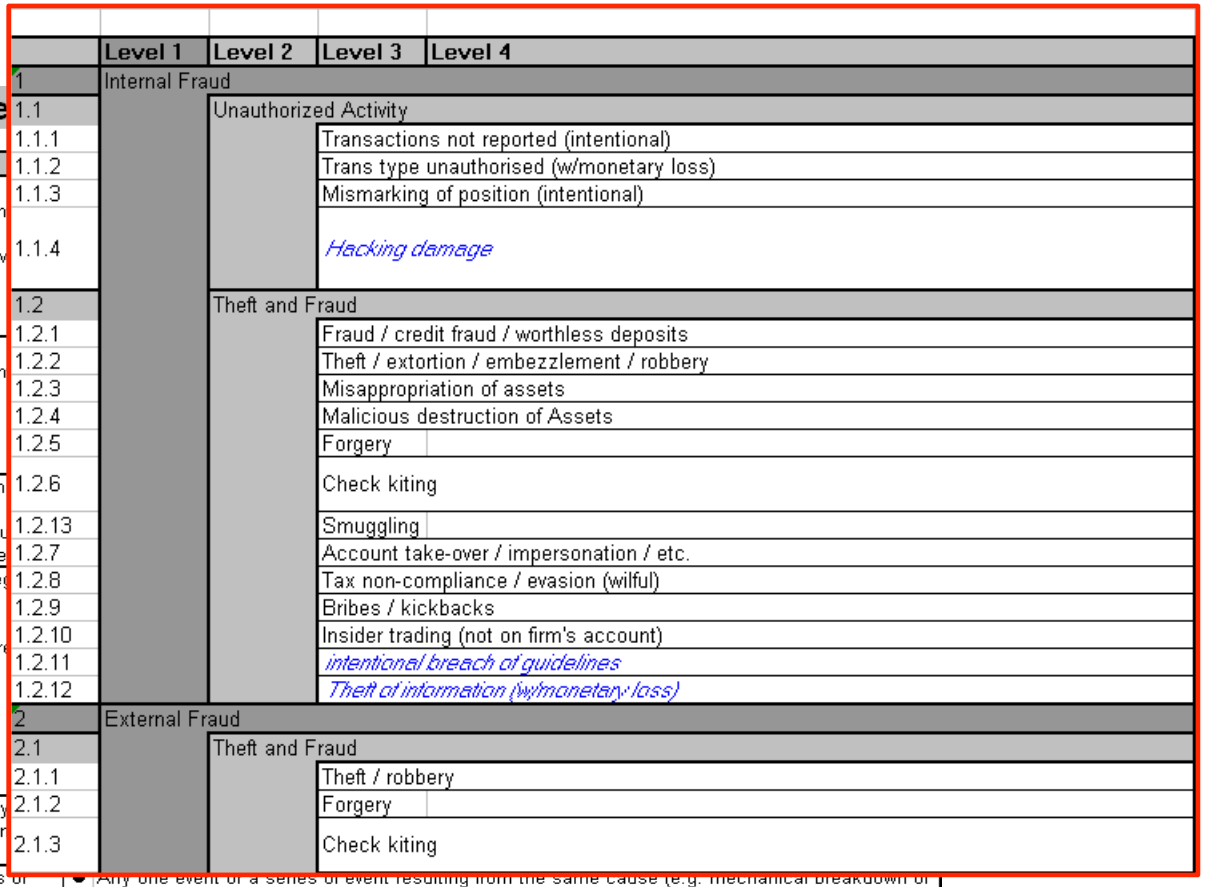
- Il piu' ampio dettaglio codificato delle tipologie di eventi nocivi si trova all'interno delle categorie dei Loss Event Type (ET) dell'accordo di Basilea II.
- Il R. Operativo e' visto talvolta in modo riduttivo come un sistema di Loss Data Collection e di classificazione degli eventi accaduti in base agli ET.
- Gli ET sono un sistema di classificazione delle perdite in base a categorie di eventi incentrati sugli effetti. Per una corretta analisi e prevenzione del R. Informatico, occorre invece riuscire a determinare la "causa origine", detta anche "fattore di rischio" (ad es. una frode sulle carte di credito puo' essere registrata negli ET 2 in quanto atto intenzionale mosso dall'esterno ai sistemi ma occorre valutare se e' avvenuta a causa di un malfunzionamento generato ai danni del S.I. o per una inconsapevolezza umana).

Per questo si e' cercato di ricondurre le minacce connesse con il R. Informatico alla tabella degli ET di Basilea II interpretando le categorie in modo piu' idoneo a descrivere gli eventi informatici. (v. all. 1 e 2)

1. Rischi IT.xls
2. Riclassificazione minacce.xls

E' R. Informatico anche qualcosa che non rientra nel R. Operativo perche' considera i casi di possibile perdita di Riservatezza, come pure le implicazioni di tipo strategico e reputazionale.

La tabella degli Event Type di Basilea II



	Level 1	Level 2	Level 3	Level 4
1	Internal Fraud			
1.1		Unauthorized Activity		
1.1.1			Transactions not reported (intentional)	
1.1.2			Trans type unauthorised (w/monetary loss)	
1.1.3			Mismarking of position (intentional)	
1.1.4			*Hacking damage*	
1.2		Theft and Fraud		
1.2.1			Fraud / credit fraud / worthless deposits	
1.2.2			Theft / extortion / embezzlement / robbery	
1.2.3			Misappropriation of assets	
1.2.4			Malicious destruction of Assets	
1.2.5			Forgery	
1.2.6			Check kiting	
1.2.13			Smuggling	
1.2.7			Account take-over / impersonation / etc.	
1.2.8			Tax non-compliance / evasion (wilful)	
1.2.9			Bribes / kickbacks	
1.2.10			Insider trading (not on firm's account)	
1.2.11			*intentional breach of guidelines*	
1.2.12			*Theft of information (w/monetary loss)*	
2	External Fraud			
2.1		Theft and Fraud		
2.1.1			Theft / robbery	
2.1.2			Forgery	
2.1.3			Check kiting	

Base

Level 1 name	Definitions	
1) Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circum regulations, the law or company policy, excluding diversity/discrimination events, v involves at least one internal party.	
2) External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circum the law, by a third party.	
3) Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal inju claims, or from diversity/discrimination eve	
4) Clients, Products and Business Practices	Losses arising from an unintentional or neg failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature design of a product.	
5) Damage to Physical Assets	Losses arising from loss or damage to phy assets from natural disasters or other even	
6) Business Disruption and System Failures	Losses arising from disruption of business or system failures	• Any one event or a series of event resulting from the same cause (e.g. mechanical breakdown of the same parts, error in the specific program) shall be deemed as a single event. • Not to be captured in this category, but either in "Internal Fraud" or "External Fraud": Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, which involve either internal or external parties. • Category is only appropriate if there was no loss or damage to physical/fixed assets.
7) Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors (unintentional or negligent failure).	• This category is Back Office related and also serves as a bracket for Level 2 categories which do not fit well in any other Level 1 category (Trade Counterparties and Vendors). • Claims, litigation and payments of restitution arising from the same cause shall be counted as a single event. • Category is only appropriate if there was no loss or damage to physical/fixed assets. • Category is only appropriate if there was no technology, telecommunication (hardware and software) disruption or utilities failure/outage or disruption.

Conduzione dell'analisi del R. (1/3)

La valutazione del R. puo' essere basata su:

1. checklist predefinite, comode per accelerare la valutazione ma con lo svantaggio che ogni volta deve essere eseguita per intero

2. un Framework impostato sulla struttura dei processi e delle attivita'

   Per ogni attivita' (o componente di servizio) i rischi sono rilevati valutando la loro esposizione ai seguenti principi (IN, DI, RI, AC, SA, VA, LE) (o trigger) divisi per categoria:

   - **INtegrita'** **Sicurezza delle Informazioni**
   - **DIsponibilita'**
   - **RIservatezza**
   - **ACcountability**

   - **SAfety – Incolumità d. persone** **Salvaguardia delle risorse umane e materiali**
   - **Protezione di beni e VAlori**

   - **Conformita' a LEggi e regolam.** **Adeguamento normativo**

   Questo secondo approccio consente il vantaggio di conservare la riferibilita' ai processi operativi e la possibilta' di un graduale e progressivo affinamento dell'analisi senza perdere il riferimento agli asset sottostanti. (V. approfondimento)

Conduzione dell'analisi del R. (2/3)

- L'analisi e' stata completata con l'individuazione dei **protocolli di controllo** di primo e secondo livello esistenti, con il riferimento agli indicatori gia' attivi, con il riferimento alla documentazione interna e alla normativa esterna che prescrive i controlli e le contromisure.

- E' stato incluso il riferimento alle registrazioni degli eventi negativi (o **incidenti**) occorsi per validare gli assunti dell'analisi o per ritararli. Di fatto la rilevazione degli incidenti e delle anomalie e' necessaria per mantenere sempre attuale l'analisi del rischio e ricalibrare il modello di previsione delle probabilita' e di valutazione dell'entita' degli impatti.

- E' stata calcolata la differenza tra la valorizzazione del **rischio inerente** (o potenziale, cioe' in assenza di contromisure o di controlli) e del **rischio residuo** (o attuale) per pesare l'efficacia dei controlli e delle contromisure attive. (Per R. residuo e' stato considerato il rischio informatico a cui un'organizzazione e' esposta una volta applicate le misure di attenuazione.)

Conduzione dell'analisi del R. (3/3)

- E' stato calcolato un **coefficiente di rischio** e una **classe di rischio** per una prioritizzazione della successiva analisi di adeguatezza.

- Per una riferibilita' dei rischi agli asset informatici e' stato necessario evidenziare il riferimento ai singoli asset su cui poggiano le specifiche attivita'. Questo consente, anche in caso di analisi svolta per processi, di poter sempre individuare i rischi che insistono su uno specifico asset e gli asset piu' esposti.

- Per i rischi piu' rilevanti sono stati espressi i fabbisogni di ulteriori indicatori di monitoraggio, di controlli o di azioni di mitigazione e ne e' stata pianificata l'attuazione.

Valorizzazione dei controlli

- Il calcolo della **differenza tra il rischio inerente e il rischio residuo** ha permesso abbastanza semplicemente di evidenziare il beneficio introdotto dai presidi di controllo e dalle misure di mitigazione, anzi ne ha consentito una valorizzazione percepibile da tutti gli operatori, sia IT sia di business. Infatti le mitigazioni permettono di operare costantemente con piu' bassi coefficienti di rischio e il **costo del mantenimento dell'apparato dei controlli e delle contromisure**, a cui oggi piu' nessuno e' disposto a rinunciare, viene **percepito come un valore**.

- Esempi sui **controlli** sono: le funzioni di quadratura ridondate, il principio dei 4 occhi, le ricertificazioni periodiche degli utenti, il confronto con configurazioni standard dei sistemi ecc.

- Si raccomanda di far stimare l'adeguatezza del sistema dei controlli IT da un esperto IT mentre la valutazione dell'impatto e il peso che le disfunzioni informatiche hanno sui processi operativi da un referente di Business. E' opportuno che l'insieme delle valutazioni sui rischi e sulle mitigazioni venga revisionato periodicamente da una funzione di controllo di secondo livello (es. ORM).

Mappatura del Rischio – la matrice di dettaglio (1/3)

Hardware	Legenda:	RI	Riservatezza	Most likely = (eventi ripetuti) =	M
Software		IN	Integrita'	Likely = (si prox 12 mesi) =	L
Dati		DI	Disponibilita'	Probab = (si prox 1-5 anni) =	P
Processi		AC	Accountability	Unlikely = (no prox 5 anni) =	U
Risorse Umane		SA	Safety - Incolumita' pers		
Impianti		VA	Protezione beni e valori		
Network		LE	Conformita' normativa		

UO - AREA	Asset	Riferimento SLA	Incidenti - anomalie	(Sotto)Processo coinvolto	Fase - Attivita'	Vulnerabilita'	Principio violato	Carenza interna - aggressione esterna - causa - MINACCIA	Tipo di rischio operativo	Codifica B II	Effetto
IES				IES-036 - Identity Management Services	Identity Administrator profile	- Non tutti gli ambienti di amministrazione hanno il 4EP (four eyes principle) - Fasi manuali	IN	Amministratore puo' abusare di autorizzazioni inadeguate o eccessive	Attivita' non autorizzata	A1b	Facolta' eccessive possono consentire operazioni illecite sui sistemi amministrati tra cui frodi
IES				IES-036 - Identity Management Services	Gestione utenti in generale	Fasi manuali senza 4EP Dimenticanza dei riferimenti per l'accountability	AC	Errori nel censimento iniziale dei dati anagrafici e nella classificazione di un'utenza	Errore di attribuzione delle entita'	E1e	Manca la possibilità di individuare con certezza il soggetto responsabile
IES				IES-036 - Identity Management Services	Gestione utenti in generale	Difficoltà di controllo su utenti cessati	RI	Utilizzo di utenze appartenenti a persone che hanno lasciato l'Azienda	Appropriazione indebita	F2b	Furto di dati mediante accesso non autorizzato ai dati tramite utenza non propria
IES				IES-036 - Identity Management Services	Gestione autorizzazioni Ambiente mainframe	Possibili errori legati a fasi manuali o interpretazioni manuali. Assenza del 4EP.	RI	Gestione inadeguata puo' consentire generazione di profili impropri o assegnazione autorizzazioni non corrette	Transazioni non autorizzate	A1b	Accesso non autorizzato ai dati puo' consentire operazioni improprie o illecite

Mappatura del Rischio - la matrice di dettaglio (2/3)

NM	= Near Miss (< 1.000 € impact)
VVL	= Very very low (< 10.000 € impact)
VL	= Very low (< 100.000 € impact)
L	= Low (< 1m€ impact)
M	= Medum (< 10 m€ impact)
H	= High (< 40 m€ impact)
S	= Seriuos (< 250 m€ impact)
T	= Material (over)

Gradi di Probabilita' attuale [U] [P] [L] [M]	Gradi di Impatto attuale [NM] [VVL] [VL] [L] [M] [H] [S] [T]	PROTOCOLLI DI CONTROLLO Primo livello	PROTOCOLLI DI CONTROLLO Secondo livello	SPI o Indicatori di monitoraggio - preventivi / di eventi	Ulteriori misure di miglioramento (se esistono gap)	Normativa interna di riferimento - KOP	Note - Aspetti di criticita' - Piani di azione	Coefficienti di Probabilita' Attuale [U] [P] [L] [M]
U	VL	Check list dei gruppi di autorizzazione Tool di richiesta ASAP, IRIS 4EP su dbLEGI	Ulteriori fasi di Sicurezza interna applicativa		Con la l'introduzione di Jupiter sarà salvaguardato il principio dei 4 occhi al momento della esecuzione della richiesta di un ID o di un'abilitazione.	...		1,25
P	VL	Report mensili che individuano utenze non classificate correttamente	Guide operative interne dettagliate			...		2,5
P	VL	Per utenti interni offboarding tramite lista proveniente da HR.	Per utenti esterni controllo tramite verifica di identita' del richiedente in caso di richiesta di reset pswd e report di utilizzo utenza Disabilitazione di utenze "sospette" Processo di ricertificazione delle utenze		Progetto di classificazione utenze esterne all'interno dei sistemi HR per un maggiore controllo	...		2,5
P	L	Modifiche agli accessi consentite solo dopo processo autorizzativo	Processo di ricertificazione periodico con tool (Gatekeeper e GRWE)		Con la l'introduzione di Jupiter sarà salvaguardato il principio dei 4 occhi al momento della esecuzione della richiesta di un ID o di un'abilitazione. Prevista eliminazione delle componenti di sicurezza interna	...		2,5
P	L	Modifiche agli accessi consentite solo dopo processo autorizzativo	Processo di ricertificazione periodico con tool (Gatekeeper e GRWE).			...		2,5

Mappatura del Rischio - la matrice di dettaglio (3/3)

				M	4,5	NM	0,3						
				L	3,5	VVL	0,6						
				P	2,5	VL	1						
				U	1,25	L	1,5						
						M	4						
						H	7,8						
						S	12,2						
						T	21						
Coefficienti di Probabilita' Attuale [U] [P] [L] [M]	Coefficienti di Impatto Attuale [NM] [VVL][VL] [L] [M] [H] [S] [T]	coeff. R.O. Attuale	Audit Risk Raiting Attuale				Gradi di Probabilita' potenziale [U] [P] [L] [M]	Gradi di Impatto potenziale [NM] [VVL][VL] [L] [M] [H] [S] [T]	coeff probabil potenziale	coeff. Impatto potenziale	coeff. R.O. potenziale	Audit Risk Raiting potenziale	
1,25	1	**1,3**	**1**				P	VL	2,5	1	**2,5**	**2**	
2,5	1	**2,5**	**2**				L	VL	3,5	1	**3,5**	**2**	
2,5	1	**2,5**	**2**				L	VL	3,5	1	**3,5**	**2**	
2,5	1,5	**3,8**	**2**				L	L	3,5	1,5	**5,3**	**2**	
2,5	1,5	**3,8**	**2**				L	L	3,5	1,5	**5,3**	**2**	

Mappatura del rischio - legenda dei campi della matrice

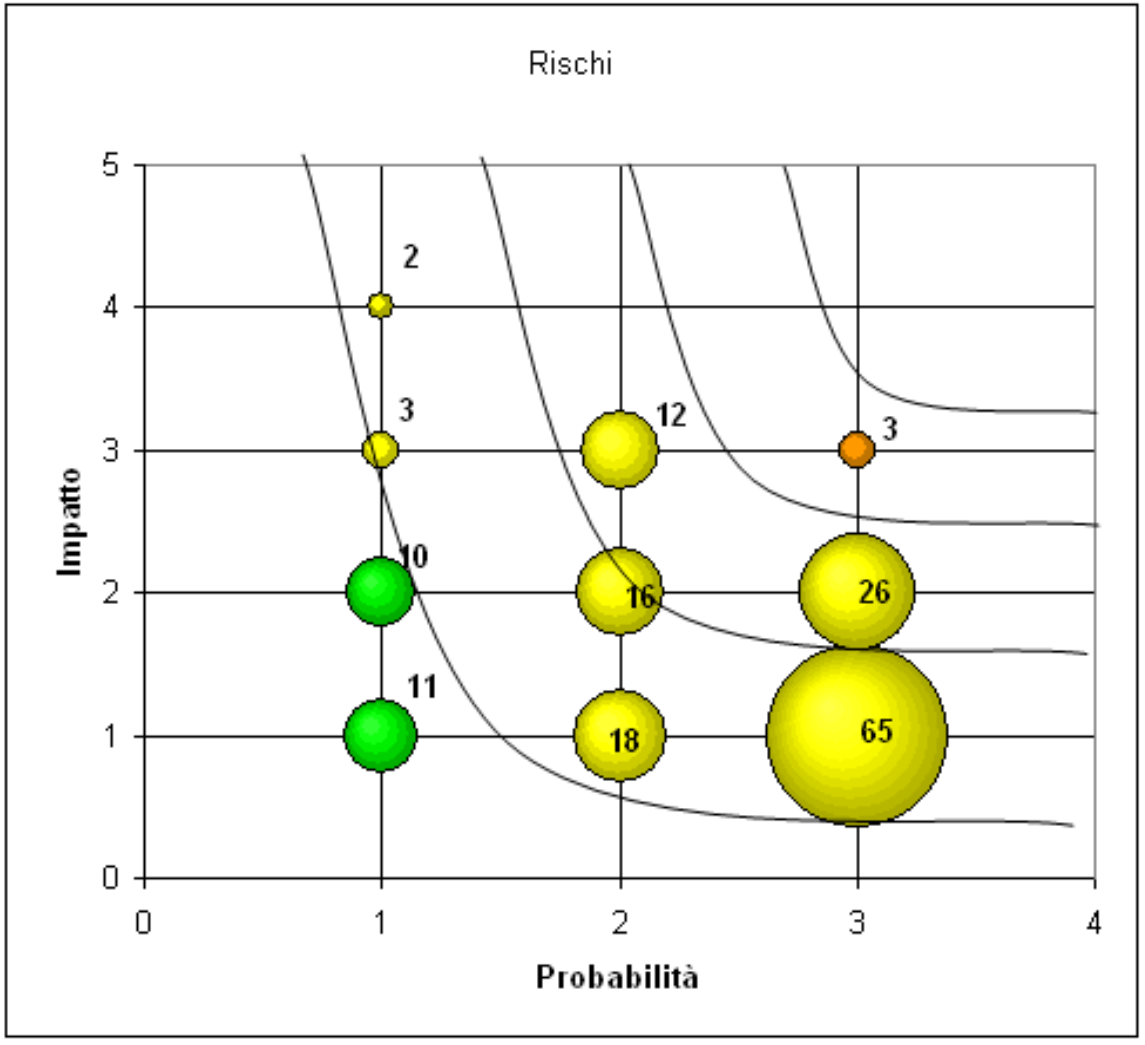
NOME CAMPO	DESCRIZIONE
UO - AREA	Riferimento all'unità operativa o all'area aziendale in esame.
(Sotto) -Processo coinvolto	Riferimento al processo / alla componente di servizio mappato negli SLA erogato dalla corrispondente unità operativa.
Fase attività	Riferimento alla specifica attività o fase di un processo esposto al rischio.
Asset	Riferimento alla componente di sistema che supporta un processo e che è investita da un rischio (HW, SW, database, network...).
Riferimento SLA	Riferimento ai documenti che contengono componenti strutturate e quantificate di servizi e processi definite tra i settori della società.
Incidenti / Anomalie	Eventi negativi registrati nell'ultimo triennio attinenti allo specifico rischio identificato.
Vulnerabilità	Riferimento alla vulnerabilità interna del sistema che consente l'attuazione della minaccia.
Principio violato [RI] [IN] [DI] [AC] [SA] [VA] [LE]	Criterio seguito per identificare il possibile rischio il cui accadimento è causa di evento nocivo.
Carenza interna - aggressione esterna - causa - Minaccia	Riferimento alla causa , sia interna sia esterna, che rappresenta un fattore di rischio.
Tipo di rischio operativo	Descrizione dell'effetto secondo la casistica prevista dall'allegato degli Event Type di Basilea II.
Codifica BII	Codifica a tre livelli dei rischi prevista dall'allegato degli Event Type di Basilea II; utile per successive funzioni di elaborazione dei dati.
Effetto	Conseguenza prodotta dall'evento, altrimenti detta "impatto".
Protocolli di controllo - primo livello	Riferimento ai controlli esistenti cosiddetti di primo livello o perché condotti in contemporanea all'esecuzione delle attività o perchè in rapporto 1:1 con queste; generalmente sono considerati di tipo "preventivo".
Protocolli di controllo - secondo livello	Riferimento ai controlli esistenti cosiddetti di secondo livello o perché condotti in differita o perché svolti da un ente diverso o perché svolti su dati di riepilogo o perché si riferiscono a una documentazione esistente o a pratiche operative prescritte; generalmente sono considerati di tipo "correttivo" o "a posteriori".
SPI o indicatori di monitoraggio / preventivi di eventi	Riferimento agli indicatori ad oggi desunti dai SPI degli SLA per il monitoraggio degli elementi che compongono le attività a rischio; possono esser indicatori di complessità delle attività (ad esempio legati a volumi crescenti di transazioni) o in indicatori di accadimenti negativi (ad esempio "numero di abend").
Ulteriori misure di miglioramento (se esistono gap)	In presenza di valori di rischio residuo superiori al valore di rischio minimo accettabile sono qui citate le ulteriori misure correttive necessarie.
Normativa interna di riferimento - KOP	Riferimento alla normativa, interna o esterna, che prescrive le modalità operative e di controllo, comprese le tracce documentali da produrre.
Note - Aspetti di criticità - Piani di Azione	Eventuali considerazioni di pro memoria o legate a iniziative non ancora pianificate o ad aspetti per cui è necessario un approfondimento.
Grado di Probabilità attuale [U] [P] [L] [M] (categoria)	Parametro legato alla Probabilità di accadimento della Minaccia (situazione attuale).
Grado di Impatto attuale [NM] [VVL] [VL] [L] [M] [H] [S] [M] (categoria)	Parametro legato alla Gravità dell'eventuale Impatto occorso (situazione attuale).
Coefficiente di Probabilità attuale [U] [P] [L] [M]	Valore numerico associato al grado di Probabilità di accadimento della Minaccia (situazione attuale).
Coefficiente di Impatto attuale [NM] [VVL] [VL] [L] [M] [H] [S] [M]	Valore numerico associato alla Gravità dell'eventuale Impatto occorso (situazione attuale).
Coefficiente R.O. attuale	Parametro legato alla Gravità dell'eventuale Impatto occorso (= rischio residuo o attuale).
Audit Risk Rating attuale	Valore di corrispondenza con la graduatoria di Rischio definita dal Group Audit (situazione attuale).
Grado di Probabilità potenziale [U] [P] [L] [M] (valore)	Parametro legato alla Probabilità di accadimento della Minaccia (situazione potenziale).
Grado di Impatto potenziale [NM] [VVL] [VL] [L] [M] [H] [S] [M] (valore)	Parametro legato alla Gravità dell'eventuale Impatto occorso (situazione potenziale).
Coefficiente di probabilità potenziale	Valore numerico associato al grado di Probabilità di accadimento della Minaccia (situazione potenziale).
Coefficiente di impatto potenziale	Valore numerico associato alla Gravità dell'eventuale Impatto occorso (situazione potenziale).
Coefficiente R.O. potenziale	Coefficiente di Rischio calcolato sulla base del prodotto Probabilità x Impatto (= rischio inerente o potenziale).
Audit Risk Rating potenziale	Valore di corrispondenza con la graduatoria di Rischio definita dal Group Audit (situazione potenziale).

Mappatura del Rischio - Coefficienti Probabilita' / Impatto

		soglia di accettazione	U	P	L	M		
			1,25	**2,5**	**3,5**	**4,5**		
> 250 M	T	**21**	26,25	52,50	73,50	94,50		
< 250 M	S	**12,2**	15,25	30,50	42,70	54,90	51 - 80	**5**
< 40 M	H	**7,8**	9,75	19,50	27,30	35,10	21 - 50	**4**
< 10 M	M	**4**	5,00	10,00	14,00	18,00	11 - 20	**3**
< 1 M	L	**1,5**	1,88	3,75	5,25	6,75		
< 100.000	VL	**1**	1,25	2,50	3,50	4,50		**2**
< 10.000	WL	**,6**	0,75	1,50	2,10	2,70	2,1 - 10	
< 1.000	NM	**,3**	0,38	0,75	1,05	1,35	1 - 2	**1**
							<1	**NC**
			accadimenti inverosimili	**accadimenti possibili (mai registrati)**	**accadimenti occasionali**	**accadimenti ripetitivi**		

Mappatura del Rischio - Risk Heat Map

			U	P	L	M		
			1,25	**2,5**	**3,5**	**4,5**		
> 250 M	T	**21**	26,25	52,50	73,50	94,50		
< 250 M	S	**12,2**	15,25	30,50	42,70	54,90	51 - 80	**5**
< 40 M	H	**7,8**	9,75	19,50	27,30	35,10	21 - 50	**4**
< 10 M	M	**4**	5,00	10,00	14,00	18,00	11-20	**3**
< 1 M	L	**1,5**	1,88	3,75	5,25	6,75		
< 100.000	VL	**1**	1,25	2,50	3,50	4,50		**2**
< 10.000	WL	**,6**	0,75	1,50	2,10	2,70	2,1 - 10	
< 1.000	NM	**,3**	0,38	0,75	1,05	1,35	1-2	**1**
							<1	**NC**



Analisi del Risk appetite nel caso del R. Informatico (1/3)

R. appetite: e' il livello di R. definito rispetto agli obiettivi strategici e di business.

- Il livello di R. appetite e' meno applicabile nel caso di R. informatico ma e' comunque opportuno definirlo perche' richiama la responsabilita' dei vertici della banca a fissare i livelli obiettivo e le soglie di propensione e di tolleranza al rischio.
- In termini di principio al R. Inf. non e' applicabile il concetto di rapporto Rischio / Rendimento e quindi il R. Appetite va riformulato in termini di R. di non conformita' o anche R. Reluctancy poiche' l'obiettivo e' quello di ridurre gli interventi ad un livello minimo comunque utile a garantire la conformita'.

- L'Assessment Guide for the Security of Internet Payments riporta che: "*gli obiettivi di sicurezza sono definiti dalla banca sulla base dell'appetito al R. che deriva:*

  - dalla sua capacita' di assorbire le perdite rilevanti (es. perdite finanziarie, danni reputazionali) e

  - dalla sua predisposizione verso l'assunzione del R. (es. se piu' cauto o piu' aggressivo".

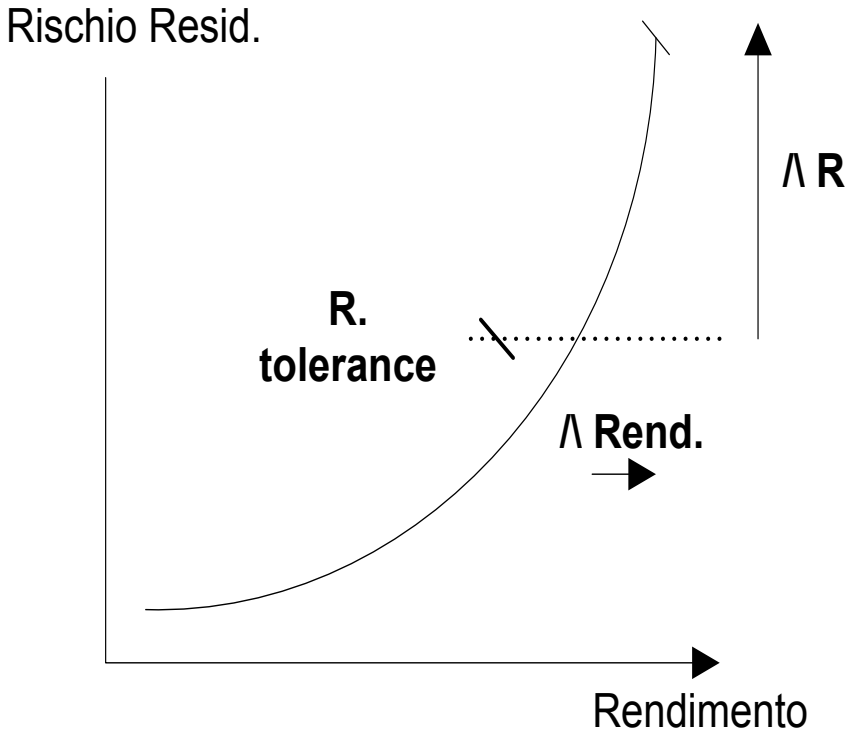
Analisi del Risk appetite nel caso del R. Informatico (2/3)

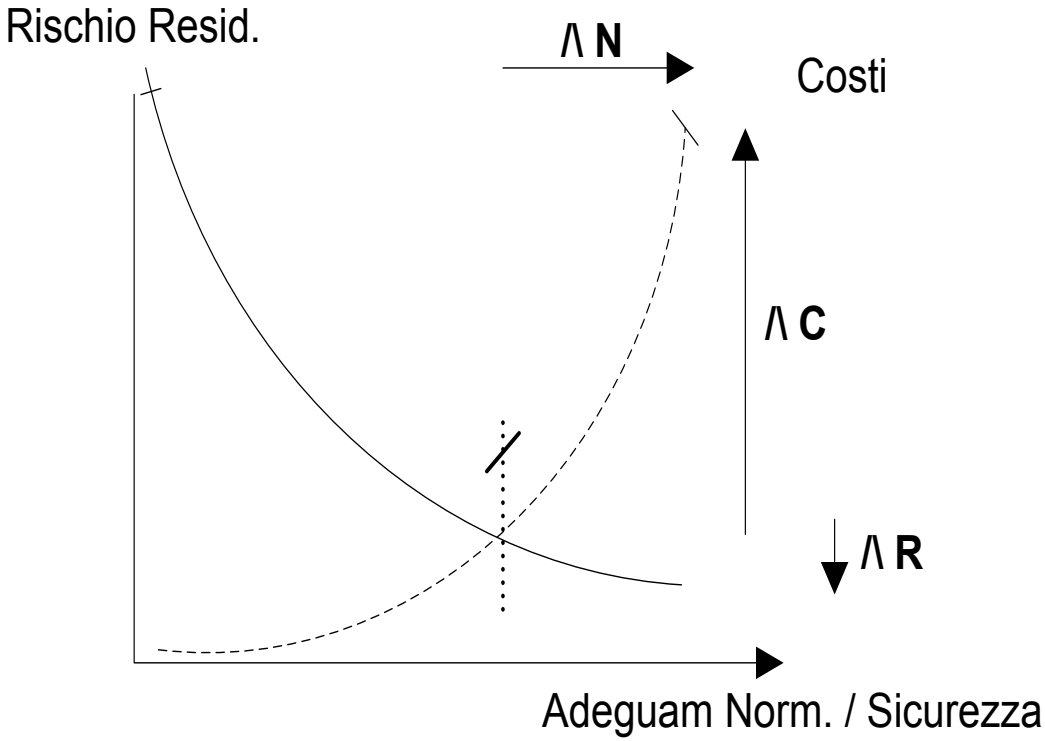
Dunque appare opportuno distinguere quando ci confrontiamo :

- rispetto agli obj. strategici o di business, caso in cui la prospettiva di un rendimento porta ad essere piu' aggressivi sul R. nel senso che si vorrebbe rischiare ma non ci si vuole esporre oltre un certo livello di R. tolerance

- rispetto agli obj. di sicurezza o normativi o comunque legati a principi di protezione, dove la prospettiva di un maggior costo porta a contenere gli interventi, nel senso che si mira a limitare il rischio per soddisfare i requisiti normativi ma fino al punto in cui i costi dei relativi interventi restano ragionevoli. Pertanto si limiteranno i costi entro un livello oltre il quale il R. marginale coperto sarebbe sproporzionato rispetto alla spesa necessaria per contenerlo.

Analisi del Risk appetite nel caso del R. Informatico (3/3)

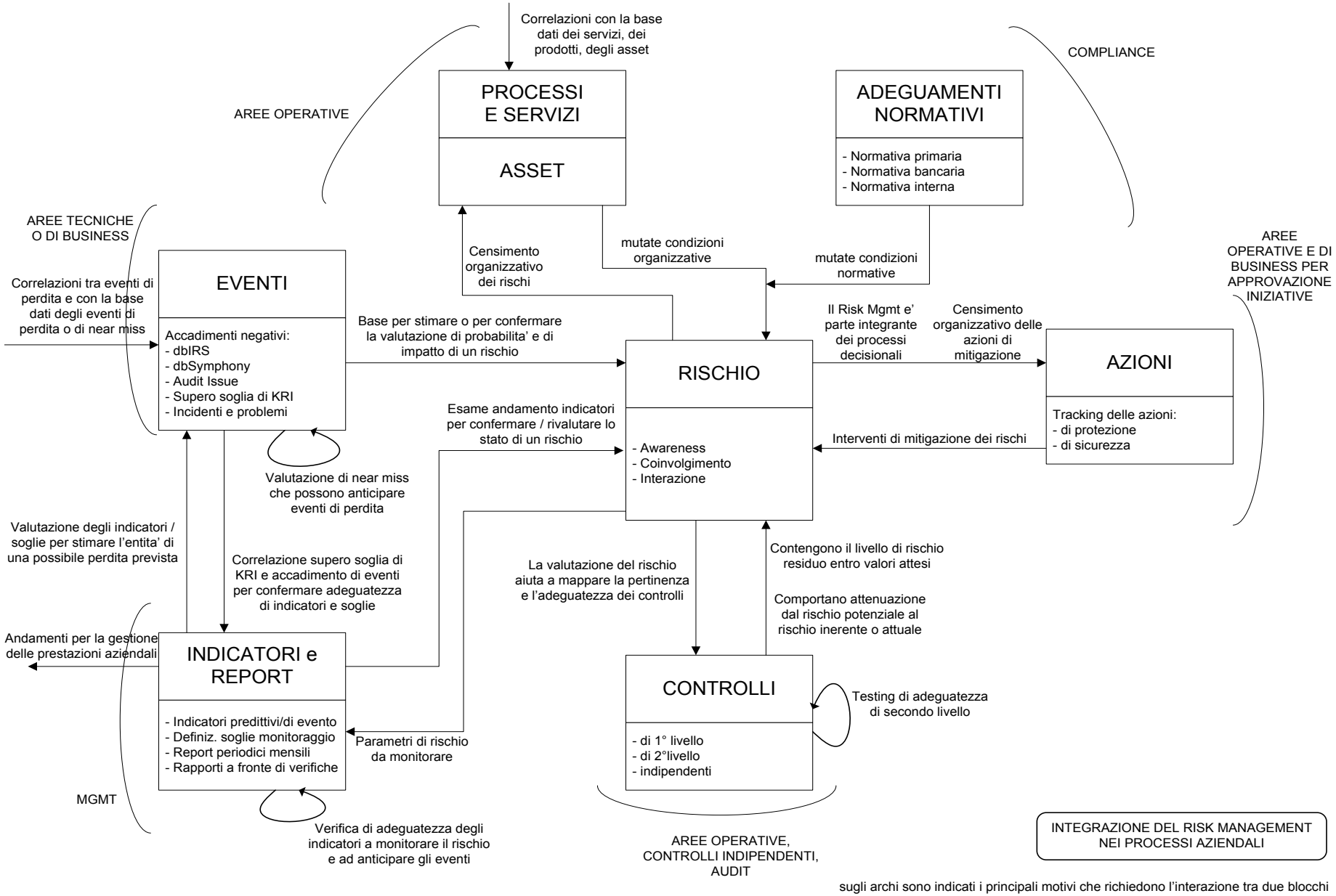




• nel caso del Risk appetite per iniziative di business a ritorno economico, si evidenzia che, oltre un certo valore, un miglioramento dei livelli di rendimento (/\ Rend) comporta un inutile incremento esponenziale del rischio residuo (/\ R)

• nel caso del Risk appetite per adeguamenti normativi si evidenzia che, oltre un certo valore, un miglioramento dei livelli di adeguamento normativo (/\ N) comporta una limitata riduzione marginale del rischio residuo (/\ R) ma anche la crescita di costi sproporzionati rispetto al beneficio atteso (/\ C)

Integrazione del ICT Risk Management nei processi aziendali



sugli archi sono indicati i principali motivi che richiedono l'interazione tra due blocchi

Q & A

risponde: Enrico Luigi Toso

enricoluigi.toso@db.com – tel. 02 4024 2802

Approfondimenti - Sviluppo del modello

- Il modello deriva da un contributo ad un precedente progetto ABILab sulla “Gestione della Sicurezza Integrata”, poi messo a punto per diventare piu’ in linea ai requisiti della circ. “263”
- Lo scopo del documento e’ quello di fornire una proposta di modello interpretativo “fattivo”, cioe’ di dare uno strumento di interazione agli uomini che trattano di sicurezza IT e di rischio IT.
- Chi si occupa di rischio vive un imbarazzo iniziale, talvolta di autentico disorientamento: “da cosa iniziare ?”, “come cogliere gli aspetti essenziali ?”, “come ottenere un risultato fruibile e non perdersi in un’attivita’ troppo analitica e difficile da mantenere ?”

- Su cosa puntiamo ? su cosa ci concentriamo ? → (Bussola) → La ricerca delle cause

Trattiamo della ricerca delle cause e del nesso “causa – effetto”. L’analisi del rischio ha per definizione un intento “proattivo”. Spesso siamo troppo concentrati sulla lettura ripetitiva degli effetti, degli indicatori, delle risultanze: dobbiamo lavorare di piu’ sull’analisi delle cause, delle minacce, dei fattori di R., dei nessi “causa – effetto”. Occorre focalizzarci sulla tripletta delle informazioni (vulnerabilita’ – minaccia – effetto) che compongono lo scenario (V. mappatura del R.)

- Con che dettaglio di analisi ? → (Binocolo) → approccio SMART: per superare un’impostazione puramente qualitativa ma senza arrivare alla pretesa di un’analisi quantitativa basata su serie storiche. Occorre iniziare in modo efficace: il mantenimento procede per approfondimenti successivi dove e’ necessario.

- Come trattiamo le informazioni ? →(Cruscotto) → Una tassonomia di possibili principi violati, di minacce e di tipologie di eventi offre categorie logiche di gestione delle unita’ di informazione.

Approfondimenti - Analisi per processi vs. analisi per asset

- La valutazione dei rischi deve arrivare a evidenziare gli asset esposti nel senso che deve essere calcolato il livello di criticita' di un asset (in base a specifici parametri)
- Tuttavia il livello di criticita' di un asset deriva dall'impiego di quell'asset all'interno di un servizio, di un prodotto o di un processo, coie' dallo scopo per cui viene utilizzato, non da una sua proprieta' intrinseca.

- Dunque occorre superare l'assunto, qualora venisse sollevato, che le prescrizioni della circ. 263 si limitano a rilevare il rischio connesso agli asset se prima non si affronta un'analisi dei processi, benche' l'analisi del rischio debba arrivare ad evidenziare gli asset critici.
- Va considerato peraltro che sempre la circ. 263 chiede che l'analisi del rischio arrivi ad evidenziare le operazioni critiche, dunque i processi.
- In definitiva l'esercizio che si propone di compiere e' quello di mappare i processi, le attivita' che li compongono e, solo dopo, gli asset che li sostengono una volta evidenziati gli ambiti di criticita' dei processi
- In questo modo potranno essere sempre identificati a posteriori sia i processi critici, sia gli asset critici, sia gli asset che sostengono i processi sia l'entita' del R. connesso con un processo o con un singolo asset.