UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN «SECURITY MANAGER»
CORSO DI FORMAZIONE IN «PROFESSIONISTA DELLA SECURITY»

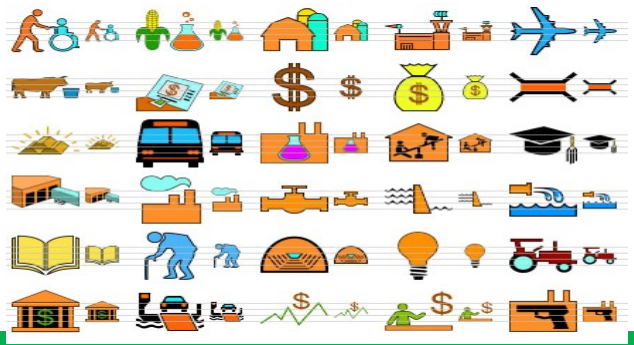
Luisa Franchina

Enterprise risk management

1

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Definizioni



2

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Formula dei rischi

M (minaccia) rappresenta la probabilità che venga tentato un attacco o avvenga un incidente o si manifesti un evento naturale (1…N) in quel determinato luogo.

V (vulnerabilità) rappresenta la probabilità che una minaccia venga attuata con successo a causa di una debolezza (1…M) nella difesa dell'obiettivo

R (rischio) rappresenta il rischio connesso con un particolare attacco in **un determinato luogo**

$$R_{luogo,N,M}(t) = f\left(M\left(\begin{smallmatrix}1\\2\\\cdots\\N\end{smallmatrix}\right); V\left(\begin{smallmatrix}1\\2\\\cdots\\M\end{smallmatrix}\right); I\left(\$\right)\right)$$

I (impatto) rappresenta il **potenziale** danno dell'attacco: beni materiali, infrastrutture, popolazione

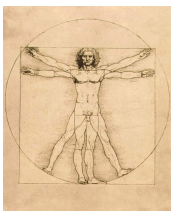
3

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le minacce

Naturali
Prevedibili e imprevedibili

Umane
Volontarie e accidentali



- Convenzionali
- Non convenzionali
- CYBER
  - strumento
  - territorio

Territori:
Terra
Acqua
Aria
Spazio
Cyber

Esposizione

4

Metriche dell'impatto

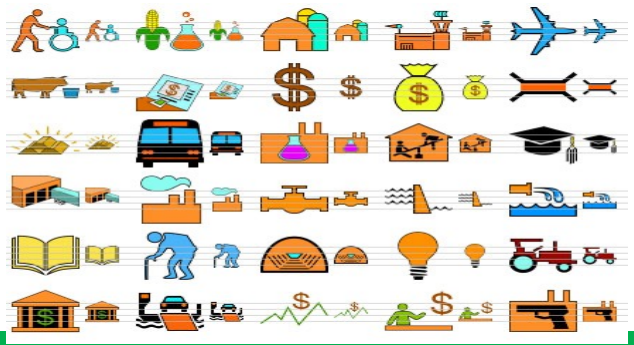
- Vittime
- Impatti economici
- Sicurezza economica
- Sofferenza fisica
- Perturbazione della vita quotidiana
- Fiducia nelle istituzioni
- Salute pubblica
- Sicurezza pubblica
- Impatti psicologici
- Sicurezza dello Stato
- Difesa della Nazione
- Impatto sull'opera delle istituzioni
- Violazione del territorio
- Disordine pubblico e panico
- Perturbazione della democrazia
- Impatto sull'ordine sociale
- Impatto geopolitico
- Morale nazionale
- Impatto ambientale
- Impatto sociopolitico
- Effetti negativi sui marchi e aziende nazionali
- NGH…

5

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Enterprise Risk Management e KII

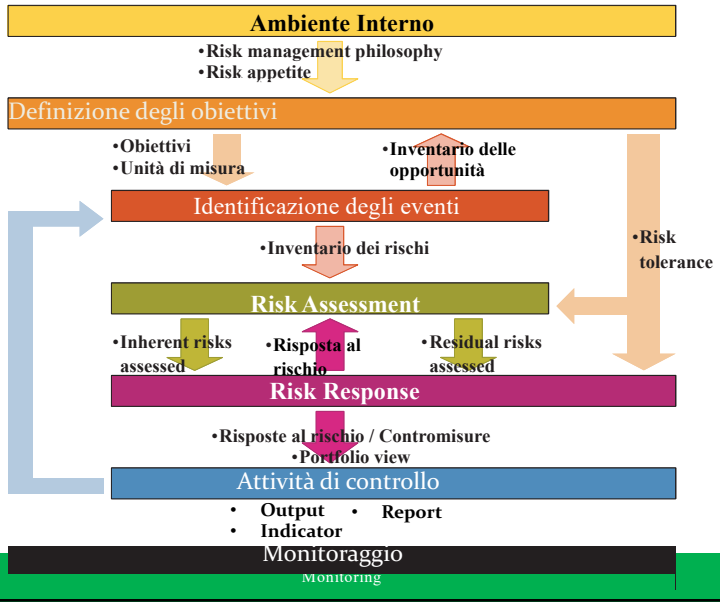
Enterprise risk management e Key Indicator



6

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

ERM



7

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

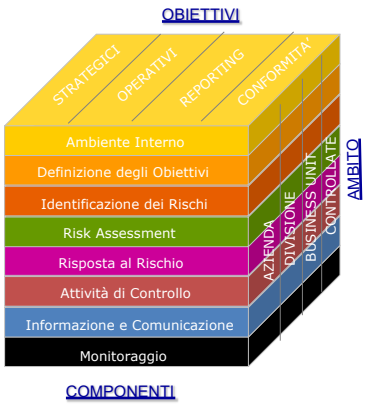
Coso ERM: metodologia (1/4)

L'ERM prevede che il SCIGR debba essere sviluppato identificando e gestendo tre dimensioni di analisi:

❑ Obiettivi: costituiscono la dimensione rispetto alla quale è possibile valutare l'efficacia del processo di Risk Management, in quanto lo stesso è volto a fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali;

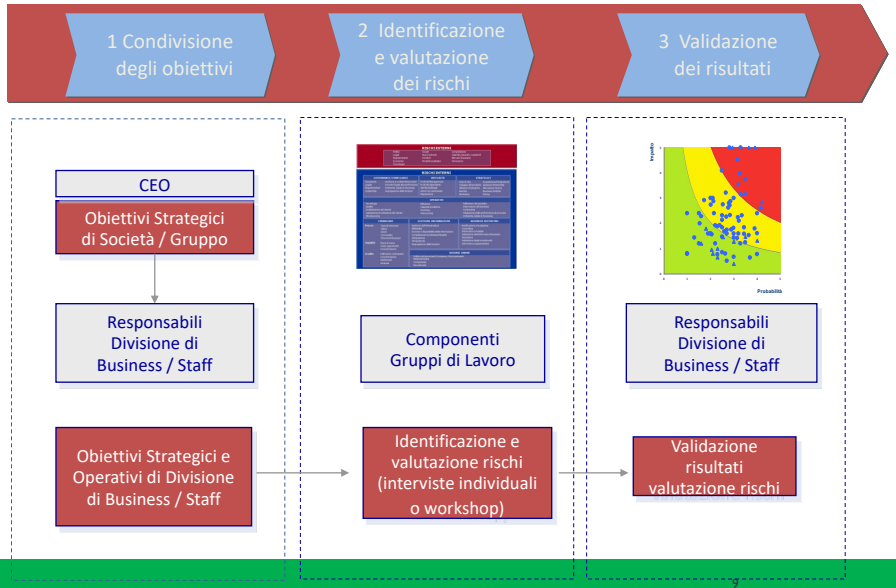
❑ Componenti: sono gli elementi che costituiscono il processo di Risk Management;

❑ Ambito: è il perimetro di applicazione del processo stesso.



8

COSO ERM: RISK ASSESSMENT (1/17)



9

9

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

COSO ERM: Risk Assessment – Principali fasi del processo (2/17)

1 Condivisione degli obiettivi

Definizione da parte dell'Amministratore Delegato di:

- Mission/Vision aziendale
- Obiettivi Strategici della società, che possono essere classificati in:
  - Obiettivi Qualitativi: obiettivi strategici mediante i quali le diverse divisioni identificano i nuovi modelli di business per sostenere il vantaggio competitivo nel lungo periodo.
  - Obiettivi Quantitativi: obiettivi legati al raggiungimento di performances economico\finanziarie nel breve\medio periodo (identificati nel Bdg e Piano Triennale).

10

10

COSO ERM: Risk Assessment – Principali fasi del processo (5/17)

2 Identificazione e valutazione dei rischi

I Rischi Interni a loro volta possono essere articolati nelle seguenti sotto-categorie:

- Governance\Compliance
- Integrità
- Strategici
- Operativi
- Finanziari
- Gestione Informazioni
- Business Reporting
- Risorse Umane.

11

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

COSO ERM: Risk Assessment – Principali fasi del processo (6/17)

RISCHI ESTERNI

Politici	Ciclo Economico	Clienti	Fornitori	Competizione	Mercato finanziario
Legali e Regolamentari	Tecnologici	Nuovi entranti	Prodotti sostitutivi	Calamità naturali e catastrofi	Mercato

RISCHI INTERNI

GOVERNANCE/COMPLIANCE		INTEGRITÀ	STRATEGICI	
Tassazione	Gestione e conferimento poteri	Frodi del Management	Ciclo di vita	Partnership/Alleanze
Legale e Regolamentare	Incentivi legati alle performance	Frodi dei dipendenti	Sviluppo del prodotto	Struttura organizzativa
Leadership	Segregazione delle funzioni	Atti illeciti/illegali	Marchio	Allocazione risorse
		Azioni non autorizzate	Marketing	Business Portfolio
		Reputazione	Acquisizione/Integrazione	Pricing

OPERATIVI

Tecnologia	Soddisfazione del cliente	Efficienza	Sourcing	Valutazione delle performance di processo	Fallimento del prodotto
Qualità	Obsolescenza	Capacità produttiva	Outsourcing	Ambiente, Salute & Sicurezza	Interruzione del business
					Contracting

FINANZIARI	GESTIONE INFORMAZIONI	BUSINESS REPORTING
Prezzo	Gestione dell'infrastruttura	Pianificazione e budgeting
Tassi di interesse	Affidabilità	Controlling
Valuta	Accesso alle informazioni (IT)	Informativa contabile
Azioni	Accesso e disponibilità delle informazioni	Valutazione dell'informativa finanziaria
Commodity	Completezza/Correttezza/Integrità	Tassazione
Strumenti finanziari	Adeguatezza	Valutazione degli asset
Credito	Disponibilità	Informativa regolamentare
Credit scoring	Segregazione delle funzioni	
Fallimento controparte		
Concentrazione		
Settlement		
Garanzie		
Liquidità		
Flussi di cassa		
Costo opportunità		
Concentrazione		

RISORSE UMANE

Politica del personale	Competenze	Performance Management	Sindacali
Formazione	Recruitment	Sviluppo della Leadership	

12

COSO ERM: Risk Assessment – Principali fasi del processo (7/17)

2 Identificazione e valutazione dei rischi

I rischi sono oggetto di due valutazioni che si differenziano per l'effetto delle azioni di mitigazione poste in essere dal management:

RISCHIO INERENTE

Concetto teorico che fa riferimento al massimo livello di rischio ipotizzabile, in assenza di qualsiasi attività di controllo.

Azioni di mitigazione

Attività poste in essere per ridurre la probabilità del manifestarsi del rischio e/o l'impatto collegato.

RISCHIO RESIDUO

Porzione di rischio che rimane in capo all'azienda dopo aver messo in atto le attività di controllo esistenti.

13

13

COSO ERM: Risk Assessment – Principali fasi del processo (8/17)

2 Identificazione e valutazione dei rischi

La valutazione del rischio si basa su due dimensioni

- IMPATTO
- PROBABILITA' DI ACCADIMENTO

In entrambi i casi viene utilizzata una scala di valutazione delle dimensioni del rischio per ordini di grandezza con 5 livelli, dove 5 rappresenta la valutazione massima e 1 la valutazione minima.

14

14

COSO ERM: Risk Assessment – Principali fasi del processo (9/17)

2 Identificazione e valutazione dei rischi

Identificare l'IMPATTO di un rischio vuol dire definire la tipologia di perdita e misurare la grandezza associata al verificarsi del rischio. E' quindi necessario quantificare il danno derivante per la Società sia in termini quantitativi che qualitativi.

I criteri per la valutazione dell'impatto dei rischi sono:

- Economico
- Mercato
- Reputazionale
- Vantaggio competitivo

15

15

UNIVERSITÀ DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

COSO ERM: Risk Assessment – Principali fasi del processo (10/17)

2 Identificazione e valutazione dei rischi

Valutazione dell'Impatto					
Livello	Descrizione	Criteri			
		Economico *	Mercato *	Reputazionale	Vantaggio competitivo
0	Nessun Impatto	Nessun Effetto economico	Nessun impatto sulla quota di mercato	Esiste consapevolezza nel pubblico, ma non vi sono manifestazioni di giudizio negativo	Nessun impatto sulla capacità di mantenere nel tempo il vantaggio competitivo acquisito
1	Marginale	Danno derivante dall'effetto stimato $< \alpha$ mln €	Impatto trascurabile sulla quota di mercato ($< \alpha$%)	Manifestazioni di giudizio negativo ingiustificate e strumentali da parte della concorrenza	Impatto marginale sulla capacità di mantenere nel tempo il vantaggio competitivo acquisito
2	Minore	Danno derivante dall'effetto stimato $\alpha - \beta$ mln €	Impatto limitato sulla quota di mercato (α% - β%)	Manifestazioni di giudizio negativo da parte della concorrenza a fronte di risultati o eventi avversi	La capacità di mantenere nel tempo il vantaggio competitivo acquisito potrebbe subire degli impatti anche se non significativi.
3	Medio	Danno derivante dall'effetto stimato $\beta - \gamma$ mln €	Impatto medio sulla quota di mercato (β% - γ%)	Manifestazioni di giudizio negativo da parte dell'opinione pubblica e dei gruppi di tutela dei consumatori a fronte di violazione, errori, imprudenze, variazione negativa del clima aziendale	La capacità di mantenere nel tempo il vantaggio competitivo acquisito potrebbe subire degli impatti.
4	Elevato	Danno derivante dall'effetto stimato $\gamma - \delta$ mln €	Impatto elevato sulla quota di mercato (γ% - δ%)	Manifestazioni di giudizio negativo a livello nazionale con sanzioni da parte dell'Organismo di Vigilanza, della Magistratura e della Pubblica Amministrazione.	La capacità di mantenere nel tempo il vantaggio competitivo acquisito potrebbe subire degli impatti elevati.
5	Significativo	Danno derivante dall'effetto stimato $> \delta$ mln €	Impatto significativo sulla quota di mercato ($> \delta$%)	Manifestazione di giudizio negativo su scala internazionale con ripercussioni sui rapporti con i Soci, sull'onorabilità della Società. Azioni potenzialmente destinate a mettere in discussione l'esercizio stesso dell'attività.	Compromesso il vantaggio competitivo acquisito.

16

COSO ERM: Risk Assessment – Principali fasi del processo (11/17)

2 Identificazione e valutazione dei rischi

- Economico: valuta l'effetto di un rischio in termini di minori ricavi o maggiori costi. Tale criterio può essere utilizzato per tutti quei rischi che hanno un effetto quantificabile sul conto economico della Società e necessita che vengano definite specifiche soglie sulla base di un *parametro di riferimento* (Costi, Ricavi, Margine).
- Mercato: possibile perdita di quote di mercato in seguito a rischi concernenti l'incapacità di soddisfare le esigenze dei clienti in termini di qualità del prodotto/servizio.
- Reputazionale: basato sul verificarsi di possibili eventi che potrebbero ledere l'immagine della Società.
- Vantaggio competitivo: misura l'eventuale perdita di vantaggio competitivo acquisito dalla Società a fronte del verificarsi dei rischi valutati.

17

17

COSO ERM: Risk Assessment – Principali fasi del processo (12/17)

2 Identificazione e valutazione dei rischi

Valutare la **PROBABILITA' DI ACCADIMENTO** di un rischio vuol dire definire la possibilità che l'evento/rischio identificato si manifesti nell'orizzonte temporale di 3 anni.

La definizione della probabilità è soggetta a ulteriori criteri valutativi di tipo qualitativo, quali:

- Vulnerabilità;
- Complessità;
- Esperienza precedente

18

18

COSO ERM: Risk Assessment – Principali fasi del processo (13/17)

2 Identificazione e valutazione dei rischi

Valutazione della probabilità di accadimento						
Livello	Descrizione		Orizzonte temporale			
			1 anno	2 anno	3 anno	oltre 3 anno
0	Nessuna probabilità	Mai	No	No	No	No
1	Improbabile	Non nei prossimi 3 anni, ma forse dopo	No	No	No	Forse
2	Poco probabile	Forse non nei prossimi 3 anni, ma sicuramente dopo	Forse	Forse	Forse	Sì
3	Probabile	Forse non nei prossimi 2 anni, ma sicuramente dopo	Forse	Forse	Sì	Sì
4	Molto probabile	Forse non entro 1 anno, ma sicuramente dopo	Forse	Sì	Sì	Sì
5	Altamente probabile	Sì, entro 1 anno	Sì	Sì	Sì	Sì

19

COSO ERM: Risk Assessment – Principali fasi del processo (14/17)

2 Identificazione e valutazione dei rischi

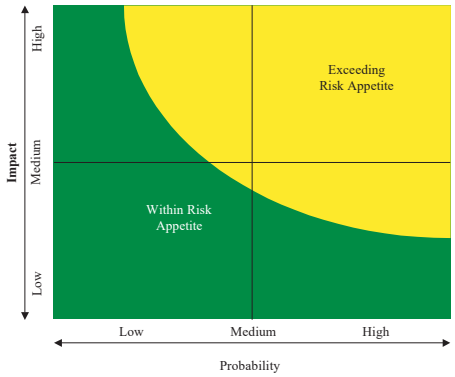
Scheda di formalizzazione dei rischi identificati e delle relative azioni di mitigazione

ID	Categoria di rischio	Sotto-categoria del rischio	Evento rischioso	Descrizione del rischio	Owner rischio	Valutazione del rischio INERENTE			Azioni mitiganti	Valutazione del rischio RESIDUO		
						Prob	Imp.	Rischio Inerente		Prob	Imp.	Rischio Residuo
Op-18	Interno	Operativi	Valutazione dei fornitori	Rischio relativo alla mancanza di procedure formali nel processo di selezione e di valutazione periodica dei fornitori che potrebbe causare le seguenti tipologie di problematiche: - carenze qualitative delle forniture; - interruzione delle forniture (monitoraggio della situazione economico / patrimoniale); - rapporti con fornitori non accreditati; - frodi da parte dei dipendenti coinvolti nel processo di acquisto; - mancato sviluppo del know-how necessario al presidio del mercato.	Direzione Acquisti di Gruppo / Ufficio Legale di Gruppo / Ufficio Affari Tributari	3,8	3,1	11,8	**Direzione Acquisti** - Accordi quadro (es. telefonia, acquisto di DVD per periodici); - Presidio continuo dei fornitori dal punto di vista dell'affidabilità finanziaria e attraverso il monitoraggio del mercato. **L'Ufficio Affari Legali** fornisce supporto alle strutture di business con riferimento a contratti e pareri. In particolare: - invio alle differenti AdB / Direzioni aziendali di un elenco di clausole standard da inserire in tutti i contratti (e.g., divieto di cessione del credito, privacy, codice etico); - analisi delle clausole contrattuali per individuare anticipatamente eventuali impatti / criticità legali derivanti dagli stessi. **L'Ufficio Affari Tributari** fornisce supporto alle strutture di business con riferimento a contratti e pareri. In particolare: mantenimento della struttura dell'Ufficio Affari Tributari, dopo il potenziamento dello scorso anno (inserimento risorsa senior), al fine di presidiare al meglio le tematiche di competenza. **DA IMPLEMENTARE:** - Vendor Manager.	2,5	2,1	5,3

Esempio

20

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT



Legenda:
CM = contromisure/risk response
OS = obiettivo strategico
OC = obiettivo correlato
R_{app} = risk appetite
R_i = rischio inerente
R_{tol} = risk tolerance

1) if OS > R_{app} → Revisione OS
2) if OS ≤ R_{app} → OC $R_{tol}(OC) \approx R_{app}$
3) OC → $R_i(OC)$
4) if $R_i(OC) > R_{tol}(OC)$ → CM→ $R_{residuo}$ $R_{residuo} \leq R_{app}$

21

COSO ERM: Risk Assessment – Principali fasi del processo (15/17)

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

3 Validazione dei risultati

Attraverso la valutazione dell'impatto e della probabilità di accadimento del rischio è possibile determinare la Matrice dei Rischi, che fornisce una rappresentazione sintetica del posizionamento relativo dei singoli rischi, consentendo al managemet di identificare le priorità di azione per le successive strategie di risposta al rischio.

La valutazione del rischio (*score*), data dal prodotto di probabilità di accadimento e impatto, genera tre livelli di rischio:

- Rischio Basso – Non rilevante: la Società non ritiene di dover attuare misure di controllo o strategie di mitigazione ulteriori.
- Rischio Medio – Monitorare: costante monitoraggio/gestione da parte della Società.
- Rischio Alto – Evitare/Ridurre: elevata attenzione da parte della Società perché il rischio supera il livello di accettabilità (Risk Appetite).

22

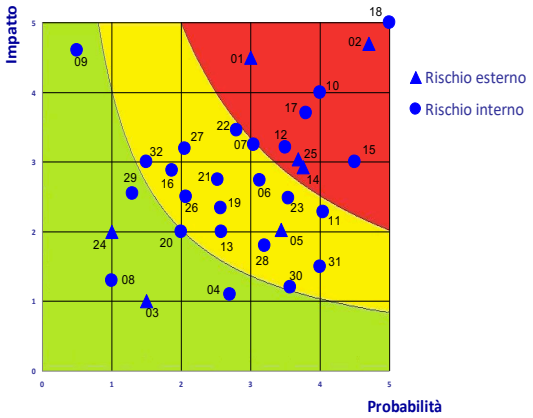
22

COSO ERM: Risk Assessment – Principali fasi del processo (16/17)

3 Validazione dei risultati

Esempio

Livello di rischio	Score
ALTO	β ≤ score ≤ γ
MEDIO	α ≤ score < β
BASSO	score < α



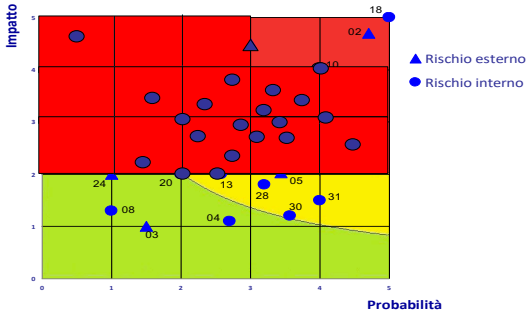
I risultati così ottenuti vengono sottoposti ai Direttori di Business/Staff che, dopo aver effettuato eventuali modifiche in maniera di judgemental, forniscono una validazione finale della situazione dei rischi per la loro area di competenza.

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La valutazione dell'impatto

Esempio

Livello di rischio	Score
ALTO	β ≤ score ≤ γ
MEDIO	α ≤ score < β
BASSO	score < α

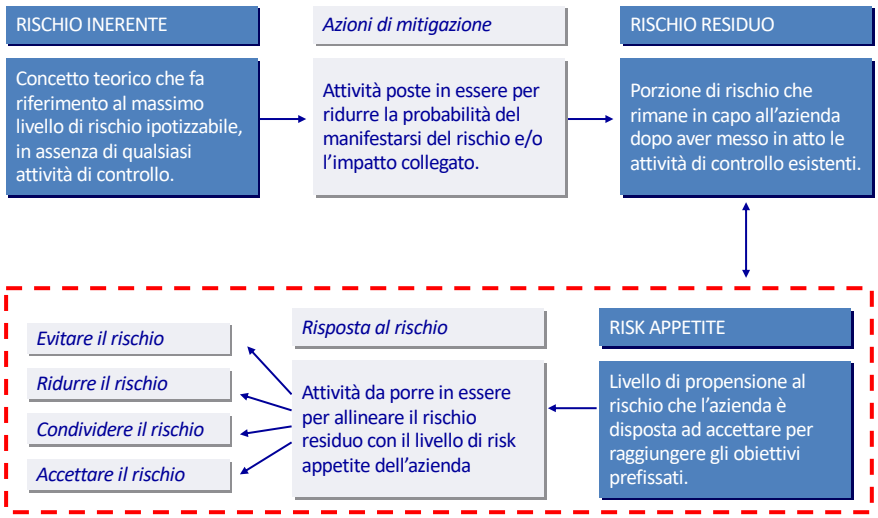


COSO ERM: Risk Assessment – Principali fasi del processo (17/17)

Per ottenere una rappresentazione sintetica a livello di Società/Gruppo, è necessario procedere ad un consolidamento dei rischi valutati nell'ambito delle singole Divisioni attraverso i seguenti passaggi:

- Aggregazione dei rischi "ricorrenti": i rischi identificati su più Divisioni e relativi ad eventi rischiosi di natura analoga vengono aggregati secondo criteri di raggruppamento identificati per tipologia di rischio.
- Rappresentazione dei rischi a livello di Società/Gruppo effettuata sulla base di aspetti quantitativi (es. EBITDA, PFN, CCN, ecc.) e dal confronto della materialità per singola Divisione (es. evoluzione del modello di business in cui opera la Società/Gruppo, discontinuità tecnologiche in atto, discontinuità legislative e regolamentari, indicatori specifici di Divisione, ecc.).

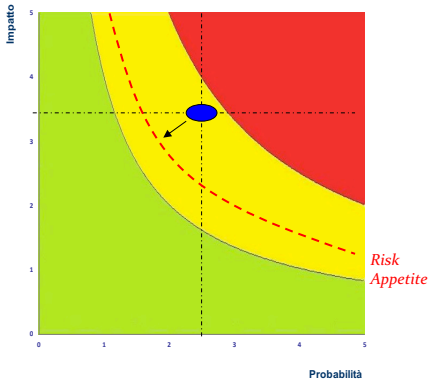
Risk response / Monitoring (1/3)



Risk response / Monitoring (2/3)

Il management, dopo aver valutato i rischi, determina come allinearli con il livello di *Risk Appetite* desiderato. Le risposte al rischio rientrano nelle seguenti categorie:

- *Evitare il rischio:* nasce dal fatto che non si è riusciti a trovare un'opzione valida che riduca l'impatto e la probabilità del rischio ad un livello accettabile;
- *Ridurre il rischio:* sono intraprese azioni per ridurre la probabilità o l'impatto del rischio, oppure entrambi, a un livello che è in linea con la tolleranza al rischio desiderata;
- *Condividere il rischio:* è ridotta la probabilità e l'impatto del rischio trasferendo oppure compartecipando una parte del rischio (e.g. acquisto di una polizza assicurativa, operazioni di copertura contro i rischi di oscillazione dei prezzi o delle valute, attività di esternalizzazione o outsourcing);
- *Accettare il rischio:* non sono intraprese azioni per incidere sulla probabilità e sull'impatto del rischio, in quanto il rischio è già posizionato nell'area di tolleranza.



27

27

	EU	G8	USA	RUS	UK	NL	FR	GER	SWE	JP	AUS	CAN	TRK	IN	CH
ICT and MEDIA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WATER, DAMS, SURFACE WATER MNGT	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓		✓
ENERGY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NUCLEAR (radiological hazard), HAZARDOUS MATERIALS	✓		✓			✓	✓	✓		✓		✓			
FOOD	✓		✓		✓	✓					✓	✓			✓
AGRICULTURE			✓	✓							✓	✓			
HEALTH, MEDICAL SERVICES	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓
FINANCE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
TRANSPORT, POSTAL, PIPELINES and LOGISTIC	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
CHEMICHAL INDUSTRY and BIOTECH	✓		✓			✓	✓					✓	✓		✓
SPACE	✓													✓	
MONUMENTS ICONS			✓								✓	✓			✓
GOVERNMENT ADM		✓	✓	✓	✓	✓		✓		✓		✓			✓
DEFENSE INDUSTRY BASE, DEFENSE			✓	✓							✓	✓	✓	✓	✓
COMMERCIAL FACILITIES			✓												
EMERGENCY SERVICES		✓	✓		✓						✓	✓			✓
CRITICAL MANUFACTURING			✓										✓		
VERY LARGE INFORMATION SYS				✓											
UTILITY INCLUDING WARMING SYSTEMS				✓											
INDUSTRY				✓											
MUNICIPAL SERVICES				✓					✓						
CIVIL DEFENSE				✓											✓
LEGAL ORDER, PUBLIC SAFETY						✓	✓							✓	
PROTECTION & SAFETY									✓			✓			✓
SERVICES, OTHER								✓							
RETAIL, PROVISIONS									✓						

28

CARVER(S) 2/2

CRITICALITY A seconda del contesto di riferimento, indica la stima dell'impatto (umano o economico) derivante da un potenziale attacco.

ACCESSIBILITY Possibilità, da parte dell'attaccante, di accedere fisicamente all'obiettivo.

RECUPERABILITY Possibilità, da parte del sistema attaccato, di recuperare le funzioni iniziali.

VULNERABILITY Indica il grado di vulnerabilità dell'obiettivo.

EFFECT È l'impatto quantificabile (di tipo economico, reputazionale, etc.) di un attacco.

RECOGNIZABILITY È il grado di facilità con cui l'attaccante può identificare il proprio bersaglio.

SHOCK Originariamente connesso agli impatti ambientali o sull'agricoltura, può indicare gli aspetti simbolici e psicologici di un attacco.

29

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CARVER(S) 1/2

La matrice **CARVER(S)** è stata sviluppata dalle Forze Speciali USA durante la guerra del Vietnam.

In ambito **Risk/Vulnerability assessment** viene utilizzata per definire il livello di vulnerabilità del target e orientare in modo efficiente le proprie risorse in relazione al tipo di target.

La CARVER(S) può essere applicata sia in prospettiva di attacco che di difesa.

C	CRITICALITY
A	ACCESSIBILITY
R	RECUPERABILITY
V	VULNERABILITY
E	EFFECT
R	RECOGNIZABILITY
S	SHOCK

30

MSHARPP 1/2

Lo schema **MSHARPP** è un'altra matrice che è possibile utilizzare per valutare le vulnerabilità intrinseche e il livello di esposizione di un asset (materiale, immateriale, umano); sia in una prospettiva di attacco che di difesa.

Nell'utilizzare lo schema MASHARPP si opera una valutazione su elementi come il grado di «attrattività» di un potenziale target, i mezzi a disposizione per accedervi, la natura dell'impatto, il possibile coinvolgimento di altri asset, etc.

- **M** MISSION
- **S** SYMBOLISM
- **H** HISTORY
- **A** ACCESSIBILITY
- **R** RECOGNIZABILITY
- **P** POPULATION
- **P** PROXIMITY

31

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

MSHARPP 2/2

MISSION ➡ Indica la capacità (es. da parte di un'azienda) di continuare a erogare servizi in maniera ottimale verso la popolazione, istituzioni pubbliche, etc.

SYMBOLISM ➡ Attiene agli aspetti simbolici/iconici dell'obiettivo di un potenziale attacco.

HISTORY ➡ Dalla valutazione dello "storico" degli attacchi avvenuti in precedenza è possibile stimare il grado di sensibilità dell'obiettivo.

ACCESSIBILITY ➡ Possibilità, da parte dell'attaccante, di accedere fisicamente all'obiettivo.

RECOGNIZABILITY ➡ Grado di facilità con cui l'attaccante può identificare il proprio bersaglio.

POPULATION ➡ Quantità di popolazione colpita attraverso l'attacco condotto sull'obiettivo.

PROXIMITY ➡ La prossimità geografica del potenziale target ad altri edifici di importanza strategica o ad aree densamente abitate.

32

Threat modelling (Electronic Frontier Foundation - https://ssd.eff.org)

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

33

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Targeting e reverse targeting

- Condurre un'attività di targeting significa compiere una scelta ben precisa sugli **obiettivi da attaccare** per ragioni di efficienza (costi-benefici)
- Entrambe sono accomunate dagli elementi che intendono studiare: **attori**, **obiettivi**, **indicatori di impatto**
- Il **targeting** individua gli indicatori per attaccare un certo obiettivo, il **reverse targeting** cerca di individuare «post mortem» cosa sia accaduto, come e perché

34

CARVER(S) E MSHARPP

- *Tools* di derivazione militare
- Esprimono, in ambito RA/VA, un giudizio circa l'**attrattività** e la **vulnerabilità** dei target al fine di allocare le risorse in maniera efficiente relativamente al bersaglio da attaccare
- Valutazione dell'impatto
- Strumenti di *targeting* e di supporto alle decisioni
- Attaccanti vs difensori? Obiettivi e punti di debolezza/zone di attacco
- Target vs asset

35

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CRITICALITY, la criticità

- Identificare gli asset critici e i singoli punti di fallimento
- Rappresenta il valore del target o la rilevanza di un sistema, ovvero il grado di «danno» sul target
- Alcune variabili:
  a) tempo dell'impatto
  b) quantità di danno
  c) backup dei servizi
  d) numero di target
  e) le posizioni dei target

Criteri della criticità	Scala
Perdita di oltre 10 mila vite; immediato arresto delle attività; il target non funziona più	9-10
Perdita tra le 1000 e le 10 mila vite; arresto delle attività entro un giorno; 66% di riduzione delle attività	7-8
Perdita tra le 100 e le 1000 vite umane; arresto entro 1 settimana; 33% di riduzione delle attività	5-6
Perdita di vite minore di 100; arresto entro 10 giorni; 10% di riduzione delle attività	3-4
Nessuna perdita di vita; non ci sono significativi effetti sulle attività	1-2

36

ACCESSIBILITY, l'accessibilità

- Grado di facilità di accesso agli asset o di raggiungimento degli obiettivi
- Sia fisicamente, sia con armi a distanza;
- Dipende:
  a) dalla possibilità di accesso/uscita e di

Criteri dell'accessibilità	Scala
Accesso facile (limitate barriere umane, accesso illimitato, fonti di informazioni disponibili)	9-10
Accessibile (limitate barriere umane, accesso per un'ora, fonti di informazioni limitate)	7-8
Parzialmente accessibile (sotto costante osservazione umana, presenti barriere fisiche, fonti di informazioni non specifiche)	5-6
Difficilmente accessibile (osservazione umana stabile, accesso controllato, limitate fonti di informazioni	3-4
Non accessibile (barriere fisiche e umane efficienti, accesso ben controllato non ci sono informazioni sul target)	1-2

37

RECUPERABILITY, la resilienza

- Indica il tempo necessario per riparare o ripristinare l'asset dal danno
- Nel valutare la resilienza, ogni target fornisce anche una stima delle motivazioni dell'attaccante (chi lo può attaccare?)
- Il concetto fa riferimento al danno materiale e non alle persone

Criteri della resilienza	Scala
Più di un anno	9-10
6-12 mesi	7-8
3-6 mesi	5-6
1-3 mesi	3-4
Meno di un mese	1-2

38

VULNERABILITY, la vulnerabilità

- Chi attacca: capacità, risorse e intenzioni dell'avversario
- Chi si difende: contromisure
- Dipende:

a) dalla natura e dalla costituzione del target;
b) dalla quantità di danno;
c) dalle risorse disponibili;
d) dalla personalità, esperienza e atteggiamento mentale dell'avversario

Criteri della vulnerabilità	Scala
Facile introduzione di sufficienti agenti di minaccia	9-10
Introduzione di sufficienti agenti di minaccia	7-8
Introduzione di agenti probabile per il 30-60%	5-6
Introduzione di agenti probabile per il 10-30%	3-4
Introduzione di agenti probabile per meno del 10%	1-2

39

EFFECT, l'effetto

- Si definisce come «lo scopo e la magnitudo delle conseguenze avverse a seguito di un attacco»
- Rappresenta l'impatto quantificabile di un attacco
- È inversamente proporzionale al numero delle strutture che producono lo stesso risultato
- Tra le variabili:

a) la reale attivazione delle contromisure
b) la disoccupazione
c) i danni collaterali

Criteri dell'effetto	Scala
Più del 50% del sistema è stato colpito	9-10
Il sistema è stato colpito per un 25-50%	7-8
Il sistema è stato colpito per un 10-25%	5-6
Il sistema è stato colpito per un 1-10%	3-4
Il sistema è stato colpito per meno dell'1%	1-2

40

RECOGNIZABILITY: il riconoscimento

- Rappresenta il grado con cui un target può essere riconosciuto in maniera inequivocabile
- Si compie una valutazione retrospettiva nei panni dell'avversario
- Fattori:
  a) dimensione e complessità

Criteri del riconoscimento	Scala
Il target è chiaramente riconoscibile	9-10
Il target è facilmente riconoscibile	7-8
Il target è difficile da riconoscere e può essere confuso	5-6
Il target è difficile da riconoscere ed è facilmente confuso con altri target	3-4
Il target non può essere riconosciuto se non da esperti	1-2

41

SHOCK, il «turbamento»

- Impone di valutare tutte le conseguenza di un attacco
- Combina la salute, gli aspetti psicologici e gli impatti economici nazionali collaterali (*downgrade strutturale*): va considerato a livello nazionale/sistemico
- Non solo il numero di vittime ma anche se il target ha un significato storico, culturale, religioso, simbolico o se le vittime appartengono ad alcune categorie di soggetti (bambini, anziani)
- Quattro variabili:
  a) distruzione di target simbolici
  b) gran numero di vittime
  c) natura di per sé sensibile dei target
  d) capacità di colpire al cuore valori ed emozioni

Criteri dello shock	Scala
Estrema rilevanza simbolica e impatto economico	9-10
Grande rilevanza simbolica e impatto economico	7-8
Moderata rilevanza simbolica e impatto economico	5-6
Limitata rilevanza simbolica e impatto economico	3-4
Non ha una rilevanza storica né un impatto economico	1-2

42

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CARVER(S)

Criticality: valore del target, la sua distruzione ha un impatto significativo

Accessibility: grado di facilità di accesso agli asset

Vulnerability: stima della vulnerabilità (capacità, intenzioni e risorse vs contromisure)

Recognizability: Identificazione / riconoscimento del target

Shock: salute, aspetti psicologici, impatti economici nazionali collaterali; particolare significato storico, culturale, religios

Effect: è la misura del danno subito dal target in termini di sistema produttivo

Recuperability: grado di resilienza e di ritorno alle condizioni «normali»

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

MISSION, la missione

- Prende in considerazione la collocazione, le attività, le capacità e le risorse del target
- Tre elementi:
  a) la rilevanza (valore dell'area e degli asset)
  b) l'effetto (aspetti psicologici, economici, sociologici e gli impatti

Criteri della missione	Scala
Il target non può continuare a svolgere la sua missione	5
La missione del target è compromessa dall'attacco	4
Metà della missione del target rimane attiva	3
Il target potrebbe continuare a svolgere la sua missione anche se con un certo grado di inefficacia	2
La distruzione della missione dell'asset non ha effetti sul compimento della missione	1

SYMBOLISM, il simbolismo

- Considerare se il target rappresenta (o è percepito come) un simbolo di una certa realtà (Stato, apparato militare, aziende private)
- Può acquisire un

Criteri del simbolismo	Scala
La posizione del target è un simbolo ben preciso delle intenzioni dell'avversario	5
Il target ha un significato storico, religioso o simbolico da difendere	4
Il target è considerato dal difensore come un punto forte invulnerabile	3
Il target è associato alla capacità produttiva o economica del difensore	2
Il target è considerato dal difensore come una popolare area di raccolta	1

45

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

HISTORICAL, la storicità

- Esperienze pregresse, attacchi simili nella storia
- Focalizzare l'attenzione non solo sulla storia degli attacchi simili ma anche sui resoconti

Criteri della storicità	Scala
Attacchi contro questi target sono condotti in maniera routinaria e con minacce note	5
Attacchi contro questi target in maniera routinaria e con minacce per lo più dirette	4
Attacchi contro questi target sono capitati	3
Questi target sono stati minacciati da tali attacchi	2
Attacchi contro questi target corrispondono a come noi ci immaginiamo il potenziale funzionamento delle minacce	1

46

ACCESSIBILITY, l'accessibilità

- Grado di facilità di accesso agli asset/raggiungimento degli obiettivi
- Si identificano e si studiano anche i percorsi critici per raggiungere il target
- L'attaccante non

Criteri dell'accessibilità	Scala
Facilmente accessibile, le difese possono essere sviluppate	5
Il target è dentro un perimetro ma all'aperto	4
Il target è dentro una costruzione ma al piano terra	3
Il target è dentro una costruzione ma al secondo piano	2
Il target non è accessibile o è accessibile solo con estrema difficoltà	1

47

RECOGNIZABILITY, il riconoscimento

- Grado con cui il target può essere riconosciuto visivamente o se sono disponibili informazioni sul target
- Le condizioni meteorologiche (neve, nebbia, pioggia) assumono un ruolo rilevante così come la strada per raggiungere il

Criteri del riconoscimento	Scala
Il target è chiaramente riconoscibile	5
Il target è facilmente riconoscibile	4
Il target è difficile da riconoscere di notte o col cattivo tempo o può essere confuso con altri target	3
Il target è difficile da riconoscere di notte o col cattivo tempo e può essere facilmente confuso con altri target	2
Il target non può essere riconosciuto sotto nessuna condizione	1

48

PROXIMITY, la prossimità

- Inquadra la localizzazione del target. Il target è prossimo ad altro personale/cittadinanza, strutture, risorse? C'è il rischio di un danno collaterale ad altri target vicini?
- Nelle vicinanze ci

Criteri della prossimità	Scala
Il target è in prossimità di altri target; ingenti rischi, vittime, distruzione totale di strutture e personale	5
Il target è in prossimità di altri target; ingenti rischi, vittime, distruzione parziale di strutture e personale	4
Il target è appena in prossimità	3
Il target è parzialmente isolato	2
Il target è isolato; non ci sono rischi per altro personale, strutture o eventuali riferimenti simbolici	1

49

POPULATION, la popolazione

- *Quantità* di popolazione
- La «*demografia*» della popolazione: chi possono essere i target? Fanno parte di un particolare

Criteri del riconoscimento	Scala
L'attacco causa più di 1000 vittime, un impatto significativo a livello internazionale e per le infrastrutture	5
L'attacco causa più di 500 vittime, un impatto significativo a livello internazionale e per le infrastrutture	4
L'attacco causa più di 100 vittime, un impatto apprezzabile a livello internazionale e per le infrastrutture	3
L'attacco causa più di 10 vittime e un basso impatto a livello internazionale e per le infrastrutture	2
Non ci sono persone presenti e non sono registrati danni per le infrastrutture critiche	1

50

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

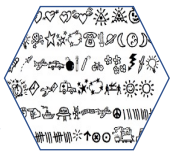
MSHARPP

Mission: Attività, scopo, capacità del target; rilevanza, effetto, resilienza del

Symbolism: Valuta il livello simbolico

Accessibility: grado di facilità di accesso agli asset

Proximity: Localizzazione del target ed eventuale vicinanza ad altri asset critici



Population: Quantità e demografia della popolazione

Recognizability: Identificazione / riconoscimento del target

Historical: «storicità» degli eventi criminali legati a quel target

51

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Che fare?

	C	A	R	V	E	R	S	Tot
	M	S	H	A	R	P	P	Tot
Asset 1	4	3	4	5	5	4	4	29
Asset 2	3	3	3	1	4	5	5	24
Asset 3	5	5	5	4	3	2	1	25

1) Decidere che tutto il target abbia come valore il massimo di quelli di ciascun asset
2) Pesare attraverso un valore moltiplicatore ogni singolo indicatore a seconda dell'importanza strategica che l'analista vuole assegnare a quel determinato indicatore
3) Fare la media tra il valore totale degli indicatori della CARVER(S) per ogni asset e il numero totale degli asset
4) Per ciascun target/asset si creano delle scale di misura attraverso cui assegnare un valore numerico a una fascia di rischio (Molto alto, Alto,

52

CARVER(S) VS MSHARPP

- Decidere di mitigare il rischio:
  - riducendo la *criticità* (sistemi di backup, sistemi ridondanti);
  - riducendo l'*accessibilità* (implementazione contromisure di sicurezza fisica);
  - riducendo la *vulnerabilità* (rinforzi strutturali, trattamenti specifici);
  - riducendo l'*identificazione* (cancellare luoghi dalle mappe, lavorare sulla conformazioni del terreno, impiantare vegetazione).

- Compiere delle valutazioni analitiche su ogni singolo risultato derivante dalle

53

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CARVER(S) VS MSHARPP nell'ERM

S = O * E * G	**Criticality**	G	Mission	I
		E	Symbolism	I
	Accessibility	I/G	Historical	P
		O	Accessibility	V
R = M * V * I	**Recuperability**	G	Recognizability	I
	Vulnerability	O/E	Proximity	I
		G		

54

Threat modelling (Electronic Frontier Foundation - https://ssd.eff.org)

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

1. What do you want to protect? Lista R
2. Who do you want to protect it from? M (ma anche what)
3. How likely is it that you will need to protect it? P (M x V)
4. How bad are the consequences if you fail? I
5. How much trouble are you willing to go through in order to try to prevent those? Contromisure e R residuo

55

Dr. Ing. Luisa Franchina, PhD

l.franchina@hermesbay.com

56