# RISCHIO

"Il tutto non è uguale alla somma delle sue parti" [Aristotele]

*Autore: Aldo Pedico* – Cybersecurity & Privacy
*Contatto:* pedicoaldo@gmail.com

***Redatto il 30 luglio 2022***

## PREMESSA

*Nelle pagine successive ho voluto sintetizzare e fissare alcuni concetti e pratiche necessarie a valutare l'impatto dei rischi ICT e come i rischi TIC o ICT siano parte integrante del Rischio complessivo aziendale.*

*Fornendo un percorso che prende spunto dal ciclo di vita dell'ICTRM ho cercato di ottenere uno "strumento guida" da usare per approfondimenti sulla valutazione del rischio con alcuni esempi.*

*Come mostrato nella Figura 9, questo documento si concentra sull'integrazione del rischio TIC all'interno del contesto dei rischi ERM (rischi finanziari, reputazionali, ecc.).*

*Inoltre, ha l'ambizione di porre dei punti fermi per ottenere come risultato finale:*

1. *la garanzia che il rischio delle tecnologie ICT riceva un'attenzione adeguata all'interno dei programmi di gestione del rischio aziendale* (ENTERPRISE RISK MANAGEMENT - ERM);
2. *l'aiuto a professionisti, all'interno di un'impresa, atto a migliorare la gestione del rischio ICT* (ICT RISK MANAGEMENT - ICTRM).

*Per cercare di fare chiarezza mi sono avvalso: della mia esperienza diretta sul campo, di materiale proveniente da vari organismi internazionali e, in particolar modo, dalla recentissima pubblicazione del NIST SP 800-221A.*

## INDICE DEGLI ARGOMENTI

**Titolo _____ Pag.**

# 1 - DEFINIZIONI

## DEF. 1: RISCHIO SECONDO OMB

*Per le agenzie federali statunitensi, la circolare A-11 dell'*OFFICE OF MANAGEMENT AND BUDGET (OMB) *definisce il rischio come "**l'effetto dell'incertezza sugli obiettivi**" [OMB-A11].*

*L'effetto dell'incertezza sulla mission aziendale e sugli obiettivi di business può quindi essere considerato come un "***rischio d'impresa***" che deve essere ugualmente gestito.*

## DEF. 2: ERM SECONDO OMB

*Nel governo federale statunitense, l'ERM è considerato "**un approccio efficace a livello di agenzia per affrontare l'intero spettro dei rischi significativi dell'organizzazione comprendendo l'impatto combinato dei rischi come un portafoglio interconnesso piuttosto che affrontare i rischi solo all'interno di silos**" [OMB-A11].*

## DEF. 3: ERM SECONDO COMMITTEE OF SPONSORING ORGANIZATIONS (COSO)

*"L**a cultura, la capacità e le pratiche che le organizzazioni integrano con la definizione della strategia e applicano quando attuano tale strategia, con lo scopo di gestire il rischio creando, preservando e realizzando valore**". [COSOERM]*

## DEF. 4: PROGRAMMI DI RISCHIO [NIST]

***I singoli programmi di rischio hanno un ruolo importante e devono integrare le attività come parte di quel portafoglio aziendale.** Ciò garantisce un focus sul raggiungimento degli obiettivi aziendali e aiuta a identificare quei rischi che avranno l'impatto più significativo sulla missione dell'entità.*

## DEF. 5: INTERCONNESSIONE TRA DISCIPLINE DEL RISCHIO ICT E LE PRATICHE D'IMPRESA [NIST]

*Come con altri sistemi complessi di sistemi, **l'interconnessione di queste tecnologie produce comportamenti del sistema che non possono essere determinati dal comportamento***

***dei singoli componenti. Tale interconnessione provoca rischi all'interno dei programmi di rischio e tra diversi programmi di rischio.***

## DEF. 6: RISCHIO D'IMPRESA [OMB]

*L'OMB afferma che "**il profilo [Rischio di impresa] deve identificare le fonti di incertezza, sia positive (opportunità) che negative (minacce).**" [OMB-A123]*

## DEF. 7: ORGANIZZAZIONE

*L'Organizzazione **è un'entità di qualsiasi dimensione, complessità o posizione all'interno di una struttura organizzativa più ampia.***

## DEF. 8: IMPRESA

*L'Impresa è un'Organizzazione al vertice livello della gerarchia.*

## DEF. 9: REGISTRO DEI RISCHI SECONDO OMB

*La circolare A-11 dell'OMB descrive un registro dei rischi come "**un archivio di informazioni sui rischi, inclusi i dati compresi sui rischi nel tempo**".*

*Afferma inoltre: "**In genere, un registro dei rischi contiene una descrizione del rischio, l'impatto se il rischio dovrebbe verificarsi, la probabilità che si verifichi, le strategie di mitigazione, i proprietari del rischio e una classifica per identificare i rischi con priorità più elevata**". [OMB-A11]*

## DEF. 10: RISK GOVERNANCE

*È il processo mediante il quale la valutazione, le decisioni e le azioni della gestione del rischio sono collegate alla strategia e agli obiettivi dell'impresa.*
*Fornisce la trasparenza e la responsabilità che consentono ai responsabili di gestire il rischio in modo accettabile.*

## DEF. 11: PROPENSIONE (APPETITE) AL RISCHIO

*OMB ha adattato questo linguaggio per l'uso da parte del governo nella Circolare A-123 affermando in modo simile che la propensione al rischio "**è la quantità di rischio su base ampia che un'organizzazione è disposta ad accettare nel perseguire la sua missione/visione**" [OMB-A123].*

## DEF. 12: TOLLERANZA AL RISCHIO

*Nella circolare A-123, OMB ha nuovamente adattato il linguaggio COSO [COSOERM] affermando che la tolleranza al rischio "**è il livello accettabile di varianza nelle prestazioni rispetto al raggiungimento degli obiettivi**".*

## DEF. 13: BIAS

*I bias, o meglio bias cognitivi, sono delle distorsioni che le persone attuano nelle valutazioni di fatti e avvenimenti. Tali distorsioni ci spingono a ricreare una propria visione soggettiva che non corrisponde fedelmente alla realtà. In sintesi, i bias cognitivi rappresentano il modo con cui il nostro cervello **distorce di fatto la realtà**.*

## DEF. 14: CAPACITÀ DI RISCHIO (RISK CAPACITY)

***"È la quantità massima di rischio che un'organizzazione è in grado di sopportare**".*

## DEF. 15: RISCHIO INTRINSECO (INHERENT RISK)

"***È il rischio per un'entità in assenza di azioni dirette o mirate da parte del management per alterarne la gravità***". *[COSOERM]*

## DEF. 16: RISCHIO RESIDUO TARGET (TARGET RESIDUAL RISK)

"***È la quantità di rischio che un'entità preferisce assumersi nel perseguimento della propria strategia e obiettivi aziendali, sapendo che il management attuerà o ha attuato azioni dirette o mirate per alterare la gravità del rischio***". *[COSOERM]*

## DEF. 17: RISCHIO RESIDUO EFFETTIVO (ACTUAL RESIDUAL RISK)

"***È ciò che rimane dopo che la direzione ha preso provvedimenti per modificarne la gravità. Esso dovrebbe essere uguale o inferiore al rischio residuo target***". *[COSOERM]*

## 2 - INTRODUZIONE

*La crescita dei sistemi informatici genera complessità, presentando vulnerabilità sfruttabili, rischi emergenti e instabilità del sistema che, una volta attivati, possono avere effetti dannosi.*

*Le attuali imprese per tutta una serie di circostanze possono trasformare un rischio relativamente minore in veri rischi operativi che interrompono la capacità di un'organizzazione di svolgere la missione o le funzioni aziendali.*

*Considerando che le discipline relative al rischio ICT (ad es. IoT, Supply Chain, Privacy, Cybersecurity) nonché la gestione del rischio (ad es. quelli per l'IA e per i sistemi e le sistemi di informazione) supportano la gestione di un mosaico di rischi interconnessi.*

*L'ampio insieme di discipline ICT forma un sistema di sistemi adattivo composto da molti componenti e canali interdipendenti (vedi definizione 4).*

*L'intento di questo documento è fornire un approccio sintetico interconnesso ai quadri e ai programmi di rischio che affronta il rischio ICT come un sottoinsieme speciale del rischio d'impresa, cercando di incoraggiare l'aggregazione e la normalizzazione delle informazioni sui rischi ICT, aiutando a identificare, quantificare e comunicare gli scenari di rischio e le loro conseguenze.*

*Come risultato dell'approccio c'è un processo decisionale efficace.*

*Tale approccio integrato garantisce che il valore per azionisti e stakeholder sia quantificato in metriche finanziarie, di missione e reputazionali simili a quelle attribuite ad altri rischi aziendali (non tecnici), consentendo a dirigenti e funzionari di riallocare prudentemente le risorse tra tutti i vari tipi di rischio concorrenti.*

*Il cyber è solo una parte di un insieme ampio e complesso di incertezze che include rischi finanziari, legali, legislativi, di sicurezza fisica e strategici.*

*Nell'ambito di un programma ERM, è necessario gestire in modo olistico l'insieme combinato dei rischi.*

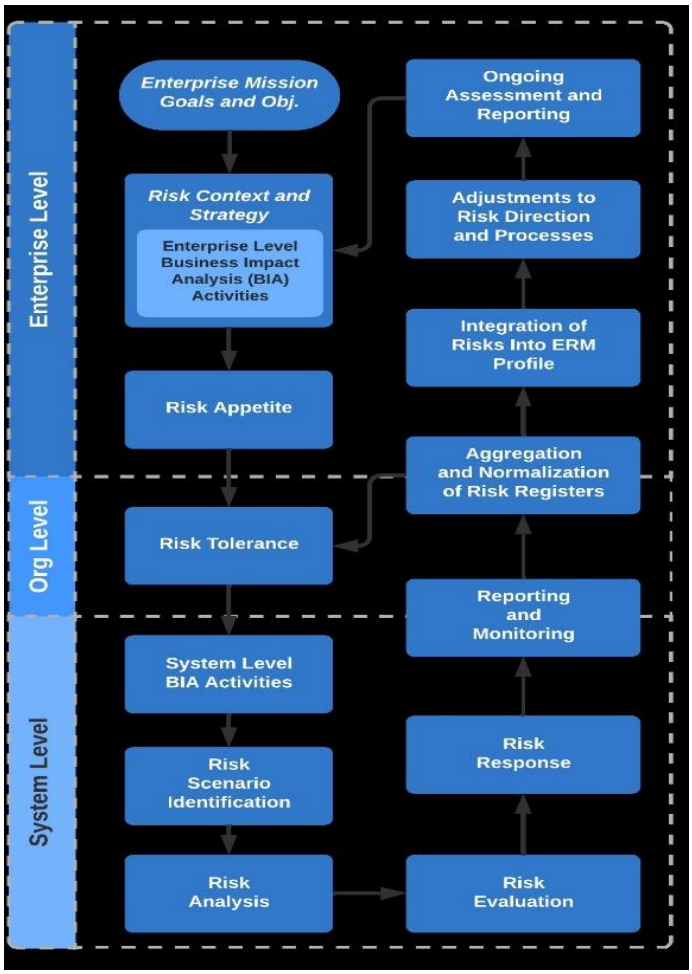
*L'ERM fornisce una copertura sotto la quale i rischi sono aggregati e classificati in base alle priorità affinché tutti i rischi possano essere valutati e sia possibile evitare la segnalazione dei rischi* "**stovepiped**".

*I responsabili aziendali dovrebbero definire i parametri di* **rischio operativo** *come parte della strategia di rischio aziendale.*

*ERM offre anche un'opportunità per l'identificazione del* **rischio operativo**, *un sottoinsieme dei rischi aziendali così significativo che potenziali perdite potrebbero mettere a repentaglio uno o più aspetti delle operazioni.*

*Questa pubblicazione esplora il processo di gestione del rischio ICT ad alto livello (*ICT RISK MANAGEMENT - ICTRM*) illustrato dalla Figura 1.*

FIGURA 1: CICLO DI INTEGRAZIONE ICTRM




*In genere includono approcci simili:*

a) *identificare il contesto,*
b) *identificare i rischi,*
c) *analizzare il rischio,*
d) *stimare l'importanza del rischio,*
e) *determinare e*
f) *eseguire la risposta al rischio e identificare e rispondere ai cambiamenti nel tempo.*

*Il processo riconosce che nessuna risposta al rischio dovrebbe verificarsi senza comprendere le aspettative degli stakeholder per la gestione del rischio a un livello accettabile, come indicato dalla propensione al rischio della leadership e dalle dichiarazioni di tolleranza al rischio.*

*Per garantire che ai responsabili aziendali possa essere fornita una comprensione delle varie minacce e conseguenze che ciascuna organizzazione e impresa debba affrontare, le informazioni sui rischi devono essere registrate e condivise attraverso i registri dei rischi. E, come stabilito nella definizione, il Rischio di impresa deve identificare le fonti di incertezza, sia positive (opportunità) che negative (minacce).*

*La strategia ERM include la definizione di terminologia, formati, criteri e altre linee guida per gli input di rischio dai livelli inferiori dell'impresa.*

*L'integrazione delle attività di gestione del rischio specifiche per la tecnologia supporta la comprensione delle esposizioni relative alla rendicontazione aziendale (ad es. conto economico, stato patrimoniale, flusso di cassa) e requisiti simili (ad es., rendicontazione per autorità di appropriazione e sorveglianza) per gli enti del settore pubblico.*

**Il processo iterativo ICTRM consente aggiustamenti alla direzione del rischio.**

*L'applicazione di un approccio coerente per* IDENTIFICARE, VALUTARE, RISPONDERE E COMUNICARE *il rischio all'interno dell'azienda in merito all'intero portafoglio di discipline di rischio ICT aiuterà a garantire che i dirigenti siano sempre informati e in grado di supportare decisioni strategiche e tattiche efficaci.*

*Il processo di gestione dei rischi a livello aziendale è noto come* ENTERPRISE RISK MANAGEMENT (ERM) *e prevede:*

1. *l'identificazione e la comprensione dei rischi principali che un'impresa deve affrontare,*
2. *la determinazione del modo migliore per affrontare tali rischi, e*
3. *la garanzia che siano intraprese le azioni necessarie.*

*Tra i numerosi tipi di rischio ci sono:*

1. *conformità,*
2. *finanziario,*
3. *informatico e tecnologico (ICT),*
4. *legale,*
5. *legislativo,*
6. *operativo,*
7. *reputazionale e*
8. *strategico.*

*Le aziende utilizzano l'ERM per gestire in modo olistico l'insieme combinato di rischi.*

## 3 - INTEGRAZIONE ICTRM CON ERM

*Di seguito una breve introduzione all'ICTRM ed esplorazione delle iniziative atte all'integrazione dell'ICTRM con i processi ERM.*

### 3.1 – COMPARAZIONE TRA ICTRM E ERM

*Distinguere ICTRM (Organization) da ERM (Enterprise) e capire come si relazionano richiede prima di tutto differenziare i termini organizzazione e impresa.*

*Ogni impresa è supportata da vari sistemi, ciascuno un insieme discreto di risorse informative organizzate espressamente per la raccolta, l'elaborazione, il mantenimento, l'uso, la condivisione, la diffusione o l'eliminazione delle informazioni.*

*La maggior parte delle responsabilità ICTRM tendono ad essere svolte dalle singole organizzazioni all'interno di un'impresa.*

*Al contrario, la responsabilità dell'ERM per il monitoraggio dei principali rischi aziendali e del loro impatto sugli obiettivi spetta all'impresa di livello più alto.*

*L'ERM richiede l'identificazione e la comprensione dei vari tipi di rischio, inclusi i rischi ICT, che un'impresa deve affrontare; determinare la probabilità che si verifichino tali rischi; e stimare il loro potenziale impatto.*

*I processi ERM forniscono ai dirigenti aziendali una visione del portafoglio dei rischi chiave all'interno dell'impresa e questo portafoglio considera i risultati di tutte le discipline ICTRM.*

## 3.2 – CICLO DI VITA DELL'ICTRM

*La tabella 1 illustra le similitudini tra diversi modelli comuni di gestione del rischio, inclusa la definizione del contesto, l'identificazione dei rischi, l'analisi dei rischi, la stima dell'importanza del rischio, la determinazione e l'esecuzione della risposta al rischio e il monitoraggio e la risposta ai cambiamenti nel tempo.*

*Le voci nella tabella 1 indicano (tra parentesi) il loro identificativo o numero di sezione dal materiale di partenza, se disponibile.*

**La tabella 1 fornisce un confronto di alto livello e non è intesa come un passaggio per le relazioni tra i modelli.**

**Rivela come l'aggregazione delle discipline di gestione del rischio nel processo ERM seguono passaggi simili per gestire il rischio.**

TABLE 1: SIMILITUDINI

<table>
<tr><th>ERM Playbook</th><th>COSO ERM Framework</th><th colspan="2">ISO 31000:2018</th><th>OMB A-123</th><th>GAO Green Book</th></tr>
<tr><td>Identify the Context</td><td>• Governance and Culture<br>• Strategy and Objective Setting</td><td colspan="2">Establish External Context (5.3.2), Establish Internal Context (5.3.3)</td><td>Establish Context</td><td>Define objectives and risk tolerances (6.01)</td></tr>
<tr><td>Identify the Risks</td><td rowspan="8">• Performance<br>• Review and Revision<br>• Information, Communication and Reporting</td><td rowspan="6">Risk Assessment</td><td>Risk Identification (5.4.2)</td><td>Identify Risks</td><td>Identification of Risks (7.02)</td></tr>
<tr><td>Analyze the Risks</td><td>Risk Analysis (5.4.3)</td><td rowspan="5">Analyze and Evaluate</td><td>Analysis of Risks (7.05)</td></tr>
<tr><td>Assess Likelihood</td><td rowspan="4">Calculate Level of Risk</td><td rowspan="4">Management estimates the significance of a risk and considers the magnitude of impact, the likelihood of occurrence, and the nature of the risk</td></tr>
<tr><td>Assess Impact</td></tr>
<tr><td>Prioritize Risks</td></tr>
<tr><td>Calculate Exposure</td></tr>
<tr><td rowspan="2">Plan and Execute Response Strategies</td><td>Risk Evaluation (5.4.4)</td><td>Develop Alternatives</td><td rowspan="2">Response to Risks (7.08)</td></tr>
<tr><td colspan="2">Risk Treatment (5.5)</td><td>Respond to Risks</td></tr>
<tr><td>Monitor, Evaluate, and Adjust</td><td>Performance Review and Revision Information, Communication and Reporting</td><td colspan="2">Monitoring and Review (5.6)</td><td>Monitor and Review</td><td>Identification of Change (9.02)<br>Analysis of and Response to Change (9.04)</td></tr>
</table>

*Le* **Sei** *passi indicativi del ciclo di vita* DELL'INFORMATION COMMUNICATION TECHNOLOGY RISK MANAGEMENT (ICTRM) *sono:*

- STEP 1 - IDENTIFICARE IL CONTESTO *(cap. Identificazione del Contesto)*

  *Il contesto è l'ambiente esterno e interno in cui l'impresa opera ed è influenzato dai rischi coinvolti. Questo passaggio include la determinazione e la documentazione della missione aziendale, inclusi obiettivi e obiettivi, e la strategia di gestione del rischio aziendale.*
  *Inoltre, include anche i leader aziendali che comunicano le aspettative di gestione del rischio alle organizzazioni che li compongono.*

- STEP 2 - IDENTIFICARE I RISCHI *(cap. Identificazione del Rischio)*

  *Ciò significa identificare l'insieme completo di rischi positivi e negativi e determinare quali eventi potrebbero aumentare o ostacolare gli obiettivi, compreso il rischio di non riuscire a perseguire un'opportunità.*

- STEP 3 - ANALIZZARE I RISCHI *(cap. Analisi del Rischio)*

  *Ciò comporta la stima della probabilità che si verifichi ogni evento di rischio identificato e il potenziale impatto delle conseguenze descritte.*

- STEP 4. STABILIRE LA PRIORITÀ DEI RISCHI *(cap. Stabilire la Priorità dei Rischi)*

  *L'esposizione è calcolata per ciascun rischio in base alla probabilità e al potenziale impatto, quindi i rischi sono classificati in base alla loro esposizione.*

- STEP 5 - PIANIFICARE ED ESEGUIRE STRATEGIE DI RISPOSTA AL RISCHIO *(cap. Pianificare e Eseguire le Strategie di Risposta al Rischio)*

  *La risposta appropriata è determinata per ciascun rischio e informata dalla guida al rischio fornita dalla leadership.*

- STEP 6 - MONITORARE, VALUTARE E ADEGUARE LA GESTIONE DEL RISCHIO *(cap. Monitorare, Valutare e Regolare la Gestione del Rischio)*

  *Il monitoraggio continuo garantisce che le condizioni di rischio aziendale rimangano entro i livelli di propensione al rischio definiti al variare dei rischi.*

**Poiché possono essere utili costrutti di raccolta di informazioni, le organizzazioni che non hanno ancora familiarità o che non utilizzano i registri dei rischi sono caldamente esortate ad adottarli e integrarli in qualunque metodologia di gestione del rischio stiano attualmente utilizzando.**

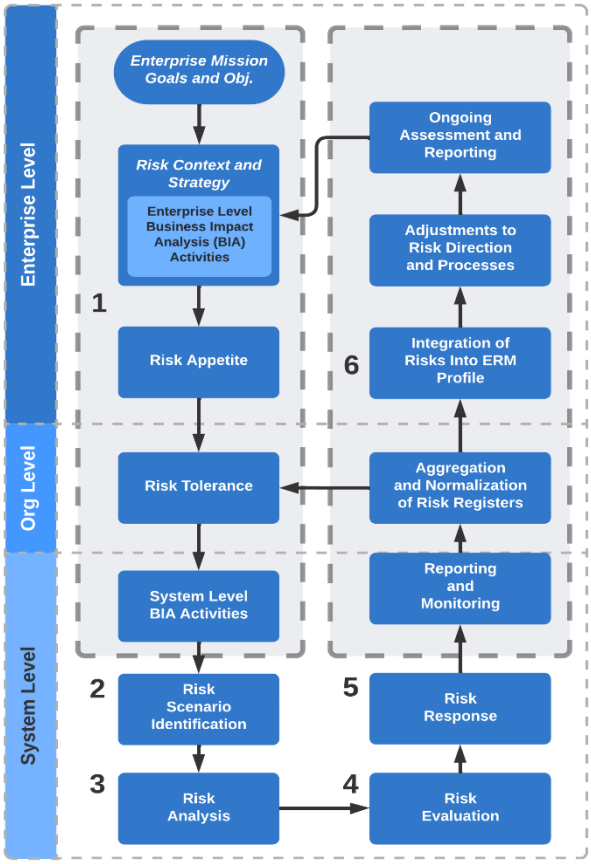
FIGURE 3: NOTIONAL LIFE CYCLE FOR INTEGRATED ICTRM/ERM

*I registri dei rischi rappresentano un principio organizzativo per comunicare i rischi ICT al processo ERM della circolare OMB A-123 per le organizzazioni che hanno già familiarità con questo costrutto di gestione.*

*La documentazione e il monitoraggio dei rischi ICT nei registri dei rischi fornisce un metodo di organizzazione comune e favorisce la comunicazione dalle discipline del rischio ICT ai decisori senior.*

*La figura 3 illustra un ciclo di vita ICTRM fittizio con i numeri per indicare dove si verifica ogni passaggio e*

*La sezione 3 fornisce maggiori dettagli su ogni passaggio e tutti gli elementi all'interno della figura 3.*




## 3.3 – INTEGRAZIONE ICTRM E ERM

*ERM e ICTRM hanno diversi punti di integrazione.*

*In primo luogo, le attività di* **governance aziendale per l'ERM indirizzano la strategia ei metodi da utilizzare per l'ICTRM** *e altre discipline di gestione del rischio.*

*Sulla base di questa guida, ogni disciplina all'interno di ogni organizzazione utilizza i registri dei rischi per documentare i propri rischi – nel caso dell'ICTRM, i rischi derivati dalle valutazioni a livello di sistema.*

*Successivamente, questi registri di rischio vengono aggregati e normalizzati, quindi utilizzati per creare registri di rischio a livello aziendale per ciascuna disciplina.*

*Questi, a loro volta, diventano parte di un più ampio registro dei rischi d'impresa* (ENTERPRISE RISK REGISTER - ERR) *che abbraccia tutte le discipline.*

*La Figura 4 dimostra che ERM e ICTRM non sono processi separati; l'ICTRM rappresenta un importante sottoinsieme del più ampio portafoglio di ERM.*

*La documentazione e il monitoraggio dei rischi ICT nei registri dei rischi di livello inferiore supporta una migliore gestione dei rischi ICT a livello aziendale.*

*L'ERR è prioritario da coloro che hanno responsabilità fiduciarie e di supervisione, creando un profilo di rischio aziendale* (ENTERPRISE RISK PROFILE - ERP), *noto anche come profilo di rischio ERM.*

*Un ERP viene creato considerando i rischi aziendali in relazione al raggiungimento degli obiettivi come tipicamente delineato in un piano strategico organizzativo.*

*La circolare OMB A-123 [OMB-A123] richiede che gli ERP includano quattro tipi di obiettivi: strategici, operativi (efficacia ed efficienza operativa), rendicontazione (affidabilità della rendicontazione) e conformità (conformità alle leggi e ai regolamenti applicabili).*

*Sebbene possano esserci alcune sovrapposizioni tra le categorie di obiettivi, la comprensione dell'incertezza in quanto influisce su questi obiettivi aiuterà a informare il processo decisionale efficace e tempestivo.*

*ERM efficace bilancia il raggiungimento degli obiettivi con l'ottimizzazione delle risorse.*

*La sezione 3 discute l'integrazione di ICTRM ed ERM in modo molto più dettagliato.*

## 4 – APPROCCIO ALLA VALUTAZIONE DEL RISCHIO

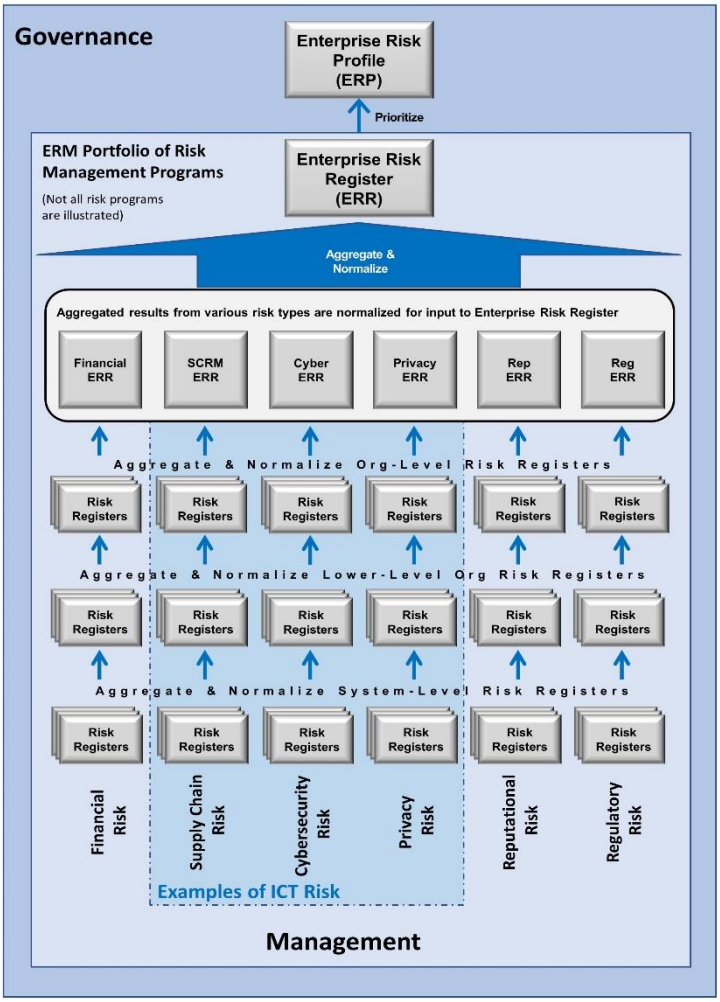
### CREAZIONE DEI REGISTRI DI RISCHIO ERR E ERP

*Le informazioni integrate sulla gestione del rischio provenienti da tutta l'azienda aiutano a creare un registro dei rischi aziendali (ERR) composito e un profilo di rischio aziendale (ERP) con priorità per informare i dirigenti dell'azienda e i funzionari dell'agenzia sulle deliberazioni, sulle decisioni e sulle azioni dell'ERM.*

*Descrive l'inclusione dei rischi ICT (compresi vari rischi legati a tecnologia operativa, catena di approvvigionamento, privacy e sicurezza informatica) come parte dell'esposizione finanziaria, di valutazione, di missione e di reputazione.*

*Un ERR completo e un ERP supportano i requisiti di comunicazione e divulgazione.*

FIGURE 4: ICTRM *COME PARTE DI* ERM




*Di seguito sono descritti alcuni fattori comuni che contribuiscono a tali carenze.*

### 4.1 - AUMENTARE COMPLESSITÀ DEL SISTEMA E ECOSISTEMA

*Molti sistemi oggi sono complessi e adattivi (***sistemi di sistemi***) composti da migliaia di componenti interdipendenti e una miriade di canali.*

*I sistemi operano in un ambiente socio-politico-tecnologico in rapida evoluzione che presenta minacce da parte di individui e gruppi con alleanze, atteggiamenti e programmi mutevoli.*

*La costante introduzione di nuove tecnologie ha cambiato e complicato il cyberspazio.*

*Connessioni wireless, big data, cloud computing e IoT presentano nuove complessità e vulnerabilità concomitanti.*

**L'informazione e la tecnologia non sono più come semplici sistemi di archiviazione automatizzati.**

*Piuttosto, sono come il sistema nervoso centrale:* **una parte delicatamente equilibrata e intricata di un'organizzazione o impresa che coordina e controlla le risorse più fondamentali della maggior parte delle organizzazioni.**

*La crescente complessità di questo ecosistema dà origine a rischi sistemici e vulnerabilità sfruttabili che, una volta attivate, possono avere un effetto travolgente con molteplici gravi conseguenze per le imprese.*

*La gestione del rischio ICT per questi ecosistemi è incredibilmente impegnativa a causa della loro complessità dinamica.*

**Questa complessità aumenta il rischio per sistemi specifici e tale rischio può creare rischi aggiuntivi a livello di sistema, organizzazione e impresa.**

*Devono inoltre essere individuate, tracciate e gestite le condizioni di rischio emergenti create dall'interdipendenza dei sistemi e del rischio di controparte.*

## 4.2 – ECCESSO DI CONCENTRAZIONE SUL LIVELLO DI SISTEMA

*La gestione del rischio ICT è condotta con modalità diverse a vari livelli, anche a livello di sistema, organizzazione e impresa.*

*Una pratica comune prevede che i singoli team a livello di sistema siano responsabili del monitoraggio dei rischi rilevanti.*

**Sebbene possa verificarsi un reporting di sistema a livello organizzativo, in genere non esiste alcun meccanismo in atto per consolidare i dati sui rischi per i sistemi a livello di organizzazione, tanto meno a livello aziendale.**

*Quando i responsabili dell'organizzazione o dell'impresa ricevono dati sui rischi del sistema, spesso si tratta di una mappa dei rischi vaga o di un volume tale da risultare poco pratico.*

*Pertanto, non sorprende che i livelli più alti di un'organizzazione o di un'impresa tendano a lottare con la comprensione del rischio ICT.*

*Questa lotta può essere meno pronunciata nelle organizzazioni con un'architettura aziendale che mappa i sistemi sui processi aziendali che supportano.*

*Molti rischi aziendali sono interdipendenti. Un esempio comune del settore è che mentre la sicurezza informatica, la privacy e i rischi di credito sono elementi diversi del portafoglio ERM, è del tutto possibile che una violazione della sicurezza informatica delle informazioni di identificazione personale possa comportare un declassamento del credito o una perdita di fiducia del pubblico.*

### 4.3 – DIVARIO TRA L'OUTPUT ICTRM E L'INPUT ERM

**Un'impresa che cerca di evitare tutti i rischi ICT potrebbe soffocare l'innovazione o l'efficienza al punto da produrre poco valore.**

**All'altra estremità dello spettro, un'impresa che applica la tecnologia indipendentemente dal rischio effettivo aumenta le possibilità che possa essere vittima di conseguenze indesiderabili.**

**È più probabile che, bilanciare efficacemente i vantaggi della tecnologia con i potenziali rischi e le conseguenze di un evento di minaccia, si traduca in un ICTRM efficace che supporti un approccio ERM completo.**

*Ai fini dell'ERM, dovrebbe esserci un processo per l'integrazione dei registri dei rischi delle varie discipline ICTRM. Ciò consente un facile scambio di conoscenze sui rischi tra i partecipanti ICTRM e ERM.*

*Molte organizzazioni non conducono queste attività in modi coerenti e ripetibili.*

*La quantificazione e l'aggregazione dei rischi ICT sono spesso effettuate in modo ad hoc e non sono eseguite con il rigore utilizzato per altri tipi di rischio.*

*Ciò riduce la qualità delle informazioni sul rischio ICT fornite a ERM.*

## 5 – CONSIDERAZIONI SUL RISCHIO ICT

*Di seguito le considerazioni sul rischio ICT, con il contenuto strutturato secondo le sei fasi del ciclo di vita nozionale ICTRM descritto nella Figura 3:*

1. IDENTIFICAZIONE DEL CONTESTO (CAP. 5.1)
2. IDENTIFY THE RISKS (CAP. 5.2)
3. ANALYZE (QUANTIFY) THE RISKS (CAP. 5.3)
4. PRIORITIZE THE RISKS (CAP. 5.4)
5. PLAN AND EXECUTE RISK RESPONSE STRATEGIES (CAP. 5.5)
6. MONITOR, EVALUATE, AND ADJUST RISK MANAGEMENT (CAP. 5.6)

*In seguito, la Sezione 5.7 discute brevemente le considerazioni sui rischi positivi.*

### 5.1 – IDENTIFICAZIONE DEL CONTESTO

*Nel ciclo di vita della gestione del rischio, il primo passo nella gestione dei rischi ICT è la comprensione del contesto:* **l'ambiente in cui l'organizzazione opera ed è influenzata dai rischi coinvolti**.

*Il contesto del fornisce le aspettative e le determinanti da considerare.*

*Il rischio comprende due fattori:*

- IL CONTESTO ESTERNO: *coinvolge le aspettative degli stakeholder esterni che influenzano e sono influenzati dall'organizzazione, come clienti, autorità di regolamentazione, legislatori e partner commerciali.*
  *Questi stakeholder hanno obiettivi, percezioni e aspettative su come il rischio sarà comunicato, gestito e monitorato.*
- IL CONTESTO INTERNO: *si riferisce a molti dei fattori all'interno dell'organizzazione e a considerazioni pertinenti all'interno dell'impresa. Ciò include tutti i fattori interni che influenzano la gestione del rischio, come gli obiettivi dell'organizzazione e dell'impresa, la governance, la cultura, la propensione al rischio, la tolleranza al rischio, le politiche e le pratiche.*

### 5.1.1 – AMMINISTRAZIONE DEL RISCHIO

*In quanto componente importante dell'ERM, l'ICTRM contribuisce a garantire che i rischi dell'ICT non ostacolino il raggiungimento degli obiettivi della missione aziendale stabiliti.*

*ICTRM aiuta anche a garantire che l'esposizione al rischio ICT rimanga entro i limiti assegnati dalla leadership aziendale.*

**Il metodo per collegare le operazioni e le comunicazioni aziendali alla strategia è la GOVERNANCE.**

**La GOVERNANCE rappresenta i metodi per valutare le opzioni strategiche e dirigere le attività per raggiungere tale strategia.**

*Le entità più grandi potrebbero implementare meccanismi di governance del rischio in tutta l'impresa con meccanismi di governance più specifici all'interno dell'organizzazione (ad esempio, divisione, portafoglio o ufficio) e applicare tale strategia a sistemi o programmi.*

*La tabella 2 illustra alcuni ruoli e responsabilità nozionali a ciascun livello.*

TABLE 2: ESEMPI DI RUOLI E RESPONSABILITÀ DEL CONTROLLO RISCHI

| Risk Functions | Notional Private-Sector Roles | Notional Federal Government Roles | Notional Responsibilities |
|---|---|---|---|
| *Enterprise-Level Oversight* | *Board of Directors, Regulators, Chief Executive Officer, Chief Operating Officer* | *OMB, U.S. Congressional Oversight Committees, Head of Agency* | *Ensures alignment with strategic priorities; monitors and corrects misalignments; holds management accountable for performance; receives periodic progress reports.* |
| *Enterprise Level Risk Governance* | *Chief Risk Officer (or Enterprise Risk Officer), Vice President – Risk Management, ERM Council* | *Senior Accountable Official for Risk Management, Chief Risk Officer, Senior Agency Information Security Officer, Senior Agency Official for Privacy, Risk Executive* | *Provides oversight, direction, and priorities for the ERM function.*<br>*Identifies those risks that may require external reporting or disclosure to the public, stakeholders, or regulators.* |

| | | | |
|---|---|---|---|
| | | *(Function) (e.g., ERM Council)* | |
| *Enterprise Level Risk Management* | *Chief Operating Officer, Chief Financial Officer or Controller, Chief Risk Officer* | *Chief Operating Officer, Chief Financial Officer, Chief Risk Officer, Enterprise Risk Management Officer* | *Leads and implements the ERM program.*<br>*Ensures frequent visibility for high-priority risks that affect the enterprise (e.g., reports quarterly to senior executives on top risks and the status of integrating risk management principles in various functions/lines of business). Aggregates and normalizes risks for comparison at the enterprise level in consultation with risk owners.*<br>*Determines enterprise risk threshold (risk appetite and tolerance) for high-priority risks in consultation with business leads and ensures that it is communicated and known by the appropriate staff.* |
| *Organization-Level Risk Governance (Subsidiary, Bureau, Operative, or Division)* | *Division President, Director of Security, Chief Information Officer, Chief Information Security Officer, Division/Unit Risk Officer* | *Division/Unit Risk Officer, Senior Agency/Chief Information Security Officer, Chief Information Officer, Chief Data Officer, Senior Agency Official for Privacy, Risk Executive (Function)* | *Establishes and communicates risk management policies, priorities, and expectations across and through the organization in specific risk domains.*<br>*Partners with enterprise-level risk functions to ensure continued visibility of organization-level risk.*<br>*Ensures sub-organization staff are aware of policies, procedures, and risk parameters (e.g., risk appetite and tolerance) to effectively balance risk with mission performance.* |
| *System-Level Risk Management* | *Business System Owner, Risk Owner, Information Owner, Information System Security Manager* | *Authorizing Official, System Owner, Risk Owner, Information Owner, Information System Security Manager, Information System Security Officer* | *Coordinates with organization-level risk managers (e.g., the CISO) to document and track identified risks and provide input on alignment with established risk parameters.*<br>*Ensures that risks are being monitored, that the status is periodically reported to the CISO, and that risk response decisions are communicated back to the risk owner.* |

*I singoli programmi di rischio, tra cui sicurezza informatica, privacy e gestione del rischio della catena di approvvigionamento informatica (C-SCRM), potrebbero quindi tradurre ulteriormente la direzione del rischio aziendale (ad esempio, dichiarazioni di propensione al rischio) in una direzione del rischio specifica del programma, consentendo processi di rischio olistici supportando al contempo l'autorità decisionale dei proprietari di sistemi.*

*La divisione delle responsabilità è tipica nelle organizzazioni più grandi in cui un funzionario è specificamente incaricato di essere responsabile della governance del programma (ad es.* CHIEF INFORMATION SECURITY OFFICER, CHIEF PRIVACY OFFICER*).*

### 5.1.2 – PROPENSIONE E TOLLERANZA AL RISCHIO

*Questo documento si basa sui principi ERM per quanto riguarda l'integrazione con la cultura, la strategia e le prestazioni.*

> *Uno di questi principi è che* "**un'organizzazione deve gestire il rischio rispetto alla strategia e agli obiettivi di business in relazione alla sua propensione al rischio, ovvero i tipi e l'entità del rischio, a livello generale, che è disposta ad accettare nella sua ricerca del valore**". *[COSOERM]*

*La propensione al rischio è definita dalla leadership di alto livello dell'impresa come parte della governance del rischio, e funge da guida per i tipi e la quantità di rischio, a livello generale, che i dirigenti senior sono disposti ad accettare nel perseguimento degli obiettivi della missione e del valore aziendale.*

*La* PROPENSIONE *al rischio può essere* **qualitativa** *o* **quantitativa**.

**Un altro importante concetto di ERM è la TOLLERANZA al rischio: la prontezza dell'organizzazione o delle parti interessate a sopportare il rischio residuo dopo aver risposto o considerato il rischio al fine di raggiungere i propri obiettivi (pur riconoscendo che tale tolleranza può essere influenzata da requisiti legali o normativi).**

*La tolleranza al rischio può essere definita è* **generalmente stabilita a livello di programma, obiettivo o componente** *(livello organizzativo).*

Mentre la propensione al rischio è definita a livello di impresa e la tolleranza al rischio a livello di impresa o organizzazione, la propensione al rischio è interpretata a livello di organizzazione e di sistema per sviluppare una specifica tolleranza al rischio ICT.

La tolleranza al rischio rappresenta il livello specifico di rischio di performance ritenuto accettabile all'interno della propensione al rischio *definita dalla dirigenza (pur riconoscendo che tale tolleranza può essere influenzata da requisiti legali o regolamentari).*

*La* **tolleranza** *al rischio è interpretata e applicata dai "custodi" della disciplina di gestione del rischio (ad esempio, sicurezza informatica, finanziaria, legale, privacy) a livello di organizzazione o di sistema.*

La propensione al rischio e la tolleranza al rischio sono correlate ma distinte in maniera analoga alla relazione tra attività di governance e gestione.

**Le dichiarazioni di propensione al rischio definiscono la guida generale al rischio e le dichiarazioni di tolleranza al rischio definiscono l'applicazione specifica di tale direzione.**

*Ciò significa che le dichiarazioni di tolleranza al rischio sono sempre più specifiche delle corrispondenti dichiarazioni di propensione al rischio.*

**Insieme, le dichiarazioni di PROPENSIONE al rischio e di TOLLERANZA al rischio rappresentano LIMITI DI RISCHIO, aiutano a comunicare le aspettative di rischio e migliorano il focus degli sforzi di gestione del rischio.**

## LIMITI DI RISCHIO = PROPENSIONE + TOLLERANZA

*La definizione di questi parametri di rischio pone l'impresa in una posizione migliore per identificare, assegnare priorità, trattare e monitorare i rischi che possono portare a perdite inaccettabili.*

*La tolleranza al rischio dovrebbe sempre rimanere entro i limiti stabiliti dalla dirigenza, entro i parametri e informati dai requisiti legali e normativi.*

Un esempio di una dichiarazione di **PROPENSIONE** al rischio è: "Il servizio di posta elettronica deve essere disponibile per la maggior parte di un periodo di 24 ore".

Una dichiarazione di **TOLLERANZA** al rischio associata a questo appetito sarebbe più ristretta: "I servizi di posta elettronica NON devono essere interrotti per più di cinque minuti durante le ore principali".

*La tabella 3 fornisce ulteriori esempi di tolleranza al rischio perseguibile e misurabile, illustrando l'applicazione della propensione al rischio a contesti specifici all'interno della struttura a livello di organizzazione.*

TABLE 3: EXAMPLES OF RISK APPETITE AND RISK TOLERANCE

| ***Example Enterprise Type*** | ***Example Risk Appetite Statement*** | ***Example Risk Tolerance Statement*** |
|---|---|---|
| *Global Retail Firm* | *Our customers associate reliability with our company's performance, so service disruptions must be minimized for any customer-facing websites.* | *Regional managers may permit website outages lasting up to four hours for no more than five percent of its customers.* |
| *Government Agency* | *Mission-critical systems must be protected from known ICT vulnerabilities.* | *Critical software vulnerabilities (severity score of 10) must be patched on systems designated as mission-critical within 14 days of discovery.* |
| *Internet Service Provider* | *The company has a low risk appetite with regard to failure to meet customer service level agreements, including network availability and communication speeds.* | *Patches must be applied to avoid attack-related outages but must also be well-tested and deployed in a manner that does not reduce availability below agreed-upon service levels.* |
| *Academic Institution* | *The institution understands that mobile computers are a necessary part of the daily life of students, and some loss is expected. The leadership, however, has no appetite for the loss of any sensitive data (as defined by the Data Classification Policy).* | *Because the cost of loss prevention for students' laptops is likely to exceed the cost of the devices, it is acceptable for up to 10 percent to be misplaced or stolen if and only if sensitive institution information is prohibited from being stored on students' devices.* |
| *Healthcare Provider* | *The Board of Directors has decided that the enterprise has a low risk appetite for any exposures caused by inadequate access control or authentication processes.* | *There will always be some devices that do not yet support advanced authentication, but 100 percent of critical healthcare business applications must use multi-factor authentication.* |

### 5.1.3 – STRATEGIA DI GESTIONE DEL RISCHIO

*Nell'ambito delle loro responsabilità di governance, i dirigenti aziendali dovrebbero stabilire linee guida chiare e attuabili per la gestione del rischio basate sulla missione aziendale e sugli obiettivi aziendali per le organizzazioni di loro competenza.*

*Ciò dovrebbe includere una strategia aziendale riguardante la priorità della missione, la propensione al rischio e la tolleranza (tipicamente sotto forma di propensione al rischio e dichiarazioni di tolleranza al rischio) e budget operativi e di capitale per gestire i rischi a un livello accettabile.*

*Le organizzazioni quindi gestiscono e monitorano i processi che bilanciano correttamente i rischi e l'allocazione delle risorse con il valore creato dall'ICT.*

*Le misurazioni (ad es. da indicatori chiave di rischio o* KEY RISK INDICATOR *- KRI) dimostrano dove sono state superate le tolleranze al rischio o convalidano che l'impresa sta operando nell'ambito della propensione definita.*

*Con l'evolversi del panorama dei rischi (ad esempio, a causa di cambiamenti tecnologici o ambientali), i responsabili aziendali dovrebbero rivedere e adattare continuamente la strategia di rischio. Ad esempio, è probabile che un'impresa soggetta a regolamentazione esterna riceva indicazioni specifiche*

*in merito a statuti e direttive nazionali aggiornati che devono essere presi in considerazione nella valutazione del rischio accettabile.*

*Presupposti diversi possono verificarsi a tutti i livelli dell'organizzazione, quindi è importante determinare le aspettative degli stakeholder interni ed esterni in merito alla comunicazione del rischio e utilizzare termini e categorie facilmente comprensibili e concordati, come obiettivi strategici, priorità organizzative, processo decisionale processi e metodologie di rendicontazione o monitoraggio dei rischi (ad es. discussioni e riunioni periodiche del comitato di gestione dei rischi).*

*La strategia deve anche includere linee guida relative ai meccanismi e alla frequenza della segnalazione del rischio.*

**La strategia di gestione del rischio è simile per le imprese sia pubbliche sia private.**

*Sia per gli enti del settore privato sia per quello pubblico, i responsabili emettono linee guida per continuare, accelerare, ridurre, ritardare o annullare iniziative aziendali significative.*

## 5.2 – IDENTIFICAZIONE DEL RISCHIO

*Il secondo passo del ciclo di vita della gestione dei rischi prevede l'identificazione di un insieme completo di rischi e la loro registrazione nel registro dei rischi.*

*Ciò comporta l'identificazione di quegli eventi che potrebbero aumentare o ostacolare gli obiettivi, compresi i rischi connessi al mancato perseguimento delle opportunità.*

*L'identificazione del rischio ICT è composta da quattro input:*

1. IDENTIFICAZIONE DELLE RISORSE *a supporto della missione dell'organizzazione e loro valutazione,*
2. DETERMINAZIONE DI POTENZIALI MINACCE *che potrebbero mettere a repentaglio la sicurezza o le prestazioni di tali risorse e potenziali opportunità ICT che potrebbero avvantaggiare l'organizzazione,*
3. CONSIDERAZIONE DELLE VULNERABILITÀ *di tali beni, e*
4. VALUTAZIONE DELLE POTENZIALI CONSEGUENZE *degli scenari di rischio.*

*Gli specialisti spesso eseguono l'identificazione del rischio sia come esercizi top-down sia bottom-up.*

*Ad esempio, dopo che l'organizzazione ha considerato le funzioni critiche o mission-essenziali, può considerare vari tipi di problemi che potrebbero mettere a repentaglio tali funzioni come input per lo sviluppo di scenari di rischio.*

*Successivamente, quando si verifica una valutazione dettagliata delle minacce e delle vulnerabilità, i valutatori valutano come tali minacce potrebbero influenzare varie risorse conducendo una valutazione dal basso verso l'alto.*

*Questo approccio bidirezionale aiuta a supportare l'identificazione del rischio olistica e completa.*

### 5.2.1 – INVENTARIO E VALUTAZIONE DELLE RISORSE HW E SW

*Poiché il rischio ICT riflette, almeno in parte, l'effetto dell'incertezza sulle componenti digitali che supportano gli obiettivi aziendali, i professionisti identificano le risorse necessarie per raggiungere tali obiettivi.*

*Il valore di un bene si estende oltre il suo costo di sostituzione.*

*Ad esempio, un'organizzazione potrebbe calcolare il costo diretto di ricerca e sviluppo per l'offerta di un nuovo prodotto, ma le perdite a lungo termine associate al furto di tale proprietà intellettuale potrebbero influire sulle entrate future, sui prezzi delle azioni, sulla reputazione dell'impresa e sul vantaggio competitivo.*

*Un concetto fondamentale in ERM è dare priorità alle risorse che hanno maggiore capacità di raggiungere la propria missione (nel caso di enti pubblici, l'impatto che colpisce il pubblico).*

*I gestori del rischio dovrebbero sfruttare un modello di analisi dell'impatto aziendale (*BUSINESS IMPACT ASSESSMENT - BIA*) che può essere utilizzato per valutare, registrare e monitorare in modo coerente la criticità e la sensibilità delle risorse aziendali.*

*L'importanza relativa di ciascuna attività dell'impresa è un input necessario per considerare la parte dell'impatto dell'analisi del rischio.*

*Il personale può includere la forza lavoro interna, fornitori di servizi esterni e partner di terze parti.*

### 5.2.2 - DETERMINAZIONE DELLE POTENZIALI THREATS

**Il rischio ICT non è intrinsecamente buono o cattivo. Piuttosto, rappresenta gli effetti di circostanze incerte, quindi i gestori del rischio dovrebbero considerare un'ampia gamma di potenziali rischi positivi e negativi.**

**Una minaccia rappresenta qualsiasi circostanza o evento che potrebbe avere un impatto negativo sulle operazioni organizzative (un rischio negativo).**

*La minaccia potrebbe derivare da un malintenzionato o da una situazione non intenzionale o inevitabile (ad esempio, un disastro naturale, un guasto tecnico o errori umani) che potrebbe attivare una vulnerabilità.*

Sono disponibili numerose TECNICHE DI MODELLAZIONE DELLE MINACCE per l'analisi di minacce specifiche.

*Può essere utile considerare sia* **un approccio** DALL'ALTO VERSO IL BASSO (TOP-DOWN **- vale a dire, rivedere le risorse critiche o sensibili per ciò che potrebbe potenzialmente andare storto, indipendentemente dalla fonte della minaccia) sia un approccio** DAL BASSO VERSO L'ALTO (BOTTOM-UP **- vale a dire, considerando il potenziale impatto di un determinato insieme di scenari di minaccia o vulnerabilità).**

*Un metodo comunemente utilizzato che può aiutare le organizzazioni a identificare potenziali esiti di rischio è un'analisi SWOT* (STRENGTHS, WEAKNESSES, OPPORTUNITIES, THREATS *- punti di forza, punti deboli, opportunità, minacce).*

*L'applicazione dell'analisi SWOT aiuta gli utenti a identificare le opportunità che derivano dai punti di forza dell'organizzazione (ad esempio, un team di sviluppo software rispettato) e dalle minacce (ad esempio, problemi della catena di approvvigionamento) che riflettono una debolezza organizzativa.*

L'uso dell'analisi SWOT aiuta a descrivere e considerare il contesto, inclusi i FATTORI INTERNI (punti di forza e di debolezza interni all'organizzazione), i FATTORI ESTERNI (le opportunità e le minacce presentate dall'ambiente esterno) e i modi in cui questi fattori si relazionano l'uno all'altro.

*Sebbene sia fondamentale che le imprese affrontino i potenziali impatti negativi sulla missione e sugli obiettivi aziendali, è altrettanto fondamentale (e necessario per le agenzie federali) che le imprese pianifichino il successo.*

*L'OMB afferma nella Circolare A-123 che "***il profilo deve identificare le fonti di incertezza, sia positive (opportunità) che negative (minacce)***."*

Tuttavia, la nozione di "pianificazione per il successo" identificando e realizzando rischi positivi (opportunità) è un concetto relativamente nuovo nell'ICTRM che sta influenzando altre discipline di gestione del rischio.

*Per il momento, va notato che sia i rischi positivi sia quelli negativi seguono gli stessi processi, dall'identificazione all'analisi fino all'inclusione nell'ERP.*

Qualunque sia il mezzo utilizzato per determinare le potenziali minacce, è importante considerarle sia in termini di attori della minaccia (ossia, le fonti dei rischi con la capacità di provocare un impatto dannoso) sia in termini di eventi di minaccia causati dalle loro azioni.

Dovrebbero essere considerate anche le combinazioni di rischi multipli.
Ad esempio, se un rischio nel registro si riferisce a un'interruzione del sito Web e un altro rischio si riferisce a un'interruzione dell'help desk del cliente, potrebbe essere necessario un terzo rischio nel registro che consideri la probabilità e l'impatto di un'interruzione che interessa entrambi i servizi subito.

**È anche importante identificare i rischi a cascata in cui un evento di rischio primario può innescare un evento secondario e persino terziario.**

*Durante il processo di modellazione delle minacce, è importante che il professionista prenda in considerazione e mitighi i casi di* BIAS *cognitivo.*

*Alcuni problemi comuni di* BIAS *includono:*

- ECCESSO DI FIDUCIA (OVERCONFIDENCE): *la tendenza delle parti interessate ad essere eccessivamente ottimiste sugli scenari di rischio (ad esempio, probabilità irragionevolmente bassa di un evento di minaccia, vantaggi sopravvalutati di un'opportunità, stima esagerata della capacità di gestire una minaccia).*
- PENSIERO DI GRUPPO (GROUP THINK): *prendere decisioni in gruppo sulle potenziali fonti di minaccia e sugli eventi di minaccia in modo da scoraggiare la creatività o la responsabilità individuale.*
- SEGUIRE LE TENDENZE (FOLLOWING TRENDS): *seguire ciecamente l'ultimo clamore o mania senza un'analisi dettagliata delle minacce specifiche che l'organizzazione deve affrontare.*
- BIAS DI DISPONIBILITÀ (AVAILABILITY BIAS): *la tendenza a concentrarsi su questioni (come le minacce) che vengono subito in mente perché se ne è sentito parlare o si è letto, magari in modi che non sono rappresentativi della reale probabilità che un evento di minaccia si verifichi e abbia un impatto negativo.*

### 5.2.3 - DETERMINAZIONE DELLE CONDIZIONI SFRUTTABILI E SENSIBILI

**Il prossimo input chiave per l'identificazione del rischio è la comprensione delle potenziali condizioni che consentono il verificarsi di un evento di minaccia.**

*È importante considerare tutti i tipi di vulnerabilità in tutte le risorse, comprese le persone, le strutture e le informazioni.*

*Ai fini del presente documento,* **la vulnerabilità è semplicemente una condizione che consente il verificarsi di un evento di minaccia**.

*Potrebbe essere un difetto del software senza patch, una limitazione della materia prima, un processo che porta a un errore umano o una condizione ambientale fisica (come una struttura in legno che è infiammabile).*

**La presenza di una vulnerabilità non provoca danni in sé e per sé, poiché per sfruttarla deve essere presente una minaccia. Inoltre, una minaccia che non presenta una vulnerabilità corrispondente potrebbe non comportare un rischio negativo.**

*L'identificazione dei rischi negativi include la comprensione delle potenziali minacce e vulnerabilità delle risorse organizzative, che possono quindi essere utilizzate per sviluppare scenari che descrivono i potenziali rischi.*

### 5.2.4 - VALUTAZIONE DELLE POTENZIALI CONSEGUENZE

*Molte organizzazioni esprimono in modo errato i rischi al di fuori del loro contesto.*

*Ad esempio, uno stakeholder potrebbe dire: "*Sono preoccupato per le inondazioni*" o "*Sono preoccupato per un attacco denial-of-service*".*

*Questi esempi non possono essere analizzati o considerati senza conoscere il quadro completo.*

*Un esempio efficace di un rischio identificato potrebbe essere (come espresso nella terminologia di* **causa ed effetto***): "Se un uragano provoca un'ondata di tempesta, potrebbe inondare il data center e danneggiare più file server critici".*

**Molti elementi di un piano di gestione del rischio sono implementati per supportare la ridondanza e la resilienza in modo che un evento di minaccia altamente probabile possa comportare conseguenze gestibili.**

### 5.2.5 – USO DEL REGISTRO DEI RISCHI

*I registri dei rischi sono utilizzati all'interno delle organizzazioni per comunicare e tenere traccia dei rischi ICT nel tempo.*

*Gli scenari di rischio forniscono un mezzo per presentare informazioni dettagliate sul rischio nel contesto.*

**Uno scenario di rischio completo descrive la fonte di incertezza, le condizioni predisponenti, le risorse interessate e il risultato previsto.**
**Per i rischi ICT, uno scenario potrebbe includere una fonte di minaccia, un evento di minaccia, una vulnerabilità che la fonte di minaccia potrebbe sfruttare, risorse aziendali interessate dalla minaccia e il conseguente impatto dannoso.**

*Ad esempio,* "L'attività di costruzione interrompe un cavo in fibra ottica critico che non era protetto nella canalina conduit, interrompendo le comunicazioni con il data center e provocando la perdita di disponibilità dei sistemi finanziari aziendali".

*Gli scenari possono anche aiutare a descrivere il* **rischio positivo (cioè l'opportunità)**.

*Un esempio potrebbe essere:* "La costruzione di un nuovo data center alternativo migliora la resilienza dell'infrastruttura finanziaria e riduce la probabilità di un'interruzione".

*La figura 5 mostra un modello di registro del rischio nozionale.*

*Le organizzazioni dovranno determinare quali valutazioni dovrebbero riflettersi nel registro dei rischi.*

**Alcune organizzazioni potrebbero voler includere sia l'attuale valutazione del rischio (prima dell'applicazione della risposta al rischio) sia le modifiche previste al rischio che dovrebbero risultare in base alla risposta al rischio.**

FIGURE 5: NOTIONAL RISK REGISTER TEMPLATE

| Notional Risk Register | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ID | Priority | Risk Description | Risk Category | Current Assessment | | | Risk Response Type | Risk Response Cost | Risk Response Description | Risk Owner | Status |
| | | | | Likelihood | Impact | Exposure Rating | | | | | |
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |

*La tabella 4 descrive ciascuno degli elementi del modello di registro del rischio nozionale.*

*La composizione effettiva del registro varia tra le imprese e può contenere più o meno punti dati rispetto a quelli descritti nella tabella 4.*

*Per esempio:*

- *Se il registro deve essere aggiornato dopo la risposta al rischio, i risultati di una valutazione successiva alla risposta potrebbero riflettersi nel registro come rischio residuo.*
- *Le organizzazioni potrebbero documentare uno stato di rischio desiderato in base alla propensione/tolleranza al rischio, il rischio residuo target.*

## TABLE 4: DESCRIPTIONS OF NOTIONAL RISK REGISTER TEMPLATE ELEMENTS

| REGISTER ELEMENT | DESCRIPTION |
|---|---|
| *ID (Risk Identifier)* | *A sequential numeric identifier for referring to a risk in the risk register.* |
| *Priority* | *A relative indicator of the criticality of this risk, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low).* |
| *Risk Description* | *A brief explanation of the risk scenario (potentially) impacting the organization and enterprise. Risk descriptions are often written in a cause-and-effect format, such as "if X occurs, then Y happens."* |
| *Risk Category* | *An organizing construct that enables multiple risk register entries to be consolidated. Consistent risk categorization is helpful for comparing risk registers during the risk aggregation step of ERM.* |
| *Current Assessment – Likelihood* | *An estimation of the probability that this scenario will occur before any risk response. On the first iteration of the risk cycle, this may also be considered the* ***initial assessment.*** |
| *Current Assessment – Impact* | *Analysis of the potential benefits or consequences that might result from this scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the* ***initial assessment.*** |
| *Current Assessment – Exposure Rating* | *A calculation of the probability of risk exposure based on the likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as exposure. Other common frameworks use different terms for this combination, such as level of risk (e.g., ISO 31000). On the first iteration of the risk cycle, this may also be considered the* ***initial assessment****.* |
| *Risk Response Type* | *The risk response (sometimes referred to as the risk treatment) for handling the identified risk. Values for risk response types are listed in Table 5 of this document.* |
| *Risk Response Cost* | *The estimated cost of applying the risk response.* |

| | |
|---|---|
| *Risk Response Description* | *A brief description of the risk response. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried," or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]."* |
| *Risk Owner* | *The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The risk owner may work with a designated risk manager who is responsible for managing and monitoring the selected risk response.* |
| *Status* | *A field for tracking the current condition of the risk and any next activities.* |

*Sebbene il registro dei rischi stesso possa essere utilizzato per documentare e comunicare informazioni sui rischi e sulle risposte attuali, potrebbe essere necessario integrare il registro con un record di dettaglio del rischio* (RISK DETAIL RECORD - *RDR).*

*L'uso di RDR consente di documentare i dettagli relativi a considerazioni, ipotesi e risultati dell'attività di gestione del rischio.*

*Consente inoltre all'impresa di registrare il personale coinvolto in tali considerazioni, eventuali azioni da intraprendere e programmi.*

*I contenuti di un RDR possono includere:*

- *Informazioni relative al rischio stesso, come una descrizione dettagliata dello scenario di rischio e le minacce sottostanti, le vulnerabilità, le risorse minacciate, la categoria di rischio e i risultati della valutazione del rischio.*
- *Ruoli coinvolti nelle decisioni e nella gestione del rischio (es. proprietario del rischio, gestore del rischio, titolare dell'azione per attività specifiche, stakeholder coinvolti nelle decisioni di risposta al rischio, accordi contrattuali per la catena di fornitura/partner esterni).*
- *Considerazioni sulla pianificazione, come la data in cui il rischio è stato documentato per la prima volta, la data dell'ultima valutazione del rischio, le date di completamento delle attenuazioni e la data della successiva valutazione prevista.*
- *Decisioni di risposta al rischio e follow-up, inclusi piani dettagliati, stato e indicatori di rischio.*

*Un RDR può essere archiviato e mantenuto in una registrazione scritta, come parte di un sistema di gestione della conoscenza organizzativa o come voce di database in un software specifico per il rischio, come un'applicazione di governance, rischio e conformità* (GOVERNANCE, RISK, AND COMPLIANCE - GRC).

## 5.3 – ANALISI (QUANTIFICAZIONE) DEI RISCHI

**Il terzo passo del ciclo di vita della gestione del rischio, ciascun rischio ICT viene analizzato per stimare la probabilità che si verifichi l'evento di rischio e viene descritto il potenziale impatto delle conseguenze.**

### 5.3.1 – TIPI DI ANALISI DEL RISCHIO

*È disponibile un'ampia gamma di metodologie di analisi del rischio per aiutare a fare una stima più accurata, come gli standard della International Electrotechnical Commission (IEC) 31010:2019 [IEC31010] e gli standard Open Factor Analysis of Information Risk (FAIR) [OPENFAIR].*

*I metodi di analisi del rischio includono:*

- ANALISI QUALITATIVA, *basata sull'assegnazione di un descrittore, come basso, medio o alto. La scala può essere formata o adattata per adattarsi alle circostanze e descrizioni diverse possono essere utilizzate per rischi diversi.*

  L'analisi qualitativa è utile come valutazione iniziale o quando si devono considerare aspetti immateriali del rischio.

  *Per migliorare l'accuratezza dell'analisi qualitativa, i valori e i dati possono essere sfruttati da fonti esterne, come benchmark o standard del settore, metriche da scenari di rischio precedenti simili o risultati di ispezioni e valutazioni.*

- L'ANALISI QUANTITATIVA *coinvolge valori numerici, che sono assegnati sia all'impatto sia alla probabilità.*

  *Questi valori si basano su probabilità statistiche e una valutazione monetizzata di perdita o guadagno.*
  *La qualità dell'analisi dipende dall'accuratezza dei valori assegnati e dalla validità dei modelli statistici utilizzati.*
  *Le conseguenze possono essere espresse in termini di impatto finanziario, tecnico o umano.*

*Ciascuno di questi tipi di analisi presenta vantaggi e svantaggi, quindi il tipo eseguito dovrebbe essere coerente con il contesto associato al rischio.*

*Le pratiche ERM comuni includono tipi di analisi del rischio sia qualitativi sia quantitativi.*

### 5.3.2 - TECNICHE PER LA STIMA DELLA PROBABILITÀ E DELL'IMPATTO

*IEC 31010 [IEC31010] è uno standard internazionale che descrive e fornisce una guida su 17 tecniche di valutazione del rischio che possono essere utilizzate per analizzare i controlli, le dipendenze e le interazioni; comprendere le conseguenze e le probabilità; e misurare il rischio complessivo.*

*La probabilità e gli elementi di impatto di un rischio possono essere suddivisi in sotto fattori.*

*Ad esempio, si consideri uno scenario di rischio in cui un server aziendale critico non è più disponibile per il reparto finanziario di un'organizzazione. L'età del server, la rete su cui risiede e l'affidabilità del suo software influenzano la probabilità di un guasto.*

*L'impatto di questo scenario può essere considerato anche attraverso vari fattori.*

*Se un altro server è altamente disponibile tramite una connessione a tolleranza di errore, la perdita del server iniziale potrebbe avere poche conseguenze.*

*Anche altri fattori influiscono sull'analisi del rischio, come la tempistica.*

*Se il server finanziario supporta un'importante funzione di gestione stipendi, l'impatto di una perdita che si verifica poco prima del giorno di paga può essere significativamente maggiore che se si verificasse dopo la distribuzione delle buste paga.*

*L'impatto può variare notevolmente a seconda che il server venga utilizzato per l'archiviazione di record legacy o per l'esecuzione di operazioni urgenti di azioni.*

*Ci sono molte considerazioni che vanno a stimare le esposizioni e gli eventi che possono innescarle.*

*Gli eventi di perdita secondari dovrebbero essere acquisiti con gli eventi di perdita primaria per rappresentare l'impatto totale e il costo di uno scenario di rischio.*

*L'omissione di perdite secondarie nella valutazione di uno scenario di rischio sottostima l'impatto totale, disinformando in tal modo la selezione della risposta al rischio e la definizione delle priorità.*

*Ad esempio, l'organizzazione potrebbe considerare il rischio che un'interruzione delle telecomunicazioni comporti la perdita di disponibilità di un server Web critico, contemporaneamente potrebbero verificarsi anche eventi di perdita secondari, inclusa la perdita di clienti per frustrazione con servizi non disponibili o sanzioni derivanti dal mancato rispetto dei livelli di servizio contrattuali.*

*Un'analisi dei rischi a cascata dovrebbe includere la considerazione dei fattori che porterebbero a un rischio secondario, come l'interruzione sopra descritta.*

*Esempi di tecniche per stimare la* **PROBABILITÀ** *che si verifichi un evento di rischio includono:*

- ANALISI BAYESIANA [BAYESIAN ANALYSIS] – *Un modello che aiuta a fornire una comprensione statistica della probabilità man mano che diventano disponibili più prove o informazioni.*
- MONTE-CARLO – *Un modello di simulazione che attinge a valori campionari casuali da un dato insieme di input, esegue calcoli per determinare i risultati e ripete iterativamente il processo per costruire una distribuzione dei risultati.*
- ANALISI DELL'ALBERO DEGLI EVENTI [EVENT TREE ANALYSIS]: *una tecnica di modellazione che rappresenta un insieme di potenziali eventi che potrebbero sorgere a seguito di un evento iniziale da cui è possibile considerare graficamente le probabilità quantificabili.*

*Quando si valutano le potenziali conseguenze di eventi di rischio, dovrebbero essere presi in considerazione sia gli impatti tangibili (ad es. perdite finanziarie dirette) sia quelli meno tangibili (ad es. danni reputazionali e compromissione della missione).*

*Questi sono collegati poiché le perdite dirette influiranno sulla reputazione e gli eventi di rischio reputazionale si tradurranno quasi sempre in spese di risposta al rischio.*

*La circolare OMB A-123 afferma che* "**il rischio reputazionale danneggia la reputazione di un ente o suo componente al punto da avere un effetto dannoso in grado di incidere sulla capacità dell'ente di portare a termine gli obiettivi della missione**".

*C'è un'ampia gamma di parti interessate da considerare quando si stima il rischio reputazionale, inclusi la forza lavoro, i partner, i fornitori, le autorità di regolamentazione, i legislatori, gli elettori pubblici e i clienti/clienti.*

*La stima della probabilità e dell'impatto di un evento di rischio dovrebbe tenere conto dei controlli esistenti e pianificati.*

## 5.4 – STABILIRE LA PRIORITÀ DEI RISCHI

**Dopo aver identificato e analizzato i rischi applicabili e averli registrati nei registri dei rischi, dovrebbero essere determinate e indicate le priorità di tali rischi.**

**Ciò si ottiene determinando l'esposizione presentata da ciascun rischio (vale a dire, in base alla probabilità che si verifichi un evento di minaccia e si traduca in un impatto negativo).**

**Inoltre, poiché le organizzazioni hanno risorse limitate, è utile ordinare i rischi all'interno del registro in ordine di importanza per dare priorità alla risposta al rischio.**

*Come mostrato nel modello in Figura 5, questo risultato aiuta a completare la colonna* **PRIORITÀ**.

*Quando si compila la colonna* **PRIORITÀ** *del registro dei rischi, considerare quanto segue:*

- *Come combinare i calcoli di probabilità e di impatto per determinare l'esposizione.*
- *Come determinare e misurare i potenziali benefici del perseguimento di una particolare risposta al rischio.*
- *Quando cercare ulteriori indicazioni su come valutare i livelli di esposizione al rischio, ad esempio durante la valutazione delle esposizioni pertinenti alle dichiarazioni di tolleranza al rischio.*

*I professionisti utilizzano modelli sia qualitativi che quantitativi per calcolare e comunicare l'esposizione.*

*La figura 6 mostra l'uso di descrittori qualitativi per la probabilità e l'impatto, nonché come questi potrebbero essere utilizzati per determinare un valore di esposizione globale.*

*Le soglie per gli intervalli di esposizione possono essere stabilite e pubblicate nell'ambito del modello di governance dell'impresa e utilizzate dalle parti interessate per dare priorità a ciascun rischio nel registro.*

| Likelihood (threat occurs and results in adverse impact) | | | | | | |
|---|---|---|---|---|---|---|
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |
| | Very Low | Low | Moderate | High | Very High |
| | | | Level of Impact | | |

FIGURE 6: EXAMPLE OF A QUALITATIVE RISK MATRIX

*La figura 7 illustra un esempio* quantitativo.

*In questa illustrazione, l'azienda ha fornito indicazioni sul fatto che qualsiasi rischio superiore a 0,20 (basato sulla probabilità per l'impatto) rappresenta un rischio elevato e i rischi classificati tra 0,06 e 0,20 sono designati come moderati.*

| Likelihood | | | | | | |
|---|---|---|---|---|---|---|
| 0.90 | 0.05 | 0.09 | 0.18 | 0.36 | 0.72 |
| 0.70 | 0.04 | 0.07 | 0.14 | 0.28 | 0.56 |
| 0.50 | 0.03 | 0.05 | 0.10 | 0.20 | 0.40 |
| 0.30 | 0.02 | 0.03 | 0.06 | 0.12 | 0.24 |
| 0.10 | 0.01 | 0.01 | 0.02 | 0.04 | 0.08 |
| | 0.05 | 0.10 | 0.20 | 0.40 | 0.80 |
| | | | Level of Impact | | |

FIGURE 7: EXAMPLE OF A QUANTITATIVE RISK MATRIX

*Sebbene la definizione delle priorità sarà fortemente influenzata dalla determinazione*

*dell'esposizione al rischio, anche altri fattori come il contesto aziendale o le priorità degli stakeholder possono influenzare tali decisioni.*

## 5.5 – PIANIFICARE E ESEGUIRE LE STRATEGIE DI RISPOSTA AL RISCHIO

***Il quinto passo del ciclo di vita della gestione del rischio consiste nel determinare la risposta appropriata a ciascun rischio.***

*L'obiettivo di una gestione efficace del rischio, compresi i rischi ICT, è identificare i modi per mantenere il rischio allineato con la propensione al rischio o la tolleranza nel modo più conveniente possibile.*

*In questa fase, si determinerà se l'esposizione associata a ciascun rischio nel registro rientra nei livelli accettabili sulla base delle potenziali conseguenze.*

*Si noti che le stesse risposte al rischio possono introdurre nuovi rischi.*

*Ad esempio, l'aggiunta dell'autenticazione a più fattori a un sistema aziendale per ridurre un rischio di controllo dell'accesso può introdurre un nuovo rischio di diminuzione della produttività quando gli utenti hanno difficoltà ad autenticarsi.*

*Sebbene vi siano alcune differenze tra i termini utilizzati dai quadri di gestione del rischio, sono disponibili quattro tipi di azioni (come descritto nella tabella 5) per rispondere ai rischi TIC negativi:*

1. ACCEPT
2. TRANSFER
3. MITIGATE
4. AVOID *(evitare)*

### TABLE 5: RESPONSE TYPES FOR NEGATIVE ICT RISKS

| TYPE | DESCRIPTION |
|---|---|
| ACCEPT | *Accept ICT risk within risk tolerance levels. No additional risk response action is needed except for monitoring.* |
| TRANSFER | *For ICT risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., ICT insurance). While some of the financial consequences may be transferable, there are often consequences that cannot be transferred, like a loss of customer trust.* |
| MITIGATE | *Apply actions (e.g., risk management controls) that reduce a given risk to an acceptable level.*<br>*Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes or succeeds) or that help limit such a loss by decreasing the amount of damage and liability.* |
| AVOID | *Apply responses to ensure that the risk (specifically the threat) does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the ICT risk to an acceptable level.*<br>*The cost of the lost opportunity associated with such a decision should be considered as well.* |

*In molti casi, la mitigazione per portare l'esposizione a rischi TIC negativi entro i livelli di tolleranza al rischio viene realizzata utilizzando controlli di gestione del rischio.*

*Ad esempio, se la funzione esecutiva del rischio dichiara che l'organizzazione deve evitare rischi con valori di probabilità e impatto alto/alto per tutti i costi superiori a € 500.000, la colonna* **TIPO** *di risposta al rischio del registro dei rischi (vedere la Figura 5) può essere aggiornata con una risposta aggiornata dalla tabella 5.*

*In generale, le persone, i processi e la tecnologia si combinano per fornire controlli di gestione del rischio che possono essere applicati per raggiungere un livello di rischio accettabile.*

*Esempi di controlli includono:*

- PREVENTIVO*: riduce o elimina casi specifici di debolezza.*
- DETERRENTE*: riduce la probabilità di un evento di minaccia dissuadendo un attore della minaccia*
- INVESTIGATIVO*: fornisce un avviso di un evento di minaccia riuscito o tentato.*
- CORRETTIVO*: ridurre l'esposizione compensando l'impatto delle conseguenze dopo un evento di rischio.*
- COMPENSATIVO*: applica uno o più controlli per correggere una debolezza in un altro controllo.*

*Si consideri un'organizzazione che identifichi diversi rischi negativi ad alta esposizione, incluso il fatto che pratiche di autenticazione inadeguate (ad es. password deboli o riutilizzate) potrebbero consentire la divulgazione di informazioni finanziarie sensibili dei clienti e che i dipendenti del fornitore del software potrebbero ottenere l'accesso non autorizzato e manometterlo dati finanziari.*

*L'organizzazione può applicare diversi controlli* DISSUASIVI *(documentando gli identificatori di controllo applicati ed eventuali note applicabili nella colonna Commenti sul registro dei rischi), inclusi banner di avviso e minaccia di perseguimento penale per tutti gli attori delle minacce che tentano intenzionalmente di ottenere un accesso non autorizzato.*

*I controlli* PREVENTIVI *includono l'applicazione di solide politiche di gestione delle identità e l'utilizzo di token di autenticazione a più fattori che aiutano a ridurre le vulnerabilità di autenticazione.*

*Il fornitore del software ha installato controlli* INVESTIGATIVI *che monitorano i registri di accesso e avvisano il centro operativo di sicurezza dell'organizzazione se il personale interno si connette al database del cliente senza che sia necessario l'accesso.*

*La risposta al rischio comporterà spesso la creazione di una* **RISERVA DI RISCHIO** *per evitare o mitigare un rischio negativo identificato o per realizzare o migliorare un rischio positivo identificato.*

*Una riserva di rischio è simile ad altri tipi di riserve di gestione in quanto i finanziamenti o le ore di lavoro vengono accantonati e impiegati se viene attivato un rischio per garantire che l'opportunità venga realizzata o che la minaccia venga evitata.*

*Ad esempio, le competenze tecniche necessarie per recuperare dopo un attacco ICT potrebbero non essere disponibili con le attuali risorse di personale.*

*Una riserva di rischio può essere utilizzata anche con il tipo di risposta accetta per affrontare questo problema (ad esempio, mettendo da parte fondi durante la pianificazione del progetto per assumere una terza parte qualificata per aumentare la risposta interna agli incidenti e lo sforzo di recupero).*

## 5.6 - MONITORARE, VALUTARE E REGOLARE LA GESTIONE DEL RISCHIO

*La gestione del rischio non dovrebbe consistere semplicemente nella gestione di elenchi di rischi.*

*Affinché le attività siano significative, i gestori del rischio in tutta l'impresa devono essere informati su obiettivi, risultati, priorità e opportunità.*

*Ciclo* MONITOR EVALUATE-ADJUST (MEA) *è illustrato nella Figura 8.*

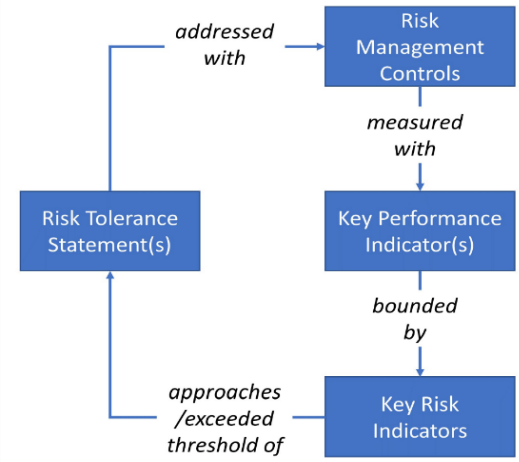
*Questo approccio iterativo inizia con la comprensione di quali limiti di rischio sono accettabili, dato il contesto aziendale e gli obiettivi strategici.*

*Lo scopo dell'integrazione ICTRM è di consentire ai dirigenti di rimanere consapevoli delle attività di gestione del rischio in corso e di applicare misure correttive al fine di raggiungere gli obiettivi strategici.*

*Quando si verificano le attività di risposta al rischio, queste vengono registrate nei registri dei rischi ICT.*

*I risultati vengono monitorati e le misurazioni delle prestazioni vengono raccolte tramite KPI e KRI e confrontate con la strategia di rischio e la direzione del rischio (basata su dichiarazioni di propensione al rischio e tolleranza al rischio).*

FIGURE 8: MONITOR-EVALUATE-ADJUST CYCLE [MEA]




*Il superamento della* **capacità di rischio** *potrebbe avere conseguenze disastrose e potrebbe persino mettere a repentaglio la continuazione dell'impresa.*

*È interessante notare che, come la* **propensione** *e la* **tolleranza** *al rischio, la* **capacità** *di rischio può estendersi a tutti i livelli aziendali gerarchici.*

*La ISO 31010:2019 descrive un esempio:* "**Per un'impresa commerciale, la capacità potrebbe essere specificata in termini di capacità di ritenzione massima coperta da attività, o la più grande perdita finanziaria che l'azienda potrebbe sopportare senza dover dichiarare fallimento**". *[IEC31010]*

### 5.6.1 - QUANDO L'EVENTO RISCHIOSO PASSA SENZA L'ATTIVAZIONE

**Le risposte al rischio saranno spesso adattate man mano che le opportunità e le minacce si evolvono.**

*Il concetto è simile all'argomento a volte chiamato "***Cono di incertezza***" all'interno delle pratiche di gestione dei progetti.*

*Per le variazioni del rischio identificato, una tecnica di mitigazione è l'utilizzo delle "***Riserve di rischio***".*

## 5.7 – CONSIDERAZIONI SUI RISCHI POSITIVI COME INGRESSO DI ERM

*Nelle discipline ICT, una parte significativa delle informazioni sui rischi viene raccolta e segnalata in relazione a punti deboli e minacce che potrebbero comportare conseguenze negative.*

*Laddove i rischi positivi devono essere considerati e inclusi nei registri dei rischi, ci sono quattro tipi di risposta generalmente utilizzati, come descritto nella Tabella 6.*

TABLE 6: RESPONSE TYPES FOR POSITIVE ICT RISKS

| TYPE | DESCRIPTION |
|---|---|
| *Realize* | *Eliminate uncertainty to make sure the opportunity is actualized (sometimes referenced as exploit).* |
| *Share* | *Allocate ownership to another party that is better able to capture the opportunity.* |
| *Enhance* | *Increase the probability and positive impact of an opportunity (e.g., hire a risk management staff member to better focus on an organization's privacy risk and data processing protections).* |
| *Accept* | *Take advantage of an opportunity if it happens to present itself (e.g., identify and prioritize those supply chain risk gaps that should be addressed at the first opportunity).* |

*Come per i rischi negativi, le voci positive nei registri dei rischi ICT dovrebbero essere normalizzate e aggregate nel registro dei rischi a livello di impresa.*

*Come mostrato nella Figura 9, questa pubblicazione si concentra sull'integrazione del rischio ICT da varie discipline a supporto di un ciclo di integrazione ERM.*

*Si riconosce la necessità di una comunicazione bidirezionale continua tra ERM e programmi di rischio, riconoscendo che le discipline di rischio informano e ricevono indicazioni da ERM.*

# 6 – COSTRUZIONE DEI REGISTRI ERR E ERP DA SPECIFICI REGISTRI ICTRM

*Il raggiungimento delle aspettative definite è veicolato attraverso registri dei rischi che documentano e comunicano le decisioni di rischio.*

*I risultati della valutazione del rischio e le azioni di risposta al rischio a livello di sistema si riflettono nei registri del rischio ICT.*

*I registri di più sistemi sono raccolti, aggregati e normalizzati, quindi forniti ai responsabili aziendali a livello di organizzazione per fornire una comprensione composita del rischio.*

*Tali responsabili possono valutare i risultati e perfezionare i criteri di tolleranza al rischio per ottimizzare l'erogazione del valore, l'utilizzo delle risorse e il rischio.*

*L'aggregazione a livello aziendale di tutti i vari registri dei rischi in un registro dei rischi aziendali (ENTERPRISE RISK REGISTER -ERR), quindi un profilo di rischio aziendale (ENTERPRISE RISK PROFILE - ERP) con priorità, consente ai responsabili di monitorare le risposte al rischio tenendo conto delle aspettative stabilite.*

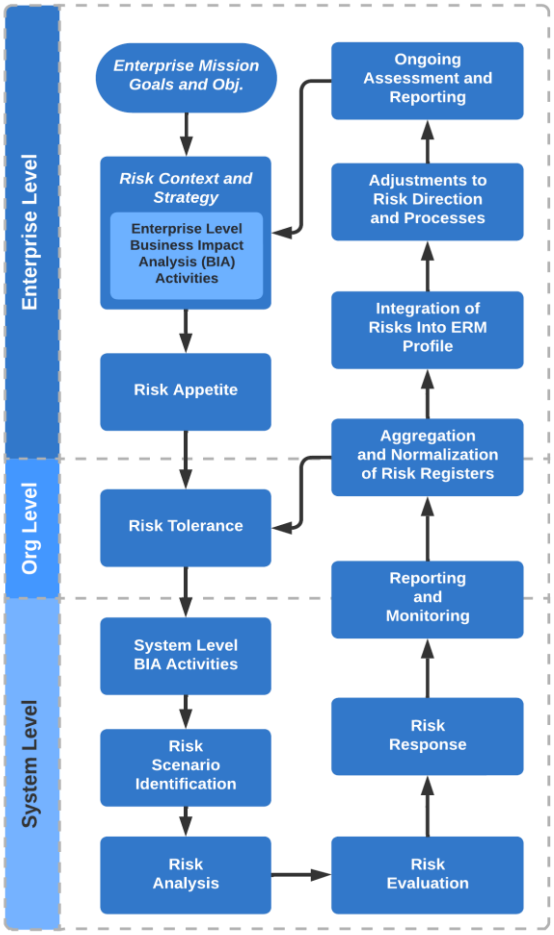



FIGURE 9: ICTRM INTEGRATION CYCLE

## 6.1 – GESTIONE DEI REGISTRI DI RISCHIO ICT A LIVELLO D'IMPRESA

*Un risultato chiave dell'identificazione del rischio e degli elementi di comunicazione è la capacità di creare registri del rischio ICT a livello aziendale come input per l'ERR più ampio.*

*L'applicazione di un registro dei rischi coerente con criteri e categorie concordati consente la normalizzazione, l'aggregazione e l'ordinamento di vari punti dati in una vista aziendale.*

*I registri dei rischi sono composti e mantenuti a tutti i livelli:*

1) *impresa (comprese le imprese di livello superiore e inferiore),*
2) *organizzazione (comprese sotto-organizzazioni e unità aziendali),*
3) *sistema.*

*Le colonne verticali nella figura 4 non dovrebbero essere interpretate come una guida per affrontare rischi come i silos isolati, ma piuttosto che le informazioni per vari tipi di rischi ICT dovrebbero essere condivise con quelle dei livelli organizzativi superiori a beneficio dell'intera impresa.*

*Allo stesso modo, l'ICTRM non dovrebbe essere isolato a un solo livello organizzativo né all'interno di una singola disciplina del rischio ICT. Invece, quelli a livello organizzativo dovrebbero collaborare e comunicare su problemi e opportunità identificati.*

*Per ciascuna disciplina di rischio, man mano che i registri dei rischi di ciascun sistema e organizzazione vengono completati, sono forniti ai responsabili del rischio designati al livello pertinente (cioè sistema o organizzazione) e condivisi con l'alta dirigenza per condurre le seguenti azioni:*

1) *normalizzare (ad esempio, garantire che le definizioni e i valori registrati dalle varie entità aziendali siano coerenti e rimuovere la segnalazione dei rischi duplicati) e*
2) *aggregare i rischi in categorie simili in una vista concisa.*

*Per supportare la successiva aggregazione dei vari registri dei rischi, le linee guida sui rischi aziendali dovrebbero identificare gli obiettivi aziendali a cui allineare i vari tipi di rischio ICT.*

*L'ERP riflette i rischi che possono avere un impatto su ciascuno dei quattro obiettivi aziendali distinti:*

1) STRATEGICO,
2) OPERATIVO,
3) REPORTING,
4) CONFORMITÀ.

*Una chiara indicazione da parte dei dirigenti su come allineare vari tipi di rischio ICT con gli obiettivi aziendali consentirà la successiva aggregazione, normalizzazione e definizione delle priorità.*

*Gli allineamenti obiettivi includono:*

- RISCHI STRATEGICI *connessi all'implementazione di una nuova offerta di servizi; opportunità di innovazione all'interno di un'area ICT; miglioramenti e sfide della gestione del cambiamento.*
- PROBLEMI OPERATIVI *riguardanti la qualità e la resilienza di prodotti o servizi (ad es. interruzione della catena di approvvigionamento che disabilita un processo di produzione); processi e procedure per la posizione di rischio per la privacy; considerazioni sulla tecnologia operativa; problemi di continuità aziendale/disaster recovery.*
- SEGNALAZIONE *in merito a questioni di rischio ICT, comprese considerazioni assicurative e fattori di rischio sostanziali che influiscono sull'informativa o sulla rendicontazione legale.*
- RISCHI DI CONFORMITÀ *in cui un evento negativo potrebbe comportare il mancato rispetto di un contratto di servizio contrattuale o una sanzione o sanzione regolamentare.*

## 6.2 - ENTERPRISE RISK REGISTER (ERR)

*I responsabili del rischio aziendale raccolgono tutti gli input di rischio, inclusi i registri dei rischi ICT, e analizzano potenziali eventi di rischio, conseguenze e impatti a livello aziendale per creare l'ERR.*

*L'ERR ha successivamente la priorità di creare il profilo di rischio aziendale (*ENTERPRISE RISK PROFILE - ERP*), che consente alle principali parti interessate esecutive di essere consapevoli dei rischi critici, compresi quelli legati alle TIC.*

*La creazione e il mantenimento dell'ERR supporta anche una revisione periodica delle linee guida sui rischi aziendali, comprese le definizioni dei rischi, il contesto e i criteri di propensione al rischio.*

*Offre l'opportunità di rivedere e convalidare le definizioni aziendali per i rischi, le categorie di rischio e le scale di valutazione del rischio.*

FIGURE 10: NOTIONAL EXAMPLE OF AN ICT-INCLUSIVE ERR

**Notional Enterprise Risk Register**

| ID | Pri. | Risk Description | Risk Category | Current Assessment | | | | | Risk Response | Risk Owner | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Financial Impact | Reputation Impact | Mission Impact | Likelihood | Exposure Rating | | | |
| 1 | 5 | Retiring staff lead to personnel shortages | Operational Risk | OpEx: M CapEx: L | Low | Mod | Mod | Mod | • Improve hiring diversity<br>• Improve employee benefits per recent survey and discussions | Dwayne Rhodes (Human Resources Department) | Open |
| 2 | 6 | A strategic opportunity to hire a famous technologist to establish a new satellite communications initiative. | Operational Risk | OpEx: M CapEx: L | High | Mod | Mod | Mod | • Allocate funds for compensation package<br>• Initiate strategic recruiting plan | Dwayne Rhodes (Human Resources Department) | Open |
| 3 | 1 | A social engineering attack on enterprise workforce leads staff to wire transfer significant funds. | Operational Risk | OpEx: M CapEx: L | High | Mod | High | High | • Update corporate IT security training<br>• Implement phishing training service<br>• Update email security products per recommendations from IT Risk Council | Carly Franklin (CISO) | Open |
| 4 | 3 | An employee of a third-party partner steals customer information. | Operational Risk | OpEx: H CapEx: M | High | High | Mod | High | • CFO and CEO to agree on plans for likely secondary financial impact from reputational risk impact.<br>• Update procurement contract requirements to include clauses per 11/3/2019 report from Legal Dept<br>• Implement 3rd Party Partner Assmt. for Tier 1 providers per CIO & CISO recommendations | Ernest Woods (Procurement) | Open |
| 5 | 7 | Sales reduction due to tariffs leads to reduced revenues. | Financial Risk | OpEx: M CapEx: L | Low | Low | Low | Low | • Increase marketing in target areas<br>• Ensure competitive pricing in target markets | Elaine Kim (VP Sales) | Open |
| 6 | 8 | Customer budget tightening results in reduced revenue and profits. | Financial Risk | OpEx: M CapEx: L | Low | Low | Mod | Mod | • Implement customer surveys to better forecast purchasing changes<br>• Use cost-cutting measures to offset reductions and maintain profitability | Elaine Kim (VP Sales) | Open |
| 7 | 9 | Failure to innovate results in market share erosion. | Strategic Risk | OpEx: M CapEx: M | Mod | Low | Mod | Low | • Approve CIO proposal to increase internal R&D funding by 10% to spur internal innovation<br>• Update technical training to include design thinking methodologies<br>• Implement customer surveys in target marketing areas | Sharika Grigsby (VP, Product Development) | Open |
| 8 | 2 | Company intellectual property data is disclosed through employee error or malicious act. | Operational Risk | OpEx: M CapEx: M | High | High | Mod | Mod | • Review and update (if needed) background screening controls<br>• Update corporate security training to reinforce the need for diligence<br>• Implement data loss prevention tools per CISO recommendation | Carly Franklin (CISO) | Closed |
| 9 | 10 | A flaw in product quality leads to reputational damage, reducing sales. | Strategic Risk | OpEx: M CapEx: M | High | High | Low | Low | • Update continuous improvement process<br>• Implement Baldrige Framework<br>• Update external provider quality standards and monitoring | Sharika Grigsby (VP, Product Development) | Open |
| 10 | 4 | Failure to implement California Consumer Privacy Act (CCPA) provisions exposes the company to fines, penalties, and legal fees. | Compliance Risk | OpEx: H CapEx: L | Mod | Mod | Mod | Mod | • Create & maintain a centralized register of compliance requirements<br>• Update employee training based on updated privacy requirements<br>• Review business impact assessment (BIA) templates to ensure ICT criteria are included. | Zoe Davidson (Chief Privacy Officer) | Open |

*Questo esempio illustra l'inclusione di un rischio positivo (elemento 2) accanto ai rischi negativi.*

*L'eccezione degna di nota è che l'esempio ERR divide il* CURRENT ASSESSMENT-IMPACT *in tre colonne, che sono descritte nella Tabella 7.*

TABLE 7: DESCRIPTIONS OF ADDITIONAL NOTIONAL ERR ELEMENTS

| ERR ELEMENT | DESCRIPTION |
|---|---|
| *Current Assessment–Financial Impact* | *Analysis of the financial potential benefits or consequences resulting from this scenario, including cost considerations. While this element could be quantitative, it is often qualitative (e.g., high, moderate, low) at the enterprise level. Financial considerations may be expressed as 1) capital expenditures that represent a longer-term business expense, such as property, facilities, or equipment, and 2) operating expenses that support day-to-day operations.* |
| *Current Assessment–Reputation Impact* | *Analysis of the potential benefits or consequences that the scenario might have on the stature, credibility, or effectiveness of the enterprise. Some enterprises perform a formal sentiment analysis using commercial services or other technical tools to support assessment.* |
| *Current Assessment–Mission Impact* | *Analysis of the potential benefits or consequences that the scenario might have on the ability of the enterprise to successfully achieve mission objectives* |

*Esiste un valore sia in un unico punto di riferimento (l'ERR) sia nelle informazioni dettagliate sul rischio (*DETAILED RISK INFORMATION - L'RDR*).*

ERR *fornisce un riepilogo facilmente consultabile per comprendere il panorama dei rischi, mentre* RDR *fornisce informazioni aggiuntive.*

RDR *consente inoltre la documentazione di informazioni aggiuntive, come informazioni storiche, dati dettagliati sull'analisi del rischio e informazioni sulla responsabilità individuale e organizzativa.*

*Ulteriori informazioni da includere in un RDR aziendale potrebbero includere:*

- *Informazioni dettagliate sui rischi (ad es., dichiarazione di rischio completa, descrizione dettagliata dello scenario, indicatori chiave di rischio, stato dell'impresa per questo particolare rischio)*
- *Informazioni relative a vari ruoli di rischio (ad es. proprietario del rischio, gestore del rischio, responsabile dell'approvazione del rischio) e stakeholder interessati*
- *Informazioni sulla sequenza temporale storica (ad es. data dell'ultimo aggiornamento, prossima revisione prevista)*
- *Informazioni sull'analisi del rischio, inclusa la comprensione aggregata di minacce, punti deboli/condizioni preesistenti, risorse interessate e impatto*
- *Informazioni dettagliate sulla risposta al rischio (ad es. risposte implementate, stato e risultati delle risposte precedenti, risposte aggiuntive pianificate)*

ERR *fornisce input per coloro che svolgono la supervisione del rischio d'impresa, come un comitato esecutivo del rischio.*

**Poiché è difficile confrontare esposizioni al rischio dissimili, come la fidelizzazione dei dipendenti e il ripristino di emergenza, i rischi si traducono spesso in impatto finanziario e possono essere ulteriormente scomposti nel costo diretto (cioè l'impatto di un determinato rischio sul budget di capitale e spese), il costo finanziario del danno reputazionale e le implicazioni finanziarie dirette dell'impatto sulla mission aziendale.**

## 6.3 - ENTERPRISE RISK PROFILE (ERP)

*Poiché le informazioni sui rischi vengono trasmesse dai livelli inferiori dell'organizzazione, il registro dei rischi di ciascun livello dovrebbe contenere le informazioni pertinenti per creare un profilo di rischio prioritario per il livello immediatamente superiore.*

*Ad esempio, un esperto in materia in una particolare disciplina del rischio ICT potrebbe fornire la propria definizione delle priorità dei rischi all'interno della propria disciplina, affinché venga presa in considerazione dal livello successivo di esperti del rischio.*

*Gli impatti delle organizzazioni subordinate possono essere diversi, simili, in conflitto, sovrapposti o non disponibili e devono essere opportunamente combinati mediante analisi finanziarie e di missione al livello immediatamente superiore all'organizzazione di rendicontazione.*

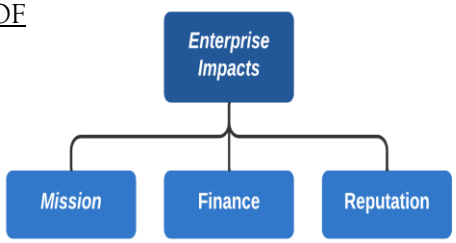
*L'ERR informa l'ERP una volta che i rischi sono prioritari al livello più alto della funzione di gestione del rischio nell'impresa, come illustrato nella Figura 11.*

*L'ERP è un sottoinsieme di rischi accuratamente selezionati dal più ampio ERR e riflette le valutazioni delle esposizioni mission, finanziarie e reputazionali organizzate secondo i quattro obiettivi aziendali.*

FIGURE 11: NOTIONAL EXAMPLE OF AN ENTERPRISE RISK PROFILE

| Risk Description | Exposure Factors | Assessment | | | Current Risk Response | Proposed Risk Response | Risk Owner |
|---|---|---|---|---|---|---|---|
| | | Last | Current | Residual | | | |
| **OPERATIONS OBJECTIVE – Manage the Risks of a Remote Workforce** | | | | | | | |
| A global pandemic may necessitate a remote workforce where Agency X could face:<br><br>• a forced reliance on potentially insecure networks;<br><br>• a reduction in managerial oversight; and<br><br>• a deterioration of Agency culture. | **Impact** | High | Medium | Medium | REDUCTION:<br>Agency X has:<br><br>• Facilitated secure remote access via the setup of a Virtual Private Network (VPN)<br>• Modified existing standard operating procedures to include formal mechanisms for increased transparency and self-reporting.<br>• Established a formal remote/telework policy including means of social interaction (e.g., virtual gatherings, campfire sessions, etc.) to foster team building. | Agency X will begin allowing employees to work remotely one day per week and closely monitor employee productivity. | Primary - Chief Operating Officer (COO) |
| | **Likelihood** | Low | Low | Low | | | |
| **REPORTING OBJECTIVE - Privacy Policies Must Accurately Describe Organizational Handling of PII** | | | | | | | |
| Agency X's privacy policies and disclosures are found to inaccurately describe its collection, use, storage, and disclosure of personally identifiable information (PII). | **Impact** | High | High | Medum | REDUCTION:<br><br>Agency X has begun an assessment of existing methods of PII processing to ensure they align with existing policies and are within the bounds of all applicable regulatory requirements. | Agency X will establish a quarterly audit of PII processing and develop a privacy-specific change management plan for inclusion of any necessary updates. | Primary - Chief Privacy Officer (CPO) |
| | **Likelihood** | Medium | Medium | Low | | | |
| **OPERATIONS OBJECTIVE - Manage the Risk of Sudden Interruptions in the Supply Chain** | | | | | | | |
| A key supplier of Agency X has abruptly gone bankrupt. | **Impact** | High | High | Medium | REDUCTION:<br><br>Agency X has begun to formally analyze downstream demand and other market variables to have a better understanding of their current suppliers' ability to handle the dynamic nature of demand. | Agency X is seeking to ensure redundancy within their supply chain by identifying backup/alternative suppliers and seeking to reduce the potential time needed to transition to a new supplier. | Primary - Logistics Coordinator |
| | **Likelihood** | Medium | Medium | Medium | | | |

FIGURE 12: IMPACTS (CONSEQUENCES) OF ENTERPRISE ASSETS FOR A BUSINESS OR AGENCY




*L'ERP supporta la governance e la gestione per misurare gli impatti finanziario, reputazionale e missione significativa (conseguenze).*

*Come mostrato nella Figura 12, le considerazioni includono:*

- IMPATTO FINANZIARIO: *vari scenari di rischio vengono convertiti in spese operative e di capitale effettive, consentendo ai dirigenti esecutivi di condurre un'analisi costi/benefici fiscalmente responsabile che tenga conto delle strategie consigliate per la risposta al rischio.*
- IMPATTO SULLA REPUTAZIONE: *mentre i registri dei rischi subordinati descrivono gli scenari di rischio, compresi quelli che possono avere un impatto sulla reputazione, i dirigenti registrano la valutazione delle conseguenze sulla reputazione dell'impresa. Ciò supporta anche la considerazione di altri impatti a valle, come perdite finanziarie o rischio di credito, che potrebbero derivare da danni alla reputazione.*
- IMPATTO SULLA MISSIONE: *i dirigenti registrano la valutazione delle conseguenze sulla capacità complessiva dell'impresa di condurre la propria missione e raggiungere gli obiettivi strategici. (L'impatto della missione nelle imprese pubbliche commerciali è spesso espresso nelle tabelle Share Value / Market Cap e Volatility delle azioni, divulgate anche nei documenti SEC e nelle comunicazioni agli azionisti.)*

*Queste tre considerazioni di impatto di alto livello sono quindi utilizzate insieme ad altre risposte al rischio aziendale per determinare tolleranze, allocazioni e informazioni commisurate all'esposizione al rischio.*

## 6.4 - ERP A SUPPORTO DELLE DECISIONI

*La definizione delle priorità aiuta i manager a valutare i costi e i benefici dell'allocazione delle risorse per mitigare un rischio rispetto a un altro.*

*La tabella 8 fornisce un supplemento al profilo di rischio aziendale fittizio che riflette una valutazione del portafoglio di vari profili di rischio organizzativo.*

*Queste informazioni, dopo essere state popolate e ordinate per priorità, informano direttamente il processo decisionale dell'esecutivo.*

TABLE 8: NOTIONAL ENTERPRISE RISK PORTFOLIO VIEW FOR A PRIVATE ENTERPRISE

| FINANCIAL RISK PROFILE | | | | | | |
|---|---|---|---|---|---|---|
| | *Current Period* | | | *Previous Period* | | |
| | Net Revenue | Capital | Free Cash Flow | Net Revenue | Capital | Free Cash Flow |
| Enterprise | | | | | | |
| Dept A | | | | | | |
| Dept B | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ... | | | | | | |
| *Dept N* | | | | | | |
| **REPUTATION RISK PROFILE** | | | | | | |
| | ***Current Period*** | | | ***Previous Period*** | | |
| | *Public* | *Regulators* | *Partners* | *Public* | *Regulators* | *Partners* |
| *Enterprise* | | | | | | |
| *Dept A* | | | | | | |
| *Dept B* | | | | | | |
| ... | | | | | | |
| *Dept N* | | | | | | |
| **MISSION RISK PROFILE** | | | | | | |
| | ***Current Period*** | | | ***Previous Period*** | | |
| | *Product/Service Capability* | *Philanthropy* | *Share Value* | *Product/Service Capability* | *Philanthropy* | *Share Value* |
| *Enterprise* | | | | | | |
| *Dept A* | | | | | | |
| *Dept B* | | | | | | |
| ... | | | | | | |
| *Dept N* | | | | | | |

## 7 - STRATEGIA PER IL COORDINAMENTO DEL RISCHIO ICT

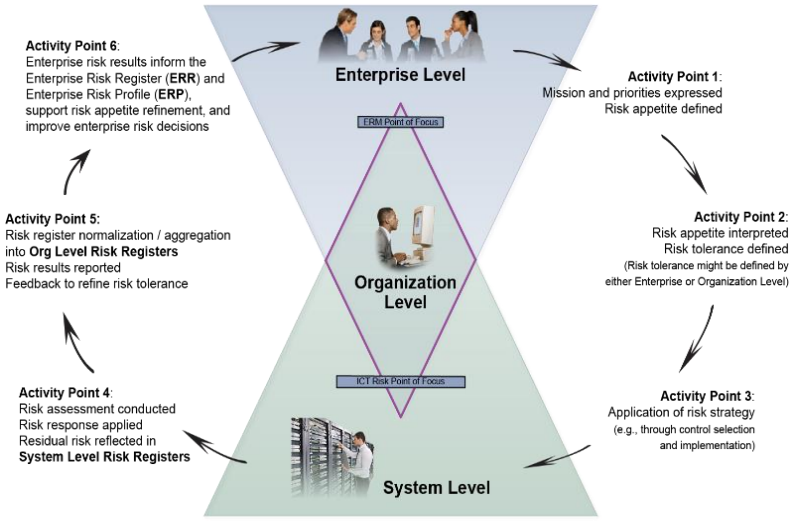
*Nell'ambito delle loro responsabilità di governance, i dirigenti dovrebbero stabilire linee guida chiare e attuabili per la gestione del rischio basate sulla missione aziendale e sugli obiettivi aziendali.*

*Esprimere aspettative chiare in merito al rischio ICT consente ai partecipanti a ogni livello dell'impresa di gestire l'incertezza a un livello accettabile.*

*Con l'evolversi del panorama del rischio, ad esempio, a causa di cambiamenti tecnologici e ambientali, le aziende dovrebbero rivedere e adattare continuamente la strategia del rischio.*

### 7.1 – ATTIVITÀ D'INTEGRAZIONE E COORDINAMENTO DEL RISCHIO

FIGURE 13: ILLUSTRATION OF ENTERPRISE RISK MANAGEMENT INTEGRATION AND COORDINATION



*La figura 13 fornisce un'illustrazione semplificata delle attività di integrazione e coordinamento dei rischi.*

*Le prime iterazioni possono includere la definizione di termini, strategie e obiettivi.*

*Le iterazioni successive possono concentrarsi sul perfezionamento di tali obiettivi sulla base di risultati precedenti, osservazioni del panorama dei rischi e cambiamenti all'interno dell'impresa.*

*La tabella 9 descrive il processo attraverso il quale i dirigenti esprimono aspettative e ricevono risultati sulla gestione del rischio ICT in tutta l'impresa.*

TABLE 9: I/O FOR ERM GOVERNANCE AND INTEGRATED ICTRM

| ACTIVITY POINT | INPUTS | OUTPUTS |
|---|---|---|
| 1. *Set risk expectations and priorities* | *Internal and external risk context; enterprise roles and responsibilities; governance framework and governance systems for managing all types of risks.* | *Documentation of enterprise priorities in light of mission objectives and stakeholder values; direction regarding budget (e.g., authorization for capital and operating expenditures); risk appetite statements pertaining to each risk management discipline, including ICT.* |
| 2. *Interpret risk appetite to define risk tolerance statements* | *Enterprise priorities in light of mission objectives and stakeholder values; direction regarding budget (e.g., authorization for capital and operating expenditures); risk appetite statements.* | *Risk tolerance statements (and metrics) to apply risk appetite direction at the organization level; direction regarding methods to apply ICTRM (e.g., centralized services, compliance/auditing methods, shared controls to be inherited and applied at the system level).* |
| 3. *Apply risk tolerance statements to achieve system level ICTRM* | *Risk tolerance statements; direction regarding shared services and controls; lessons learned from previous ICTRM implementation (and those of peers).* | *Inputs to preparatory activities; system categorization; selection and implementation of risk management controls.* |
| 4. *Assess ICT risks and report system-level risk response through risk registers* | *Security plans; risk response; system authorization (or denial of authorization with referral back for plan revision).* | *Risk assessment results; risk registers describing residual risk and response actions taken; risk categorization and metrics that support ongoing assessment, authorization, and continuous monitoring.* |
| 5. *Aggregate organization-level risk registers* | *Risk registers show system-level risk decisions and metrics; internal reports from compliance/auditing and monitoring processes to confirm alignment with enterprise risk strategy; observations regarding ICTRM achievement in light of risk strategy.* | *Risk registers aggregated, normalized, and communicated based on enterprise-defined risk categories and measurement criteria; refinement of risk tolerance statements, if needed, to ensure balance among value, resources, and risk.* |
| 6. *Integrate risk registers into ERR and ERP* | *Normalized and harmonized risk registers from various organization-level ICTRM reports; compliance and audit reports; results from other nontechnology risk management activities (e.g., credit risk, market risk, labor risk); observations regarding ERM and ICTRM achievement.* | *Integrated ERR aligning ICTRM results with those of other risk categories; refinement of risk appetite tolerance statements and risk management direction to ensure balance among value, resources, and risk; ERP for monitoring and reporting overall risk management activities and results.* |

### 7.1.1 - STRATEGIA PER L'INTEGRAZIONE DEL RISCHIO

*La figura 14 illustra un flusso di informazioni più dettagliato di I/O tra i partecipanti ICTRM ai tre livelli.*

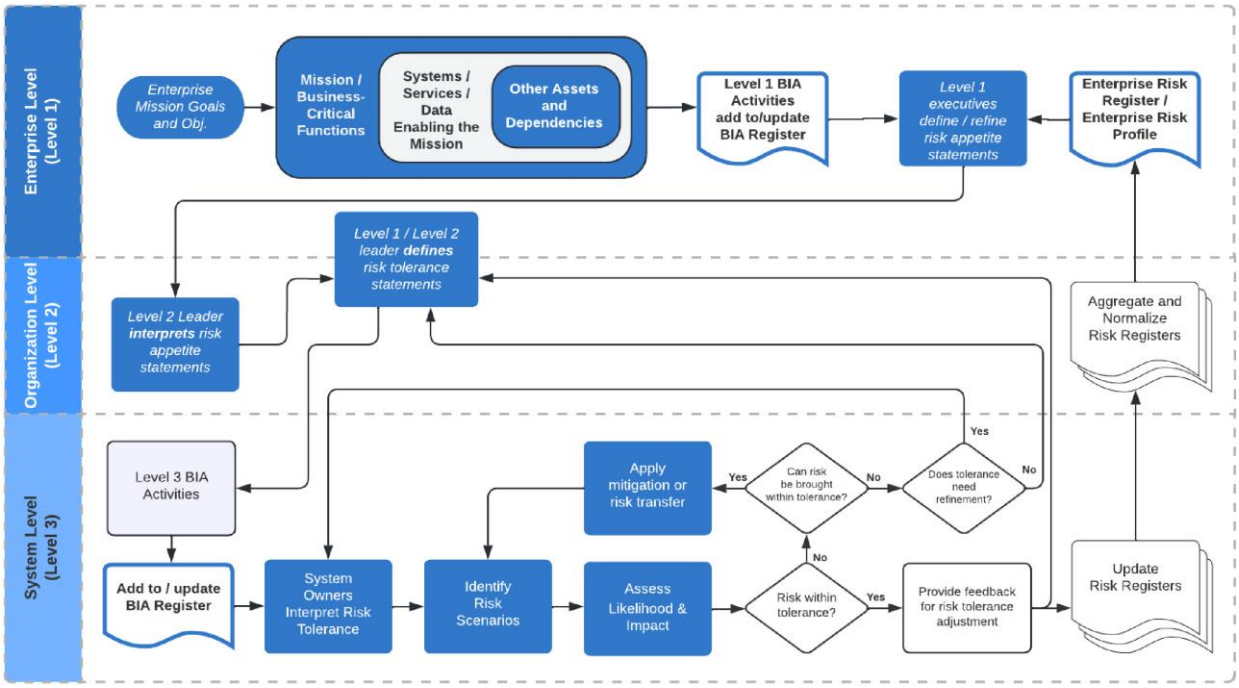
1. *L'azienda definisce la direzione di tolleranza al rischio che viene applicata a livello di sistema.*

2. *I professionisti a livello di sistema interpretano tali dichiarazioni di tolleranza al rischio e applicano le attività ICTRM per raggiungere gli obiettivi di gestione del rischio.*
3. *Attraverso il monitoraggio del rischio, i risultati vengono quindi riesaminati per confermare l'efficacia, evidenziare opportunità di miglioramento e identificare tendenze importanti che potrebbero richiedere un'azione a livello di organizzazione o impresa.*

*L'output di questa attività aiuta a migliorare la comunicazione su* **PRESTAZIONI, TENDENZE DI RISCHIO** *e* **OPPORTUNITÀ** *a tutti i livelli.*

*Le attività specifiche del processo si baseranno sui metodi di gestione del rischio applicati, ma includeranno generalmente quelli di seguito.*

FIGURE 14: CONTINUOUS ERM/ICTRM INTERACTION




*Le attività nella Figura 14 sono discusse di seguito.*

## CONTESTO DEL RISCHIO E ATTIVITÀ STRATEGICHE

- *Sulla base della missione aziendale, i dirigenti identificano i sistemi e i servizi che rappresentano "funzioni missione/business-critical" essenziali per il buon funzionamento dell'impresa.*

  *Sulla base di tale elenco, si identificano le risorse a livello aziendale che abilitano tali funzioni.*

  **Tali asset ereditano la criticità/priorità delle funzioni che supportano.**

  **Vengono identificate le risorse aziendali a supporto di tali obiettivi (ad es. attraverso una BIA).**

- *I leader di* LIVELLO 1 (IMPRESA) E LIVELLO 2 (ORGANIZZAZIONE) *definiscono specifiche e propensioni misurabili al rischio e dichiarazioni di tolleranza al rischio che rafforzano gli obiettivi della missione aziendale e gli obiettivi dell'organizzazione.*
- AL LIVELLO 3 (SISTEMA), *i tecnici interpretano la direzione di criticità/priorità dei leader, espressa attraverso dichiarazioni di propensione al rischio e tolleranza al rischio, per determinare le risorse, i processi e le attività ICT che supportano le operazioni di consegna essenziali per la missione.*

  *Le risorse a livello di sistema sono classificate in base alla sensibilità e alla criticità delle operazioni aziendali, in linea con i risultati BIA a livello aziendale.*

  *Coloro che ricoprono vari ruoli (ad es. proprietari di sistema, responsabili della sicurezza) lavorano insieme per derivare i requisiti a livello di sistema e registrare la comprensione dell'impatto nel registro BIA del sistema.*

## ATTIVITÀ PER L'IDENTIFICAZIONE DEL RISCHIO

- *Viene valutato il valore di ciascuna risorsa di un dato sistema (ad es. tipo di informazione, componente tecnica, personale, fornitore di servizi) per determinare quanto sia critica o sensibile per il funzionamento del sistema.*
- *Per ciascuna di queste componenti, si identificano le fonti di minaccia che potrebbero avere un effetto dannoso e le vulnerabilità o condizioni che potrebbero consentire tale effetto.*

  *Per completare lo sviluppo dello scenario di rischio, è necessario determinare l'effetto negativo della fonte di minaccia sfruttando le condizioni vulnerabili.*

## ATTIVITÀ PER L'ANALISI DEL RISCHIO

- *Si esegue l'analisi del rischio per determinare la probabilità che gli eventi di minaccia e le condizioni vulnerabili comportino impatti dannosi per l'asset del sistema.*

  *Allo stesso modo, si analizza il valore dell'impatto e calcola l'esposizione al rischio utilizzando la metodologia definita nella strategia per il rischio aziendale (ad esempio, come prodotto di [probabilità del rischio] x [impatto del rischio].)*

## ATTIVITÀ PER LA RISPOSTA AL RISCHIO

- *L'esposizione determinata viene confrontata con la tolleranza al rischio.*
  - ✓ *Se l'esposizione rientra nei limiti di tolleranza al rischio, il rischio può essere accettato.*

- *Se l'esposizione supera i livelli di rischio tollerabili, i professionisti possono valutare se possono raggiungere la tolleranza al rischio attraverso altre forme di risposta al rischio.*
  - ✓ *In molti casi, i controlli possono essere applicati per mitigare il rischio riducendone la probabilità o l'impatto a un livello tollerabile.*
    **I controlli dovrebbero essere implementati con una scala di prestazioni corrispondente (cioè, KPI), che viene utilizzata come base per i KRI.**
  - ✓ *La risposta al rischio può includere anche il trasferimento del rischio, noto anche come condivisione del rischio.*
    *Ad esempio, un'organizzazione potrebbe assumere un'organizzazione esterna per elaborare transazioni sensibili (ad esempio, transazioni con carte di pagamento), riducendo così la probabilità che tali dati sensibili vengano elaborati da un sistema interno.*
    *Un altro metodo comune di trasferimento del rischio prevede l'uso di polizze assicurative ICT che possono aiutare a ridurre l'impatto economico se si verifica un evento avverso.*
  - ✓ *In alcuni casi, si potrebbe determinare che l'esposizione eccede la tolleranza al rischio e non può essere portata entro limiti attraverso una combinazione di mitigazione o trasferimento del rischio.*
    *In questo caso, i professionisti (ad es. il proprietario del sistema) potrebbero aver bisogno di lavorare con i leader di livello 2 per rivedere la tolleranza al rischio stessa.*
    *Questa negoziazione offre ai manager di livello 2 e 3 l'opportunità di determinare la migliore linea d'azione per affinare la direzione del rischio alla luce degli obiettivi della missione (ad esempio, attraverso un processo di eccezione, un adeguamento alla dichiarazione di tolleranza al rischio o requisiti di sicurezza aumentati per il relativo sistema).*
    *In ogni caso, gli stakeholder avranno applicato un approccio proattivo per bilanciare rischio e valore.*
  - ✓ *Se un rischio ICT inaccettabile non può essere adeguatamente trattato in modo conveniente,* **tale rischio deve essere evitato**.
    *Tale condizione può richiedere una significativa riprogettazione del sistema o del servizio.*
    **In particolare, evitare il rischio non equivale a ignorare un rischio.**

### 7.1.2 -ATTIVITÀ DI MONITORAGGIO E COMUNICAZIONE DEL RISCHIO

*I gestori del rischio in tutta l'impresa devono essere informati su obiettivi, risultati, priorità e opportunità che risultano dalle risposte al rischio di cui sopra.*

*Uno scopo fondamentale dei vari registri dei rischi è quello di consentire il monitoraggio continuo delle attività di rischio d'impresa. Gran parte di tale monitoraggio avviene attraverso l'osservazione delle metriche delle prestazioni, comprese quelle che indicano i cambiamenti nel rischio (KRI).*

**I KRI informano le organizzazioni se i controlli stanno affrontando adeguatamente i rischi e se i rischi stanno cambiando nel tempo.**

**Quando i KRI non rientrano nelle soglie prestabilite, significa che una risposta al rischio è oltre i livelli accettabili.**

*La tabella 10 fornisce diversi esempi di propensione al rischio, tolleranza al rischio, controlli, KPI e KRI in anticipo e in ritardo relativi alle TIC.*

*Tutti questi esempi aiutano a supportare il ciclo* MONITOR-EVALUATE-ADJUST (MEA) *della Figura 8.*

TABLE 10: NOTIONAL ICT-RELATED EXAMPLES SUPPORTING THE MEA CYCLE

| | EXAMPLE 1 | EXAMPLE 2 | EXAMPLE 3 |
|---|---|---|---|
| ***Risk Appetite*** | *Mission-critical systems must be protected from known cybersecurity vulnerabilities.* | *In keeping with the enterprise designation as a data processor, as described in the GDPR (European Union General Data Protection Regulation), all personal data processed is kept confidential.* | *Our customers associate reliability with our company's performance, so outsourced hosting services must minimize outages for any customer-facing websites.* |
| ***Risk Tolerance*** | *Systems designated as mission-critical must be patched against critical software vulnerabilities (severity score of 10) within 14 days of discovery.* | *While there may be some tolerance for limited low-risk corporate information disclosures, there is zero tolerance for disclosure of PII.* | *Regional managers may permit website outages by supply chain partners, but those must not exceed two hours and may affect no more than five percent of customers.* |
| ***Controls*** | • *Periodic vulnerability assessments*<br>• *Patch deployment capabilities* | • *Authentication method(s)*<br>• *PII processing and transparency policy*<br>• *Authority to process PII*<br>• *Audit log alerting/evaluation* | • *Service level agreements*<br>• *Redundant provider circuits*<br>• *Web load balancers*<br>• *Web servers* |
| ***KPIs*** | • *Percentage of vulnerabilities patched* | • *Days without a loss of PII* | • *Outage time in hours* |
| ***Leading KRIs*** | • *Number of computers with critical vulnerabilities (CVSS score of 10) that have not been patched in 10 days* | • *Failed facility reviews for unprotected physical records*<br>• *Audit log records showing violation of separation of duty requirements* | • *Outages affecting more than five percent of customers that have lasted 1.5 hours*<br>• *Outages lasting over two hours and affecting fewer than five percent of customers* |
| ***Lagging KRIs*** | • *Number of computers with critical vulnerabilities that have not been patched in 15 days* | • *One or more violation indications from data loss prevention tools* | • *Current outages affecting more than five percent of customers that have lasted more than two hours* |

*È importante che i processi aziendali assicurino un'adeguata comunicazione del rischio accettato (e del rischio implicitamente accettato, ad esempio attraverso un processo di eccezione).*

*Uno degli scopi principali dei vari registri dei rischi e dei metodi di rendicontazione è garantire che siano disponibili informazioni di governance adeguate a monitorare le decisioni sui rischi aziendali.*

ESEMPIO.

*Si consideri un'azienda di vendita al dettaglio globale in cui il proprietario di un sistema di un sito Web rivolto al cliente selezionerà i controlli che garantiranno il rispetto dei livelli di servizio di disponibilità. Nel decidere quali controlli applicare, il proprietario del sistema collabora con un team di sicurezza per considerare i metodi per raggiungere gli obiettivi del livello di servizio. Il team può contattare il fornitore di servizi energetici locale per determinare la cronologia della disponibilità elettrica e raccogliere altre informazioni relative alla probabilità di una perdita di alimentazione al sito Web importante. Queste informazioni aggiuntive potrebbero aiutare il proprietario del sistema a decidere se investire in un generatore di backup per garantire una disponibilità di energia sufficiente. I risultati di precedenti valutazioni possono essere utili per stimare la probabilità di raggiungere gli*

*obiettivi di rischio in futuro. Il team passerebbe quindi allo scenario di rischio successivo (ad esempio, forse un'interruzione del servizio Internet) e rivedrebbe la cronologia e l'affidabilità del fornitore di telecomunicazioni dell'organizzazione per accertare la probabilità e l'impatto di una perdita di servizio. Iterando attraverso ogni potenziale rischio, come descritto nella Figura 14, i professionisti possono sviluppare un approccio basato sul rischio per soddisfare gli obiettivi di gestione del rischio basato sulla propensione al rischio e sulla tolleranza al rischio.*

## 7.2 - AGGREGAZIONE E NORMALIZZAZIONE DEI REGISTRI DI RISCHIO

*I contenuti e il formato precisi variano a seconda dell'impresa, ma generalmente seguiranno la struttura illustrata in questa pubblicazione.*

### 7.2.1 - NORMALIZZAZIONE INFORMAZIONI DEL REGISTRO DEI RISCHI

*Durante l'aggregazione, il risk manager ICT normalizzerà anche le informazioni contenute nei vari registri dei rischi.*

*Man mano che i punti dati vengono riuniti, è probabile che vi siano alcuni rischi che si verificano così raramente (o hanno conseguenze sufficientemente basse) da non meritare l'inclusione nel registro di livello successivo.*

*Le decisioni su cosa integrare e come farlo dipendono dall'uso di uno schema comune di valutazione del rischio che consente di tradurre e integrare le valutazioni del rischio a livelli aziendali più elevati.*

*Come minimo, il processo di normalizzazione al livello superiore (ad esempio, per l'ERR) dovrebbe utilizzare gli stessi criteri di rating per consentire il confronto e il monitoraggio. Ciò include in genere le definizioni di come misurare le conseguenze negative (e positive) e la probabilità per consentire la comparabilità tra i risultati della valutazione.*

*I criteri di rischio possono anche descrivere come considerare i fattori temporali, come la velocità del rischio, nel determinare la gravità del rischio.*

*Come indicato in questa pubblicazione, i criteri di rischio possono considerare gli obiettivi dell'organizzazione e il contesto interno/esterno.*

*I criteri per l'escalation o l'aumento del rischio possono anche essere considerati come parte dell'equazione per stabilire se i rischi ICT specifici soddisfano la soglia minima per la discussione a livello di impresa.*

*Ad esempio, l'impresa può rilevare rischi condivisi che rappresentano un'ampia minaccia che trarrebbe vantaggio da un'attenuazione del rischio centralizzata o un rischio reputazionale che richiede un'azione preventiva immediata.*

*Alcuni esempi di normalizzazione del rischio ICT sono descritti nella Tabella 11.*

*Un elemento chiave della normalizzazione è l'identificazione e la risoluzione dei casi in cui uno scenario di rischio simile è trattato in modo diverso dai diversi partecipanti all'impresa.*

TABLE 11: EXAMPLES OF ICT RISK NORMALIZATION

| | |
|---|---|
| *De-duplicate and combine identical or similar risks* | • *An external attacker deploys a remote access tool and uses it to exfiltrate the plans for the company's upcoming merger.*<br>• *External threat actors steal information about marketing plans through malicious code deployed in the sales department.* |

| | |
|---|---|
| | • *Malicious parties plant a web shell in an external site that enables them to access documents stored in the Legal Affairs shared document folder, resulting in the loss of critical corporate information.* |
| *Reprioritize according to risk appetite, tolerance, and sensibilities* | • *Since priorities have been established at organization and system levels, it may be necessary to review their collective priority and recommend adjustments to a higher or lower priority.* |
| *Resolve risk register disparities* | *One of two alternatives might be applied:*<br>• *The combined risk description could be listed in the risk register for each risk response selected by system owners at lower levels. If two system owners had mitigated the above exfiltration risk and one had chosen to accept it, then the risk would appear in the combined risk register twice, with each row indicating the respective response.*<br>• *The combined ICT risk would be included once in the risk register, with both of the responses included in the Risk Response Type column.* |
| *Adjudicate key risks* | • *Those risks that warrant tracking and further communication in the ERR are highlighted and reviewed by enterprise-level risk managers.* |

*È probabile che vari proprietari di rischi utilizzino descrizioni di rischio diverse per lo stesso scenario. In tal caso questi rischi ICT confluirebbero in un unico rischio rappresentativo.*

*Le attività descritte sono destinate esclusivamente a supportare la raccolta e la rendicontazione di informazioni sulle imprese del settore pubblico e privato.*

*Il riepilogo aggregato è un prezioso strumento di reporting, ma non dovrebbe impedire ai manager di rivedere specifiche decisioni di rischio.*

### 7.2.2 – INTEGRAZIONE DEI DETTAGLI DEL REGISTRO DEI RISCHI

*Poiché il processo di analisi e risposta ai fattori di rischio è altamente iterativo, un'impresa potrebbe dover iniziare con valori di rischio* **qualitativi** *e identificare le* **opportunità** *per applicare sempre più approcci* **quantitativi** *man mano che più informazioni e cronologia diventano disponibili.*

*La condivisione delle informazioni e le comunicazioni sulla risposta al rischio sono vitali poiché la risposta al rischio potrebbe essere continua, iterativa o abbracciare diversi cicli di segnalazione.*

*Il completamento delle colonne rimanenti presenta opportunità per la determinazione dell'impresa come segue:*

- *Per un'aggregazione della colonna dei costi di risposta al rischio, in alcuni casi, un gestore del rischio a livello di organizzazione potrebbe voler registrare una media statisticamente ponderata dei costi di risposta al rischio.*
  *In altri casi, il manager potrebbe voler fornire un costo totale allocato su tutti i sistemi e le organizzazioni sussidiarie.*
- *La colonna per il proprietario del rischio dovrebbe indicare un rappresentante a livello di organizzazione che ha la responsabilità e l'autorità per gestire tale rischio.*
  *La proprietà del rischio è un punto informativo chiave che deve essere attentamente considerato e applicato.*
  *La parte designata come proprietario del rischio deve essere costantemente informata sulle condizioni di rischio rilevanti e deve anche avere la responsabilità e l'autorità per gestire il rischio.*
  *Poiché le condizioni di rischio possono cambiare man mano che le informazioni vengono aggregate, la responsabilità e la responsabilità dovrebbero essere riviste periodicamente per garantire che il proprietario del rischio sia il designato appropriato.*
- *Lo stato di rischio per ciascun rischio ICT aggregato dovrebbe utilizzare un insieme coerente di indicatori.*

*Lo stato potrebbe essere un semplice indicatore (ad es. aperto, chiuso, in sospeso) o fornire una spiegazione più dettagliata (ad es. "Rischio accettato in attesa di revisione entro la riunione trimestrale del comitato dei rischi del 24 gennaio").*

*Sebbene i metodi e gli algoritmi utilizzati varino a seconda dell'impresa, dovrebbe esistere una strategia coerente di aggregazione del rischio che sia espressa come parte di una politica all'interno di una determinata impresa.*

*Dato il processo di roll-up, ICTRM, in collaborazione con i gestori del rischio aziendale, può includere dichiarazioni di politica del rischio pertinenti, inclusi i requisiti per la registrazione dei rischi, la fornitura di aggiornamenti regolarmente e la comunicazione delle attività di rischio con i dirigenti e la Direzione aziendale.*

## 7.3 – REGOLAZIONE (ADJUSTING) DELLE RISPOSTE AL RISCHIO

Aristotele è comunemente accreditato di aver insegnato che "**il tutto non è uguale alla somma delle sue parti**". Tale osservazione evidenzia che l'insieme composito di probabilità e impatto del rischio d'impresa è qualcosa di aggiuntivo e non necessariamente equivalente alla somma delle analisi di rischio descritte nei vari registri dei rischi.

*Tenuto conto delle conseguenti osservazioni, possono essere giustificati alcuni adeguamenti, come di seguito descritto.*

- ADEGUARE LA DIREZIONE STRATEGICA

  *Sulla base dei risultati collettivi, i dirigenti possono aggiornare le dichiarazioni di propensione al rischio per aumentare o diminuire i limiti di rischio, compresa la possibile modifica di una specifica direzione quantitativa.*

  *In aggiunta o in sostituzione dell'aggiustamento della propensione al rischio, l'interpretazione della tolleranza al rischio può essere analogamente modificata per sfruttare opportunità o ridurre la probabilità o l'impatto di rischi dannosi.*

- ADEGUARE LE RISPOSTE AL RISCHIO

  *Per affrontare le risposte incoerenti ai rischi o per ottenere un risultato diverso, i responsabili possono scegliere di indirizzare azioni di risposta specifiche a uno o più scenari di rischio.*

  *L'aggiustamento può consistere nel ridurre l'esposizione complessiva adottando una risposta più rigorosa oppure nell'allentare le restrizioni per ottenere qualche vantaggio in cambio di un aumento misurato del rischio.*

- ADEGUARE KPI E KRI

  *Sebbene l'impresa possa adeguare la propria specifica direzione o trattamento del rischio, il risultato della valutazione sarà spesso un maggiore monitoraggio delle varie condizioni.*

*Soprattutto quando le condizioni indicano un'ampia varianza nelle metriche risultanti, i manager possono indirizzare le modifiche ai KPI e ai KRI monitorati per ottenere una migliore visibilità.* ***Se le modifiche all'impatto e alla probabilità non possono essere adeguatamente osservate con gli attuali indicatori, possono essere giustificate metriche diverse (o aggiuntive).***

*Ulteriori adeguamenti possono essere basati su indicazioni esterne, come i requisiti di un'autorità di regolamentazione per una maggiore gestione del rischio o nuovi criteri di segnalazione (ad esempio, divieto di condividere o divulgare informazioni da un contatore intelligente sull'utilizzo di un cliente senza il consenso di tale cliente).*

### 7.3.1 - FATTORI CHE INFLUENZANO LA PRIORITÀ

*Numerosi fattori (ad es. perdita finanziaria, reputazione aziendale, sentiment degli azionisti) influenzano la priorità e dovrebbero essere inclusi nella strategia di rischio aziendale.*

*È probabile che un rischio ICT che influisca direttamente sulla missione sia una priorità assoluta, ma molte altre considerazioni, come la reputazione dell'agenzia o dell'azienda, possono spostare un particolare tipo di rischio in cima alla lista.*

*Un'altra considerazione potrebbe verificarsi se un'entità aziendale si stesse preparando per una fusione.*

*La comunità ha visto esempi recenti che hanno dimostrato che la scoperta di un rischio ICT può influenzare la valutazione di un'impresa e le successive negoziazioni.*

*Potrebbero anche esserci fattori che non sono direttamente correlati al rischio, ma che potrebbero supportare il miglioramento dell'organizzazione (ad esempio, vittorie rapide che creano fiducia nel team e guadagnano slancio, rischi relativi a un obiettivo che i leader hanno stabilito come priorità chiave).*

*I valori di priorità come basso, moderato e alto sono spesso usati come categorie di priorità del rischio.*

*Questo approccio* **qualitativo** *può essere più limitante dell'analisi* **quantitativa** *in quanto è più facile ordinare un intervallo di valori numerici, anche quelli relativamente vicini, piuttosto che ordinare un elenco di rischi contrassegnati come "Molto alto".*

*Nella maggior parte delle imprese, la strategia di rischio dovrebbe fornire indicazioni sia per metodi di generalizzazione (ad es. basso, moderato, alto) sia per metodi di definizione delle priorità del rischio più specifici.*

### 7.3.2 – OTTIMIZZAZIONE DEL RISCHIO ICT

**Un obiettivo chiave del coordinamento ERM/ICTRM è aiutare le parti interessate dell'impresa a raccogliere vari dati sui rischi per il supporto alle decisioni, il monitoraggio e le comunicazioni.**

*Diverse definizioni fondamentali sono rilevanti per assegnare correttamente la priorità al rischio in ogni fase del ciclo di vita, inclusa l'aggregazione e l'assegnazione di priorità ai dati del registro dei rischi discussi in questo documento:*

1. AGGREGAZIONE DEL RISCHIO

   *La combinazione di più rischi in un rischio per sviluppare una comprensione più completa del rischio complessivo [ISO73].*

2. CRITERI DI RISCHIO

   *Termini di riferimento rispetto ai quali viene valutata la significatività di un rischio, come obiettivi organizzativi, contesto interno/esterno e requisiti obbligatori (ad es. standard, leggi, politiche) [ISO73].*

3. OTTIMIZZAZIONE DEL RISCHIO

   *Un processo correlato al rischio per ridurre al minimo le conseguenze negative e massimizzare le conseguenze positive e le rispettive probabilità; l'ottimizzazione del rischio dipende da criteri di rischio, inclusi costi e requisiti legali.*

*I processi per* **aggregare**, **assegnare** *priorità e* **ottimizzare** *il rischio saranno diversi a ogni livello dell'impresa, in base ai criteri di rischio pertinenti a quel livello.*

*I metodi utilizzati per ottimizzare il rischio sono a discrezione dei responsabili aziendali e sono spesso eseguiti da un consiglio di leadership del rischio o da un altro organismo di governance del rischio.*

*Poiché è probabile che i budget di capitale e spese operative per la risposta al rischio siano limitati, ciascun metodo deve includere un processo su come rispondere a tali scenari quando i finanziamenti non sono disponibili.*

*Alcuni esempi includono:*

- OTTIMIZZAZIONE FISCALE

  *Una semplice classificazione dei rischi in ordine decrescente dal più impattante al minimo.*

  *I gestori del rischio calcolano i costi totali di risposta al rischio fino all'esaurimento del finanziamento.*

- OTTIMIZZAZIONE ALGORITMICA

  *L'applicazione di formule matematiche per calcolare il costo-beneficio aggregato per l'impresa, dati i costi stimati, in un approccio puramente meccanico.*

- OTTIMIZZAZIONE OPERATIVA

  *La selezione dal registro dei rischi più importanti per le operazioni (in base alle preferenze della leadership, agli obiettivi della missione e al sentimento degli stakeholder.*

  *Il coordinamento operativo dipende da un ciclo di comunicazione iterativo di reportistica e analisi dei rischi.*

- OTTIMIZZAZIONE FORZATA DELLA CLASSIFICA

*Assegnare priorità ai rischi nel modo che utilizzerà al meglio le risorse disponibili per ottenere il massimo beneficio, date specifiche conseguenze negative e positive.*

*Vari fattori di business e conseguenze del rischio hanno pesi diversi per lo sviluppo di un punteggio, aiutando ad andare oltre il semplicistico approccio* "**minaccia moltiplicata per vulnerabilità**" *per costruire obiettivi aziendali in quell'equazione.*

*In definitiva, l'ottimizzazione eseguita sarà probabilmente una combinazione di questi metodi.*

*Per alcune aziende, l'ottimizzazione del rischio può avere anche un fattore temporale.*

*Ad esempio, i proprietari del rischio potrebbero essere disposti ad accettare alcuni scenari di rischio per ridurre le spese e aumentare la redditività verso la fine di un trimestre fiscale. Quegli stessi scenari potrebbero essere pienamente trattati in circostanze finanziarie più favorevoli.*

### 7.3.3 – PRIORITÀ DEL RISCHIO ICT A LIVELLO AZIENDA

*A supporto della definizione delle priorità del rischio, come per i rischi ICT stessi, i fattori di ranking riflettono i vari strati dell'impresa.*

- *A livello di sistema, il registro dei rischi riflette le priorità di rischio relative a particolari sistemi e tecnologie.*
- *Il livello dell'organizzazione ha priorità basate su mission uniche e driver di business unit.*
- *L'impresa ha priorità ICT generali che potrebbero non essere le stesse di livelli tecnici di astrazione inferiori e possono avere priorità variabile se considerate insieme ad altri rischi per l'impresa.*

*Questo equilibrio è fondamentale per il concetto di ICTRM come input per l'ERM.*

*Sebbene i rischi per l'informazione e la tecnologia istituzionali siano parti critiche dell'impresa e un obiettivo primario di coloro che sono incaricati di dirigere l'ICTRM, i funzionari aziendali e i fiduciari hanno una prospettiva ampia e devono bilanciare le dozzine di tipi di incertezza nell'universo del rischio aziendale.*

*La comunicazione bidirezionale è fondamentale, poiché consente ai leader di trasmettere strategia e direzione, consentendo anche ai manager di sistema e di business di tenere informata la leadership.*

*Questo processo non significa che ogni decisione di rischio a livello di sistema debba essere elevata alla massima leadership, ma piuttosto che molte decisioni di rischio a livello di sistema e organizzazione debbano essere considerate provvisorie e che i leader possono successivamente raccomandare una priorità o un approccio diverso in base alla loro comprensione dell'impatto aggregato sui fattori aziendali (ad es. entrate, reputazione, normative, politiche).*

## 7.4 – ADEGUAMENTI (ADJUSTING) AZIENDALI BASATI SUI RISULTATI DEL RISCHIO ICT

*In molte organizzazioni, le TIC (ICT) consentono un approccio flessibile al raggiungimento della missione aziendale e alla garanzia del valore degli stakeholder.*

### 7.4.1 - ADEGUAMENTI A PROPENSIONE (APPETITE) E TOLLERANZA AI RISCHI

*Oltre alle considerazioni fiscali, le osservazioni durante il ciclo di vita possono anche fornire un feedback sui criteri di rischio dei leader relativi alla propensione e alla tolleranza al rischio.*

*La Figura 14 illustra diversi punti decisionali chiave, tra cui:*

- ACCETTAZIONE DEL RISCHIO A LIVELLO DI SISTEMA*: Nella selezione dei controlli appropriati per un dato sistema informativo (o insieme condiviso di controlli), un rischio è già accettabile, date le dichiarazioni di tolleranza al rischio applicabili?*
  - ✓ *Se non è accettabile, il proprietario del sistema ha la possibilità di applicare un'ulteriore risposta al rischio, attraverso la condivisione del rischio o l'attenuazione mediante vari controlli?*
  - ✓ *A volte, il rischio non può essere portato entro la tolleranza attraverso una qualsiasi combinazione di controlli, oppure il costo dei controlli potrebbe essere irragionevole per il sistema.*
- ULTERIORI PUNTI DI DECISIONE SI VERIFICANO DOPO L'AGGREGAZIONE E L'INTEGRAZIONE DEI REGISTRI DEI RISCHI AI VARI LIVELLI: *Man mano che i gestori del rischio riesaminano i registri del rischio e gli RDR, i risultati della gestione del rischio verranno confrontati con le aspettative degli stakeholder.*

  *Sulla base dei risultati aggregati, i gestori del rischio ICT potrebbero dover considerare le seguenti domande:*
  - ✓ *La risposta al rischio è coerente tra le varie strutture e livelli organizzativi?*

    *Sulla base dell'analisi del rischio, della risposta e dei risultati del monitoraggio, i gestori del rischio possono stabilire che sono necessarie ulteriori linee guida per ottenere meglio un'attività di gestione del rischio ripetibile e affidabile.*

    *Per migliorare la maturità del processo possono essere necessari adeguamenti delle politiche, delle procedure, della formazione del personale e di altre componenti di governance.*
  - ✓ *L'ambiente di rischio si è evoluto (forse a causa di cambiamenti nel contesto interno o esterno, come nuove normative o accordi con i clienti) a tal punto che è necessario adeguare la direzione oi criteri del rischio?*

    *In tal caso, ciò offre l'opportunità di ripetere il ciclo.*

*Oltre a questi aggiustamenti programmatici, durante il monitoraggio continuo e le attività di valutazione continua potrebbero essere identificati aggiustamenti specifici del trattamento del rischio.*

### 7.4.2 - ADEGUAMENTI DELLA PRIORITÀ

*Un ultimo adeguamento a livello di programma riguarda le priorità delle imprese.*

*Le decisioni sul rischio ICT derivano dalla missione e dalle priorità dell'impresa.*

*Ciò è illustrato dal Punto di attività 1 nella Figura 13 in cui i dirigenti stabiliscono la missione e le priorità, che guidano gli obiettivi strategici e la pianificazione, che vengono quindi utilizzati per dirigere le attività ICTRM.*

*Successivamente, i rischi individuati e valutati sono registrati nel registro dei rischi secondo tali priorità.*

*L'ordine in cui vengono affrontati i rischi, la direzione di una risposta appropriata e persino l'accordo su quali rischi verranno affrontati derivano tutti dalle priorità dell'impresa. Per questo motivo, un'attività chiave dell'impresa sarà una revisione periodica di tali priorità e degli effetti che hanno sull'ICTRM.*

*Sulla base dei risultati di tali revisioni, le priorità potrebbero essere adeguate o chiarite per garantire il continuo allineamento tra l'attività ICTRM e gli obiettivi della missione.*

## ESEMPIO DI RISK DETAIL RECORD (RDR)

*A supporto di un registro dei rischi ICT, un record di dettaglio del rischio (*RISK DETAIL RECORD - RDR*), consente la comunicazione di informazioni aggiuntive.*

FIGURE 15: NOTIONAL RISK DETAIL RECORD

| *Notional Risk Detail Record* | | |
|---|---|---|
| Risk ID numbers | | |
| System affected | | |
| Organization or business unit | | |
| Risk Scenario Description | | |
| ✓ *Assets affected* | | |
| ✓ *Threat sources/actors (with intent? with motivation?)* | | |
| ✓ *Threat vectors* | | |
| ✓ *Threat events* | | |
| ✓ *Vulnerability/predisposing conditions* | | |
| ✓ *Primary adverse impact (be sure to reconcile impact vs consequences)* | | |
| ✓ *Secondary adverse impacts* | | |
| ✓ *Other scenario details* | | |
| *Risk category* | | |
| *Current risk analysis* | | |
| *Likelihood before controls (%):* | *Impact before controls ($):* | *Exposure rating before controls ($):* |
| *Planned residual risk response* | *Select all that apply:* □ *Accept* □ *Avoid* □ *Transfer* □ *Mitigate* | |
| *Planned risk response description* | | |
| *Resource requirements for planned risk response* | | |
| *Planned response cost ($)* | | |
| *Likelihood after controls will be (%):* | *Impact ($):* | *Expected exposure rating ($):* |

| | | |
|---|---|---|
| *Residual risk response as Implemented* | *Actual response cost ($):* | |
| *After controls are in place, measured Likelihood is (%):* | *Impact ($):* | *Final exposure rating ($):* |
| *Risk owner/point of contact* | | |
| *Date of risk identification* | | |
| *Source of risk information* | | |
| *Current status date* | | |
| *Dependencies* | | |
| *Follow-up date* | | |
| *Comments* | | |