APPUNTI

Risk management e analisi dei processi
Esempio applicazione modello ISO

Analisi processi e risk management – AA 2026-2027. Appunti
Università degli Studi di Teramo – Massimo De Angelis

INDICE

1 Definizioni ed acronimi 3

2 Le Policy di gestione del rischio 4

2.1 Principi della gestione del rischio 4
2.2 Ruoli, responsabilità e risorse nel processo di gestione del rischio 5
2.3 Classificazione dei rischi 5
2.4 Identificazione e categorie dei rischi 6
2.5 Sistema di controllo interno 6
2.6 Criteri di accettazione del rischio 6

3 Il processo di gestione del rischi 7

3.1 Analisi del contesto 7
3.2 Valutazione del rischio 8
3.2.1 Identificazione del rischio 8
3.2.2 Valutazione del Rischio inerente 8
3.2.3 Valutazione dei fattori abilitanti e dei controlli 10
3.2.4 Valutazione dell'organizzazione dei controlli interni esistenti 10
3.2.5 Valutazione dell'efficacia dei controlli interni esistenti 11
3.3 Ponderazione del rischio 11
3.3.1 Valutazione Rischio e dei controlli: rischio risiduale 11
3.3.2 Valutazione Risk appetite e Rischio finale 11
3.3.3 Identificazione degli elementi di Controllo interno 11
3.4 Trattamento del rischio 11
3.4.1 Identificazione dei Risk Owner e delle azioni di mitigazione 12
3.5 Monitoraggio e riesame 12

1 Definizioni ed acronimi

- La **procedura** è un insieme di attività sequenziali la cui corretta esecuzione nell'ordine prescritto si assume possa garantire il raggiungimento di un determinato risultato. In pratica è la regola che ci dice cosa deve essere fatto per avere un certo effetto;
- Il **processo** è l'insieme delle risorse utilizzate per realizzare una procedura determinata, ovvero l'insieme degli input utilizzati per ottenere un determinato output e le modalità con cui questi input si combinano e susseguono;
- Il **procedimento** amministrativo è una sequenza preordinata di atti, individuati da norme, tra loro collegati e tutti diretti alla produzione di un unico atto conclusivo con rilevanza esterna, denominato provvedimento amministrativo;
- Il **rischio** è l'incertezza che eventi inaspettati possano manifestarsi producendo effetti sugli obiettivi (strategici,operativi,azioni,etc…) dell'organizzazione. Un effetto è uno scostamento da quanto atteso – positivo e/o negativo. Il livello di rischio è calcolato moltiplicando l'impatto per la probabilità;
- La **probabilità** rappresenta la possibilità, ovvero la plausibilità di un accadimento;
- L**'impatto** è la conseguenza del verificarsi di un evento dannoso. Gli impatti possono essere distinti per livelli di severità;
- **Risk management:** attività coordinate per guidare e tenere sotto controllo una organizzazione con riferimento al rischio"[1]; "tutte le attività di progetto legate alla identificazione, valutazione, riduzione, accettazione e feedback dei rischi"[2], attraverso azioni di mitigazione per fornire una ragionevole assicurazione circa il raggiungimento degli obiettivi (Linee guida Commissione Europea);
- I **risk driver inerenti** sono fattori che prescindono dalla quantità o qualità dei controlli interni; la loro presenza può aumentare la probabilità che un determinato evento negativo possa verificarsi (Esempi: contatti diretti verso terzi, gestione di denaro contante, presenza di personale a contratto determinato, ecc …). I risk driver inerenti sono funzionali alla valutazione del rischio;
- **Fattori abilitanti**: aspetti organizzativi e modalità gestionali la cui presenza incide sul livello di probabilità e impatto;
- Le **operazioni a rischio o eventi rischosi** sono quelle attività / predisposizione di documenti o atti, / assunzione di comportamenti che possono influire in senso negativo sul conseguimento dell'utilizzo trasparente, efficiente, efficace ed equo delle risorse pubbliche e che potenzialmente possono favorire il verificarsi eventi non etici, non integri o legati al rischio oggetto di identificazione e valutazione;
- **Tipologie di rischio in relazione alle tipologie di obiettivi:** rischi strategici, rischi operativi, di reporting, rischi di conformità, rischi di corruzione;
- Indicatori di rischio: **sono metriche i cui valori tracciano l'andamento in aumento o in diminuzione** della probabilità che un determinato evento negativo possa verificarsi e impattare in modo significativo sul livello di rischio a cui l'evento si riferisce (*Key Risk Indicator - KRI*). Gli indicatori di rischio possono essere di processo se l'evento negativo ha un impatto sulle attività del processo oppure di impatto se le metriche tracciano l'andamento che ha per oggetto un evento negativo che impatta sul risultato del processo (es.: se si prende ad esempio il processo di Pianificazione delle attività triennale, l'evento negativo può avere un impatto sulle dinamiche delle attività collegate al processo (ad esempio non terminare il processo entro la data predefinita) o può avere un impatto sulle attività collegate all'output del processo (l'evento negativo che si è verificato durante la realizzazione processo ha determinato una pianificazione che non consente di realizzare gli obiettivi previsti);
- **Process owner**, il soggetto responsabile della performance del processoe che ha la competenza e l'autorità per apportare modifiche al processo. Le attività del process owner nell'ambito della gestione del rischio possono essere svolte da un focus group nominato ad hoc e coordinato dal process owner;
- **Responsabile di procedimento**, il soggetto di cui alla Legge 241 del 1990 e ssmmii;
- **Risk Owner**, il soggetto che ha la responsabilità e l'autorità della gestione del rischio (responsabilità dell'implementazione delle azioni per la gestione del rischio);
- **Attività di controllo**: l'applicazione delle policy e delle procedure che garantiscono al management che le sue direttive siano attuate per mitigare i rischi connessi al raggiungimento degli obiettivi. Le attività di controllo si attuano a tutti i livelli dell'organizzazione, nelle varie fasi dei processi di business e sull'ambiente tecnologico.

2 Le Policy di gestione del rischio

La presente metodologia ha per oggetto, laddove applicabile, i processi e i procedimenti amministrativi dell'Ente maggiormente esposti a rischi.

La gestione del rischio deve essere incorporata nelle prassi e nei processi dell'organizzazione ed essere orientata al raggiungimento dei seguenti obiettivi strategici:

- ridurre le opportunità che si manifestino eventi che possono minacciare la realizzazione degli obiettivi strategici, operativi e di performance;
- aumentare la capacità di individuare quali eventi possono compromettere tali obiettivi;
- contribuire a rafforzare il sistema di controllo interno dell'Ente al fine di intervenire sulle probabilità che eventi negativi possano materializzarsi;
- attenuare gli impatti originati dal verificarsi di un evento non desiderato e dannoso per l'Ente.

Il valore aggiunto che si intende ottenere dall'implementazione del processo di risk management riguarda l'organizzazione a diversi livelli:

- a livello di Direzione generale per rafforzare i processi interni di comunicazione, di supporto strategico e di gestione delle decisioni operative;
- a livello di Direzioni per agevolare il coordinamento, l'analisi e la gestione degli eventi che possono avere un effetto negativo sulla realizzazione degli obiettivi delle direzioni (parimenti per identificare opportunità emergenti dall'analisi dei rischi);
- a livello di Responsabili di unità, per contribuire a supportare gli stessi responsabili nella individuazione di misure per prevenire rischi che potrebbero influire sulla realizzazione dei loro obiettivi in modo efficiente ed efficace (parimenti per identificare opportunità emergenti dall'analisi dei rischi).

La gestione del rischio coinvolge l'organizzazione a tutti i livelli. I soggetti istituzionali coinvolti nella gestione del rischio per quanto di loro competenza sono:

- Organo di indirizzo politico;
- Responsabile della gestione (Direttore generale);
- Responsabile della Prevenzione della Corruzione e della Trasparenza
- referenti per la prevenzione della corruzione e della performance;
- tutti i dirigenti o responsabili di UO;
- OIV e gli altri organismi di controllo interno, Ufficio Provvedimenti Disciplinari - UPD,
- Dipendenti dell'ente.

Per ogni processo saranno coinvolti in particolare:

- il Process owner. Le attività del process owner nell'ambito della gestione del rischio possono essere svolte da un focus group nominato ad hoc e coordinato dal process owner;
- Responsabile di procedimento (se applicabile);
- il Risk Owner.

2.1 Principi della gestione del rischio

Una efficace gestione del rischio deve tener conto dei seguenti principi:

a. La gestione del rischio crea e protegge valore: contribuisce al raggiungimento degli obiettivi ed al miglioramento delle prestazioni;
b. La gestione del rischio è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti o del cambiamento; non è, pertanto, una attività indipendente;
c. La gestione del rischio è parte del processo decisionale;
d. La gestione del rischio tratta esplicitamente l'incertezza;
e. La gestione del rischio è sistematica, strutturata e tempestiva;
f. La gestione del rischio si basa sulle migliori informazioni disponibili: fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori di interesse, ecc.;
g. La gestione del rischio è "su misura": deve essere in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione;
h. La gestione del rischio tiene conto dei fattori umani e culturali;
i. La gestione del rischio è trasparente e inclusiva: il coinvolgimento appropriato e tempestivo dei portatori di interesse, assicura che la gestione del rischio rimanga pertinente e aggiornata e fa sì che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio;

j. La gestione del rischio è dinamica, iterativa e reattiva al cambiamento;
k. La gestione del rischio favorisce il miglioramento continuo dell'organizzazione.

2.2 Ruoli, responsabilità e risorse nel processo di gestione del rischio

La struttura organizzativa attiva sul processo di gestione del rischio è di norma composta da:

- Responsabile dell'UO incarica di svolgere attività di risk management (*Risk Manager*), che vigila sull'attuazione del processo ed è responsabile dell'approvazione degli output attesi delle varie fasi;
- Process owner/Responsabile di procedimento;
- Risk Owner;
- facilitatori: soggetti aventi il compito di aiutare un gruppo (una organizzazione) nelle fasi di analisi, al fine di meglio valutare l'oggetto di analisi e addivenire a delle conclusioni;
- un *Risk Management Board*[1] per le analisi, le valutazioni e le proposte (azioni di contrasto, di mitigazione, accettazione, designazione dei Risk Owners) a supporto delle decisioni e delle azioni del Responsabile della gestione. Il Board ha una funzione consultiva, opera secondo opportunità e necessità ed è coordinato dal Risk Manager. Il Board, laddove presente, è nominato dal Direttore generale ed è composto di norma dai principali Risk Owners. Il Risk Management Board in particolare:
  - predispone il piano di gestione del rischio sulla base delle direttive strategiche dell'Organo di indirizzo politico;
  - individua i Key Risk Indicator;
  - definisce i pesi delle leve di probabilità e impatto;
  - stabilisce il *range* delle fasce di impatto e probabilità;
  - approva nuove leve di probabilità e di impatto;
  - sottomette i rischi "sensibili" la cui azione di riduzione non ha ricondotto il livello di rischio ad un stato accettabile, ad un livello gerarchico adeguato per la discussione e accettazione;
  - approva le azioni di mitigazione individuate dai focus group ed esprime le motivazioni per le azioni di mitigazione non approvate.
- Il focus group, costituito da soggetti rappresentativi del processo/procedimento oggetto di valutazione dei rischi, è individuato dal Risk Management Board. Il focus group è coinvolto nella fase di identificazione, valutazione dei rischi, identificazione delle azioni di mitigazione, di caratterizzazione di alcuni aspetti propedeutici alla valutazione dei rischi. Laddove non presente le funzioni del focus group sono assicurate dal process owner;
- Soggetti istituzionali coinvolti nella gestione del rischio per quanto di loro competenza: autorità di indirizzo politico, Responsabile della gestione (Direttore generale), referenti per la prevenzione, tutti i dirigenti o responsabili di UO, OIV e gli altri organismi di controllo interno, Ufficio Provvedimenti Disciplinari - UPD, dipendenti, collaboratori a qualsiasi titolo.

2.3 Classificazione dei rischi

I principali rischi gestiti sono i seguenti:

- **Il rischio operativo[2];**
- **Il rischio strategico[3];**
- **Il rischio reputazionale;**
- **Il rischio di non compliance della normativa vigente;**
- **Il rischio collegato alla prevenzione della corruzione (vedi appendice B).**

[1] La costituzione del Risk Management Board è opzionale. In assenza le funzioni del Risk Management Board sono svolte dal responsile dell'UO incaricata di svolgere attività di risk management.

[2] Rischio di perdite dirette o indirette derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni; Risorse umane: perdite dovute a negligenza o incompetenza, attività non autorizzate, frodi, appropriazioni indebite o violazione di leggi, regolamenti e direttive aziendali da parte di soggetti interni all'impresa;

- Procedure: perdite derivanti da carenze nelle procedure operative e nella gestione dei processi, ovvero nel sistema di controllo interno;
- Eventi esterni: danni originati da eventi esogeni di natura politica, normativa, sociale, ambientale, nonché da attività illecite commesse da soggetti esterni alla struttura aziendale.
- Tecnologie: perdite dovute a inefficienze e malfunzionamenti dei sistemi informatici e degli impianti produttivi.

[3] Rischio che deriva dalle possibili perdite immediate e prospettiche scaturenti da ripercussioni negative delle scelte strategiche dell'Ente o da mutamenti del contesto in cui opera che non consentono la realizzazione della missione istituzionale.

2.4 Identificazione e categorie dei rischi

L'identificazione e la caratterizzazione dei rischi, svolta anche attraverso focus group dedicati e supportati da facilitatori nelle fasi di analisi, si sostanzia:

- nella mappatura dei processi, delle attività e degli obiettivi collegati, laddove non già presente una mappatura delle fasi/attività/input-output/ruoli che intervengono e la rilevazione della natura obiettivi perseguiti (strategici, operativi, etc..);
- nella individuazione delle sorgenti e delle cause più probabili di ciascun rischio identificato. I risk drivers possono essere inerenti o di controllo;
- nella fase di rilevazione e valutazione dei rischi;
- nell'elaborazione di un catalogo e registro degli eventi rischiosi per ciascuna attività;
- nell'individuazione delle possibili azioni di mitigazione.

I rischi, in funzione della loro origine, possono essere raggruppati nelle seguenti categorie, a ciascuna delle quali sono associate le aree da considerare nella fase di identificazione dei rischi:

1. *Rischi legati all'ambiente esterno*
   - *Rischi macro ambientali (eventi geopolitici, disastri naturali, economici)*
   - *Decisioni politiche e priorità definite dall'esterno*
   - *Partner esterni*
2. *Rischi legati alla pianificazione, ai processi e sistemi*
   - *Strategie, policy e pianificazione, incluse le decisioni politiche interne*
   - *Processi operativi*
   - *Allocazione budget e processi finanziari*
   - *IT e supporto sistemi*
3. *Rischi relativi al personale e all'organizzazione*
   - *Risorse umane (assunzioni, competenze, incarichi e collaborazioni, ...)*
   - *Comportamenti etici e organizzativi (conflitti di interessi, frodi, ...)*
   - *Organizzazione interna (governance, ruoli e responsabilità, sistema di deleghe)*
   - *Sicurezza del personale, della struttura, etc…*
4. *Rischi collegati ad aspetti di legittimità e regolarità*
   - *Chiarezza, adeguatezza e coerenza nell'applicazione della legge, regolamenti e altre norme*
   - *Altre cause collegate alla legalità e regolarità*
5. *Rischi connessi alla comunicazione e informazione*
   - *Metodi e canali di comunicazione*
   - *Qualità e tempestività delle informazioni*

2.5 Sistema di controllo interno

L'attività di valutazione dei rischi è uno degli elementi del sistema di controllo interno. L'attività di risk management è integrata in diversi step nelle attività di auditing e nel ciclo di pianificazione e programmazione strategica.

Gli elementi del sistema di controllo interno oggetto di valutazione da parte dell'internal audit sono:

1. *Missione e valori*
2. *Risorse umane*
3. *Processo di pianificazione e valutazione dei rischi*
4. *Attività operative e di controllo interno*
5. *Informazione e reporting*
6. *Valutazione e audit*

Per il dettaglio dei requisiti si rinvia al **Doc.** A6 di cui al riferimento.

A fronte dei rischi rilevati, il risk manager, nel corso delle sua analisi e delle interviste, rileva i fattori abilitanti che innescano gli eventi rischiosi e i controlli ideali associabili a ciascuna fase.

Il processo di valutazione del controllo tiene conto del contesto interno ed esterno e di tutti gli elementi informativi forniti dal process owner e del livello di maturità dei controlli interni e dei fattori abilitanti.

2.6 Criteri di accettazione del rischio

I criteri di accettazione del rischio sono in funzione del suo *risk appetite (propensione al rischio dell'Ente).*

I criteri di accettabilità, poiché stabiliscono la significatività dei valori riportati nella matrice di rischio impatto/probabilità, incidono sulla classificazione della valutazione del rischio, e consentono di fornire un giudizio sulla eventuale non accettabilità (qualora il rischio fosse eccessivo rispetto al *risk appetite*) e sulla necessità di porre in essere azioni di mitigazione (trattamento) del rischio in esame.
Le decisioni circa le strategie per la gestione dei rischi, dovrebbero tenere conto del più ampio contesto di riferimento riguardante il rischio: collegamenti e rilevanza dei reati collegati al processo, loro impatto sugli outcome dell'Ente, quantità di eventi rischiosi collegati a reati o a danni non tollerabili dall'Ente.
In alcune circostanze la ponderazione del rischio può portare alla decisione d'intraprendere ulteriori analisi, oppure di non sottoporre ad ulteriore trattamento il rischio, limitandosi a mantenere attivi i controlli esistenti. Di seguito una sintesi delle possibili strategie di gestione dei rischi.

Il risk appetite dell'Ente è indicato dal vertice dell'Ente (Direzione generale).

Figura 1.



3 Il processo di gestione del rischi

Si riporta lo schema del processo come descritto nel documento di Policy.
Figura 2.



Il processo è ricorsivo e prevede quattro fasi conseguenziali, più la fase di comunicazione e consultazione le cui attività sono previste all'interno delle altre fasi.
Di seguito si riporta la descrizione delle fasi nel processo.

3.1 Analisi del contesto

Prevede l'analisi sia del contesto interno che esterno. Tra gli obiettivi di questa fase c'è quello di identificare le tipologie di rischio che rientrano nel contesto in cui si opera e, tra queste, quelle che si ritengono prioritarie.
Il contesto esterno consiste nell'ambiente in cui opera l'Ente, negli attori privati ed istituzionali con cui ha rapporti e portatori di intesse delle attività istituzionali (Stakeholder) e cioè le agenzie governative internazionali, gli istituti di ricerca, le industrie di settore, gli enti governativi e le autorità di vigilanza, solo

per citarne i principali. L'analisi del contesto prevede l'identificazione delle relazioni esistenti tra l'organizzazione e gli Stakeholder, dei rispettivi compiti e competenze e degli obblighi che l'Azienda ha nei loro confronti, anche attraverso lo studio dei documenti istituzionali.
Tra gli scopi dell'analisi del contesto esterno c'è quello di evidenziare le ripercussioni che le eventuali inefficienze dell'Ente possono avere nell'ambiente in cui opera.
Anche l'analisi del contesto interno parte dall'analisi della documentazione istituzionale dell'Ente, della Macro Organizzazione e delle relative declaratorie, delle competenze di ciascuna unità, organizzative e delle relazioni esistenti tra di esse.
Come previsto dalle Policy, la gestione del rischio è volta all'individuazione preventiva dei processi e dei procedimenti amministrativi dell'Ente maggiormente esposti a rischi e non riguarda i rischi tecnici dei programmi istituzionali dell'Ente. L'analisi del contesto, quindi, sarà orientata all'analisi dei procesi mappati e delle attività in essi svolte.
Per ogni processo sono idenficati il Process Owner e il Risk Owner.

3.2 Valutazione del rischio

In questa fase vengono identificati i rischi, i fattori abilitanti, vengono valorizzati i parametri per la misura della probabilità e dell'impatto di ciascun rischio, viene valorizzato il controllo esistente sull'attività soggetta al rischio e vengono identificate le eventuali azioni di mitigazione.
Per tali ragioni questa fase è la più critica e richede la massima attenzione.Viene svolta insieme al Process Owner ed è raccomandato che preveda il coinvolgimento dei responsabili di tutte le strutture operative coinvolte nel processo.
Sono previsti degli incontri singoli con le Direzioni e le Unità organizzative nelle quali il team di Risk Management descriverà innanzitutto gli obiettivi della Gestione del Rischio, illustrando come essa possa portare ad un miglioramento nel proprio lavoro.
Di seguito si descrivono le attività che compongono la fase di valutazione del rischio.

3.2.1 Identificazione del rischio

Questa è la parte più importante perché è quella in cui si analizzano le attività svolte nei singoli processi amministrativi con lo scopo di rilevarne i rischi e i fattori abilitanti.
Ci sono molte metodologie per l'identificazione dei rischi ciascuna basata su criteri e approcci differenti. La norma di riferimento, ovvero la ISO 31010 "Risk assessment Techniques", descrive in maniera dettagliate ben 41 tecniche di identificazione e valutazione dei rischi che vanno dal classico brainstorming alle metodologie più strutturate. La scelta ovviamente dipende dalla realtà che si deve analizzare.
L'elemento comune a queste metodologie è comunque quello di stimolare il personale ad identificare in modo più compiuto e dettagliato possibile gli elementi variabili del proprio lavoro e del contesto in cui si svolge, che possono portare a risultati diversi da quelli attesi.
L'attività di identificazione del rischio viene svolta con il pieno coinvolgimento del Process Owner al quale viene chiesto prima di tutto di descrivere in modo ampio e completo il processo (laddove non già presente una mappatura aggiornata del processo), le fasi e le attività che la compongono, identificando i documenti, i soggetti coinvolti e gli obiettivi, e infine di indicare quali sono i punti più critici del processo e gli eventi rischiosi che possono intervenire, non solo rispetto alle proprie esperienze ma anche in relazione ad eventi e prospettive che non vengono normalmente presi in considerazione.
Al termine dell'incontro sono identificati i rischi per i quali si valuta essere necessario procedere con la loro valutazione, ponderazione e trattamento.

3.2.2 Valutazione del Rischio inerente

Il rischio inerente è il rischio rilevato sulla base della probabilità e dell'impatto dell'evento rischioso, prima della valutazione delle eventuali attività di controllo già poste in essere finalizzate ad impedire l'evento rischioso rilevato.
Per **valutare la probabilità** dell'evento rischioso sono somministrate al Process Owner delle domande specifiche formulate anche sulla base delle seguenti leve e di cui alla tabella 3:

- **frequenza:** se e **quante volte è l'evento** si è già presentato nel passato,
- **complessità:** quanto **complessa e difficile è l'attività**,
- **formazione ed esperienza:** quanta **esperienza e formazione** specifica possiede il personale che la svolge,
- **discrezionalità:** quanto **soggettivo e discrezionale** è il suo svolgimento,

- **performance/motivazione:** se e come l'attività è **collegata ad obiettivi di performance** e quindi è soggetta a monitoraggio.

Dalle risposte ottenute dal Process Owner, il Risk manager assegna un punteggio compreso tra 1 e 5 a ciascuno degli elementi di valutazione tenendo conto dei parametri riportati nella Tabella di valutazione della probabilità relativi al rischio e all'attività soggetta all'evento rischioso (Appendice A, Tabella 3).
Sulla base delle valutazioni si individua il livello di probabilità di accadimento dell'evento rischioso (es: calcolando la media dei valori assegnati a ciascuna leva). Ad ogni punteggio finale si assegnano i seguenti significati:

Punteggio 1 = Raro
Punteggio 2 = Poco probabile
Punteggio 3 = Probabile
Punteggio 4 = Molto Probabile
Punteggio 5 = Altamente probabile.

Successivamente sono somministrate al Process Owner delle domande formulate anche sulla base della tabella n. 4, per valutare il livello di impatto in funzione delle seguenti leve:

- **economico** (perdite economiche dirette, maggiori costi rispetto alle stime)
- **operativo** (maggiori tempi di esecuzione e/o di risorse, impatto sugli obiettivi di perfomance
- **strategico** (impatto sugli obiettivi istituzionali dell'Ente)
- **reputazionale** (immagine dell'Ente verso gli stakeholders)
- **compliance normativa** (rispetto delle norme, dei regolementi e delle procedure)

Dalle risposte ottenute dal Process Owner si assegnerà un punteggio compreso tra 1 e 5 a ciascuno degli elementi di valutazione tenendo conto dei parametri riportati nella Tabella di valutazione dell'impatto dell'evento rischioso (Appendice A, Tabella 4).
Sulla base di quanto valutato (es: calcolando la media dei valori assegnati a ciascuna leva), si procede all'individuazione dell'impatto dell'evento rischioso assegnando ad ogni punteggio i seguenti significati:

Punteggio 1 = Irrilevante
Punteggio 2 = Basso
Punteggio 3 = Moderato
Punteggio 4 = Elevato
Punteggio 5 = Molto elevato

Il rischio inerente si valuta moltiplicando la probabilità per l'impatto dell'evento rischioso secondo la matrice riportata nella figura seguente:

Tabella 1.

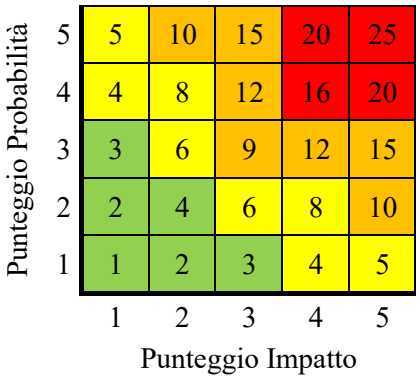
Punteggio Probabilità					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Punteggio Impatto				

Il valore del rischio inerente è indicato nella seguente tabella.

Tabella 2

Valore Rischio Inerente
da 1 a 4 = basso
da 5 a 8 = moderato
da 9 a 15 = alto
da 16 a 25 = altissimo

I valori della tabella 2 sono definiti e condivisi con il vertice dell'Amministrazione (direzione generale).



3.2.3 *Valutazione dei fattori abilitanti e dei controlli*

La valutazione del controllo avviene analizzando le eventuali attività già esistenti che abbiano la funzione di prevenire i rischi e/o di assicuare le modaltà gestionali/organizzative/operative ritenute adeguate e congrue dal management dell'Ente. Al Process Owner viene chiesto di descrivere in modo ampio e dettagliato i controlli esistenti in relazione all'evento rischioso e alla fase soggetta all'evento rischioso.
Prima della valutazione dei controlli, si valuta la maturità dei fattori abilitanti individuati per gli eventi rischiosi. La valutazione avviene attraverso la somministrazione di domande. Ad esempio:

Punteggio 1 = Non siamo attivi in questo campo. Il fattore abilitante non è gestito o non è presente in nessuna procedura;
Punteggio 2 = Un approccio è stato pianificato;
Punteggio 3 = La gestione del fattore abilitante è implementata;
Punteggio 4 = Il fattore abilitante è gestito nella documentazione che regola il processo. L'Ente monitora sistematicamente la sua efficacia mediante indicatori e apporta i correttivi regolarmente.

3.2.4 *Valutazione dell'organizzazione dei controlli interni esistenti*

Con questa operazione si valuta l'efficacia complessiva dei controlli esistenti **nella fase** del processo in base alla loro organizzazione interna e in relazione ai **rischi rilevati**. Il Risk manager, con il supporto del Process Owner, valuta il controllo della fase del processo assegnando un punteggio sulla base delle seguenti considerazioni assegnando un punteggio da **1 a 5** (es: media aritmetica)**:**
Punteggio 1 = i controlli sono assenti
Punteggio 2 = i controlli sono presenti ma non formalizzati e/o poco strutturati
Punteggio 3 = i controlli sono strutturati (anche solo in parte, più del 50%) e/o formalizzati (anche solo in parte, più del 50%) ma attivi e/o i risultati sono solo in parte oggetto di reporting
Punteggio 4 = i controlli sono strutturati e formalizzati - sono quasi pienamente attivi e/o i risultati sono oggetto di reporting nella maggior parte dei casi
Punteggio 5 = i controlli sono presenti, formalizzati, strutturati, attivi e i risultati sono sistematicamente oggetto di reporting.

3.2.5 Valutazione dell'efficacia dei controlli interni esistenti

Con questa operazione si valuta l'efficacia dei controlli esistenti nella fase del processo in base alla forza di gestione/trattamento dei rischi rilevati. Il Risk manager, con il supporto del Process Owner, **valuta il controllo per ciascun evento rischioso** assegnando un punteggio sulla base delle seguenti considerazioni assegnando un punteggio da **1 a 5** (es.: media aritmetica):

Punteggio 1: => l'evento rischioso rimane indifferente e non è gestito;
Punteggio 2: => l'evento rischioso è gestito, ma in minima parte;
Punteggio 3:=> l'evento rischioso è gestito per una percentuale di circa del 50% (casistica di accadimento degli eventi rischiosi);
Punteggio 4: => l'evento rischioso è gestito in modo molto efficace;
Punteggio 5: => il controllo attivo costituisce strumento di neutralizzazione dell'evento rischioso.

La valutazione è individuata moltiplicando il livello di organizzazione dei controlli con l'efficacia dei controlli interni.

3.3 Ponderazione del rischio

3.3.1 Valutazione Rischio e dei controlli: rischio risiduale

Le valutazioni del rischio e del controllo interno sono oggetto di un'analisi di coerenza, e quindi confermando o variando quanto emerso, sulla base del contesto e delle valutazioni sulla maturità dei fattori abilitanti.
Le valutazioni complessive del rischio e dei controlli interni sono oggetto di debriefing e condivisione con il Process owner per rilevare cricità o ulteriori elementi informativi correttivi e per successivo loro consolidamento.

Il valore del rischio residuo si ottiene confrontanto il valore del controllo al valore del rischio inerente.

3.3.2 Valutazione Risk appetite e Rischio finale

Il Risk appetite indica il livello di valutazione di rischo che l'Ente è disposto ad accettare.
Dalla combinazione del risk appetite e del livello di rischio residuale si possono distinguere 3 aree di intervento:

- area di rischio che richiede un intervento immediato;
- area in cui sono presenti controlli eccessivi rispetto alle reali esigenze;
- area correttamente presidiata.

La valutazione del risk appetite viene svolta dal Risk manager ma sulla base delle indicazioni del vertice dell'Ente.

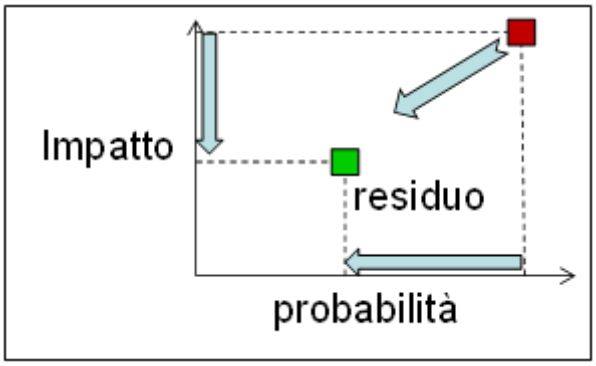
3.3.3 Identificazione degli elementi di Controllo interno

Per ogni rischio rilevato è identificato l'elemento del controllo interno coinvolto, sulla base di quanto descritto dalle Policy nel paragrafo 4.3.
Lo scopo è quello di utilizzare le informazioni che emergono dall'analisi dei rischi per la verifica e l'eventuale aggiornamento degli elementi del controllo interno, identificando così i punti di debolezza e di forza interni all'organizzazione.
Nell'Appendice A, tabella n. 5, è riportato lo schema di raccordo tra gli elementi del controllo interno e le aree di rischio che valorizza e massimizza l'utilizzo delle risultanze emerse dalle attività di valutazione del rischio.
L'output della fase di valutazione del rischio è inserito nel Registro dei Rischi il cui formato è riportato nella tabella 6 dell'Appendice A.

3.4 Trattamento del rischio

In questa fase vengono identificate e pianificate tutte le azioni mirate a diminuire i rischi per i quali è stato deciso di intervenire.
Le azioni di mitigazione dei rischi sono individuate per tutti quei processi in cui sono presenti eventi rischiosi con un alto livello di rischio e senza un adeguato presidio in termini di controllo interno. Le azioni sono poste in essere al fine di gestire gli eventi rischiosi e ricondurre il rischio a valori accettabili.

Le azioni di mitigazione consistono in qualsiasi azione (controllo) che sia in grado di contenere il livello di rischio agendo sulla probabilità (controllo interno attenuatore della probabilità) o sull'impatto (controllo interno attenuatore dell'impatto), oppure su entrambi. L'implementazione delle azioni di mitigazione dovrebbe nel tempo restituire un valore residuale del rischio accettabile.



Graf. 1 - Effetti delle azioni di mitigazione

3.4.1 Identificazione dei Risk Owner e delle azioni di mitigazione

Le azioni di mitigazione sono identificate dai Process Onwer (con l'eventuale supporto metodologico del Risk Manager) e assegnate ai Risk Owner.
Le azioni di mitigazione sono generalmente selezionate tra i "controlli ideali" e sulla base dei fattori abilitanti, individuati nella fase di analisi e di confronto con il process owner.
Per procedere all'individuazione delle azioni di mitigazione, si suggerisce di svolgere una sessione di brainstorming per analizzare tutte le informazioni acquisite: la natura del rischio, le cause che generano il rischio (fattori che agevolano l'insorgere del rischio), la criticità degli effetti, i fattori attenuanti (per impatto e probabilità) che possono agire sul livello del rischio;

- un'analisi di affinità e di interrelazione delle cause rilevate;
- la rilevazione dei punti di forza e i punti di debolezza del processo che genera i rischi da mitigare sulla base delle informazioni acquisite;
- un'analisi dei controlli interni rilevati durante la mappatura dei processi (es.: controlli solo pianificati e non implementati, in funzione del criterio di accettabilità del rischio);
- un'analisi dei costi/benefici attesi in seguito all'implementazione delle azioni di mitigazione selezionate.

Le azioni di mitigazione possono essere selezionate (in termini di priorità) sulla base dei seguenti criteri:

- livello di esposizione al rischio del processo a cui l'azione si riferisce (estremo, alto, moderato …);
- impatto dell'azione di mitigazione sugli obiettivi strategici (alto, medio, basso, nullo);
- livello di accettazione del rischio da parte dell'Ente;
- facilità di implementazione dell'azione di mitigazione (livello di interdisciplinarietà richiesto e di specializzazione);
- risorse (finanziarie e materiali) necessarie per l'implementazione;
- tempi di realizzazione.

In Appendice A, tabella 7, si riporta lo schema che riepiloga le azioni di monitoraggio e mitigazione identificate**.** Ciascuna azione dovrà essere ampiamente descritta indicando l'impatto atteso sul valore del relativo rischio e la pianificazione temporale della sua implementazione.
L'output di questa fase è il Piano di gestione e mitigazione dei rischi.

3.5 Monitoraggio e riesame

L'attività di monitoraggio consiste nella verifica periodica dello stato di avanzamento delle azioni di mitigazione.
Ai Risk Owner viene chiesto di riportare periodicamente al Risk manager lo stato di avanzamento di ciascuna azione e di comunicare tempestivamente ogni situazione che possa pregiudicare il rispetto delle pianificazioni previste e l'efficacia delle azioni..
L'output di questa fase è il Report periodico sulle attività di gestione dei rischi.

Le risultanze dei controlli interni, laddove efficaci, hanno un impatto sulla valutazione del controllo interno e sul loro stato di maturità.

APPENDICE A

Tabella 3. – Valorizzazione della probabilità – *Elementi indicativi*

	Punteggio				
Leve	**5 - Altamente probabile**	**4 - Molto Probabile**	**3 - Probabile**	**2 - Poco Probabile**	**1 - Raro**
Frequenza evento /casistica	L'evento negativo si è presentato con normalità (con una casistica superiore al 50%) negli ultimi 5 anni	L'evento negativo si è presentato spesso (con una casistica compresa tra il 30% e il 50%) negli ultimi 5 anni	L'evento negativo si è presentato sporadicamente (con una casistica maggiore del 10% e minore del 30%) negli ultimi 5 anni	L'evento negativo si è presentato raramente (con una casistica inferiore al 10%) negli ultimi 5 anni	L'evento negativo non si è mai presentato negli ultimi 5 anni
complessità e difficoltà dell'attività /competenze rischieste	l'attività è particolarmente complessa e richiede competenze ed esperienza specifiche del contesto operativo dell'Ente	l'attività non è particolarmente complessa ma richiede competenze ed esperienze specifiche del contesto operativo dell'Ente	l'attività è complessa e richiede competenze ed esperienze della materia ma non specifiche del contesto operativo dell'Ente	l'attività non è complessa e non richiede particolari competenze ed esperienze	l'attività è molto semplice e non richiede particolari competenze ed esperienze
formazione esperienza	Il personale che svolge l'attività (o dell'ufficio preposto) non ha esperienza né formazione specifica	Il personale che svolge l'attività ha mediamente poca esperienza (inferiore a 3 anni) e non ha seguito corsi di formazione e/o aggiornamento	Il personale che svolge l'attività ha mediamente una buona esperienza (superiore a 3 anni) e non ha seguito corsi di aggiornamento recenti (negli ultimi 3 anni)	Il personale che svolge l'attività ha mediamente una discreta esperienza (superiore a 5 anni) e ha seguito almeno un corso di aggiornamento recente (negli ultimi 3) anni	Il personale che svolge l'attività ha mediamente un'elevata esperienza (superiore a 10 anni) e ha seguito più di un corso di aggiornamento recente (negli ultimi 3 anni)
soggettività discrezionalità	l'attività non è regolamentata	l'attività è regolamentata da prassi consolidata o da Policy	l'attività è regolamentata dalla normativa	l'attività è regolamentata da regolamenti interni senza procedure con istruzioni operative	l'attività è regolamentata da regolamenti interni con procedure con istruzioni operative
performance motivazione	l'attività non è collegata a nessun obiettivo di performance	l'attività è collegata indirettamente ad un obiettivo di performance	l'attività è collegata direttamente ad un obiettivo di performance	l'attività ha un proprio obiettivo di performance	l'attività ha un proprio obiettivo di performance oggetto di monitoraggio della performance

Tabella 4. – Valorizzazione impatto – *Elementi indicativi*

	Punteggio				
Leve	**5 - Elevatissimo**	**4 - Elevato**	**3 - Moderato**	**2 - Basso**	**1 - Irrilevante**
Economico (perdite economiche dirette, maggiori costi rispetto alle stime)	L'evento rischioso può determinare direttamente danni economici significativi rispetto al budget dell'Ente	L'evento rischioso può determinare indirettamente danni economici significativi rispetto al budget dell'Ente	L'evento rischioso può determinare direttamente danni economici non rilevanti	L'evento rischioso può determinare danni economici ma solo indirettamente	l'evento non ha impatto economico diretto o indiretto
Operativo (tempi di esecuzione, aggravio di risorse, impatto sugli obiettivi di perfomance)	L'evento è bloccante e determina l'impossibilità di portare a termine il processo e/o di raggiungere obiettivi di performance di ente	L'evento determina un ritardo nei tempi e/o un aggravio di risorse e/o di mancato raggiungimento di obiettivi delle performance, superiori al 50%	L'evento determina un ritardo nei tempi e/o un aggravio di risorse e/o di mancato raggiugimento di obiettivi delle performance, superiori al 20%	L'evento determina un ritardo nei tempi e/o un aggravio di risorse e/o di mancato raggiugimento di obiettivi delle performance, superiori al 10%	L'evento non determina alcun ritardo nei tempi o aggravio di risorse o impatto su obiettivi di performance
Strategico (finalità istituzionali)	L'evento determina in modo diretto il mancato raggiungimento di più di uno o più obiettivi istituzionali PTA e/o DVSS	L'evento causa il mancato raggiungimento in modo anche indiretto degli obiettivi istituzionali strategici PTA	L'evento può determinare il raggiungimento parziale di uno o più obiettivi istituzionali strategici (PTA), anche in modo indiretto	L'evento può causare, ma solo potenzialmetne e in via indiretta, il raggiungimento parziale di uno o più obiettivi istutizionali strategici (PTA)	L'evento non determina impatti sugli obiettivi istituzionali strategici (PTA, DVSS)
Reputazionale (immagine dell'Ente verso gli stakholders)	L'evento ha impatto con molti soggetti esterni particolarmente rilevanti per l'Ente per interesse e influenza e comporta possibili danni di immagine (pubblicazioni su quotidiani nazionali)	L'evento ha impatto con molti soggetti esterni ma non particolarmente rilevanti per interesse/influenza	L'evento ha impatto con un solo soggetto esterni ma particolarmente rilevanti per interesse/influenza	L'evento ha impatto con un solo soggetto esterni ma non particolarmente rilevanti per interesse/influenza	L'evento non ha impatti su soggetti interni ed esterni
Compliance normativa (rispetto delle norme, dei regolementi e delle procedure)	L'evento determina violazioni delle leggi	L'evento determina delle non conformità dei regolamenti (aspetti non collegati a disposizione di legge) o delle prassi e/o procedure interne (quest'ultime con una cadenza sistematica e strutturale)	L'evento genera delle non conformità delle prassi e/o procedure interne (ma non risultano evidenze di sistematicità)	L'evento genera delle non conformità ma lievi e comunque rispetto ad una modalità non formalizzata interna	L'evento non genera non conformità

Tabella 5. – Elementi del Controllo interno

ELEMENTI DI CONTROLLO INTERNO	AREE DA CONSIDERARE NELLA FASE DI IDENTIFICAZIONE DEI RISCHI
ICS 1. MISSIONE E VALORI	Comportamenti etici e organizzativi Chiarezza, adeguatezza e coerenza nell'applicazione delle Leggi, regolamenti e altre norme Organizzazione interna Strategie
ICS 2. RISORSE UMANE	Risorse umane Organizzazione interna (ruoli e responsabilità, gestione competenze, sistema deleghe, …) Sicurezza del personale
ICS 3. PROCESSI DI PIANIFICAZIONE E VALUTAZIONE DEI RISCHI	Processi operativi Policy e pianificazione, incluse decisioni politiche interne Qualità e tempestività delle informazioni Sicurezza della struttura Ambiente esterno (eventi economici, decisioni legislatore) Partner esterni Assunzioni risorse umane e disponibilità competenze
ICS 4. OPERAZIONI E ATTIVITÀ DI CONTROLLO (con riferimento alle aree che riportano direttamente o indirettamente alla Direzione Generale)	Conformità alle Leggi, norme e regolamenti Altre cause collegate alla legalità e regolarità Conflitto di interessi Qualità e tempestività delle informazioni Processi operativi (ciclo Performance) Organizzazione interna (ruoli e responsabilità, governance)
ICS 5. INFORMAZIONE E REPORTING	Metodi e canali di comunicazione Qualità e tempestività delle informazioni Processi operativi (controlli operativi, monitoraggio, analisi)
ICS 6. VALUTAZIONE E AUDIT	Strategie, policy e pianificazione, incluse decisioni politiche Eventi economici Decisioni legislatore Partner esterni Adeguatezza applicazione Leggi e norme Processi operativi (ciclo Performance) Organizzazione interna (governance, sistema deleghe) Sicurezza del personale e della struttura Comportamenti etici (frodi e altri illeciti

Tabella 6. – Esempio di Registro dei Rischi

Processo / Fasi	**Process Owner**	**Eventi Rischiosi**	**Tipologia Rischio** (operativo, strategico, reputazionale, conformità)	**Livello di rischio (1-4)**	**Valutazione Rischio inerente (1-25)**	**Valutazione controllo (1-25)**	**Rischio residuale** (intervento/presidio/non rilevante)	**Risk appetite** (intervento/presidio/non rilevante)	**Priorità** (Altissimo, Alto, medio, basso)	**Elementi Controllo Interno**	**Azioni di mitigazione**	**Risk Owner**

Tabella 7. – Piano delle azioni di mitigazione

Processo/ Fasi	Process Owner	Azione di mitigazione/monitoraggio	Risk Owner	Livello di rischio residuale a tendere (1-4)	Data inizio implementazione	Data fine implementazione