

UNI/PdR xx:2026	Framework per la gestione del rischio – Requisiti
Sommario	La presente Prassi di Riferimento definisce requisiti per sviluppare, attuare, monitorare, riesaminare e migliorare un framework per la gestione del rischio integrato nella governance, nei processi decisionali e nelle attività operative dell'organizzazione. In particolare, la prassi disciplina: • ruoli, responsabilità e flussi decisionali connessi alla gestione del rischio; • le principali fasi operative di comunicazione e consultazione, campo di applicazione, contesto e criteri, valutazione e di trattamento del rischio; • le attività di riesame e monitoraggio dei rischi, degli indicatori e dei piani di trattamento; • il coordinamento con i presidi specialistici e con le funzioni di controllo; • la diffusione della cultura del rischio e la formazione dei ruoli rilevanti; • il reporting, le informazioni documentate e le evidenze necessarie alla verifica della conformità.
Data	2026-xx-xx

AVVERTENZA

Il presente documento è un progetto di Prassi di Riferimento (UNI/PdR) sottoposta alla fase di consultazione, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti.

Il processo di elaborazione delle Prassi di Riferimento prevede che i progetti vengano sottoposti alla consultazione sul sito web UNI per raccogliere i commenti

del mercato: la UNI/PdR definitiva potrebbe quindi presentare differenze rispetto al documento messo in consultazione.

Questo documento perde qualsiasi valore al termine della consultazione, cioè il: 6 novembre 2026.

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti di Prassi di Riferimento in consultazione.

PREMESSA

La presente prassi di riferimento UNI/PdR xx:2026 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento UE n.1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno del seguente soggetto firmatario di un accordo di collaborazione con UNI:

TERNA S.p.A

Via Egidio Galbani, n. 70

Roma

La presente prassi di riferimento è stata elaborata dal Tavolo “Gestione del rischio per organizzazioni di grandi dimensioni” condotto da UNI, costituito dai seguenti esperti:

Nome Cognome 1 – Project Leader (organizzazione xyz)

Nome Cognome 2 (organizzazione yz)

Nome Cognome 3 (organizzazione xyz)

Nome Cognome 4 (organizzazione y)

Nome Cognome 5 (organizzazione xz)

Nome Cognome 6 (organizzazione z)

La presente prassi di riferimento è stata ratificata dal Presidente dell'UNI il xx xxxx 2026.

Le prassi di riferimento, adottate esclusivamente in ambito nazionale, rientrano fra i “prodotti della normazione europea”, come previsti dal Regolamento UE n.1025/2012, e sono documenti che introducono prescrizioni tecniche, elaborati sulla base di un rapido processo ristretto ai soli autori, sotto la conduzione operativa di UNI.

Le prassi di riferimento sono disponibili per un periodo non superiore a 5 anni, tempo massimo dalla loro pubblicazione entro il quale possono essere trasformate in un documento normativo (UNI, UNI/TS, UNI/TR) oppure devono essere ritirate.

Chiunque ritenesse, a seguito dell'applicazione della presente prassi di riferimento, di poter fornire suggerimenti per un suo miglioramento è pregato di inviare i propri contributi all'UNI, Ente Italiano di Normazione, che li terrà in considerazione.

SOMMARIO

INTRODUZIONE	7
0.1 Generalità	7
0.2 Principi.....	8
1 SCOPO E CAMPO DI APPLICAZIONE	8
2 RIFERIMENTI NORMATIVI E LEGISLATIVI.....	8
3 TERMINI E DEFINIZIONI	9
4 PRINCIPIO	15
5 REQUISITI GENERALI DEL FRAMEWORK PER LA GESTIONE DEL RISCHIO	16
5.1 Comprensione del contesto e delle parti interessate	16
5.2 Definizione campo di applicazione	17
5.3 Integrazione con governance, processi e altri sistemi	17
5.4 Criteri di rischio	17
5.5 Elementi essenziali del framework	18
6 LEADERSHIP, GOVERNANCE E RESPONSABILITÀ	18
6.1 Leadership e impegno.....	18
6.2 Politica per la gestione del rischio	18
6.3 Ruoli, responsabilità e autorità	19
6.3.1 Organo di governo.....	19
6.3.2 Alta Direzione	19
6.3.3 Funzione ERM o presidio equivalente.....	19
6.3.4 Prima linea, seconde linee e terza linea	20
6.3.5 Escalation e decisioni	20
7 PIANIFICAZIONE DEL FRAMEWORK E SUA APPLICAZIONE	20
7.1 Obiettivi del framework per la gestione del rischio	20
7.2 Pianificazione delle attività ERM	20
7.3 Pianificazione delle modifiche	21

8	SUPPORTO, RISORSE, FORMAZIONE, CULTURA DEL RISCHIO E INFORMAZIONI DOCUMENTATE	21
8.1	Generalità	21
8.2	Competenza	21
8.3	Formazione	22
8.4	Consapevolezza e cultura del rischio	22
8.5	Comunicazione	22
8.6	Informazioni documentate	23
9	ATTIVITÀ OPERATIVE DEL PROCESSO DI RISCHIO	23
9.1	Pianificazione e controllo operativo del processo	23
9.2	Identificazione dei rischi	23
9.3	Analisi e ponderazione del rischio	23
9.4	Accettazione del rischio, priorità ed escalation	24
9.5	Trattamento del rischio	24
9.6	Monitoraggio di rischi, indicatori e piani	25
9.7	Coordinamento con seconde linee e presidi specialistici	25
9.8	Reporting integrato	25
10	VALUTAZIONE DELLE PRESTAZIONI	26
10.1	Monitoraggio, analisi e valutazione del framework	26
10.2	Audit interno	26
10.3	Riesame di direzione	26
11	MIGLIORAMENTO	27
11.1	Non conformità e azioni correttive	27
11.2	Miglioramento continuo e apprendimento	27
12	VALUTAZIONE DI CONFORMITÀ	28
	APPENDICE A – Valutazione di conformità di terza parte	29
	APPENDICE B – Criteri di supporto per l'applicazione proporzionata	32

APPENDICE C - Esempio di contenuti raccomandati per il registro dei rischi e il reporting.....	33
APPENDICE D – Indicazioni operative per il coordinamento con seconde linee di controllo	33
APPENDICE E - Matrice RACI del framework per la gestione del rischio	34
APPENDICE F - Esempi di evidenze documentate, versioning e criteri di conservazione.....	34
APPENDICE G - Matrice requisito, evidenza e criterio di verifica	35
APPENDICE H – Correlazione tra i punti della presente Pdr, della UNI ISO 31000:2018 e della UNI 11865:2022.....	39
BIBLIOGRAFIA.....	41

INTRODUZIONE

0.1 Generalità

La presente Prassi di Riferimento definisce i requisiti per sviluppare, attuare, riesaminare e migliorare un framework per la gestione del rischio integrato nella governance, nei processi decisionali e nelle attività operative dell'organizzazione. L'obiettivo non è descrivere soltanto un processo di risk assessment, ma definire un insieme coerente di presidi minimi, responsabilità, flussi decisionali, evidenze documentate e meccanismi di verifica tali da consentire un'applicazione omogenea del risk management in contesti differenti.

La prassi è stata costruita con un duplice criterio: da un lato mantenere la coerenza con i principi della gestione del rischio riconosciuti a livello internazionale; dall'altro tradurli in requisiti sufficientemente chiari da poter essere verificati. Il testo adotta pertanto una formulazione neutra e generalista nel corpo principale, rinviando alle appendici informative eventuali esempi e modalità applicative dello specifico requisito.

La prassi intende inoltre favorire l'uso del framework per la gestione del rischio come leva di integrazione delle varie discipline nel sistema di gestione, raccordando presidi specialistici e funzioni di controllo eventualmente presenti nell'organizzazione, al fine di migliorare la coerenza delle informazioni, evitare duplicazioni, valorizzare le evidenze già disponibili e supportare decisioni integrate.

La presente prassi assume il rischio in coerenza con la definizione di effetto dell'incertezza in relazione agli obiettivi. L'applicazione dei requisiti è orientata a cogliere le opportunità facendo leva sui punti di forza (abilità) mentre si contrastano possibili effetti negativi derivanti da minacce, pericoli in grado di sfruttare e punti di debolezza (vulnerabilità).

Sebbene alcuni distinguano tra le azioni per affrontare le minacce e quelle per cogliere le opportunità, tutte le organizzazioni possono trarre vantaggio da un processo strutturato e sistematico che integri entrambe le classi di azioni, coinvolgendo le parti interessate.

La presente prassi tiene conto, in particolare, delle esigenze di:

- chiarire la natura del documento;
- definire gli elementi essenziali del framework;
- rendere operativo il principio di proporzionalità;
- impostare criteri di verifica e valutazione della conformità;
- formalizzare il richiamo ai termini e alle definizioni UNI/ISO;
- esplicitare i requisiti in merito alla formazione e cultura del rischio;
- disciplinare in modo proporzionato l'accettazione del rischio anche in assenza di un Risk Appetite Framework formalizzato.

0.2 Principi

Nell'applicazione della presente prassi è utile considerare:

- i principi che sono alla base della gestione del rischio (punto 4 della UNI ISO 31000:2018) che partono dal mettere in evidenza quello che è lo scopo fondamentale della gestione del rischio: la creazione e la protezione del valore;
- gli approfondimenti contenuti nell'Appendice A della UNI 11865:2022 e relativi alle norme che, nei principi, hanno alcuni aspetti in comune con quelli della UNI ISO 31000:2018 e sulle sinergie che possono essere sfruttate con l'obiettivo di intraprendere un percorso verso l'eccellenza nella propria organizzazione.

1 SCOPO E CAMPO DI APPLICAZIONE

La presente Prassi di Riferimento definisce i requisiti minimi per sviluppare, attuare, mantenere, riesaminare e migliorare un framework di gestione del rischio integrato nella governance, nei processi decisionali e nelle attività operative dell'organizzazione. Il framework deve essere coerente con il contesto, le dimensioni e la complessità organizzativa, adeguatamente documentato per consentire attività di verifica interne ed esterne e orientato al miglioramento continuo. La Prassi promuove inoltre l'adozione di un linguaggio comune e di un approccio metodologico condiviso tra funzioni operative, funzioni di controllo e organi di governo.

La presente Prassi è applicabile a organizzazioni di qualsiasi natura, pubbliche, private o del terzo settore, indipendentemente dal settore di attività e dalle dimensioni. Sebbene sia stata sviluppata con particolare riferimento alle realtà medio-grandi, può essere adottata da qualsiasi organizzazione. L'applicazione può riguardare l'intera organizzazione oppure, qualora adeguatamente motivato e documentato, un perimetro specifico, come una società, una business unit, un processo, un programma o un progetto.

2 RIFERIMENTI NORMATIVI E LEGISLATIVI

La presente Prassi di Riferimento rimanda, mediante riferimenti datati e non, a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi e legislativi sono citati nei punti appropriati del testo e sono di seguito elencati. Per quanto riguarda i riferimenti datati, successive modifiche o revisioni apportate a dette pubblicazioni valgono unicamente se introdotte nel presente documento come aggiornamento o revisione. Per i riferimenti non datati vale l'ultima edizione della pubblicazione alla quale si fa riferimento.

UNI 11865:2022 Gestione del rischio - Linea guida per l'integrazione della gestione del rischio nella governance e nelle attività operative di un'organizzazione in accordo alla UNI ISO 31000, con particolare riferimento ai sistemi di gestione basati sulle norme ISO che seguono la struttura di alto livello (HLS)

UNI 12012:2026 Attività professionali non regolamentate - Professionista della gestione del rischio (Risk manager) - Requisiti di conoscenza, abilità, autonomia e responsabilità

UNI CEI EN IEC 31010:2019 Risk management - Risk assessment techniques

UNI ISO 31000:2018 Gestione del rischio - Linee guida

UNI ISO 37000:2021 Governance delle organizzazioni - Guida

3 TERMINI E DEFINIZIONI

Ai fini del presente documento si applicano i termini e le definizioni seguenti.

Accettazione del rischio (*Risk acceptance*): decisione informata di correre un particolare rischio.

Nota 1: l'accettazione del rischio può avvenire senza trattamento del rischio o durante il processo di trattamento del rischio.

Nota 2: i rischi accettati sono soggetti a monitoraggio e riesame.

[Fonte: UNI ISO 31073:2022, 3.3.31]

Alta direzione (*Top management*): persona o gruppo di persone che, al livello più elevato, guidano e tengono sotto controllo un'organizzazione.

Nota 1: l'alta direzione ha il potere di delegare le autorità e mettere a disposizione le risorse all'interno dell'organizzazione.

Nota 2: se il campo di applicazione del sistema di gestione copre solo parte di un'organizzazione, il termine "alta direzione" si riferisce a coloro che guidano e tengono sotto controllo quella parte dell'organizzazione stessa.

Nota 3: l'alta direzione ha l'obbligo di rendere conto delle proprie decisioni, anche quando esercita il potere di delega.

[Fonte: UNI 11865:2022, 3.5]

Analisi del rischio (*Risk analysis*): processo per comprendere la natura del rischio e per determinare il livello di rischio.

Nota: l'analisi del rischio fornisce la base per la ponderazione del rischio e le decisioni circa il trattamento del rischio.

[Fonte: UNI ISO 31073:2022, 3.3.15]

Azione correttiva (*Corrective action*): azione per eliminare la causa di una non conformità e prevenirne la ripetizione.

[Fonte: UNI 11865:2022, 3.20]

Audit di gestione del rischio (*risk management audit*): processo sistematico, indipendente e documentato per ottenere evidenze e valutarle in modo obiettivo al fine di determinare in quale misura il framework per la gestione del rischio, o qualsiasi parte selezionata di esso, è adeguato ed efficace.

[Fonte: UNI ISO 31073:2022, 3.3.43]

Comunicazione e consultazione (*Communication and consultation*): Processi continui ed iterativi che un'organizzazione attua per fornire, condividere od ottenere informazioni e per coinvolgere le parti interessate in un dialogo.

Nota 1: La comunicazione implica la condivisione delle informazioni, mentre la consultazione implica l'ottenere informazioni di ritorno complete e tali da essere di supporto al processo decisionale.

Nota 2: la consultazione è un processo bidirezionale di comunicazione tra un'organizzazione e le proprie parti interessate. Un processo volto alla ricerca di pareri che costituiscono elementi in ingresso

al processo decisionale esercitando influenza; non è un processo decisionale congiunto, per il quale si usa il termine “partecipazione”

Nota 3: nell’ambito della gestione del rischio, comunicazione e consultazione sono volte a:

- mettere insieme differenti aree di competenza per ogni fase del processo di gestione del rischio;
- assicurare che differenti punti di vista siano adeguatamente presi in considerazione nel definire i criteri di rischio e nel ponderare i rischi;
- fornire informazioni sufficienti per facilitare la supervisione del rischio ed il processo decisionale;
- creare un senso di inclusione e di appartenenza tra coloro che sono influenzati dal rischio.

[Fonte: UNI 11865:2022, 3.39]

Conformità (*Conformity*): soddisfacimento di un requisito.

[Fonte: UNI 11865:2022, 3.18]

Conseguenza (*Consequence*): risultato di un evento che influenza gli obiettivi.

Nota 1: una conseguenza può avere effetti positivi o negativi, diretti o indiretti, sugli obiettivi.

Nota 2: le conseguenze possono essere espresse qualitativamente o quantitativamente.

Nota 3: qualunque conseguenza può amplificarsi attraverso effetti in cascata e di tipo cumulativo.

[Fonte: ISO 31073:2022, 3.3.18]

Controllo del rischio (*Risk control*): misura che mantiene e/o modifica il rischio.

Nota 1: i controlli del rischio comprendono, ma non solo, qualsiasi processo, politica, dispositivo, prassi, oppure altre condizioni e/o azioni che mantengano e/o modifichino il rischio.

Nota 2: può darsi che i controlli del rischio non esercitino sempre l’effetto di modifica previsto o presunto.

[Fonte: UNI ISO 31073:2022, 3.3.33]

Criteri di rischio (*Risk criteria*): termini di riferimento a fronte dei quali si valuta la significatività del rischio.

Nota 1: i criteri di rischio si basano sugli obiettivi dell’organizzazione e sul contesto esterno e interno.

Nota 2: i criteri di rischio possono avere origine da norme, leggi, politiche e altri requisiti.

Nota 3: la valutazione della significatività del rischio coincide con la fase di “ponderazione” nel processo di gestione del rischio.

Nota 4: i criteri di rischio rappresentano la discriminante fondamentale nelle diverse discipline per valutare la significatività dei rischi, definire e scegliere tra le opzioni di trattamento, supportare il processo decisionale, nei tre aspetti di governance (ambientale, sociale, economico)

[Fonte: UNI 11865:2022, 3.37]

Cultura del rischio (*Risk culture*): valori, etica, principi e opinioni che esistono all’interno di un’organizzazione e interagiscono con le strutture e i sistemi di controllo dell’organizzazione stessa per stimolare atteggiamenti mentali orientati al rischio e dare origine a norme comportamentali che favoriscano e stimolino l’attenzione di ciascuno nei confronti delle incertezze in relazione agli obiettivi.

Nota: la cultura, in generale, può essere definita come conoscenze, comprensioni, opinioni e valori condivisi da un gruppo di persone che hanno finalità comuni.

[Fonte: UNI 11865:2022, 3.25 – modificata parte finale della Nota da “finalità in comune” a “finalità comuni”]

Escalation (*Escalation*): meccanismo formalizzato mediante il quale rischi, superamento di soglia, eventi, criticità o ritardi, ritenuti rilevanti sulla base di criteri definiti dall'organizzazione, sono sottoposti ai livelli organizzativi superiori o agli organi competenti.

Evento (*Event*): il verificarsi o il modificarsi di un particolare insieme di circostanze.

Nota 1: un evento può consistere in uno o più episodi e può avere una pluralità di cause e di conseguenze.

Nota 2: un evento può anche essere qualcosa di previsto che non accade, o qualcosa di non previsto che invece accade.

Nota 3: un evento può essere una fonte di rischio.

[Fonte: UNI ISO 31073:2022, 3.3.11]

Fonte di rischio (*Risk source*): elemento che da solo o in combinazione possiede il potenziale di dare origine al rischio.

[Fonte: UNI ISO 31073:2022, 3.3.10]

Framework per la gestione del rischio, RMF (*Risk management framework*): Insieme di componenti che forniscono le fondamenta e gli assetti organizzativi per progettare, attuare, monitorare, riesaminare e migliorare in modo continuo la gestione del rischio nell'intera organizzazione.

Nota 1: Le fondamenta comprendono la cultura, il comportamento etico, la politica, gli obiettivi, il mandato e l'impegno per la gestione del rischio.

Nota 2: Gli assetti organizzativi comprendono piani, relazioni, responsabilità, risorse, processi e attività.

Nota 3: Il framework per la gestione del rischio è inserita all'interno delle politiche e prassi strategiche ed operative complessive dell'organizzazione.

Nota 4: Lo scopo del RMF è quello di integrare la gestione del rischio nei processi dell'organizzazione, mentre il sistema di gestione riguarda l'intera organizzazione per una o più discipline.

[Fonte: Adattata dalla UNI 11865:2022 punto 3.40 Modificato il termine da struttura a framework, aggiunto il comportamento etico in nota 1, modificata la nota 4 ed eliminata la nota 5].

Funzione ERM o presidio equivalente (*Enterprise risk management function or equivalent function*): struttura, ruolo o combinazione di ruoli cui sono attribuiti il presidio e l'aggiornamento della metodologia, il coordinamento dei cicli di valutazione del rischio, il consolidamento delle informazioni sui rischi, il supporto ai risk owner, il coordinamento con i presidi specialistici, la predisposizione della reportistica e la promozione del miglioramento del framework.

Nota: la denominazione, la collocazione e l'articolazione organizzativa della funzione o del presidio possono variare in relazione alle caratteristiche dell'organizzazione, purché i compiti e le responsabilità siano chiaramente attribuiti.

Gestione del rischio (*Risk management*): processo strutturato e sistematico basato sui principi e sulla cultura del rischio, costituito da un insieme di attività indirizzate a concretizzare opportunità potenziali mentre si gestiscono possibili effetti negativi, derivanti da minacce o pericoli.

Nota 1: La gestione del rischio può essere definita anche come “attività coordinate per guidare e tenere sotto controllo un’organizzazione con riferimento al rischio”.

Nota 2: I principi su cui si fonda la gestione del rischio sono trattati in UNI ISO 31000.

[Fonte: UNI 11865:2022, 3.22]

Identificazione del rischio (*Risk identification*): processo di ricerca, individuazione e descrizione dei rischi.

Nota 1: l’identificazione del rischio implica l’identificazione delle fonti di rischio, degli eventi, relative cause e delle loro potenziali conseguenze.

Nota 2: l’identificazione del rischio può implicare l’esame di dati storici, analisi teoriche, opinioni basate su conoscenze precise e su pareri di esperti, ed esigenze delle parti interessate.

[Fonte: UNI ISO 31073:2022, 3.3.9]

Indicatore di rischio (*Risk indicator*): informazione o misura utilizzata per rappresentare o segnalare lo stato di un rischio o una variazione della relativa esposizione.

Nota: un indicatore di rischio può avere natura quantitativa o qualitativa, predittiva o consuntiva, e può essere rappresentato da un indicatore indiretto o proxy quando non sia disponibile una misurazione diretta.

Informazioni documentate (*Documented information*): informazioni che devono essere tenute sotto controllo e mantenute da parte di un’organizzazione e il mezzo che le contiene.

Nota 1: le informazioni documentate possono essere in qualsiasi formato, su qualsiasi mezzo e provenire da qualsiasi fonte.

Nota 2: le informazioni documentate possono riferirsi:

- al sistema di gestione, compresi i relativi processi;
- alle informazioni prodotte per il funzionamento dell’organizzazione;
- all’evidenza dei risultati conseguiti.

[Fonte: UNI 11865:2022, 3.11]

Livello di rischio (*Level of risk*): dimensione di un rischio o di una combinazione di rischi, espressa in termini di combinazione di conseguenze e loro probabilità.

[Fonte: UNI ISO 31073:2022, 3.3.22]

Miglioramento continuo (*Continual improvement*): attività ricorrente per accrescere le prestazioni.

[Fonte: UNI 11865:2022, 3.21]

Monitoraggio (*Monitoring*): verifica, supervisione, osservazione critica o determinazione in continuo dello stato al fine d’identificare variazioni rispetto al livello di prestazione richiesto o atteso.

Nota: il monitoraggio può essere applicato al framework per la gestione del rischio, al processo di gestione del rischio, al rischio o al controllo del rischio.
[Fonte: UNI ISO 31073:2022, 3.3.40]

Non conformità (*Nonconformity*): mancato soddisfacimento di un requisito.

[Fonte: UNI 11865:2022, 3.19]

Organo di governo (*Governing body*):

Persona o gruppo di persone che ha l'obbligo di rendere conto in ultima istanza per l'intera organizzazione.

Nota 1: all'organo di governo competono, secondo l'assetto giuridico e organizzativo applicabile, le responsabilità ultime di indirizzo e supervisione dell'organizzazione o del campo di applicazione cui si riferisce il framework.

Nota 2: la configurazione dell'organo di governo dipende dalla forma giuridica e dall'assetto di governance dell'organizzazione.

[Fonte: Adattata dalla UNI ISO 37000:2021, 3.3.4, – le note originali sono state sostituite dalle note 1 e 2]

Ponderazione del rischio (*Risk evaluation*): processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio sia accettabile o tollerabile.

Nota: la ponderazione del rischio aiuta nelle decisioni relative al trattamento del rischio.

[Fonte: UNI ISO 31073:2022, 3.3.25]

Presidio specialistico (*Specialist risk function*): struttura o ruolo dotato di competenze specialistiche in relazione a una determinata famiglia di rischi o disciplina, che svolge attività di indirizzo, supporto, monitoraggio o controllo e mette a disposizione metodologie, informazioni ed evidenze pertinenti.

Nota: ai fini della presente PdR, i presidi specialistici comprendono le funzioni di controllo e gli altri ruoli organizzativi che presidiano specifiche categorie di rischio secondo l'assetto adottato dall'organizzazione.

Probabilità (*Likelihood*): plausibilità di un accadimento ipotizzabile.

Nota 1: nella terminologia della gestione del rischio, il termine “possibilità” è utilizzato per riferirsi alla plausibilità di un accadimento ipotizzabile, sia essa definita, misurata, determinata oggettivamente o soggettivamente, qualitativamente o quantitativamente, e descritta utilizzando termini generici o matematici, come probabilità o frequenza.

Nota 2: il termine anglosassone “likelihood” non ha un diretto equivalente in altre lingue; invece, è spesso usato il termine equivalente di “probability”. Tuttavia, in inglese, il termine “probability” è spesso interpretato in senso restrittivo come termine matematico. Pertanto, nella terminologia della gestione del rischio, il termine “likelihood” è utilizzato con l'accezione più ampia, come ha il termine “probability” in altre lingue diverse dall'inglese.

[Fonte: UNI ISO 31073:2022, 3.3.16]

Process owner – Titolare del processo (*Process owner*): persona o funzione cui sono attribuite autorità e responsabilità per il funzionamento, il monitoraggio e il miglioramento di un processo e per il conseguimento dei relativi obiettivi.

Nota: il process owner può coincidere con il risk owner dei rischi relativi al processo di propria competenza, purché le rispettive responsabilità siano chiaramente definite.

[Fonte: definizione applicativa della presente PdR]

Processo di gestione del rischio (*Risk management process*): applicazione sistematica delle politiche, procedure e prassi gestionali alle attività di comunicazione, consultazione, definizione del contesto, e di identificazione, analisi, ponderazione, trattamento, monitoraggio e riesame del rischio.

[Fonte: UNI ISO 31073:2022, 3.3.1]

Propensione al rischio (*Risk appetite*): livello e tipo di rischio che un'organizzazione è disposta a ricercare o ritenere.

[Fonte: UNI ISO 31073:2022, 3.3.27]

Registrazione e reporting (*Recording and reporting*): attività mediante le quali il processo di gestione del rischio e i relativi risultati sono documentati e comunicati attraverso meccanismi appropriati.

Nota: registrazione e reporting sono finalizzati a comunicare le attività e i risultati della gestione del rischio, fornire informazioni per il processo decisionale, migliorare le attività di gestione del rischio e favorire l'interazione con le parti interessate.

[Fonte: Definizione ricavata dal punto 6.7 della UNI ISO 31000:2018]

Registro dei rischi (*Risk register*): raccolta strutturata delle informazioni relative ai rischi identificati e ai corrispondenti elementi di gestione.

Nota: ai fini della presente PdR, il registro dei rischi o strumento equivalente può comprendere le informazioni indicate nell'Appendice C.

[Fonte: definizione applicativa della presente PdR]

Requisito (*requirement*): esigenza o aspettativa che può essere esplicita, generalmente implicita, oppure obbligatoria.

[Fonte: UNI 11865:2022, 3.3]

Riesame (*Review*): attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia di qualcosa a conseguire gli obiettivi stabiliti.

Nota: il riesame può essere applicato al framework per la gestione del rischio, al processo di gestione del rischio, al rischio o al controllo del rischio.

[Fonte: UNI ISO 31073:2022, 3.3.41]

Rischio (*Risk*): effetto dell'incertezza in relazione agli obiettivi.

Nota 1: un effetto riguarda ciò che potrebbe essere diverso da quanto atteso. Può essere positivo, negativo o di entrambi i segni e può affrontare, creare o avere come risultato in cascata successive nuove opportunità e minacce.

Nota 2: gli obiettivi possono presentare aspetti e categorie differenti e possono essere stabiliti per livelli differenti.

Nota 3: il rischio è di solito espresso in termini di fonti di rischio, eventi potenziali, loro conseguenze e loro probabilità.

[Fonte: UNI ISO 31073:2022, 3.1.1]

Rischio intrinseco (*Inherent risk*): livello di rischio determinato senza considerare gli effetti dei controlli esistenti o degli altri trattamenti già operanti.

Rischio residuo (*Residual risk*): rischio rimanente a seguito del trattamento del rischio.

Nota 1: il rischio residuo può comprendere rischi non identificati.

Nota 2: il rischio residuo può anche essere noto come “rischio ritenuto”.

[Fonte: UNI ISO 31073:2022, 3.3.38]

Risk owner – Titolare del rischio (*Risk owner*): persona o entità con l'obbligo di rendere conto (accountability) e l'autorità per gestire il rischio.

[Fonte: UNI ISO 31073:2022, 3.3.14]

Trattamento del rischio (*Risk treatment*): processo per modificare il rischio.

Nota 1: il trattamento del rischio può implicare:

- evitare il rischio decidendo di non iniziare o non continuare l'attività che dà origine ad esso;
- assumere o aumentare l'esposizione al rischio al fine di cogliere un'opportunità;
- rimuovere la fonte di rischio;
- modificare la probabilità;
- modificare le conseguenze;
- condividere il rischio con una o più altre parti, compresi contratti e finanziamento del rischio;
- ritenere il rischio con una decisione consapevole.

Nota 2: i trattamenti del rischio che affrontano conseguenze negative sono talvolta denominati “protezione dal rischio”, “eliminazione del rischio”, “prevenzione del rischio” e “riduzione del rischio”.

Nota 3: il trattamento del rischio può generare nuovi rischi o modificare rischi esistenti.

[Fonte: UNI ISO 31073:2022, 3.3.32]

Valutazione del rischio (*Risk assessment*): processo complessivo di identificazione del rischio, analisi del rischio e ponderazione del rischio.

[Fonte: UNI ISO 31073:2022, 3.3.8]

4 PRINCIPIO

La presente prassi di riferimento è fondata sull'esigenza di rendere la gestione del rischio parte integrante della governance, dei processi decisionali e delle attività operative dell'organizzazione, secondo un approccio coerente con la UNI ISO 31000 e con la UNI 11865.

Il framework per la gestione del rischio deve essere sviluppato e applicato in modo proporzionato al contesto, al perimetro, agli obiettivi, alla complessità dell'organizzazione e alla rilevanza dei rischi trattati. La proporzionalità incide sul livello di formalizzazione, sull'approfondimento delle analisi, sulle

modalità di reporting e sulla frequenza delle attività, ma non può giustificare l'assenza degli elementi essenziali necessari al funzionamento del framework.

Il framework deve essere orientato alla produzione di informazioni utili alle decisioni, alla chiara attribuzione delle responsabilità, al coordinamento tra funzioni operative e presidi di controllo, alla tracciabilità delle evidenze e al miglioramento continuo.

In coerenza con la natura verificabile della presente prassi, i requisiti declinati nel presente documento devono essere formulati in modo da poter essere associati a evidenze documentate e a criteri di verifica, ferma restando la possibilità di adattare strumenti, tecniche e livello di dettaglio al contesto applicabile.

La presente prassi non sostituisce obblighi di legge, regolamentari e norme settoriali specialistiche. Essa consente all'organizzazione di adottare tecniche di valutazione del rischio adeguate al proprio contesto, senza vincoli metodologici specifici, nonché di definire un assetto organizzativo coerente con le proprie caratteristiche.

L'organizzazione può altresì dotarsi di un Risk Appetite Framework formalizzato; in sua assenza, assicura comunque la definizione e approvazione di criteri per l'accettazione, la priorità e l'escalation del rischio.

5 REQUISITI GENERALI DEL FRAMEWORK PER LA GESTIONE DEL RISCHIO

5.1 Comprensione del contesto e delle parti interessate

L'organizzazione deve determinare e riesaminare periodicamente i fattori interni ed esterni che possono influenzare il proprio profilo di rischio e la capacità del framework per la gestione del rischio di produrre risultati attesi. L'analisi del contesto deve considerare, in modo proporzionato ove applicabile:

- visione, missione, obiettivi, strategia e modello di business;
- assetti di governance;
- compliance e quadro regolatorio di riferimento;
- processi aziendali con particolare riferimento a quelli in outsourcing;
- disponibilità e adeguatezza delle risorse;
- cultura organizzativa;
- livello di digitalizzazione;
- principali dinamiche del contesto esterno.

L'organizzazione deve inoltre individuare le parti interessate rilevanti ai fini del framework per la gestione del rischio, le loro esigenze e aspettative pertinenti e le eventuali implicazioni sui criteri di rischio, sulle priorità di monitoraggio e sulle modalità di comunicazione dei risultati attesi. Tale analisi deve essere aggiornata con periodicità definita o al verificarsi di cambiamenti significativi.

Le informazioni risultanti dall'analisi del contesto e delle parti interessate devono essere mantenute come informazione documentata.

5.2 Definizione campo di applicazione

L'organizzazione deve definire e mantenere informazioni documentate relative al campo di applicazione del framework, precisando perimetro organizzativo, digitale e fisico, processi e attività inclusi interfacce rilevanti con terzi o altri sistemi ed eventuali esclusioni.

La non applicabilità dei requisiti declinati nella presente prassi deve essere motivata, approvata al livello appropriato, tale da non compromettere l'efficace gestione dei rischi rilevanti del contesto considerato.

5.3 Integrazione con governance, processi e altri sistemi

Il framework per la gestione del rischio deve essere integrato, per quanto applicabile, nella governance, nella pianificazione strategica, nelle attività operative, nel budgeting, nei progetti, nel monitoraggio delle prestazioni e nei presidi di controllo dell'organizzazione.

L'organizzazione deve definire le modalità di raccordo tra il framework per la gestione del rischio e gli altri sistemi di gestione in atto, al fine di coordinare presidi specialistici e funzioni di controllo eventualmente presenti, oltre a evitare duplicazioni, sovrapposizioni e disallineamenti, assicurando coerenza metodologica e informativa.

Tale raccordo deve chiarire almeno:

- ruoli e responsabilità dei soggetti coinvolti;
- input e output informativi minimi;
- frequenza e modalità di interazione;
- criteri di utilizzo o valorizzazione delle evidenze prodotte da altri sistemi o presidi;
- responsabilità di aggiornamento, consolidamento e condivisione delle informazioni rilevanti.

Ove sia presente un sistema di gestione multidisciplinare, il framework per la gestione del rischio deve tenerne conto in misura proporzionata, valorizzando le informazioni rilevanti già disponibili e l'allineamento del perimetro di applicazione, la coerenza dei criteri di valutazione del rischio e l'integrazione dei flussi di reporting definiti dalla presente prassi.

5.4 Criteri di rischio

L'organizzazione deve definire e approvare i criteri di rischio da utilizzare per l'identificazione, l'analisi, la ponderazione, l'accettazione, il monitoraggio, e il reporting. Tali criteri devono essere coerenti con gli obiettivi strategici, manageriali e operativi, con il contesto, con il perimetro del framework e con il profilo di complessità dell'organizzazione. I criteri devono indicare, almeno:

- orizzonte temporale;
- dimensioni e scale utilizzate per valutare le conseguenze;
- modalità e le scale utilizzate per stimare la possibilità o probabilità;
- regole per determinare e classificare il livello di rischio e le eventuali soglie decisionali;
- principi per il trattamento;
- le condizioni per l'accettazione del rischio.

I criteri devono essere riesaminati con periodicità definita e, ove necessario, aggiornati ogni volta che mutino in modo rilevante il contesto, il perimetro o le regole decisionali del framework.

5.5 Elementi essenziali del framework

L'Organizzazione, in relazione al proprio contesto e alla propria complessità, deve prendere in considerazione almeno i seguenti elementi:

- campo di applicazione del framework per la gestione del rischio definito e aggiornato;
- politica per la gestione del rischio o documento equivalente di indirizzo che prenda in considerazione gli obiettivi per la gestione del rischio e che stabilisca un approccio, un piano o una linea d'azione per conseguirli;
- criteri di rischio approvati e comunicati ai ruoli pertinenti;
- ruoli, responsabilità, autorità;
- registro dei rischi o strumento equivalente;
- processo di identificazione, analisi e ponderazione dei rischi;
- decisioni di trattamento formalizzate con scadenze e monitoraggio dello stato di avanzamento;
- reporting periodico verso livelli decisionali competenti;
- informazioni documentate ed evidenze tracciabili;
- riesame periodico del framework;
- audit interno di gestione del rischio;
- gestione dei rilievi emersi dagli audit interni di gestione del rischio e/o di terza parte, delle debolezze rilevate e delle relative azioni correttive.

6 LEADERSHIP, GOVERNANCE E RESPONSABILITÀ

6.1 Leadership e impegno

L'organo di governo, ove presente, e l'alta direzione devono assicurare indirizzo, sostegno e supervisione del framework per la gestione del rischio. Tali soggetti devono assicurare l'integrazione del processo di gestione del rischio nelle decisioni strategiche e assicurare la disponibilità di risorse necessarie alla corretta gestione del rischio. L'alta direzione deve assicurare la coerenza tra obiettivi, criteri di rischio, flussi informativi e responsabilità organizzative.

6.2 Politica per la gestione del rischio

L'Organizzazione deve adottare una politica per la gestione del rischio.

Tale politica deve:

- definire l'ambito organizzativo di applicazione e le finalità del framework per la gestione del rischio;
- costituire un quadro di riferimento per la definizione degli obiettivi del framework per la gestione del rischio;
- stabilire l'adozione dell'approccio "basato sul rischio" nei processi aziendali;
- contenere un impegno al miglioramento continuo.

La politica per la gestione del rischio deve essere approvata dall'organo di governo e/o dall'alta direzione e deve essere disponibile come informazione documentata.

6.3 Ruoli, responsabilità e autorità

L'Organizzazione deve definire, documentare e garantire che siano comunicate a tutti i livelli ruoli principali, responsabilità e autorità in materia di gestione del rischio per:

- organo di governo;
- alta direzione;
- funzione ERM o presidio equivalente;
- risk owner;
- process owner.

Qualora non sia possibile una chiara separazione tra tali ruoli, è ammessa la loro aggregazione, a condizione che sia comunque assicurata la chiara attribuzione delle responsabilità e la prevenzione di potenziali conflitti di interesse.

6.3.1 Organo di governo

L'organo di governo, ove presente, deve ricevere la reportistica periodica sui rischi principali e riesaminare l'adeguatezza complessiva del framework e del processo di gestione del rischio adottati. L'organo di governo definisce gli indirizzi generali del framework per la gestione del rischio.

NOTA: Per approfondire autorità e responsabilità dell'organo di governo vedere UNI ISO 37000:2021.

6.3.2 Alta Direzione

L'alta direzione deve assicurare l'operatività del framework, l'assegnazione delle responsabilità, la coerenza con i processi aziendali e l'esecuzione delle decisioni di trattamento ed escalation.

6.3.3 Funzione ERM o presidio equivalente

La funzione ERM o il presidio equivalente deve assicurare almeno:

- presidio e aggiornamento della metodologia;
- coordinamento dei cicli di assessment;
- consolidamento del registro dei rischi; supporto ai risk owner;
- coordinamento con le seconde linee;
- predisposizione della reportistica periodica;
- promozione del miglioramento del framework.

Nelle organizzazioni prive di una funzione dedicata, l'alta direzione deve attribuire esplicitamente tali compiti a un ruolo o a una struttura identificata.

6.3.4 Prima linea, seconde linee e terza linea

L'organizzazione deve rappresentare, in modo proporzionato alla propria struttura, il raccordo tra responsabilità operative, presidi di controllo specialistici e assurance indipendente, secondo una logica coerente con il modello delle tre linee.

- la prima linea è responsabile della gestione dei rischi connessi ai processi, attività, progetti o obiettivi di competenza;
- le seconde linee supportano, indirizzano, monitorano o controllano specifiche famiglie di rischio, anche attraverso metodologie e flussi informativi;
- la terza linea, ove presente, fornisce assicurazione indipendente per dare fiducia sull'adeguatezza e sul funzionamento dei presidi e del framework.

6.3.5 Escalation e decisioni

L'Organizzazione deve definire i meccanismi mediante i quali i rischi principali, i superamenti di soglia e le criticità di attuazione dei piani vengono sottoposti al livello decisionale competente. Le decisioni rilevanti in merito alle azioni per affrontare i rischi sopra soglia di accettabilità e/o criticità di attuazione dei piani devono essere tracciate e riportare almeno:

- oggetto;
- motivazione;
- soggetto decisionale;
- responsabilità attuative;
- tempi;
- risorse;
- eventuale necessità di follow up.

7 PIANIFICAZIONE DEL FRAMEWORK E SUA APPLICAZIONE

7.1 Obiettivi del framework per la gestione del rischio

L'Organizzazione deve stabilire obiettivi per il framework per la gestione del rischio coerenti con la politica, con il contesto e con il livello di complessità dell'Organizzazione. Nel monitoraggio e nel riesame di tali obiettivi, l'organizzazione deve considerare, ove pertinenti, anche gli esiti aggregati delle attività di valutazione del rischio, gli eventuali scostamenti rilevati e le esigenze di miglioramento del framework.

Gli obiettivi devono essere riesaminati e monitorati periodicamente, valutandone la coerenza rispetto alla politica per la gestione del rischio verificandone l'efficacia.

7.2 Pianificazione delle attività ERM

L'Organizzazione deve definire e documentare un programma periodico di attività di gestione del rischio coerente con il perimetro del framework, con la natura dei rischi, con la criticità e l'importanza degli obiettivi interessati e con eventuali requisiti legali, regolatori o settoriali applicabili. Il programma deve essere coordinato con le altre attività di pianificazione dell'organizzazione. Nel programma devono essere indicati:

- principali assessment pianificati;

- tempi di aggiornamento del registro;
- incontri di coordinamento con seconde linee;
- reporting programmato;
- audit interno di gestione del rischio di prima e seconda parte;
- attività di formazione;
- riesami di direzione del framework;
- eventuali progetti di miglioramento.

7.3 Pianificazione delle modifiche

L'Organizzazione deve monitorare e affrontare i cambiamenti rilevanti del contesto interno ed esterno (inclusi perimetro organizzativo, tecnologie e requisiti normativi) e deve assicurare che ogni necessaria e conseguente modifica del framework, sia gestita in modo strutturato, tracciabile e coerente con l'approccio risk-based. Per quanto possibile le modifiche devono essere pianificate specificando:

- cosa cambia;
- chi ne è responsabile;
- tempi di attuazione;
- le criticità nell'attuazione delle modifiche;
- impatto delle modifiche sui rischi aziendali (livello di esposizione, efficacia dei controlli, adeguatezza del framework);
- valutazione e trattamento dei rischi emergenti/modificati
- modalità di verifica successiva.

L'Organizzazione deve assicurare inoltre la tracciabilità delle decisioni, delle valutazioni svolte e delle responsabilità assegnate.

8 SUPPORTO, RISORSE, FORMAZIONE, CULTURA DEL RISCHIO E INFORMAZIONI DOCUMENTATE

8.1 Generalità

L'Organizzazione deve mettere a disposizione risorse adeguate (umane, organizzative, informative e tecnologiche) per lo sviluppo, l'attuazione, il mantenimento e il miglioramento continuo del framework di gestione del rischio. Le risorse devono essere coerenti con le caratteristiche del framework, commisurate alla natura e complessità dei rischi, allineate alla pianificazione delle attività.

8.2 Competenza

L'Organizzazione deve identificare le competenze necessarie per i ruoli che incidono sul funzionamento del framework per la gestione del rischio. Deve inoltre assicurare che tali ruoli siano competenti in misura proporzionata alle responsabilità attribuite. L'Organizzazione deve inoltre

definire modalità idonee per assicurare o sviluppare e mantenere tali competenze, conservandone evidenza.

8.3 Formazione

L'Organizzazione deve adottare un piano formativo sul framework per la gestione del rischio basato sui ruoli e su un'analisi dei fabbisogni formativi. Il piano deve essere aggiornato periodicamente in coerenza con le frequenze definite nel programma periodico di cui al punto 7.2.

Il piano formativo deve indicare:

- destinatari;
- obiettivi;
- sintesi dei contenuti;
- modalità di erogazione;
- tempi;
- criteri di verifica.

L'organizzazione deve conservare evidenza della partecipazione e della verifica di efficacia della formazione. In caso di modifica significativa del framework, introduzione di nuovi strumenti, nuovi ruoli o nuovi rischi emergenti, l'organizzazione deve prevedere sessioni di aggiornamento dedicate.

Nota: nelle iniziative formative si può prevedere, a titolo esemplificativo, formazione iniziale, aggiornamenti periodici, moduli specifici per Alta Direzione e Organo di Governo ove presente, formazione operativa per risk owner e process owner, aggiornamenti per seconde e terze linee in relazione alle rispettive responsabilità.

8.4 Consapevolezza e cultura del rischio

L'Organizzazione deve promuovere una cultura del rischio a supporto di tutta la gestione del rischio, incluso il framework adottato. Ciò implica che le persone interessate comprendano il proprio ruolo, conoscano le modalità di comunicazione e di escalation e riconoscano l'importanza della qualità dei dati, della tempestività delle informazioni e del rispetto delle responsabilità assegnate.

8.5 Comunicazione

L'Organizzazione deve determinare le comunicazioni interne ed esterne pertinenti al framework per la gestione del rischio, includendo:

- a) l'oggetto della comunicazione;
- b) quando comunicare;
- c) con chi comunicare;
- d) come comunicare;
- e) chi è il responsabile della comunicazione

8.6 Informazioni documentate

L'Organizzazione deve istituire, aggiornare, proteggere e rendere reperibili le informazioni documentate necessarie a dimostrare lo sviluppo, attuazione e miglioramento continuo del framework. Le informazioni documentate devono essere governate con regole minime di identificazione, approvazione, aggiornamento, accesso, conservazione e archiviazione.

9 ATTIVITÀ OPERATIVE DEL PROCESSO DI RISCHIO

9.1 Pianificazione e controllo operativo del processo

L'organizzazione deve pianificare e tenere sotto controllo le attività operative del framework per la gestione del rischio in coerenza con i criteri adottati e con il programma periodico delle attività. Devono essere disponibili informazioni documentate in merito a ruoli e responsabilità su:

- avvio e validazione degli assessment;
- aggiornamento e validazione del registro dei rischi;
- monitoraggio piani e redazione di reportistica.

Devono inoltre essere definiti input minimi, output attesi e responsabilità di riesame delle principali fasi del processo.

9.2 Identificazione dei rischi

Le tecniche per identificare i rischi devono essere selezionate ed applicate in coerenza con il contesto esterno e interno, con la complessità effettiva dell'organizzazione e con il campo di applicazione.

L'Organizzazione deve considerare almeno:

- obiettivi cui il rischio si riferisce;
- principali fonti o fattori abilitanti,
- evento temuto/auspicato e potenziali conseguenze.

L'organizzazione deve scegliere la metodologia e la scelta deve essere adeguata al tipo di rischio da identificare, coerente con il contesto, motivata e tracciabile.

Nota: le tecniche di identificazione possono comprendere interviste, workshop, analisi documentale, analisi di scenario, esame di incidenti, indicatori, evidenze di audit, analisi di contesto o altre tecniche idonee.

9.3 Analisi e ponderazione del rischio

L'Organizzazione deve definire, documentare e applicare una metodologia strutturata di analisi e ponderazione dei rischi.

Nel caso di evoluzione di fattori rilevanti che possono influenzare significativamente i rischi di competenza, la prima linea deve segnalare tempestivamente alla funzione ERM o presidio equivalente, che valuterà se è necessario procedere alla rivalutazione dei rischi.

Nota: l'approccio utilizzato può prevedere l'adozione di differenti modalità di analisi e ponderazione, in funzione delle caratteristiche dei rischi analizzati e delle informazioni disponibili e delle competenze disponibili. La norma UNI CEI EN IEC 31010:2019 fornisce un ampio repertorio di tecniche di risk assessment, incluse identificazione, analisi e ponderazione e relative "istruzioni per l'uso".

9.4 Accettazione del rischio, priorità ed escalation

L'Organizzazione deve adottare e documentare i criteri di accettazione del rischio che precisino almeno:

- condizioni alle quali il rischio può essere accettato;
- casi che richiedono escalation;
- necessità di motivazione formale per accettazioni in deroga o sopra soglia;
- periodicità di riesame delle decisioni di accettazione.

L'Organizzazione deve determinare e applicare criteri di prioritizzazione.

Tali criteri devono essere definiti in modo coerente e applicati in maniera documentata.

Nota: L'organizzazione dovrebbe considerare anche, ma non solo, uno o più dei seguenti elementi: criticità del processo o del prodotto/servizio; esposizione regolatoria o reputazionale; concentrazione degli impatti; velocità di manifestazione; affidabilità dei controlli esistenti; presenza di trend peggiorativi; eventi recenti; ecc..

9.5 Trattamento del rischio

Per i rischi che richiedono un intervento, l'organizzazione deve decidere e documentare l'opzione di trattamento prescelto:

- evitare il rischio decidendo di non avviare o di non continuare l'attività che genera il rischio;
- assumere o aumentare il rischio al fine di cogliere un'opportunità;
- rimuovere la fonte di rischio;
- modificare la probabilità;
- modificare le conseguenze;
- condividere il rischio (per esempio tramite contratti, stipulando un'assicurazione);
- ritenere il rischio con una decisione informata.

La decisione sull'azione di trattamento deve tenere conto di:

- risultati attesi,
- tempi,
- costi,
- impatti operativi,
- vincoli regolatori
- responsabilità attuative.

La motivazione per il trattamento del rischio è più ampia delle sole considerazioni economiche e deve tener conto di tutti gli obblighi, gli impegni volontari ed i punti di vista delle parti interessate.

La selezione delle opzioni di trattamento del rischio deve essere effettuata in conformità agli obiettivi, ai criteri di rischio ed alle risorse disponibili dell'organizzazione.

I piani devono essere monitorati e le deviazioni rilevanti devono generare riesame, escalation o azioni correttive.

Nota: i piani di trattamento, a seconda della loro rilevanza, dovrebbero indicare: rischio di riferimento, azioni previste, owner, eventuali co-owner o funzioni coinvolte, scadenze, milestone rilevanti, risorse essenziali, indicatori di avanzamento, stato, criterio di chiusura e modalità di validazione dell'attuazione.

9.6 Monitoraggio di rischi, indicatori e piani

L'Organizzazione deve monitorare con frequenza definita, almeno:

- i rischi prioritari;
- gli indicatori rilevanti;
- lo stato dei piani di trattamento;
- gli eventi significativi;
- i superamenti di soglia;
- le criticità informative o di coordinamento.

Per i rischi maggiormente rilevanti, l'organizzazione deve individuare indicatori di rischio o indicatori proxy idonei a supportare una rilevazione tempestiva dei cambiamenti di esposizione, salvo motivata impossibilità documentata.

9.7 Coordinamento con seconde linee e presidi specialistici

L'Organizzazione deve definire un modello minimo di coordinamento tra la funzione ERM o presidio equivalente e presidi specialistici pertinenti in coerenza con il framework per la gestione del rischio al fine di migliorarne l'efficacia e l'efficienza. Tale modello deve prevedere almeno:

- un calendario minimo di coordinamento;
- modalità di utilizzo reciproco delle evidenze;
- flussi minimi di condivisione delle informazioni;
- criteri di integrazione nel reporting.

9.8 Reporting integrato

L'Organizzazione deve predisporre reporting periodico coerente con il campo di applicazione del framework, con i destinatari e con la rilevanza dei rischi trattati. Il reporting minimo deve includere:

- quadro sintetico dei rischi principali;
- variazioni rilevanti; superamenti di soglia o escalation;
- stato dei piani di trattamento;
- indicatori significativi;
- esiti di verifiche.

10 VALUTAZIONE DELLE PRESTAZIONI

10.1 Monitoraggio, analisi e valutazione del framework

L'Organizzazione deve determinare come valutare l'efficacia del framework per la gestione del rischio, definendo criteri e modalità di monitoraggio coerenti con i propri obiettivi e il contesto di riferimento.

Nota: l'Organizzazione dovrebbe definire una frequenza di monitoraggio degli obiettivi del framework, al fine di individuare tempestivamente eventuali scostamenti e attuare le necessarie azioni.

10.2 Audit interno

L'Organizzazione deve programmare, eseguire e documentare audit interni sul framework per la gestione del rischio secondo quanto previsto dal programma periodico delle attività di cui al punto 7.2. Gli auditor devono essere competenti e assicurare obiettività e imparzialità nello svolgimento degli audit. Devono essere definiti criteri, campo di applicazione, frequenza, responsabilità, esiti, azioni conseguenti e follow up.

Nota: per approfondimenti sul processo e conduzione degli audit interni vedere UNI CEI EN ISO 19011:2026.

10.3 Riesame di direzione

L'Alta Direzione deve riesaminare periodicamente il framework per la gestione del rischio, con frequenza pianificata e coerente con le esigenze dell'Organizzazione, al fine di verificarne la continua idoneità, adeguatezza ed efficacia, nonché l'allineamento agli obiettivi del framework. Gli esiti del riesame e le principali evidenze rilevate sono portati all'attenzione dell'Organo di Governo e dei livelli di governance competenti, secondo modalità e flussi informativi coerenti con l'assetto organizzativo, al fine di supportare il processo decisionale e garantire il presidio strategico del framework.

Il riesame del framework per la gestione del rischio deve considerare, almeno, i seguenti elementi come input:

- modifiche al contesto interno ed esterno ed evoluzione delle esigenze/aspettative delle parti interessate;
- adeguatezza del framework;
- effettiva integrazione del framework nei processi decisionali dell'organizzazione;
- risultati del processo di gestione del rischio e il trend degli indicatori definiti e i relativi scostamenti;
- esito degli audit interni ed esterni sulla gestione del rischio e il relativo stato dei rilievi (ove rilevati);
- stato delle azioni derivanti da precedenti riesami e relativa efficacia;
- adeguatezza delle risorse.
- opportunità di miglioramento continuo.

Gli output del riesame devono essere verbalizzati e includere decisioni, responsabilità e tempi ed eventuali modifiche del framework.

L'organizzazione deve assicurare che le decisioni e le azioni derivanti dal riesame siano attuate, monitorate e riesaminate nel ciclo successivo.

11 MIGLIORAMENTO

11.1 Non conformità e azioni correttive

L'organizzazione deve migliorare le prestazioni e l'efficacia del framework per la gestione del rischio.

Quando si verifica una non conformità l'Organizzazione deve:

- reagire alla non conformità, e, per quanto applicabile:
 - intraprendere azioni per tenerla sotto controllo e correggerla;
 - affrontarne le conseguenze;
- valutare l'esigenza di azioni per eliminare le cause della non conformità, in modo che non si ripeta o non si verifichi altrove:
 - riesaminando la non conformità;
 - determinando le cause della non conformità;
 - determinando se esistono o possono verificarsi non conformità simili;
- attuare ogni azione necessaria;
- riesaminare l'efficacia di ogni azione correttiva intrapresa;
- apportare, se necessario, modifiche al framework per la gestione del rischio

L'Organizzazione deve conservare informazioni documentate quale evidenza della tipologia della non conformità, l'azione correttiva definita e dei relativi risultati del riesame dell'efficacia.

Le azioni correttive devono essere adeguate agli effetti delle non conformità riscontrate.

11.2 Miglioramento continuo e apprendimento

L'Organizzazione deve considerare gli esiti del monitoraggio, delle verifiche, degli output del riesame per migliorare in modo continuo il framework per la gestione del rischio.

Nota: Il miglioramento può riguardare metodologia, ruoli, strumenti, coordinamento, cultura del rischio, formazione, qualità dei dati, processo di escalation.

12 VALUTAZIONE DI CONFORMITÀ

La valutazione di conformità è utilizzata nel mercato al fine di accrescere la fiducia nelle caratteristiche e nelle prestazioni un'entità.

Lo scopo del framework per la gestione del rischio è quello di aiutare l'organizzazione a integrare efficacemente il processo di gestione del rischio nei processi del suo sistema di gestione, nelle sue attività e nelle sue funzioni.

La valutazione di conformità del processo di gestione del rischio è effettuata sulla base delle evidenze di conformità ai requisiti del framework di cui alla presente prassi di riferimento.

Tale valutazione può essere effettuata da:

- prima parte – un'organizzazione sul proprio framework per dare fiducia ai propri clienti ed alle altre parti interessate nella efficace integrazione del processo di gestione del rischio nei propri processi gestionali, di supporto e produttivi;
- seconda parte – un'organizzazione sul framework dei propri fornitori critici per avere fiducia nella efficace integrazione del processo di gestione del rischio nei loro processi gestionali, di supporto e produttivi;
- terza parte - un organismo di certificazione indipendente (), accreditato in conformità alla UNI CEI EN ISO/IEC 17065:2012, per fornire un'assicurazione indipendente e imparziale che il processo di gestione del rischio sia efficacemente integrato nei processi gestionali, di supporto e produttivi dell'organizzazione.

Qualora l'organizzazione intenda effettuare una valutazione di conformità di prima parte, quest'ultima deve essere conforme alla UNI CEI EN ISO/IEC 17050. Qualora l'organizzazione e l'utilizzatore del processo concordino di effettuare una valutazione di conformità di seconda parte, quest'ultima deve essere effettuata in conformità a criteri condivisi tra le parti.

Qualora l'organizzazione intenda ottenere una certificazione (valutazione della conformità di terza parte), si applicano i criteri riportati nell'Appendice A.

APPENDICE A – Valutazione di conformità di terza parte

A.1 Generalità

La presente appendice specifica i requisiti per la valutazione della conformità di terza parte del processo di gestione del rischio effettuata:

- sulla base delle evidenze di conformità ai requisiti del framework di cui alla presente prassi di riferimento;
- secondo la UNI CEI EN ISO/IEC 17065:2012, il cui obiettivo è assicurare una sempre maggiore uniformità e trasparenza del processo di certificazione.

A.2 Riferimenti per l'accreditamento

I seguenti documenti sono citati nel testo in modo tale che alcuni o tutti i loro contenuti costituiscono requisiti della presente appendice. In relazione ai riferimenti datati, si applica esclusivamente l'edizione citata. Per i riferimenti non datati vale l'ultima edizione del documento di riferimento (compresi gli aggiornamenti).

Norma di accreditamento	UNI CEI EN ISO/IEC 17065:2012
Schema di certificazione	La presente UNI/PdR, che è stata redatta tenendo in considerazione le norme: • UNI ISO 31000:2018 - Gestione del rischio - Linee guida. • UNI 11865:2022 - Gestione del rischio - Linea guida per l'integrazione della gestione del rischio nella governance e nelle attività operative di un'organizzazione in accordo alla UNI ISO 31000, con particolare riferimento ai sistemi di gestione basati sulle norme ISO che seguono la struttura di alto livello (HLS).
Documenti IAF applicabili	I documenti IAF previsti per i sistemi di gestione, per quanto applicabili. Tali documenti sono elencati in Bibliografia.
Soggetti che possono richiedere la certificazione	La certificazione prevista dalla presente UNI/PdR può essere richiesta da qualsiasi tipo di organizzazione, italiana o estera.

A.3 Requisiti per gli organismi di certificazione (OdC)

L'OdC che intende valutare la conformità del processo ai requisiti della presente UNI/PdR deve applicare la UNI CEI EN ISO/IEC 17065:2012 e i requisiti aggiuntivi del prospetto A.1.

Prospetto A.1 – Requisiti per gli organismi di certificazione (OdC)

Punti della UNI CEI EN	Requisiti aggiuntivi

ISO/IEC 17065		
Punto 5. Requisiti strutturali		-
Punto 6. Requisiti per le risorse	b)	Si applicano i punti 6.1.2.1 a) e b) del punto 6.1.2 “Gestione della competenza del personale coinvolto nel processo di certificazione”, in conformità a quanto segue. Criteri di competenza del gruppo di audit Il gruppo di audit deve essere composto da professionisti, e se del caso esperti tecnici, che nel loro insieme siano in grado di comprendere appieno i requisiti e l'applicazione dei requisiti di questa UNI/PdR e la loro applicazione. È responsabilità dell'OdC accertarsi della qualifica degli auditor e del mantenimento della stessa. Nel gruppo di audit le competenze si ritengono soddisfatte quando, tenendo conto delle competenze complessive del gruppo (auditor ed eventuali esperti/e tecnici/che), siano presenti: 1. conoscenza dei principi, delle prassi e delle tecniche di audit (UNI EN ISO 19011) acquisita tramite formazione erogata anche internamente da enti di certificazione (almeno 8 ore); 2. conoscenza specifica di questa UNI/PdR, acquisita attraverso un corso di formazione di almeno 16 ore che può essere anche erogato internamente da enti di certificazione; 3. competenza di gestione del rischio delle imprese: - conoscenza dei criteri base di Risk Management, con riferimento ad almeno le seguenti norme: • UNI ISO 31000, • UNI 11865, • UNI CEI EN IEC 31010; - conoscenza dei principali modelli organizzativi; 4. competenza: Il team, in sintesi, dovrebbe essere composto da: a) auditor tutti competenti con riferimento ai punti 1, 2 e 3 citati (distinguendo il livello di competenza fra Lead auditor e auditor); b) almeno un auditor competente per il settore di appartenenza dell'organizzazione. Qualora nessun auditor fosse esperto del settore, il team potrebbe essere affiancato da un esperto tecnico di settore (dunque competente per gli aspetti tecnici, non necessariamente per le procedure di audit); c) almeno un auditor con conoscenze previste per il professionista della gestione del rischio (Risk Manager – UNI 12012:2026), in

		assenza del quale può intervenire un esperto di gestione del rischio. Esperienza Con riferimento al punto 1, si richiede: – una significativa esperienza nell'attività di valutazione della conformità di almeno 2 anni che includa almeno 2 audit di terza parte (schemi di certificazione ISO 17021-1 o ISO 17065), rispettivamente nel ruolo di RGVI o di auditor a seconda del ruolo previsto nel gruppo di verifica. Si presume adeguata la competenza nel caso di auditor certificato sotto accreditamento, operativi in schemi di certificazione ISO 17021-1 o ISO 17065. Con riferimento al punto 3, si richiede: l'esperto tecnico deve poter dimostrare una significativa e comprovata esperienza di almeno 10 anni in questi ambiti. Se ritenuto necessario, il team può essere integrato anche da un esperto tecnico di settore.
Punto 7. Requisiti di processo	c) Criteri di competenza del comitato di delibera (o del decision maker)	Il personale che prende decisioni relative alla certificazione deve possedere conoscenze ed esperienze sufficienti per comprendere il processo di certificazione, al fine di poter determinare se i requisiti di certificazione siano soddisfatti. Si ritiene necessaria una competenza ed esperienza equivalente al Gruppo di verifica.
	d) Criteri di competenza di chi gestisce la domanda di certificazione	In aggiunta a quanto specificato al punto 7.2 "Domanda", si applica quanto segue. Organizzazioni che possono richiedere la valutazione di conformità di terza parte La valutazione di conformità di terza parte può essere richiesta da qualunque organizzazione, di qualsiasi dimensione e/o forma giuridica, il cui oggetto sociale o ambito di applicazione sia ricompreso nel punto 1.
	e) Tempi di audit e periodicità degli audit di terza parte	Si applicano i tempi riportati nell'MD05 – Table QMS.
	f)	Per applicare il punto 7.7.1 c), si deve specificare la sede legale dell'organizzazione e le sedi operative pertinenti;
	g)	Per applicare il punto 7.7.1 d), si deve specificare il riferimento al presente documento, completo dell'anno di edizione.
	h)	Per applicare il punto 7.7.1 e), si deve tenere conto che la certificazione ha validità triennale
	i)	In aggiunta a quanto specificato al punto 7.7 "Documentazione riguardante la certificazione", si applica quanto segue.

		Il certificato deve contenere un codice univoco di identificazione.
	l)	In aggiunta a quanto specificato al punto 7.9 “Sorveglianza”, si applica quanto segue. I.1) Periodicità degli audit di sorveglianza Gli audit di sorveglianza devono essere effettuati con periodicità annuale. [La possibilità di effettuare audit con breve preavviso, audit senza preavviso e/o audit in incognito (mystery audit) deve essere prevista nell'accordo di certificazione tra l'OdC e l'organizzazione richiedente.] I.2) Durata degli audit di sorveglianza La durata degli audit di sorveglianza deve essere 50 % della durata dell'audit di certificazione iniziale. I.3) Attività degli audit di sorveglianza Negli audit di sorveglianza è ammesso un campionamento dei processi, purché sia assicurata la copertura dello scopo del ciclo di certificazione.
	m)	In aggiunta a quanto specificato al punto 7, si applica quanto segue. Rinnovo della certificazione Il processo di rinnovo deve essere completato prima della scadenza del certificato. Negli audit di rinnovo è ammesso un campionamento dei processi, purché sia assicurata la copertura dello scopo del ciclo di certificazione. La durata degli audit di rinnovo deve essere 75% della durata dell'audit di certificazione iniziale.

APPENDICE B – Criteri di supporto per l'applicazione proporzionata

La presente appendice è informativa e fornisce criteri di supporto per motivare l'applicazione proporzionata della presente prassi. Essa non introduce profili prescrittivi predefiniti e non condiziona, di per sé, la valutazione di conformità. Ai fini dell'applicazione proporzionata, l'organizzazione può considerare, in funzione del proprio contesto e ove pertinenti, elementi quali:

- natura e criticità degli obiettivi interessati dal framework;
- dimensione e articolazione organizzativa;
- numero, complessità e interdipendenza dei processi rilevanti;
- intensità regolatoria e obblighi settoriali applicabili;
- criticità del servizio o dell'attività svolta;
- presenza di società controllate, terzi rilevanti o catene di fornitura critiche;
- esposizione verso stakeholder, autorità, utenti o comunità;
- maturità dei presidi di controllo e dei sistemi informativi disponibili.

Le scelte di semplificazione o rafforzamento del framework dovrebbero essere motivate, documentate

e riesaminate periodicamente, in modo da dimostrarne la coerenza con il contesto effettivo dell'organizzazione.

APPENDICE C - Esempio di contenuti raccomandati per il registro dei rischi e il reporting

La presente appendice è informativa. Il contenuto qui riportato individua esempi di contenuti raccomandati per rendere il framework omogeneo e verificabile.

Elemento	Esempi di contenuti raccomandati
Registro dei rischi	Identificativo del rischio o riferimento equivalente, descrizione sintetica del rischio, obiettivo o ambito interessato, orizzonte temporale o periodo di riferimento della valutazione, soggetto responsabile o funzione competente, processo/area ove pertinente, principali cause o fattori abilitanti, conseguenze attese, controlli o presidi rilevanti ove presenti, esito della valutazione secondo i criteri adottati, decisione assunta, eventuale piano di trattamento o stato di accettazione, data dell'ultimo riesame ove applicabile
Campi aggiuntivi utili (opzionali)	Indicatori/KRI, collegamento a rischi specialistici, interdipendenze, escalation aperte, stato dei piani, note di verifica

Elemento	Esempi di contenuti raccomandati
Reporting periodico	Informazioni proporzionate alla rilevanza dei rischi e ai destinatari del reporting, quali: rischi principali e relative ownership, variazioni rilevanti, eventuali superamenti di soglia o escalation, eventi o incidenti rilevanti, stato delle azioni, indicatori significativi ove definiti, eventuali richieste decisionali, sintesi delle verifiche e principali criticità metodologiche o informative, ove pertinenti.

APPENDICE D – Indicazioni operative per il coordinamento con seconde linee di controllo

La presente appendice è informativa e traduce in forma pratica i requisiti del punto 9.7.

- definire, ove pertinente e in misura proporzionata alla complessità dell'organizzazione, criteri comuni di classificazione dei rischi;
- definire un calendario minimo di attività di pianificazione e coordinamento e i suoi output attesi;
- definire i criteri secondo cui la funzione ERM o presidio equivalente e le seconde linee di controllo possono valorizzare reciprocamente le evidenze disponibili, evitando duplicazioni e assicurando coerenza metodologica e informativa;
- definire campi informativi minimi condivisi per la condivisione delle informazioni e reporting integrato.

APPENDICE E - Matrice RACI del framework per la gestione del rischio

La presente appendice è informativa. La matrice seguente riporta un modello di responsabilità ad alto livello, da adattare alla struttura dell'organizzazione. La matrice ha valore esemplificativo e deve essere adattata all'assetto di governance, alla dimensione, alla complessità e al perimetro dell'organizzazione. Le attribuzioni indicate non modificano i requisiti del corpo principale e non escludono assetti equivalenti purché responsabilità, autorità e flussi decisionali risultino chiaramente definiti e documentati.

Attività	Organo di governo	Alta direzione	ERM / presidio equivalente	Prima linea	Seconda linee di controllo	Terza linea di controllo
Politica e indirizzi	A	R	C	I	C	I
Criteri di rischio	I	A	R	I	C/R	I
Assessment periodico	I	A	R per coordinamento e metodologia	R per identificazione e valutazione dei rischi di competenza	C/R	I
Piani di trattamento	I	A	C	R	C	I
Reporting integrato	I / destinatario, ove previsto	A	R	C	C	I
Audit interno di gestione del rischio / verifica indipendente	I	I	C	I	I	A/R
Riesame del framework	I	I	R/C	C	C	I

Leggenda Matrice RACI (R – Responsible, A – Accountable, C – Consulted, I – Informed).

APPENDICE F - Esempi di evidenze documentate, versioning e criteri di conservazione

La presente appendice è informativa. I tempi indicati hanno valore esemplificativo e possono essere adattati dall'organizzazione in funzione del proprio contesto, dei requisiti legali, regolatori, contrattuali o interni applicabili, della rilevanza delle informazioni e delle esigenze di tracciabilità del framework. L'Appendice G integra la presente sezione fornendo la correlazione operativa tra requisiti, evidenze e criteri di verifica.

Ambito	Esempi di evidenze documentate	Tracciabilità e versioning	Conservazione, ove applicabile
Perimetro, politica, criteri, ruoli	Documenti approvati e relative revisioni	Identificativo, data, approvatore, versione, stato	Versione vigente + storico essenziale per almeno 24 mesi dopo sostituzione
Registro rischi e piani	Storico delle valutazioni principali, aggiornamenti, owner, decisioni e stato piani	Data ultimo aggiornamento, autore modifica, versione o log	Per un periodo coerente con il ciclo di assessment, con le esigenze di riesame del framework e con eventuali requisiti legali, regolatori o interni applicabili
Reporting ed escalation	Report periodici, note di escalation, decisioni assunte	Data, destinatario, riferimento al rischio o al trigger	Almeno 36 mesi
Riesami e verifiche	Verbalì, esiti, rilievi, follow up	Data, perimetro, responsabili, chiusura azioni	Almeno 36 mesi
Formazione	Piano formativo, presenze, verifica efficacia	Versione piano, edizioni, destinatari, esiti	Per un periodo coerente con il ciclo formativo definito, con il riesame delle competenze e con eventuali requisiti applicabili
Rivalutazioni straordinarie	Analisi evento, decisioni, azioni e chiusura	Trigger, data, responsabili, esito	Almeno 36 mesi

APPENDICE G - Matrice requisito, evidenza e criterio di verifica

La presente appendice è informativa e supporta la correlazione tra requisiti della presente PdR, evidenze attese e possibili criteri di verifica. La matrice non esaurisce tutti i controlli possibili e fornisce un riferimento applicativo da adattare al contesto, al perimetro e alla complessità dell'organizzazione.

Punto	Requisito chiave	Evidenze di riferimento	Criterio di verifica
12	Valutazione di conformità	Registrazione degli esiti della valutazione, perimetro valutato, requisiti esaminati, eventuali esclusioni motivate e azioni conseguenti.	Verificare che la valutazione sia svolta rispetto ai requisiti applicabili della PdR e che eventuali esclusioni o non pertinenze siano motivate e approvate.
5.2	Perimetro del framework	Documento di campo di applicazione, confini, esclusioni, relazioni con terzi o altre società	Verificare chiarezza del perimetro, coerenza con il contesto e assenza di esclusioni tali da creare zone d'ombra rilevanti
5.4	Criteri di rischio	Documento approvato con scale, soglie, criteri di accettazione ed escalation	Verificare approvazione, comunicazione ai ruoli pertinenti e applicazione coerente nei casi esaminati
5.5	Elementi essenziali del framework	Perimetro, politica, ruoli, registro, assessment, piani, reporting, riesame, audit/verifica, gestione, Non conformità	Verificare la presenza e il funzionamento degli elementi essenziali del framework, tenendo conto di eventuali presidi equivalenti documentati e della loro idoneità a soddisfare il requisito applicabile
6.3	Ruoli, responsabilità e autorità	Organigramma, job description, RACI, delibere o attribuzioni formali	Verificare chiarezza delle responsabilità, assenza di vuoti di presidio e coerenza tra ruoli dichiarati e prassi operative
7.2	Programma periodico delle attività	Piano periodico; calendario assessment, reporting, coordinamento, verifiche, formazione e riesami	Verificare coerenza delle frequenze definite, motivazione delle scelte e tracciabilità degli scostamenti o delle ripianificazioni
8.2	Formazione	Piano formativo, presenze, materiali, verifiche di efficacia	Verificare copertura dei ruoli chiave, onboarding, refresh e presenza di evidenze di efficacia

Punto	Requisito chiave	Evidenze di riferimento	Criterio di verifica
8.3	Consapevolezza e cultura del rischio	Iniziative di comunicazione o sensibilizzazione, evidenze di integrazione nei processi, informazioni sui canali di comunicazione o escalation pertinenti al framework	Verificare che i ruoli pertinenti conoscano responsabilità, canali di escalation e importanza della qualità dei dati.
8.5	Informazioni documentate e tracciabilità	Regole di versioning, log modifiche, repository, criteri di accesso e conservazione	Verificare reperibilità, aggiornamento, controllo versioni e integrità minima delle informazioni
5.5 / 9.1 / 10.1	Registro dei rischi o strumento equivalente	Registro dei rischi o strumento equivalente, aggiornato secondo le frequenze definite, contenente informazioni proporzionate al perimetro e ai criteri adottati	Verificare che il registro o strumento equivalente sia presente, coerente con i criteri di rischio adottati, aggiornato e riesaminato secondo modalità definite, idoneo a supportare monitoraggio, reporting, decisioni di trattamento e tracciabilità delle responsabilità
9.2	Identificazione dei rischi	Evidenze delle attività di identificazione, criteri o tecniche utilizzate, rischi individuati, obiettivi/ambiti interessati, principali cause o fattori abilitanti e conseguenze attese	Verificare che l'identificazione dei rischi sia svolta con modalità coerenti con contesto, complessità e perimetro, e che le informazioni siano tracciabili e sufficienti rispetto alla metodologia adottata
9.3	Analisi e valutazione del rischio	Metodologia di analisi e valutazione, criteri applicati, evidenze di valutazione, esiti, eventuali riesami o rivalutazioni	Verificare che l'analisi e la valutazione siano documentate, coerenti con i criteri di rischio adottati e applicate in modo uniforme nel perimetro considerato

Punto	Requisito chiave	Evidenze di riferimento	Criterio di verifica
9.4	Accettazione del rischio ed escalation	Decisioni di accettazione, soglie, motivazioni, escalation aperte/chiusure	Verificare che le accettazioni siano deliberate al livello appropriato e che i casi sopra soglia siano tracciati
9.7	Coordinamento con seconde linee e presidi specialistici	Calendario o modalità di raccordo, criteri comuni di classificazione ove presenti, flussi informativi condivisi, verbali o output dei momenti di coordinamento ove applicabili	Verificare che il modello di coordinamento sia definito, proporzionato al contesto, coerente con i presidi specialistici pertinenti e idoneo a evitare duplicazioni, disallineamenti informativi o lacune nel reporting
9.8	Reporting integrato	Report periodici, indicatori, stato piani, escalation, decisioni	Verificare periodicità, destinatari, contenuti minimi e capacità del reporting di supportare decisioni e follow up
10.2	Audit interno di gestione del rischio o verifica indipendente	Programma di audit/verifiche, criteri, campo, rapporti, azioni conseguenti	Verificare indipendenza sufficiente, frequenza definita, qualità degli esiti e chiusura dei follow up
10.3	Riesame di direzione	Verbali, presentazioni, decisioni	Verificare che il riesame sia svolto con frequenza pianificata e coerente con le esigenze dell'organizzazione, considerando la completezza degli input e la presenza di output, decisioni, responsabilità e tempi
11.1	Non conformità e azioni correttive	Registro rilievi, cause, piani correttivi, responsabili, scadenze, esiti di efficacia	Verificare che le azioni siano tracciate fino a chiusura e che le criticità significative siano seguite con follow up adeguato

Punto	Requisito chiave	Evidenze di riferimento	Criterio di verifica
Principi / requisito trasversale	Applicazione proporzionata del framework	Motivazione documentata delle principali scelte di semplificazione o rafforzamento del framework, ove rilevanti	Verificare che le scelte applicative siano coerenti con contesto, perimetro, complessità e rilevanza dei rischi, e che non compromettano gli elementi essenziali del framework

APPENDICE H – Correlazione tra i punti della presente Pdr, della UNI ISO 31000:2018 e della UNI 11865:2022

La presente appendice, di carattere informativo, riporta la correlazione tra i punti della presente Pdr e i corrispondenti contenuti della UNI ISO 31000:2018 e della UNI 11865:2022, al fine di evidenziarne le principali coerenze e agevolare la lettura integrata dei tre documenti.

PdR – Framework per la Gestione del rischio	UNI ISO 31000:2018	UNI 11865:2022
Introduzione 0.2 Principi	4 – Principi	0.3 – Principi Appendice A
5.1 – Comprensione del contesto e delle parti interessate	5.4.1 – Comprendere l'organizzazione e il suo contesto; 6.3.3 – Contesto esterno e interno	4.1 – Comprendere l'organizzazione e il suo contesto; 4.2 – Comprendere le esigenze e le aspettative delle parti interessate
5.2 – Definizione del campo di applicazione	6.3.2 – Definire il campo di applicazione	4.3 – Determinare il campo di applicazione del sistema di gestione
5.3 – Integrazione con governance, processi e altri sistemi	5.3 – Integrazione	0.2 – Il concetto di integrazione; 4.4 – Sistema di gestione
5.4 – Criteri di rischio	6.3.4 – Definire i criteri di rischio	3.37 – Criteri di rischio
5.5 – Elementi essenziali del framework	5 – Struttura di riferimento; 6 – Processo	3.40 – Struttura per la gestione del rischio; 4.4 – Sistema di gestione
6.1 – Leadership e impegno 6.2 – Politica per la gestione del rischio	5.2 – Leadership e impegno 5.4.2 – Esprimere chiaramente l'impegno per la gestione del rischio	5.1 – Leadership e impegno 5.2 – Politica 6 - Pianificazione
6.2 – Politica per la gestione del rischio	5.2 Leadership e Impegno 5.4.2 – Esprimere chiaramente l'impegno per la gestione del rischio	5.2 – Politica
6.3 – Ruoli, responsabilità e autorità	5.4.3 – Assegnare ruoli, autorità, responsabilità e obbligo di rendere conto	5.3 – Ruoli, responsabilità e autorità nell'organizzazione
7.1 – Obiettivi del framework per la gestione del rischio	5.4.2 – Esprimere chiaramente l'impegno per la gestione del rischio	6.2 – Obiettivi e pianificazione per il loro raggiungimento
7.2 – Pianificazione delle attività ERM	5.4.2 – Esprimere chiaramente l'impegno per la gestione del rischio	6 – Pianificazione

PdR – Framework per la Gestione del rischio	UNI ISO 31000:2018	UNI 11865:2022
	6.1 – Processo Generalità 6.3.4 - Definire i criteri di rischio 6.4 - Valutazione del rischio 6.5 - Trattamento del rischio	6.1 - Azioni per affrontare rischi e opportunità 8 – Attività operative
7.3 – Pianificazione delle modifiche	5.7.1 – Adattare	6.3 – Pianificazione delle modifiche
8 – Risorse	5.4.4 – Mettere a disposizione le risorse	7.1 – Risorse
8.2 – Competenza 8.3 - Formazione	5.4.4 – Mettere a disposizione le risorse 5.3 – Integrazione 5.5 - Attuazione	7.2 – Competenza
8.4 – Consapevolezza e cultura del rischio	5.2 Leadership e Impegno	3.23 – Risk based thinking; 3.25 – Cultura del rischio; 7.3 – Consapevolezza
8.4 – Comunicazione	5.4.5 – Stabilire comunicazione e consultazione; 6.2 – Comunicazione e consultazione	4.2 – Comprendere le esigenze e le aspettative delle parti interessate 7.4 – Comunicazione
8.5 – Informazioni documentate	6.7 – Registrazione e reporting	7.5 – Informazioni documentate
9.1 – Pianificazione e controllo operativo del processo	5.5 – Attuazione; 6.1 – Generalità del processo	7 – Supporto 8.1 – Pianificazione e controllo operativi
9.2 – Identificazione dei rischi	6.4.2 – Identificazione del rischio	6.1 - Azioni per affrontare rischi e opportunità 8.1 – Pianificazione e controllo operativi
9.3 – Analisi e ponderazione del rischio	6.4.3 – Analisi del rischio; 6.4.4 – Ponderazione del rischio	6.1 - Azioni per affrontare rischi e opportunità 8.1 – Pianificazione e controllo operativi
9.5 – Trattamento del rischio	6.5 – Trattamento del rischio	6.1 – Azioni per affrontare rischi e opportunità; 8.1 – Pianificazione e controllo operativi
9.6 – Monitoraggio di rischi, indicatori e piani	5.6 – Valutazione 6.6 – Monitoraggio e riesame	9.1 – Monitoraggio, misurazione, analisi e valutazione
9.8 – Reporting integrato	6.7 – Registrazione e reporting	9.1 – Monitoraggio, misurazione, analisi e valutazione
10.1 – Monitoraggio, analisi e valutazione del framework	5.6 – Valutazione	9.1 – Monitoraggio, misurazione, analisi e valutazione
10.2 – Audit interno	5.6 – Valutazione	9.2 – Audit interno
10.3 – Riesame di direzione	5.6 – Valutazione; 5.7 – Miglioramento; 6.6 Monitoraggio e Riesame	9.3 – Riesame di direzione
11.1 – Non conformità e azioni correttive	5.7 – Miglioramento	10.1 – Non conformità e azioni correttive
11.2 – Miglioramento continuo e apprendimento	5.7.2 – Migliorare in modo continuo	10.2 – Miglioramento continuo

BIBLIOGRAFIA

- [1] UNI CEI EN ISO/IEC 17050 - Valutazione della conformità - Dichiarazione di conformità del fornitore;
- [2] UNI CEI EN ISO/IEC 17065:2012 - Valutazione della conformità - Requisiti per organismi che certificano prodotti, processi e servizi.
- [3] UNI ISO 31073:2022 Gestione del rischio - Vocabolario
- [4] COSO, Enterprise Risk Management – Integrating with Strategy and Performance.