

# **ISO 31000**

## **Risk management**

### **Principles and guidelines on implementation**

- Il processo di gestione del rischio comporta l'applicazione di metodi logici e sistematici per:
  - comunicazione e consultazione durante tutto il processo;
  - definizione del contesto;
  - individuare, analizzare, valutare e trattare il rischio associato a qualsiasi processo, attività, funzione, progetto, prodotto, servizio o bene;
  - monitoraggio e revisione dei rischi;
  - registrazione e comunicazione dei risultati in modo appropriato.

- Questa norma riconosce la varietà della natura, del livello e la complessità dei rischi e fornisce delle linee guida generali sui principi e sull'attuazione della gestione dei rischi. Per applicare queste linee guida generali in una situazione concreta, la presente norma internazionale definisce come un'organizzazione deve comprendere il contesto specifico in cui si attua la gestione del rischio
- La gestione del rischio può essere applicata a tutta l'organizzazione, attraverso le sue molte aree e livelli, in qualsiasi momento, nonché a specifiche funzioni ed attività.

# ISO31000

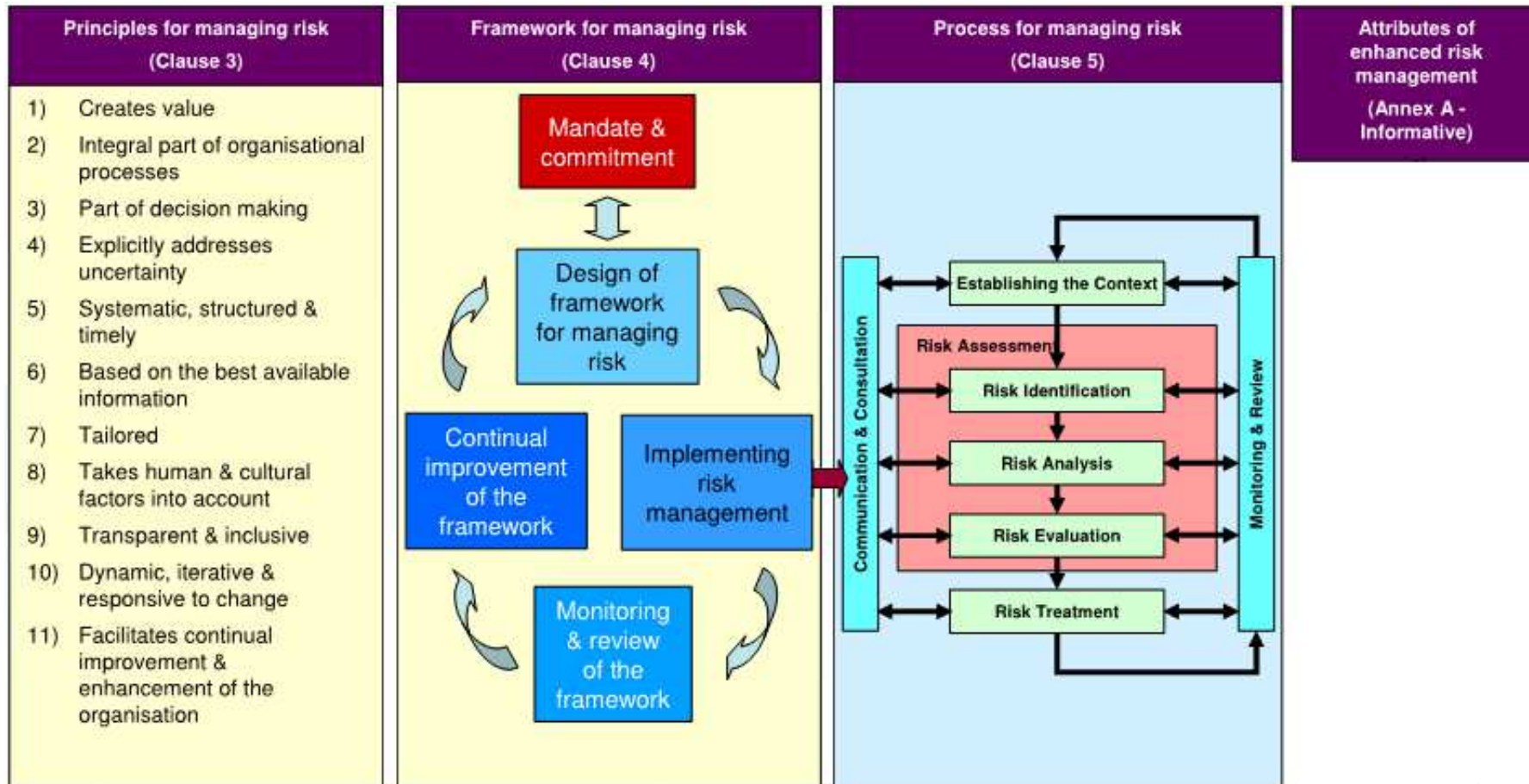
- Una volta implementato e mantenuto in conformità alla presente norma internazionale, la gestione del rischio consente a un'organizzazione, per esempio:
  - incoraggiare la gestione proattiva piuttosto che reattiva;
  - essere consapevoli della necessità di individuare e trattare il rischio in tutta l'organizzazione;
  - migliorare l'identificazione delle opportunità e delle minacce;
  - essere conformi ai rilevanti requisiti legali e normativi e alle norme internazionali;
  - migliorare l'informativa finanziaria;
  - migliorare la corporate governance;
  - migliorare la fiducia degli stakeholder;
  - stabilire una base affidabile per il processo decisionale e di pianificazione;
  - migliorare i controlli;
  - allocare efficacemente e utilizzare le risorse per il trattamento del rischio;
  - migliorare l'efficacia e l'efficienza operativa;
  - migliorare la salute e la sicurezza;
  - migliorare la gestione degli incidenti e la prevenzione;
  - minimizzare la perdita;
  - Migliorare l'apprendimento organizzativo;
  - Migliorare la resilienza organizzativa.

# ISO31000

- Per essere efficaci all'interno di una organizzazione, la gestione dovrebbe essere parte integrante della organizzazione generale di governo, gestione, reporting dei processi, politiche, filosofia e cultura
- Lo stesso approccio di gestione del rischio può essere adottato per tutte le attività di un'organizzazione, inclusi i progetti, le funzioni definite, i prodotti o attività, a sua volta rafforzare i collegamenti tra queste attività e gli obiettivi generali dell'organizzazione

# ISO31000

- Il rapporto tra i principi per la gestione del rischio, il framework di gestione del rischio e il processo di gestione dei rischi descritti nella presente norma è mostrato nella Figura seguente



- Scope
- La norma si propone di armonizzare i processi di gestione del rischio nelle norme esistenti e future. Esso fornisce un approccio comune a sostegno delle norme relative ai rischi e non sostituisce tali norme.



# Principi per la gestione del rischio

- Per essere più efficace, la gestione del rischio di un'organizzazione deve rispettare i seguenti principi.
  - a) **la gestione del rischio crea valore.** La gestione del rischio contribuisce al raggiungimento degli obiettivi dimostrabili
  - b) **La gestione del rischio è parte integrante dei processi organizzativi.** La gestione dei rischi fa parte delle responsabilità di gestione ed è parte integrante dei normali processi organizzativi, nonché di tutti i progetti e processi di gestione del cambiamento.
  - c) **La gestione del rischio è parte del processo decisionale.** La gestione del rischio aiuta i decisori a compiere scelte supportate da informazioni. La gestione del rischio può aiutare a definire le priorità e a distinguere tra corsi d'azione alternativi.
  - d) **La gestione del rischio affronta esplicitamente l'incertezza.** La gestione dei rischi si occupa di quegli aspetti del processo decisionale che sono incerti, la natura di tale incertezza, e come può essere affrontata.

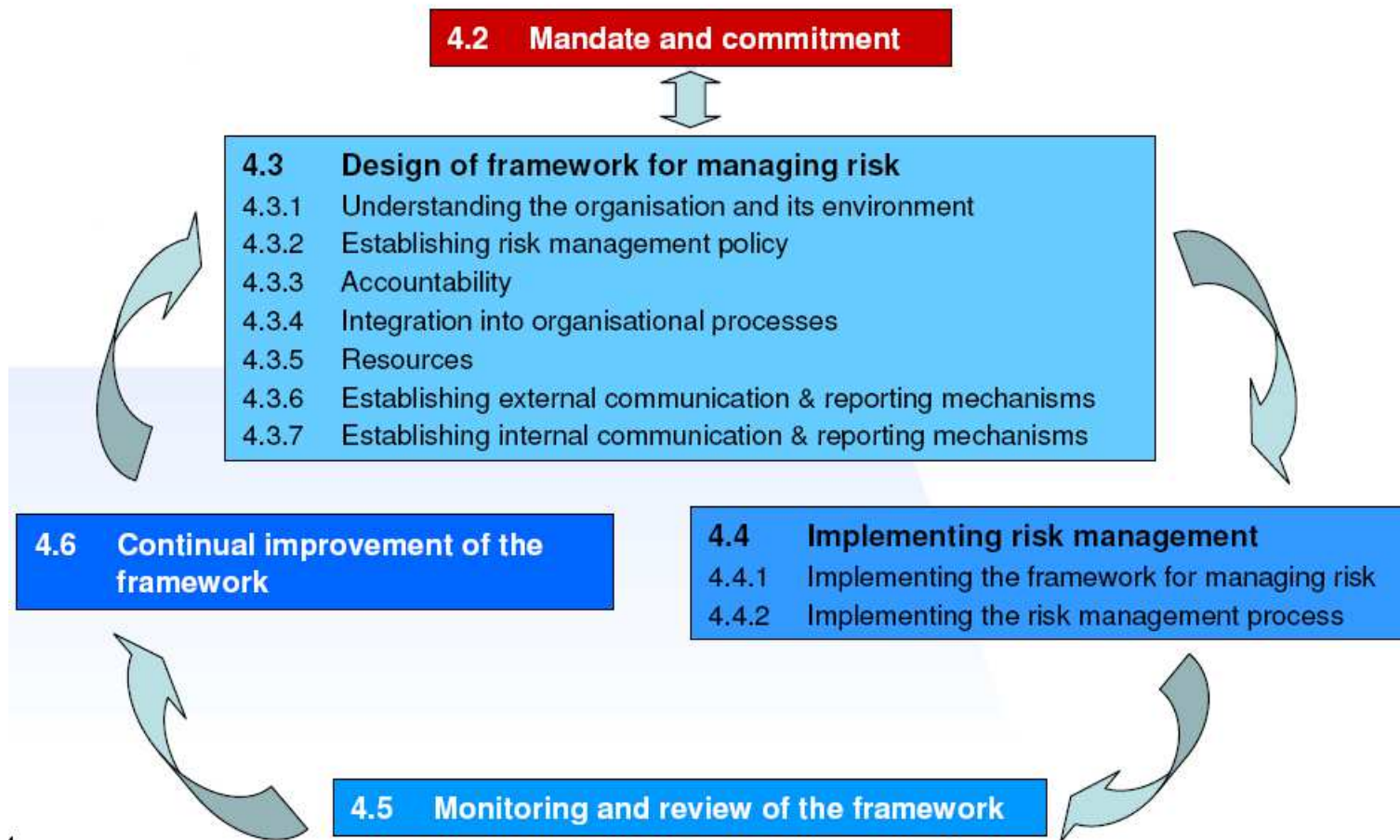
- e) **La gestione del rischio è sistematica, strutturata e tempestiva.** Un approccio sistematico, tempestivo e strutturato per la gestione del rischio contribuisce alla efficienza e a risultati coerenti, comparabili e affidabili.
- f) **La gestione del rischio si basa sulle migliori informazioni disponibili.** Gli ingressi per il processo di gestione del rischio si basano su fonti di informazione, come esperienza, commenti, osservazioni, previsioni e giudizi degli esperti.
- g) **La gestione del rischio è su misura.** La gestione del rischio è allineata con il contesto esterno ed interno dell'organizzazione e al profilo di rischio.
- h) **La gestione del rischio prende in considerazione i fattori umani e culturali.** La gestione dei rischi dell'organizzazione riconosce le percezioni, le capacità e le intenzioni delle persone esterne e interne che possono facilitare o ostacolare il raggiungimento degli obiettivi dell'organizzazione.

- i) **La gestione dei rischi è trasparente e inclusiva.** Appropriato e tempestivo coinvolgimento delle parti interessate e, in particolare, i decisori a tutti i livelli dell'organizzazione, assicurano che la gestione del rischio rimane rilevante.
- j) **La gestione del rischio è dinamica, interattiva e sensibile al cambiamento.** Quando eventi interni ed esterni si verificano, il contesto cambia ed emergono nuovi rischi, qualche cambiamento, e altri scompaiono.
- k) **La gestione del rischio facilita un continuo miglioramento e potenziamento dell'organizzazione.** Le organizzazioni dovrebbero sviluppare e attuare strategie per migliorare la loro maturità di gestione del rischio insieme a tutti gli altri aspetti della loro organizzazione.

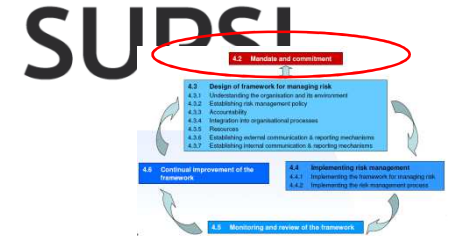
# Framework per la gestione dei rischi

Il framework per la gestione dei rischi non è inteso a prescrivere un sistema di gestione, ma piuttosto ad aiutare le organizzazioni ad integrare la gestione del rischio nel suo sistema complessivo di gestione.

# Framework per la gestione dei rischi



- 4 Framework per la gestione del rischio
- 4.1 Generalità
  - Per avere successo, la gestione del rischio dovrebbe funzionare in un quadro di gestione del rischio che fornisce le basi e le modalità organizzative affinché incorpori tutta l'organizzazione a tutti i livelli. Il framework assiste una organizzazione nella gestione dei propri rischi in modo efficace attraverso l'applicazione del processo di gestione del rischio a diversi livelli e nei contesti specifici dell'organizzazione. Il framework dovrebbe garantire che le informazioni sui rischi derivanti da tali processi siano adeguatamente segnalate e utilizzate come base per il processo decisionale e per la responsabilità a tutti i livelli organizzativi.
  - Questa clausola descrive i componenti del framework per la gestione del rischio che sono necessari e il modo in cui essi interagiscono come mostrato nella Figura



# Mandato e impegno

- 4.2 Mandato e impegno

- L'introduzione della gestione del rischio è la garanzia della sua efficacia, **richiede un forte impegno e deve essere sostenuta dalla gestione dell'organizzazione così come la strategia e la rigorosa pianificazione. La direzione dovrebbe:**
  - articolare e sostenere la politica di gestione dei rischi;
  - individuare gli indicatori di performance di gestione dei rischi che si allineano con gli indicatori di performance organizzativa;
  - assicurare l'allineamento degli obiettivi di gestione del rischio con gli obiettivi e le strategie dell'organizzazione;
  - garantire la conformità legale e normativa;
  - assegnare le responsabilità di gestione e le responsabilità a livelli adeguati all'interno dell'organizzazione;
  - garantire che le risorse necessarie siano state assegnate alla gestione del rischio;
  - comunicare i vantaggi della gestione del rischio a tutte le parti interessate;
  - garantire che il quadro di gestione del rischio continui a essere adeguato.

# Comprendere l'organizzazione e il suo contesto

- 4.3 Progettazione di un framework per la gestione del rischio
- 4.3.1 Comprendere l'organizzazione e il suo contesto
  - Prima di iniziare la progettazione e la realizzazione del quadro per la gestione del rischio, è importante **capire sia il contesto interno ed esterno dell'organizzazione** in quanto questi possono influenzare in modo significativo il disegno del framework.
  - Aspetti del contesto esterno dell'organizzazione includono, ma non sono limitati a:
    - l'ambiente culturale, politico, giuridico, normativo, finanziario, tecnologico, economico, naturale e competitivo, sia internazionale, nazionale, regionale o locale;
    - fattori chiave e le tendenze che hanno impatto sugli obiettivi dell'organizzazione,
    - percezioni e valori di stakeholders esterni





# Comprendere l'organizzazione e il suo contesto

- Aspetti del contesto interno dell'organizzazione includono, ma non si limitano a:
  - le capacità, intese in termini di risorse e conoscenze (es. capitale, tempo, persone, processi, sistemi e tecnologie);
  - sistemi di informazione, flussi informativi, e dei processi decisionali (sia formali che informali);
  - stakeholder interni;
  - politiche, gli obiettivi e le strategie che sono in atto per raggiungerli; percezioni, valori e cultura;
  - standard e modelli di riferimento adottati dalla organizzazione;
  - strutture (ad esempio la governance, i ruoli e le responsabilità).

# Politica di gestione del rischio

- 4.3.2 politica di gestione del rischio
  - La politica di gestione del rischio **dovrebbe chiarire gli obiettivi dell'organizzazione e il relativo impegno alla gestione dei rischi** e dovrebbe specificare quanto segue:
    - legami tra la politica di gestione del rischio e gli obiettivi dell'organizzazione e le altre politiche;
    - i razionali dell'organizzazione per la gestione dei rischi;
    - le responsabilità per la gestione del rischio;
    - il modo in cui vengono trattati gli interessi in conflitto;
    - la propensione al rischio dell'organizzazione o di avversione al rischio;

# Politica di gestione del rischio

- processi, metodi e strumenti da utilizzare per la gestione del rischio;
- risorse disponibili per aiutare i responsabili della gestione del rischio;
- il modo in cui le prestazioni di gestione del rischio saranno misurate e segnalate;
- impegno per la revisione periodica e di verifica della politica di gestione del rischio e il quadro per il suo miglioramento continuo;
- La politica di gestione del rischio deve essere comunicata in modo appropriato.

- 4.3.3 Responsabilità
  - L'organizzazione deve garantire che vi sia la responsabilità, l'autorità e le competenze adeguate per la gestione dei rischi, inclusa l'implementazione e il mantenimento del processo di gestione del rischio e garantire l'adeguatezza, l'efficacia e l'efficienza di eventuali controlli. Ciò può essere agevolato da:
    - individuare i responsabili dei rischi che hanno la responsabilità e l'autorità per gestire i rischi;
    - identificare chi è responsabile per l'attuazione dello sviluppo, e la manutenzione del framework per la gestione del rischio;
    - individuare le responsabilità di altre persone, a tutti i livelli dell'organizzazione, per il processo della gestione dei rischi;
    - definire un sistema per misurare le performance, una reportistica interna ed esterna e i processi di escalation;
    - assicurare adeguati livelli di riconoscimento.

# L'integrazione nei processi organizzativi

- 4.3.4 Integrazione nei processi organizzativi
- La gestione del rischio dovrebbe essere inserita in tutte le pratiche dell'organizzazione e dei processi in modo che sia pertinente, efficace ed efficiente. Il processo di gestione del rischio dovrebbe diventare una parte integrante e non separata da quelle dei processi organizzativi. In particolare, la gestione del rischio dovrebbe essere incorporata nella politica di sviluppo, di business e nella pianificazione strategica e di revisione.

# Risorse

- 4.3.5 Risorse
- L'organizzazione dovrebbe sviluppare gli strumenti pratici per allocare le risorse adeguate per la gestione del rischio.
- Occorre prendere in considerazione quanto segue:
  - persone, capacità, esperienza e competenze;
  - risorse necessarie per ciascuna fase del processo di gestione dei rischi;
  - processi e procedure documentate;
  - informazioni e sistemi di gestione delle conoscenze.

## **Stabilire comunicazioni interne e meccanismi di reporting**

- 4.3.6 Stabilire comunicazioni interne e meccanismi di reporting
- L'organizzazione deve stabilire la comunicazione interna e i meccanismi di reporting. Tali misure dovrebbero garantire che:
  - componenti chiave del framework di gestione del rischio, e ogni successiva modifica, siano comunicati in modo adeguato;
  - vi sia un adeguato reporting interno del framework, la sua efficacia e i risultati;
  - informazioni pertinenti desunte dall'applicazione della gestione dei rischi sono disponibili ai livelli appropriati;
  - ci sono processi di consultazione con gli stakeholder interni

## Stabilire comunicazioni esterne e meccanismi di reportistica

- 4.3.7 Stabilire comunicazioni esterne e meccanismi di reportistica
- L'organizzazione dovrebbe sviluppare e implementare un piano su come si comunica con gli stakeholder esterni. Ciò dovrebbe comprendere:
  - opportunità di coinvolgere gli stakeholder esterni e la garanzia di un efficace scambio di informazioni;
  - relazioni esterne per soddisfare i requisiti di governance legali, normativi e aziendali;
  - fornire feedback e reporting sulla comunicazione e la consultazione;
  - utilizzare la comunicazione per costruire la fiducia nell'organizzazione;
  - comunicare con gli stakeholder, in caso di crisi o emergenza.



# Attuare il framework per la gestione del rischio

- 4.4 Attuare la gestione del rischio
- 4.4.1 Attuare il framework per la gestione del rischio  
Nel framework di attuazione dell'organizzazione per la gestione del rischio, l'organizzazione dovrebbe:



- definire una tempistica adeguata e una strategia per l'attuazione del framework;
- applicare la politica di gestione e di processo del rischio ai processi organizzativi;
- conforme ai requisiti di legge e regolamentari;
- tenere sessioni di informazione e formazione;
- comunicare e consultarsi con gli stakeholder per garantire che il suo framework di gestione del rischio resti appropriato.

# **Attuazione del processo di gestione del rischio**

- 4.4.2 Attuazione del processo di gestione del rischio
- La gestione del rischio viene implementata per garantire che il processo di gestione dei rischi sia applicato a tutti i livelli e alle funzioni di una organizzazione come parte delle pratiche dell'organizzazione e dei processi aziendali.

# Monitoraggio e revisione del framework

- 4.5 Monitoraggio e revisione del framework
- Per garantire che la gestione dei rischi sia efficace e continua a sostenere le performance organizzative, l'organizzazione dovrebbe:
  - stabilire le misure delle performance;
  - periodicamente misurare i progressi e la deviazione dal piano di gestione dei rischi;
  - periodicamente verificare se il framework di gestione del rischio, della politica, e il piano sono ancora adeguati dato il contesto interno ed esterno delle organizzazioni;
  - report sui rischi, progressi con il piano di gestione dei rischi e garantire che la politica di gestione del rischio venga seguita correttamente;
  - verificare l'efficacia del quadro di gestione del rischio.

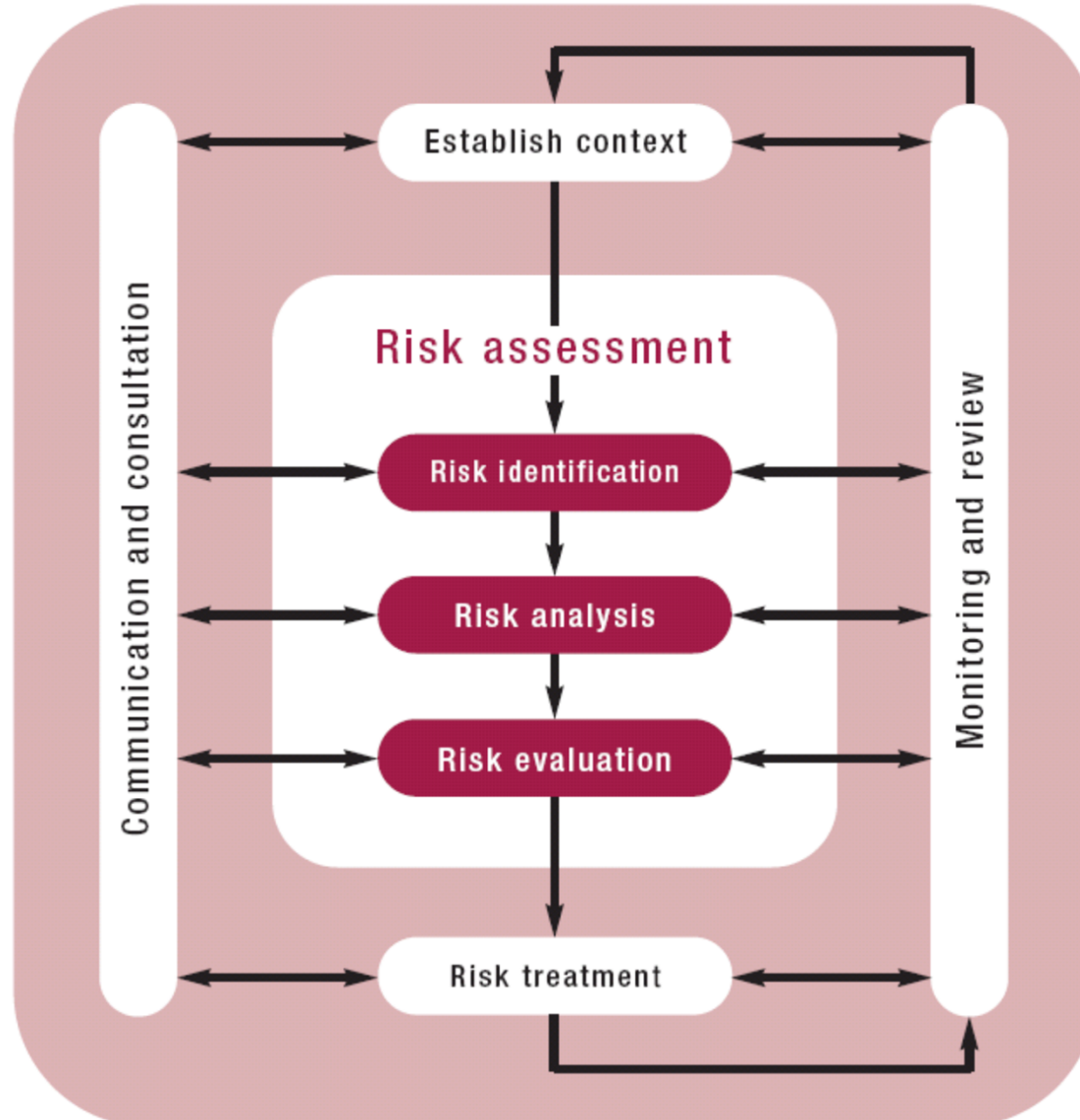


# Miglioramento continuo del framework

- 4.6 Miglioramento continuo del framework
- Sulla base della revisione, le decisioni dovrebbero essere prese su come il framework di gestione del rischio, la politica e il piano possano essere migliorati. Tali decisioni dovrebbero portare a miglioramenti nella gestione del rischio dell'organizzazione, e nella cultura di gestione del rischio.



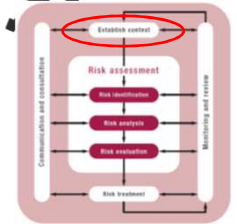
# Processi per la gestione dei rischi





# Comunicazione e consultazione

- 5.2 Comunicazione e consultazione
- La comunicazione e consultazione con gli stakeholder interni ed esterni, per quanto necessario, deve avvenire in ogni fase del processo di gestione del rischio.
- **Un approccio consultivo di gruppo è utile**, ma non solo, contribuisce a definire il contesto adeguato;
  - assicurare che gli interessi degli stakeholder siano compresi e considerati;
  - contribuire a garantire che i rischi siano adeguatamente identificati;
  - garantire che i diversi punti di vista siano adeguatamente considerati nella valutazione dei rischi;
  - migliorare la gestione del cambiamento durante il processo di gestione dei rischi;
  - sviluppare un'adeguata comunicazione interna ed esterna e un piano di consultazione.



# Creare il contesto

- 5.3 Creare il contesto
- 5.3.1 Generale
- Con la costituzione del contesto l'organizzazione definisce i parametri interni ed esterni da prendere in considerazione nella gestione del rischio e nella definizione dei criteri dello scope e del rischio per i processi rimanenti.

## Stabilire il contesto esterno

- 5.3.2 Stabilire il contesto esterno
- Il contesto esterno è l'ambiente esterno in cui l'organizzazione si propone di raggiungere i suoi obiettivi.
- Comprendere il contesto esterno è importante per garantire che gli stakeholder esterni, i loro obiettivi e le preoccupazioni siano considerati nello sviluppo dei criteri di rischio.
- Il contesto esterno può includere, ma non è limitato a:
  - culturali, politici, giuridici, normativi, finanziari, tecnologici, economici, naturali e competitivi;
  - ambiente, sia internazionale, nazionale, regionale o locale; fattori chiave e tendenze che hanno impatto sugli obiettivi dell'organizzazione,
  - percezioni e valori di soggetti esterni.



## Stabilire il contesto interno

- 5.3.3 Stabilire il contesto interno
- Il contesto interno è l'ambiente interno in cui l'organizzazione si propone di raggiungere i suoi obiettivi.
- Il processo di gestione del rischio deve essere allineato con la cultura dell'organizzazione, dei processi e della struttura.
- Il contesto interno è tutto all'interno della organizzazione che può influenzare il modo in cui un'organizzazione gestirà il rischio. Occorre stabilire perché:
  - la gestione del rischio si realizza nel contesto degli obiettivi dell'organizzazione;
  - Gli obiettivi e i criteri di un progetto o un'attività particolare deve essere considerata alla luce degli obiettivi dell'organizzazione nel suo insieme,
  - un grande rischio per alcune organizzazioni è il mancato raggiungimento della loro strategia, progetto o obiettivi di business,
  - Tale rischio riguarda l'impegno, la credibilità, la fiducia e il valore dell'organizzazione.

## **Stabilire il contesto del processo di gestione del rischio**

- 5.3.4 Stabilire il contesto del processo di gestione del rischio
- La gestione del rischio deve essere svolta con piena considerazione della necessità di giustificare le risorse utilizzate nello svolgimento della gestione dei rischi. Le risorse necessarie, le responsabilità e le autorità, e le registrazioni da tenere devono essere specificate.

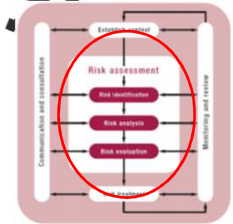
## **Stabilire il contesto del processo di gestione del rischio**

- Il contesto del processo di gestione del rischio varia in base alle esigenze di un'organizzazione. Può comprendere, ma non è limitato a:
  - definire le responsabilità del processo di gestione dei rischi; definire la portata, così come la profondità e l'ampiezza delle attività di gestione dei rischi da effettuare, comprese le specifiche inclusioni ed esclusioni;
  - definizione del processo, attività, funzione, progetto, prodotto, servizio o attività in termini di tempo e di luogo, nonché i suoi obiettivi;
  - definire i rapporti tra un particolare progetto o attività e altri progetti o attività dell'organizzazione;
  - definire le metodologie di valutazione dei rischi;
  - definire il modo in cui viene valutata la prestazione nella gestione del rischio;
  - individuare e specificare le decisioni che devono essere prese;

# Sviluppo dei criteri di rischio

- 5.3.5 Sviluppo dei criteri di rischio
- L'organizzazione dovrebbe sviluppare criteri che vengono utilizzati per valutare l'entità del rischio. I criteri possono riflettere i valori di organizzazioni, obiettivi e risorse. Alcuni criteri possono essere prelevati da, o ottenuti, da requisiti legali e normativi e da altri requisiti che l'organizzazione sottoscrive. I criteri di rischio devono essere coerenti con la politica di gestione dei rischi dell'organizzazione. I criteri di rischio dovrebbero essere sviluppati all'inizio di qualsiasi processo di gestione del rischio e essere continuamente rivisti.

- Quando si definiscono i criteri di rischio, i fattori che devono essere considerati dovrebbe includere i seguenti:
  - natura e il tipo di conseguenze che possono verificarsi e come saranno misurati;
  - come verrà definita la probabilità;
  - l'arco di tempo del rischio e / o la conseguenza;
  - come è determinato il livello di rischio;
  - il livello al quale il rischio diventa accettabile o tollerabile;
  - quale livello di rischio richiede un trattamento;
  - se le combinazioni di rischi multipli dovrebbero essere prese in considerazione.



# Risk assessment

- 5.4 Risk assessment
- 5.4.1 Generale
- La valutazione dei rischi è il processo globale di identificazione dei rischi, di analisi del rischio e di valutazione del rischio.

# Identificazione del rischio

- 5.4.2 Identificazione del rischio
- L'organizzazione dovrebbe individuare le fonti di rischio, le aree di impatto, gli eventi e le loro cause e le loro potenziali conseguenze. L'obiettivo di questa fase è quello di generare un elenco completo di rischi sulla base di quegli eventi che potrebbero migliorare, prevenire, degradare o ritardare il raggiungimento degli obiettivi. E' anche importante identificare i rischi associati al fatto di non perseguire un'opportunità.

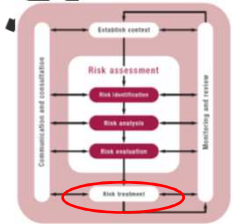
# Analisi del rischio

- 5.4.3 Analisi del rischio
  - L'analisi del rischio sviluppa la comprensione del rischio. L'analisi del rischio fornisce un contributo alla valutazione dei rischi e alle decisioni riguardanti i rischi che devono essere trattati e le strategie di rischio più adeguate. **L'analisi dei rischi comporta la considerazione delle cause e delle fonti di rischio, le loro conseguenze positive e negative, e la probabilità che tali conseguenze si possano verificare.** I fattori che influenzano le conseguenze e le probabilità dovrebbero essere identificate. Il rischio è analizzato per determinare le conseguenze e la loro probabilità, e altri attributi del rischio. Un evento può avere multiple conseguenze e può interessare multipli obiettivi.
  - L'analisi dei rischi può essere effettuata con diversi gradi di dettaglio in funzione del rischio, scopo dell'analisi, delle informazioni, dei dati e risorse disponibili. L'analisi può essere qualitativa, semi-quantitativa o quantitativa, o a una combinazione di questi, a seconda delle circostanze. In pratica, **l'analisi qualitativa è spesso usata per ottenere una prima indicazione generale del livello di rischio e per rivelare i rischi principali. Quando possibile e opportuno, si dovrebbe effettuare un'analisi più specifica e quantitativa dei rischi come passo successivo.**



# Valutazione dei rischi

- 5.4.4 Valutazione dei rischi
- Lo scopo della valutazione del rischio è di aiutare a prendere decisioni, sulla base dei risultati dell'analisi di rischio, su quali rischi è necessario un trattamento per dare priorità all'implementazione del trattamento.
- La valutazione dei rischi consiste nel confrontare il livello di rischio rilevato durante il processo di analisi dei rischi con i criteri stabiliti quando il contesto è stato considerato. **Se il livello di rischio non soddisfa i criteri di rischio, il rischio dovrebbe essere trattato.**
- Le decisioni devono tener conto del più ampio contesto del rischio e prendere in considerazione la tolleranza dei rischi a carico di soggetti diversi dall'organizzazione che beneficiano del rischio. Decisioni devono essere prese in conformità con i requisiti legali, normativi e di altri.



# Trattamento del rischio

- 5.5 Trattamento del rischio
- 5.5.1 Generale
- Il trattamento del rischio comporta la selezione di una o più opzioni per la modifica dei rischi, e l'attuazione di tali opzioni.
- Il trattamento del rischio implica un processo ciclico di valutazione di un trattamento del rischio; di decidere se i livelli di rischio residuo sono tollerabili o meno, se non tollerabile la generazione di un nuovo trattamento del rischio; e valutare l'effetto di tale trattamento fino a quando il rischio residuo è conforme ai criteri di rischio dell'organizzazione.

# Trattamento del rischio

- Le opzioni di trattamento del rischio non sono necessariamente mutuamente esclusive o appropriate in ogni circostanza. Le opzioni possono includere i seguenti:
  - evitare il rischio decidendo di non iniziare o continuare con l'attività che dà origine al rischio;
  - in cerca di un'opportunità, decidendo di avviare o continuare con un'attività che può creare o aggravare il rischio;
  - rimuovere la fonte del rischio;
  - cambiare la natura e l'entità del rischio;
  - cambiando le conseguenze;
  - condivisione del rischio con un altro soggetto o soggetti;
  - mantenendo il rischio per scelta.

## **Selezione delle opzioni di trattamento del rischio**

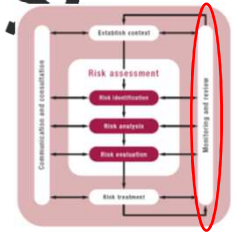
- 5.5.2 Selezione delle opzioni di trattamento del rischio
- La selezione dell'opzione di trattamento dei rischi più appropriato comporta il bilanciamento dei costi e dell'effort di attuazione in relazione ai benefici derivanti visti i requisiti legali, normativi, e altri, la responsabilità sociale e la tutela dell'ambiente naturale. Le decisioni devono anche tener conto dei rischi che possono giustificare le azioni di trattamento del rischio che non sono giustificate da motivi economici ad esempio grave (alto conseguenza negativa), ma raro (basso rischio) i rischi. Un certo numero di opzioni di trattamento può essere considerato di applicarle singolarmente o in combinazione. L'organizzazione può beneficiare dell'adozione di una combinazione di opzioni di trattamento.

## **Selezione delle opzioni di trattamento del rischio**

- Quando si selezionano le opzioni di trattamento del rischio, l'organizzazione dovrebbe considerare i valori e le percezioni degli stakeholder e le modalità più opportune per comunicare con loro. **Nei casi in cui le opzioni di trattamento del rischio possono avere un impatto sul rischio nel resto della organizzazione, questi settori dovrebbero essere coinvolti nella decisione.**
- Anche se ugualmente efficace, alcuni trattamenti di rischio possono essere più accettabili per gli stakeholder di altri.
- **Il trattamento del rischio può presentare dei rischi. Un rischio significativo può essere il fallimento o l'inefficacia delle misure di trattamento dei rischi.** Il monitoraggio deve essere parte integrante del piano di trattamento del rischio per dare assicurazione che le misure rimangano efficaci.
- **Il trattamento del rischio può anche introdurre rischi secondari che devono essere valutati, trattati, monitorati e esaminati.**

## La preparazione e l'attuazione dei piani di trattamento del rischio

- 5.5.3 La preparazione e l'attuazione dei piani di trattamento del rischio
- Lo scopo dei piani di trattamento del rischio è quello di documentare in che modo le opzioni del trattamento scelto saranno attuate.
- Le informazioni fornite nei piani di trattamento devono comprendere:
  - benefici attesi da ottenere;
  - misure di performance e vincoli;
  - persone che sono responsabili dell'approvazione del piano ed i responsabili dell'attuazione del programma;
  - azioni proposte;
  - reporting e monitoraggio dei requisiti;
  - requisiti delle risorse;
  - tempi e orari.



# Monitoraggio e revisione

- 5.6 Monitoraggio e revisione
- Il monitoraggio e la revisione dovrebbe essere una parte del piano, del processo di gestione del rischio. La responsabilità per il monitoraggio e la revisione dovrebbe essere chiaramente definito.
- Il monitoraggio dell'organizzazione e la revisione dei processi dovrebbe comprendere tutti gli aspetti del processo di gestione del rischio ai fini di:
  - analizzare e trarre insegnamento dagli eventi, i cambiamenti e le tendenze;
  - rilevazione dei cambiamenti del contesto esterno e interno, comprese le modifiche del rischio stesso, che può richiedere una revisione dei trattamenti di rischio e priorità;
  - garantire che il controllo del rischio e le misure di trattamento siano efficaci sia nel disegno e nel funzionamento;
  - individuazione dei rischi emergenti.

## Registrazione del processo di gestione del rischio

- 5.7 Registrazione del processo di gestione del rischio
- L'attività di gestione del rischio deve essere rintracciabile. Nel processo di gestione del rischio, i record forniscono le basi per migliorare metodi e strumenti, nonché l'intero processo.
- Le decisioni riguardanti la creazione di record dovrebbe tener conto:
  - benefici del riutilizzo delle informazioni a fini di gestione;
  - i costi e gli sforzi coinvolti nella creazione e mantenimento di registri;
  - esigenze legali, normative e operative per i record;
  - metodo di accesso, la facilità di recuperare e archiviare i media;
  - periodo di conservazione;



- A.1 generale
  - La capacità di gestire il rischio è una delle competenze fondamentali di qualsiasi organizzazione e dei suoi dipendenti. I metodi di gestione del rischio e gli strumenti assistono qualsiasi organizzazione nel pianificare e attuare azioni concrete e programmi volti a massimizzare le loro opportunità e di controllare le loro minacce.
  - L'organizzazione ha un maggiore controllo della propria crescita e sviluppo, quando la gestione del rischio è applicata.
  - Tutte le organizzazioni devono mirare al più alto livello di prestazioni del loro quadro di gestione del rischio in linea con la criticità delle decisioni che devono essere prese. L'elenco degli attributi (...segue...) rappresenta un alto livello di performance nella gestione del rischio. Per aiutare le organizzazioni a misurare la propria performance nei confronti di questi criteri, alcuni indicatori tangibili sono dati per ciascun attributo.

- A.2 Attributi
  - A.2.1 L'accento posto sul **miglioramento continuo** nella gestione del rischio attraverso la fissazione di obiettivi di performance organizzative, di misura, la revisione e la successiva modifica di processi, sistemi, risorse, capacità e competenze.  
Questo sarebbe indicato dall'esistenza di obiettivi di performance espliciti nei confronti dei quali si misura l'organizzazione e le prestazioni del manager. Le prestazioni di un'organizzazione possono essere pubblicate e comunicate. Normalmente, ci sarebbe almeno un esame annuale delle prestazioni e quindi una revisione dei processi, e la fissazione di obiettivi di performance riveduti per il periodo successivo.  
Questa valutazione della gestione del rischio delle performance è parte integrante della valutazione delle prestazioni dell'organizzazione generale e del sistema di misura per i reparti e gli individui.

- A.2.2 Completa, pienamente definita e pienamente accettata la **responsabilità** per i rischi, controlli del rischio e attività di trattamento del rischio. Persone designate, integralmente accettate, sono adeguatamente qualificate e dotate di risorse adeguate per controllare i rischi, monitorare i rischi, migliorare i controlli del rischio e comunicare in modo efficace i rischi e la loro gestione agli stakeholder interni ed esterni.

Questo sarebbe indicato da tutti i membri di un'organizzazione di essere pienamente consapevole dei rischi, controlli dei rischi e dei compiti di cui sono responsabili. Normalmente questa sarà registrata nel lavoro / descrizioni posizione, banche dati o sistemi d'informazione. La definizione dei ruoli di gestione dei rischi, le responsabilità devono essere parte di tutti i programmi di introduzione dell'organizzazione.

L'organizzazione assicura che coloro che sono responsabili sono in grado di assolvere il proprio ruolo fornendo loro l'autorità, il tempo, la formazione, le risorse e le competenze sufficienti per assumere le proprie responsabilità.

- A.2.3 Tutti i **processi** decisionali all'interno dell'organizzazione, indipendentemente dal livello di importanza e significato, implicano la considerazione esplicita dei rischi e l'applicazione di gestione del rischio in qualche misura appropriate.

Questo è indicato attraverso l'esame dei verbali delle riunioni e delle decisioni per dimostrare che le discussioni esplicite sui rischi ha avuto luogo. Inoltre, dovrebbe essere possibile vedere che tutti i componenti della gestione del rischio sono rappresentati all'interno di processi chiave per il processo decisionale all'interno dell'organizzazione, ad esempio, per le decisioni relative alla concessione di capitali, sui grandi progetti e sulla ristrutturazione e cambiamenti organizzativi. Per queste ragioni, la gestione del rischio con solide basi, è visto all'interno dell'organizzazione per fornire le basi per una governance efficace e prudente.

- A.2.4 **Comunicazioni** continue con gli stakeholder interni ed esterni tra cui reporting completo e frequente delle prestazioni di gestione del rischio fa parte del buon governo. Questo è indicato dalla comunicazione con gli stakeholder e diviene chiaramente considerato come una componente integrante ed essenziale della gestione del rischio, in modo che la comunicazione con gli stakeholder possa avvenire nell'ambito di ogni attività del processo di gestione del rischio. La comunicazione è giustamente considerata come un processo a due vie tra stakeholder e progetto. Comprensivi e frequenti reporting interni ed esterni, su entrambi i rischi significativi e sulle prestazioni di gestione del rischio, contribuisce in modo sostanziale alla governance efficace all'interno di un'organizzazione.

- A.2.5 La gestione del rischio è visto come fondamentale per la gestione dell'organizzazione dei processi in modo che i rischi siano considerati in termini di effetto di incertezza sugli obiettivi. La struttura di governo dell'organizzazione e il processo si basano sulla gestione del rischio. L'efficace gestione del rischio è considerata dai responsabili come essenziale per il raggiungimento degli obiettivi dell'organizzazione.