Corso di
SICUREZZA NEL TRASPORTO E NELLE INFRASTRUTTURE STRATEGICHE

Metodologie di Valutazione e Gestione del Rischio

Cpt. Claudia Brisotto
claudia.brisotto@me.com

Scopo e contenuti delle lezioni

Risk Management

Scopo e contenuti delle lezioni

Prima parte
- Capire come le organizzazioni **gestiscono** il rischio
- Capire il processo organizzativo e documentale

Seconda parte
- Le tecniche di valutazione del rischio
- Alcuni esempi

Terza parte
- La gestione del rischio nel settore aeronautico
- Peculiarità

Risk Management

ISO, the International Organization for Standardization.
develops and publishes International Standards.

ISO 31000(2018) Gestione del rischio - Principi e linee guida

ISO 31010(2019) Risk management - Risk assessment techniques

ISO/IEC Guide 73, Risk management – Vocabulary – Guidelines for use in standards

Risk Management

ISO 31000

Tutte le attività di un'organizzazione comportano dei rischi.

Le organizzazioni **gestiscono** il rischio **identificandolo**, **analizzandolo** e **valutando** se esso debba essere modificato attraverso il trattamento (del rischio) per soddisfare i **propri criteri di rischio**.

.

Risk Management

ISO 31000

Raccomanda che le organizzazioni sviluppino, attuino e migliorino in continuo una **struttura di riferimento*** il cui lo scopo è **integrare il processo per gestire il rischio nella governance complessiva dell'organizzazione**, nella **strategia e nella pianificazione**, nella **gestione**, nei processi di **reporting**, nelle **politiche**, nei **valori** e nella **cultura**.

Risk Management

ISO 31000

Relazioni tra i principi della gestione del rischio, la struttura di riferimento ed il processo

ISO 31000

Risk Management

a) Crea valore

b) Parte integrante dei processi dell'organizzazione

c) Parte del processo decisionale

d) Tratta esplicitamente l'incertezza

e) Sistematico, strutturato e tempestivo

f) Basato sulle migliori informazioni disponibili

g) Su misura

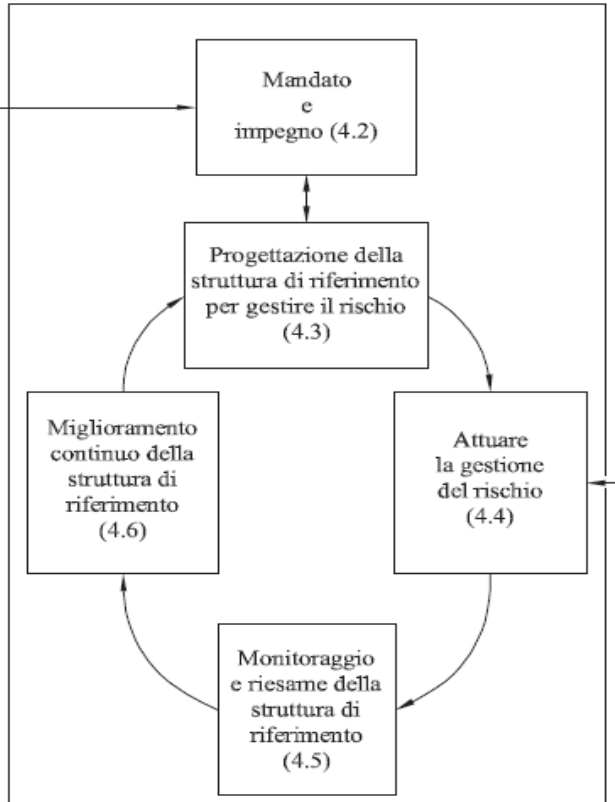
h) Tiene conto dei fattori umani e culturali

i) Transparente e inclusivo

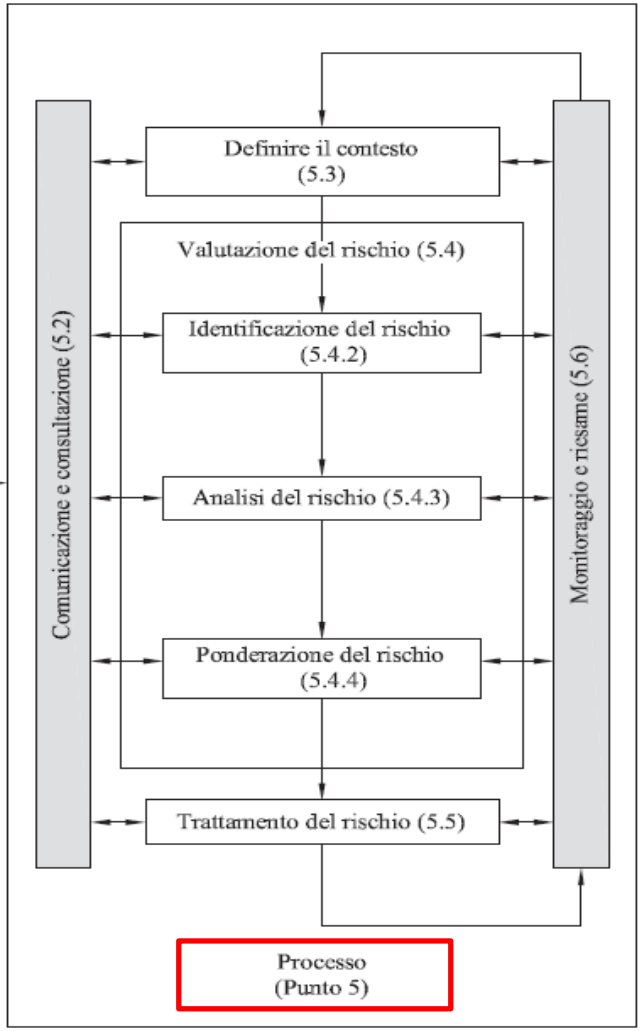
j) Dinamico, iterativo e reattivo al cambiamento

k) Favorisce il miglioramento continuo e il consolidamento dell'organizzazione

Principi (Punto 3)



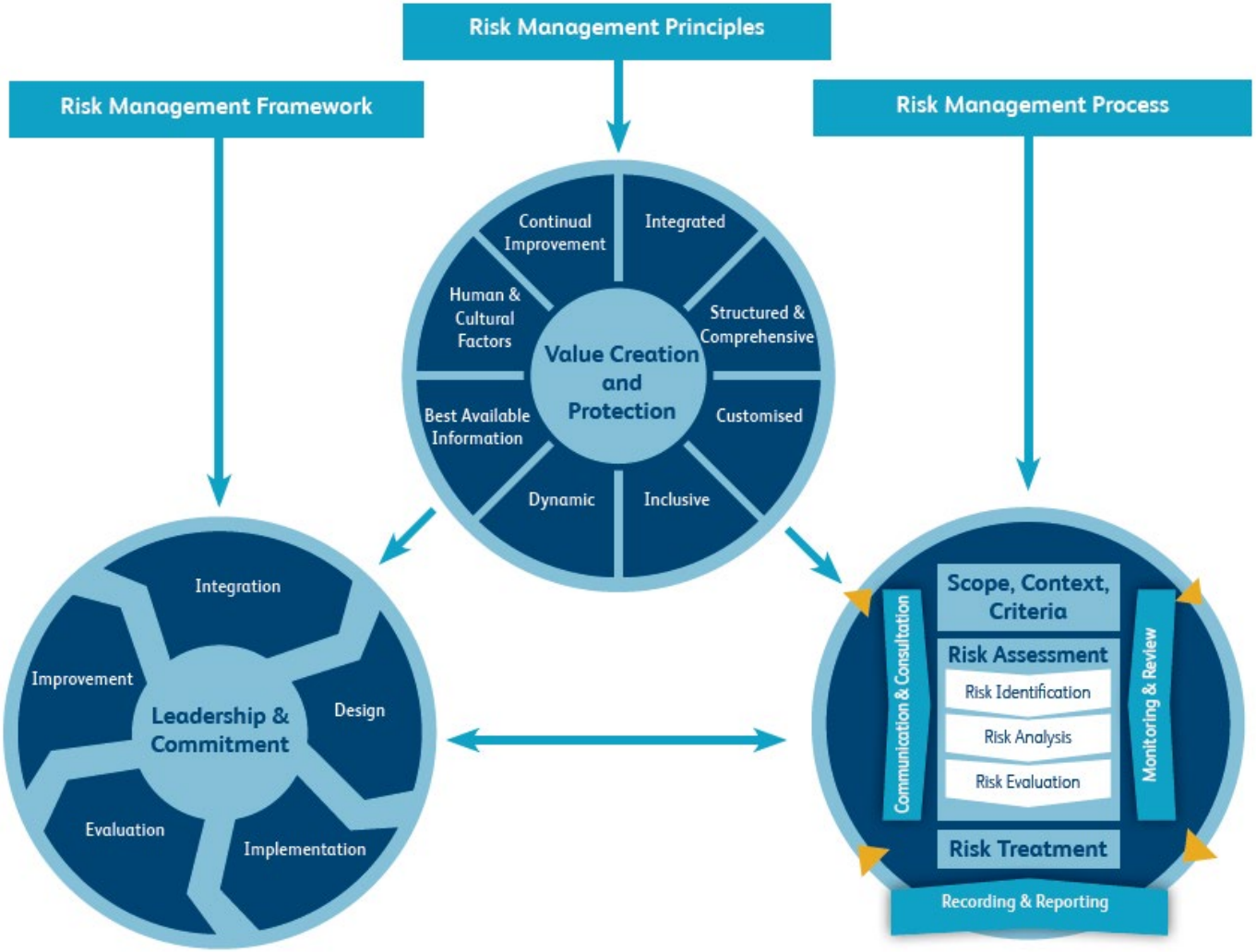
Struttura di riferimento (Punto 4)



Processo (Punto 5)

ISO 31000 2018

Risk Management



Risk Management

ISO 31000

PRINCIPI

Risk Management

ISO 31000
PRINCIPI

Per far sì che la gestione del rischio sia efficace, un'organizzazione dovrebbe, a tutti i livelli, seguire i principi riportati definiti.

a) La gestione del rischio crea e protegge il valore.

La gestione del rischio contribuisce in maniera dimostrabile al **raggiungimento degli obiettivi** ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto, gestione dei progetti, efficienza nelle operazioni, governance e reputazione.

b) La gestione del rischio è parte integrante di tutti i processi* dell'organizzazione.

La gestione del rischio **non è un'attività indipendente**, separata dalle attività e dai processi principali dell'organizzazione. La gestione del rischio fa parte delle responsabilità della direzione ed è parte integrante **di tutti i processi** dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei **progetti e del cambiamento.**

Risk Management

ISO 31000

…

c) **La gestione del rischio è parte del processo decisionale**.
La gestione del rischio aiuta i responsabili delle decisioni ad **effettuare scelte consapevoli,** determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.

d) **La gestione del rischio tratta esplicitamente l'incertezza.**
La gestione del rischio tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata.

e) **La gestione del rischio è sistematica, strutturata e tempestiva.**
Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.

Risk Management

ISO 31000

…

f) **La gestione del rischio si basa sulle migliori informazioni disponibili.**
Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne conto, di qualsiasi **limitazione dei dati** o del modello utilizzati o della possibilità di divergenza di opinione tra gli specialisti.

g) **La gestione del rischio è "su misura".**
La gestione del rischio è in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione.

h) **La gestione del rischio tiene conto dei fattori umani e culturali.**
Nell'ambito della gestione del rischio individua **capacità**,**comportamenti**, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

Risk Management

ISO 31000

…

i) **La gestione del rischio è trasparente e inclusiva.**
Il **coinvolgimento** appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio.

j) **La gestione del rischio è dinamica, iterativa e reattiva al cambiamento.**
La gestione del rischio è **sensibile** e **risponde al cambiamento** continuamente. Si applica ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

Risk Management

ISO 31000

…

k) **La gestione del rischio favorisce il miglioramento continuo dell'organizzazione.**

Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la **maturità** della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione

Risk Management

ISO 31000
BENEFICI

La gestione del rischio, quando attuata e mantenuta attiva in conformità alle norme, consente ad un'organizzazione di:

- aumentare la probabilità di raggiungere gli obiettivi;
- incoraggiare una gestione proattiva;
- essere consapevoli della necessità di identificare e trattare il rischio nell'intera organizzazione;
- migliorare l'identificazione delle opportunità e delle minacce;
- soddisfare i requisiti cogenti e le norme internazionali pertinenti;
- migliorare il reporting cogente e volontario;
- migliorare la governance;
- migliorare la confidenza e la fiducia dei portatori d'interesse;
- …

Risk Management

ISO 31000
BENEFICI
…

- costituire una base affidabile per il processo decisionale e la pianificazione;
- migliorare i controlli;
- assegnare ed utilizzare efficacemente risorse per il trattamento dei rischi;
- migliorare l'efficacia e l'efficienza operative;
- accrescere le prestazioni in ambito di salute e sicurezza, così come di protezione ambientale;
- migliorare la gestione della prevenzione delle perdite e la gestione degli incidenti;
- minimizzare le perdite;
- migliorare l'apprendimento organizzativo;
- migliorare la resilienza organizzativa.

Risk Management

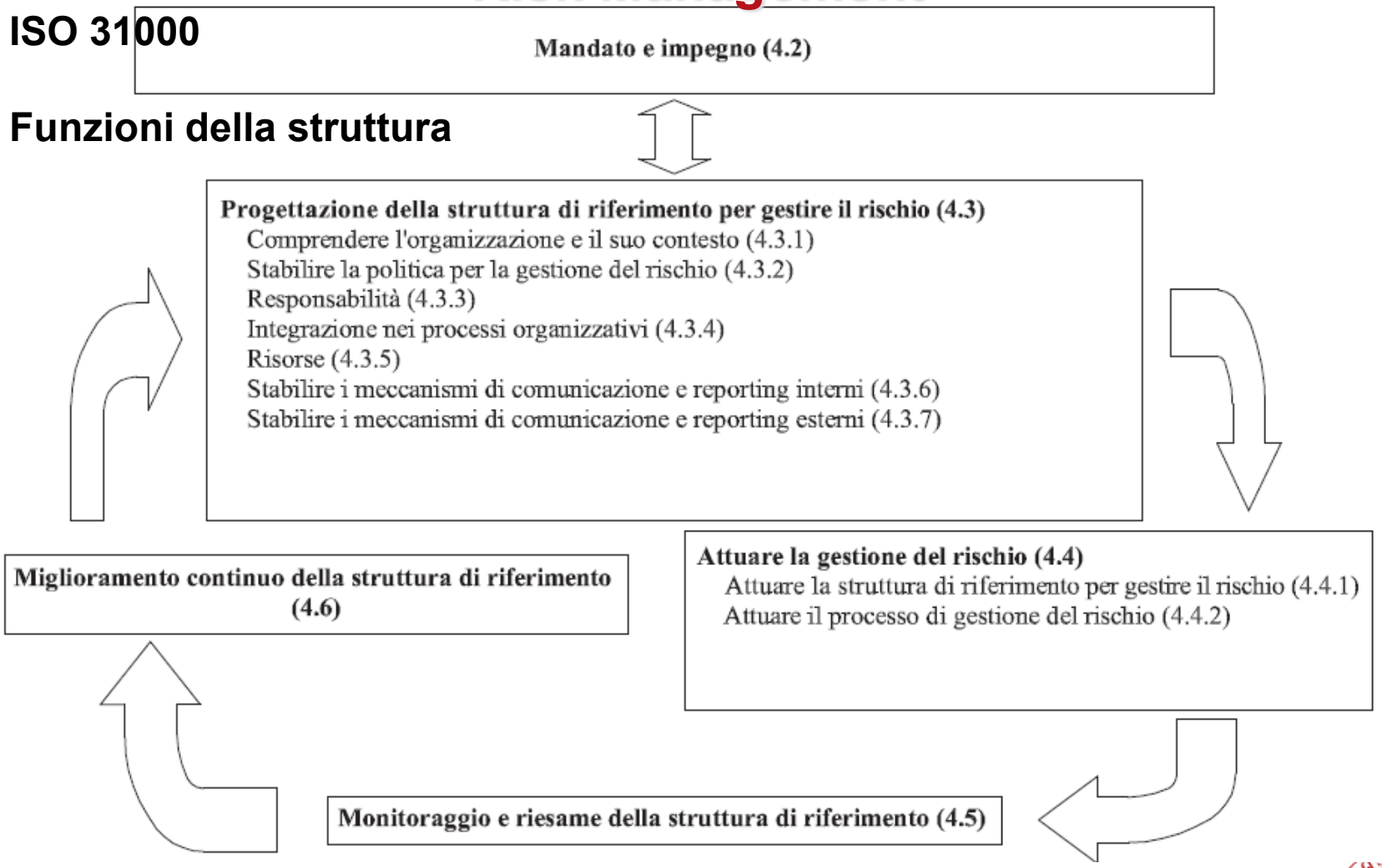
ISO 31000

STRUTTURA DI RIFERIMENTO

Risk Management

ISO 31000

Funzioni della struttura



Risk Management

ISO 31000

Mandato e impegno

Risk Management

ISO 31000

Mandato e impegno

L'introduzione della gestione del rischio e l'assicurazione della sua continua efficacia richiedono un **impegno forte e costante da parte della direzione dell'organizzazione**, così come una pianificazione strategica e rigorosa per ottenere tale impegno a tutti i livelli.

La direzione dovrebbe:

- **definire e sottoscrivere** una politica per la gestione del rischio;
- assicurare che la politica per la gestione del rischio sia in linea con la cultura dell'organizzazione;
- determinare indicatori di prestazione della gestione del rischio che siano in linea con gli indicatori di prestazione dell'organizzazione;
- allineare gli obiettivi della gestione del rischio con gli obiettivi e le strategie
- dell'organizzazione;*
- assicurare il rispetto dei requisiti cogenti;
- …

Risk Management

ISO 31000

…

- assegnare i vari gradi di **responsabilità*** ai livelli appropriati all'interno
- dell'organizzazione;
- assicurare che alla gestione del rischio siano allocate le **risorse** necessarie;
- comunicare ai **portatori d'interesse* i benefici della gestione del rischio**; e
- assicurare che la struttura di riferimento per gestire il rischio continui ad essere appropriata

Risk Management

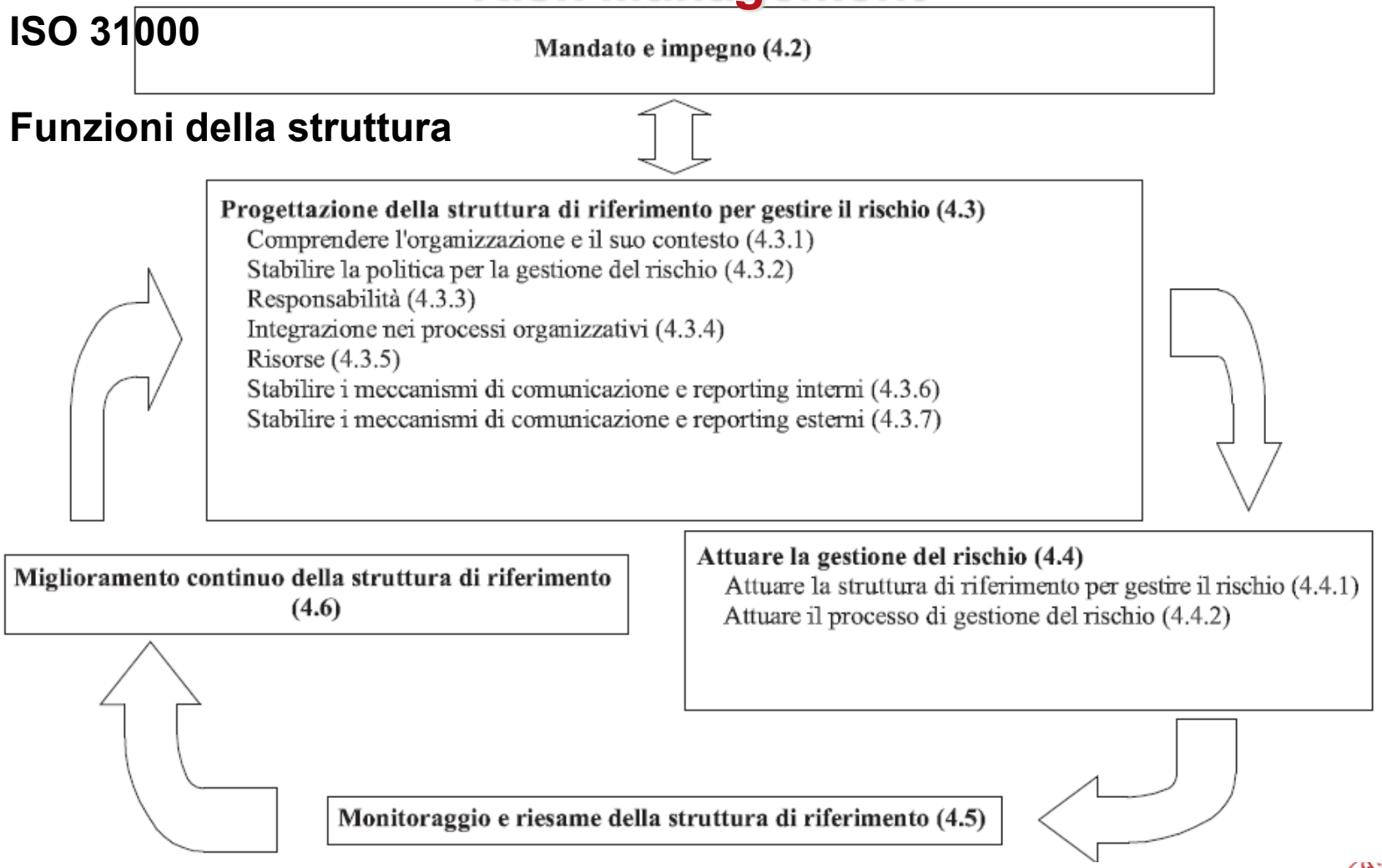
ISO 31000

Progettazione della struttura di riferimento per gestire il rischio

Risk Management

ISO 31000

Funzioni della struttura



Risk Management

ISO 31000

Comprendere l'organizzazione ed il suo contesto

Prima d'iniziare la progettazione e l'attuazione della struttura di riferimento per gestire il rischio, è importante valutare e comprendere **il contesto** dell'organizzazione, sia **interno**, sia **esterno**, poiché questi possono influenzare significativamente la progettazione della struttura medesima.

La valutazione del **contesto esterno** all'organizzazione può includere, ma non è limitato a:

a) **l'ambiente sociale***, culturale, politico, cogente, finanziario, **tecnologico*,** economico, naturale e competitivo, a livello **internazionale*,** nazionale, regionale o locale;
b) elementi determinanti e tendenze fondamentali che hanno un impatto sugli obiettivi dell'organizzazione; e
c) relazioni con i portatori d'interesse esterni, loro percezioni e valori.

Risk Management

ISO 31000

Comprendere l'organizzazione ed il suo contesto

…

La valutazione del **contesto interno** all'organizzazione può includere, ma non è limitato a:

- governance, struttura organizzativa, ruoli e responsabilità;
- politiche, obiettivi e le strategie in atto per il loro conseguimento;
- capacità, intese in termini di risorse e conoscenza (per esempio capitale, tempo, persone, processi, sistemi e tecnologie);
- sistemi e **flussi informativi***, processi decisionali (sia formali sia informali);
- relazioni con i portatori d'interesse interni, loro percezioni e valori;
- la cultura dell'organizzazione;
- norme, linee guida e modelli adottati dall'organizzazione; e
- la forma e l'estensione delle relazioni contrattuali.

Risk Management

ISO 31000

Stabilire la politica per la gestione del rischio

La politica per la gestione del rischio dovrebbe definire chiaramente gli obiettivi, ed il relativo **impegno**, per la gestione del rischio e tipicamente tratta quanto segue:

- il fondamento logico dell'organizzazione per gestire il rischio;
- i legami tra gli obiettivi dell'organizzazione, le politiche e la politica per la gestione del rischio;*
- i vari gradi di responsabilità per gestire il rischio;
- il modo in cui sono trattati i **conflitti d'interesse*;**
- l'impegno di rendere disponibili le risorse necessarie per supportare coloro che hanno i vari gradi di responsabilità per gestire il rischio;
- il modo in cui viene misurata e riferita la prestazione relativa alla gestione del rischio;
- l'**impegno** a riesaminare e migliorare periodicamente, e in risposta ad un evento o ad un cambiamento di circostanze, la politica per la gestione del rischio e la struttura di riferimento.

La politica per la gestione del rischio dovrebbe essere adeguatamente comunicata.

Risk Management

ISO 31000

Responsabilità

L'organizzazione dovrebbe assicurare che vi siano responsabilità, autorità e competenza appropriate per gestire il rischio, compresi l'attuazione e il mantenimento del processo di gestione del rischio e l'assicurazione della sua adeguatezza, efficacia ed efficienza di tutti i controlli.

Ciò può essere facilitato mediante:

- l'identificazione dei titolari del rischio che detengono la responsabilità e autorità per gestire i rischi;
- l'identificazione di chi deve rendere conto dello sviluppo, attuazione, e mantenimento della struttura di riferimento per gestire il rischio;
- l'identificazione delle altre responsabilità, riguardanti il processo di gestione del rischio, per le persone a tutti i livelli nell'organizzazione;
- stabilendo processi per la misurazione delle prestazioni, per il reporting esterno e/o interno e per il coinvolgimento dei livelli gerarchici; e
- l'assicurazione di appropriati livelli di riconoscimento.

Risk Management

ISO 31000

Integrazione nei processi organizzativi

La gestione del rischio dovrebbe essere incorporata in tutte le prassi e processi dell'organizzazione, in una maniera tale da essere pertinente, efficace ed efficiente.

Il processo di gestione del rischio dovrebbe diventare parte di tali processi organizzativi e non essere separato da essi. In particolare, la gestione del rischio dovrebbe essere incorporata nello sviluppo della **politica,** nella **pianificazione strategica** e commerciale, nel loro riesame, e nei processi di **gestione del cambiamento**.

Dovrebbe esistere un piano di gestione del rischio riguardante l'intera organizzazione per assicurare che sia attuata la politica di gestione del rischio e che la gestione del rischio sia integrata in tutte la prassi e tutti i processi dell'organizzazione. Il piano di gestione del rischio può essere integrato in altri piani dell'organizzazione, come un piano strategico.

Risk Management

ISO 31000

Risorse

L'organizzazione dovrebbe assegnare risorse appropriate per la gestione del rischio.

Dovrebbe essere preso in considerazione quanto segue:

- le persone e le loro abilità, esperienza e competenza*;
- le risorse necessarie per ciascuna fase del processo di gestione del rischio;
- i processi, i metodi e gli strumenti dell'organizzazione da utilizzare per gestire il rischio;
- i processi e le procedure documentati;
- i sistemi di gestione dell'informazioni e della conoscenza; e
- i programmi di formazione-addestramento*.

Risk Management

ISO 31000

Stabilire i meccanismi di comunicazione e reporting interni

L'organizzazione dovrebbe stabilire i meccanismi di **comunicazione e reporting interni*** al fine di supportare e incoraggiare la responsabilità e la presa in carico del rischio. Questi meccanismi dovrebbero assicurare che:

- i componenti chiave della struttura di riferimento per la gestione del rischio, e qualsiasi successiva modifica, siano adeguatamente comunicati;
- vi sia un **adeguato reporting interno** circa la struttura di riferimento, la sua efficacia e gli esiti;
- le informazioni pertinenti derivanti dall'applicazione della gestione del rischio siano disponibili ai livelli e nei tempi appropriati; e
- vi siano processi di consultazione con i portatori d'interesse interni.

Questi meccanismi dovrebbero, ove appropriato, includere processi per **consolidare** le informazioni relative al rischio **provenienti da varie fonti**, ed è probabile che sia necessario prendere in considerazione la delicatezza delle informazioni.

Risk Management

ISO 31000

Stabilire i meccanismi di comunicazione e reporting esterni

L'organizzazione dovrebbe sviluppare a attuare un piano circa le modalità di **comunicazione** con i portatori d'interesse esterni. Ciò dovrebbe implicare:

- il coinvolgimento di portatori d'interesse esterni appropriati e l'assicurazione di uno scambio d'informazioni efficace;
- la conformità del reporting esterno ai requisiti **cogenti*** e di governance;
- l'acquisizione di informazioni di ritorno e rapporti sulla comunicazione e
- consultazione;
- l'utilizzazione della comunicazione per creare fiducia nei confronti
- dell'organizzazione; e
- la comunicazione con i portatori d'interesse nel caso di una crisi o di un'**emergenza**.

Questi meccanismi dovrebbero includere, ove appropriato, processi per consolidare le informazioni relative al rischio provenienti da varie fonti, ed è probabile che sia necessario prendere in considerazione la delicatezza delle informazioni.

Risk Management

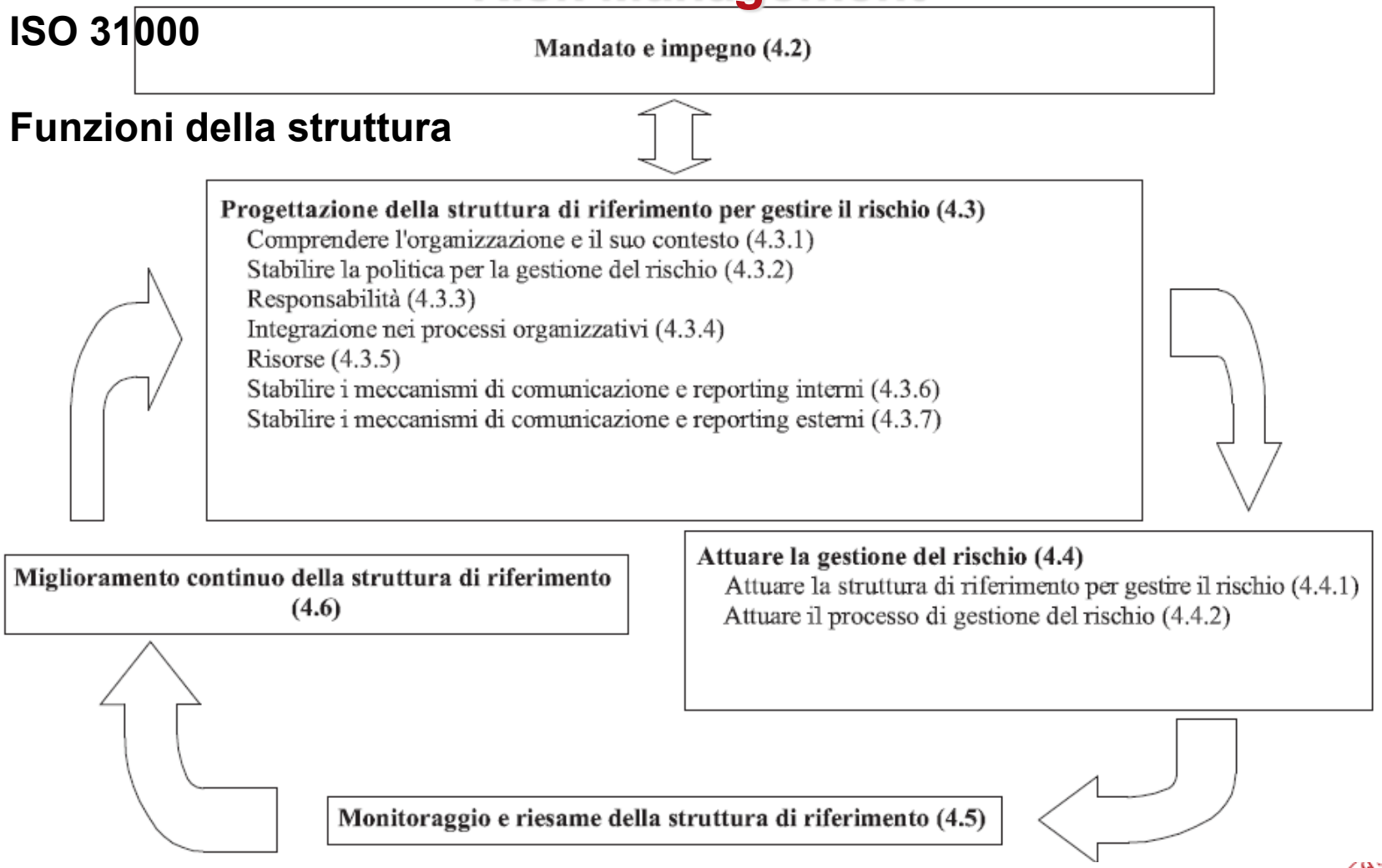
ISO 31000

Attuare la gestione del rischio

Risk Management

ISO 31000

Funzioni della struttura



Risk Management

ISO 31000

Attuare la struttura di riferimento per gestire il rischio

Nell'attuazione della struttura di riferimento dell'organizzazione per gestire il rischio, essa dovrebbe:

- definire la tempistica e la strategia appropriate per attuare la struttura di riferimento;
- applicare la politica e il processo di gestione del rischio ai processi organizzativi;
- rispettare i requisiti cogenti;
- assicurare che il processo decisionale, compresi lo sviluppo e la definizione degli obiettivi, sia in linea con gli esiti dei processi di gestione del rischio;
- svolgere sessioni di informazione e formazione-addestramento; e
- comunicare e consultarsi con i portatori d'interesse per assicurare che la propria struttura di riferimento per la gestione del rischio rimanga adeguata.

Risk Management

ISO 31000

Attuare il processo di gestione del rischio

La gestione del rischio dovrebbe essere attuata mediante l'assicurazione che il processo di gestione del rischio sia applicato attraverso un piano di gestione del rischio a tutti i livelli e funzioni pertinenti dell'organizzazione, come parte delle proprie prassi e processi.

Risk Management

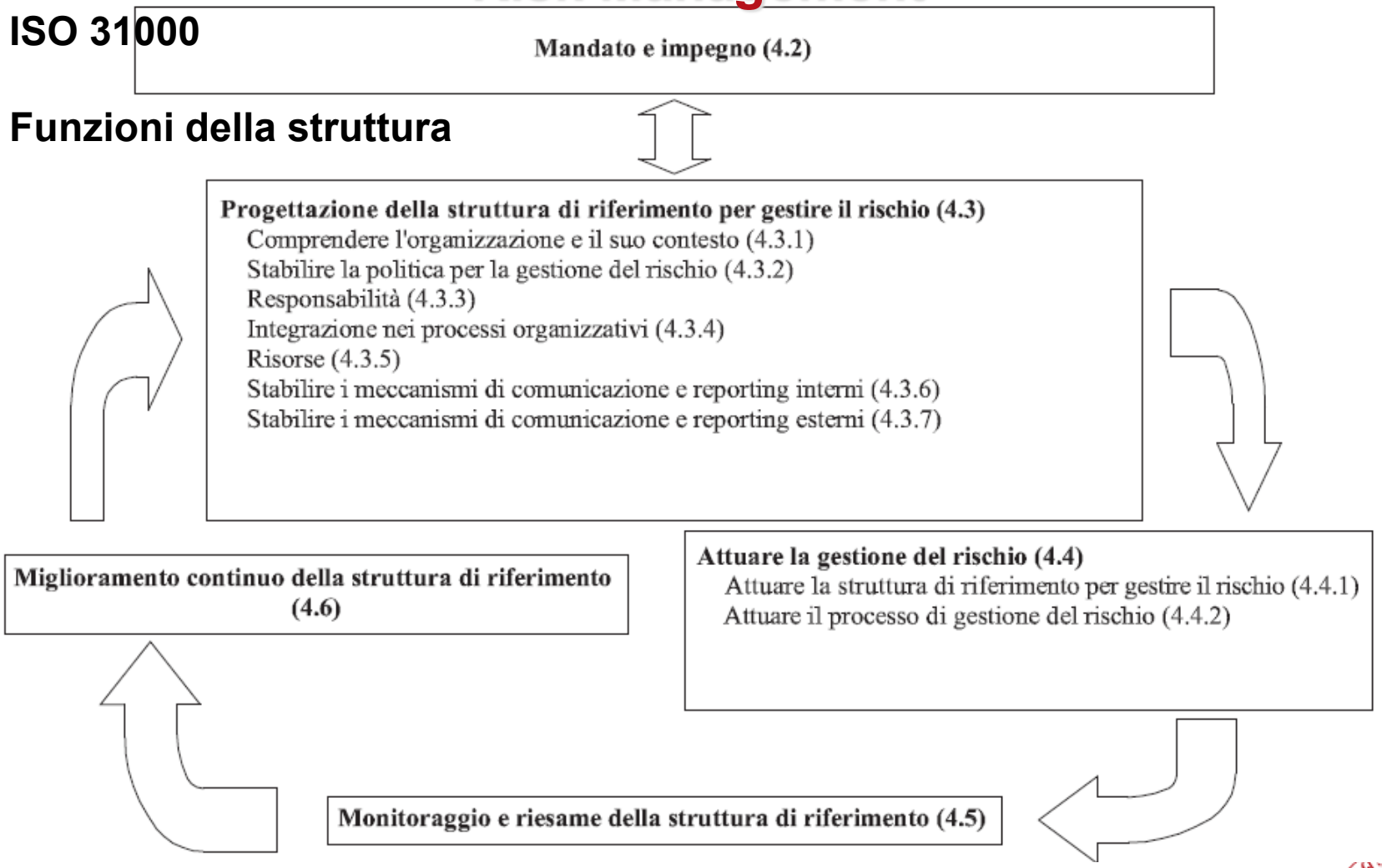
ISO 31000

Monitoraggio e riesame della struttura di riferimento

Risk Management

ISO 31000

Funzioni della struttura



Risk Management

ISO 31000

Monitoraggio e riesame della struttura di riferimento

Al fine di assicurare che la gestione del rischio sia efficace e continui a supportare la prestazione dell'**organizzazione**, quest'ultima dovrebbe:

- misurare la prestazione della gestione del rischio a fronte d'indicatori, che siano periodicamente riesaminati in termini di adeguatezza;
- misurare periodicamente i **progressi*** a fronte del piano di gestione del rischio e gli eventuali scostamenti da esso;
- accertare periodicamente se la struttura di riferimento, la politica e il piano di gestione del rischio siano ancora adeguati, dato il contesto esterno ed interno dell'organizzazione;
- riferire circa il rischio, i progressi relativi al piano di gestione del rischio e il livello di adesione alla politica per la gestione del rischio; e
- riesaminare l'efficacia della struttura di riferimento per la gestione del rischio.

Risk Management

ISO 31000

Miglioramento continuo della struttura di riferimento

Risk Management

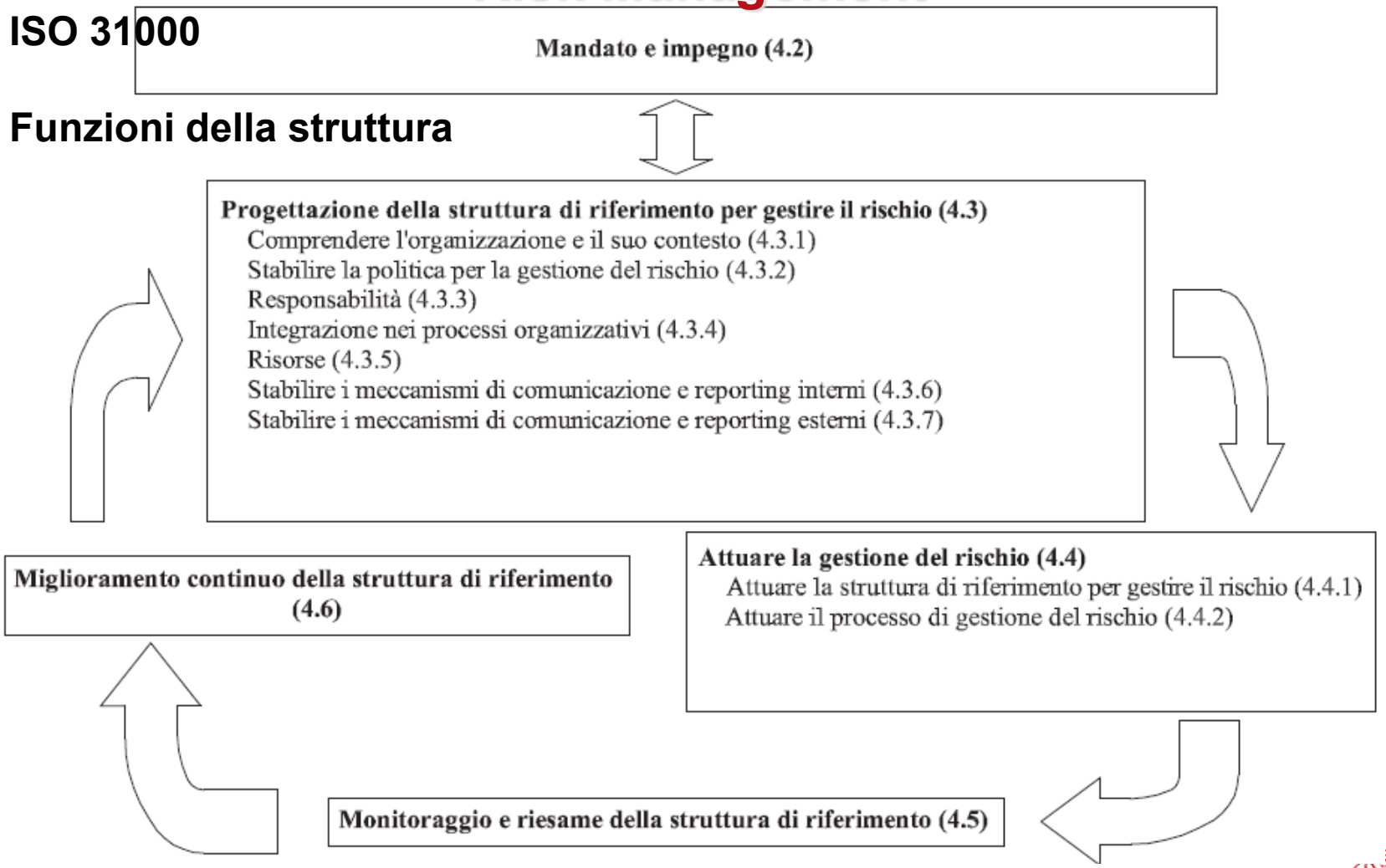
ISO 31000

Miglioramento continuo della struttura di riferimento
Le decisioni su come la struttura di riferimento, la politica e il piano di gestione del rischio **possano essere migliorati** dovrebbero essere prese **sulla base dei risultati di monitoraggio e riesame***. Tali decisioni dovrebbero portare a miglioramenti da parte dell'organizzazione nella gestione del rischio e nella relativa cultura.

Risk Management

ISO 31000

Funzioni della struttura



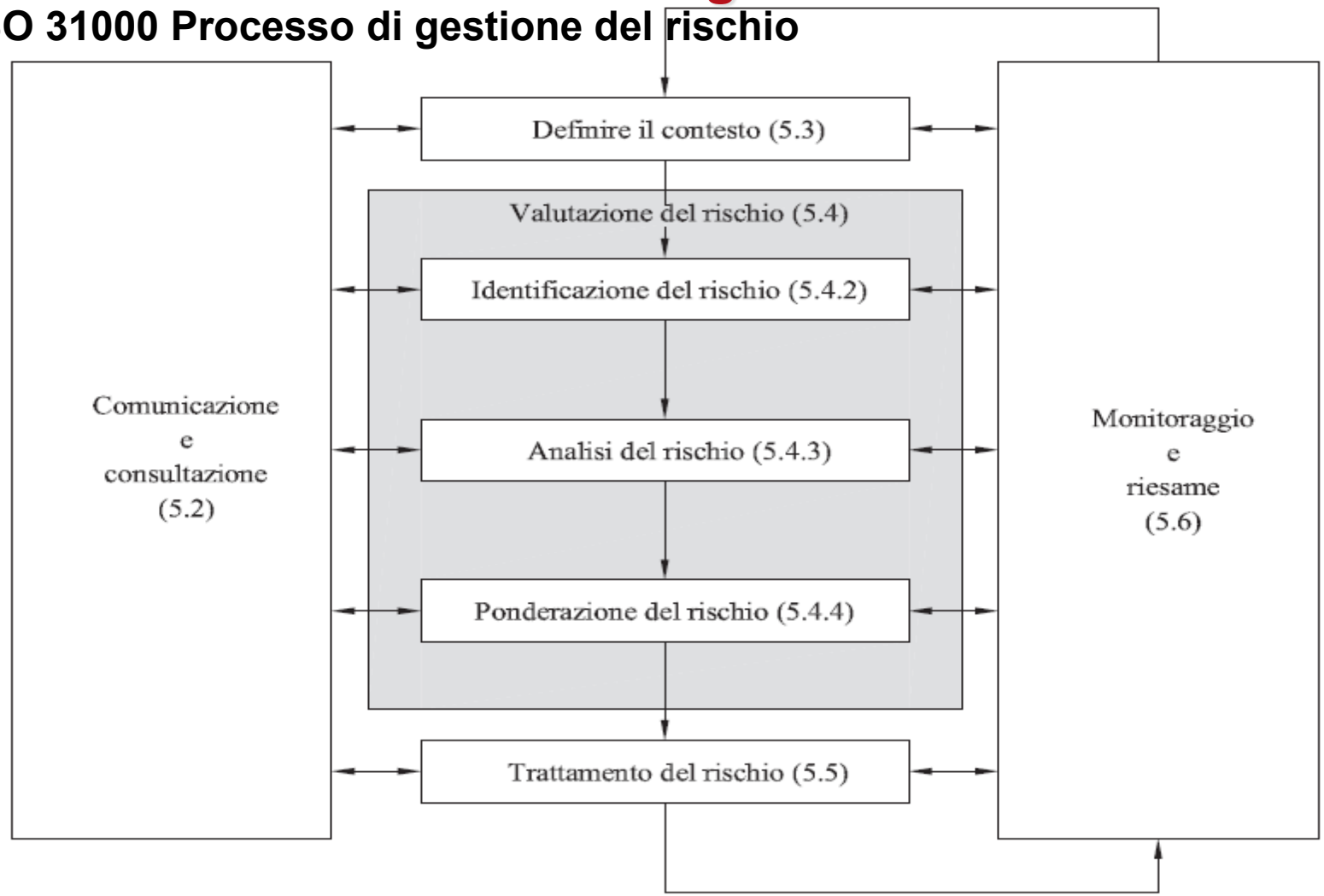
Risk Management

ISO 31000

PROCESSO DI GESTIONE DEL RISCHIO

Risk Management

ISO 31000 Processo di gestione del rischio



Risk Management

ISO 31000

Comunicazione e consultazione

Risk Management

ISO 31000

Comunicazione e consultazione

La comunicazione e la consultazione con i portatori d'interesse esterni e interni dovrebbe aver luogo durante tutte le fasi del processo di gestione del rischio.
Pertanto, i **piani per la comunicazione** e la consultazione dovrebbero essere sviluppati in una fase iniziale. Questi dovrebbero trattare questioni riguardanti il rischio in sé, le sue cause, conseguenze (se note) e le misure prese per il relativo trattamento.
Dovrebbero aver luogo comunicazioni e consultazioni esterne ed interne efficaci per assicurare che chi deve rendere conto per l'attuazione del processo di gestione del rischio ed i portatori d'interesse **comprendano su quali basi sono prese le decisioni** e le **ragioni** per cui sono richieste particolari azioni.*

Risk Management

ISO 31000

Comunicazione e consultazione

….

Un **approccio di squadra alla consultazione** potrebbe:

- aiutare a definire il contesto in modo appropriato;
- assicurare che le esigenze dei portatori d'interesse siano comprese e considerate;
- aiutare ad assicurare che i rischi siano adeguatamente identificati;
- mettere insieme diverse aree di competenza per analizzare i rischi;
- assicurare che siano presi in considerazione in misura appropriata differenti punti di vista quando si definiscono i criteri di rischio e si ponderano i rischi;
- garantire approvazione e supporto per un piano di trattamento;
- intensificare un'appropriata gestione del cambiamento durante il processo di gestione del rischio; e
- Innescare e sviluppare un piano appropriato per la comunicazione e la consultazione interne ed esterne.

Risk Management

ISO 31000

Comunicazione e consultazione

….

La comunicazione e la consultazione con i portatori d'interesse sono importanti poiché essi emettono giudizi sul rischio in base alle proprie percezioni.

Queste percezioni possono variare per le differenze nei valori, esigenze, ipotesi, opinioni e preoccupazioni dei portatori d'interesse.

Le percezioni di quest'ultimi dovrebbero essere identificate, registrate e tenute in considerazione nel processo decisionale, dato che i loro punti di vista possono avere un impatto significativo sulle decisioni prese.

La comunicazione e la consultazione dovrebbero facilitare uno scambio di informazioni sincero, pertinente, accurato e comprensibile, tenendo conto degli aspetti di integrità personale e riservatezza.

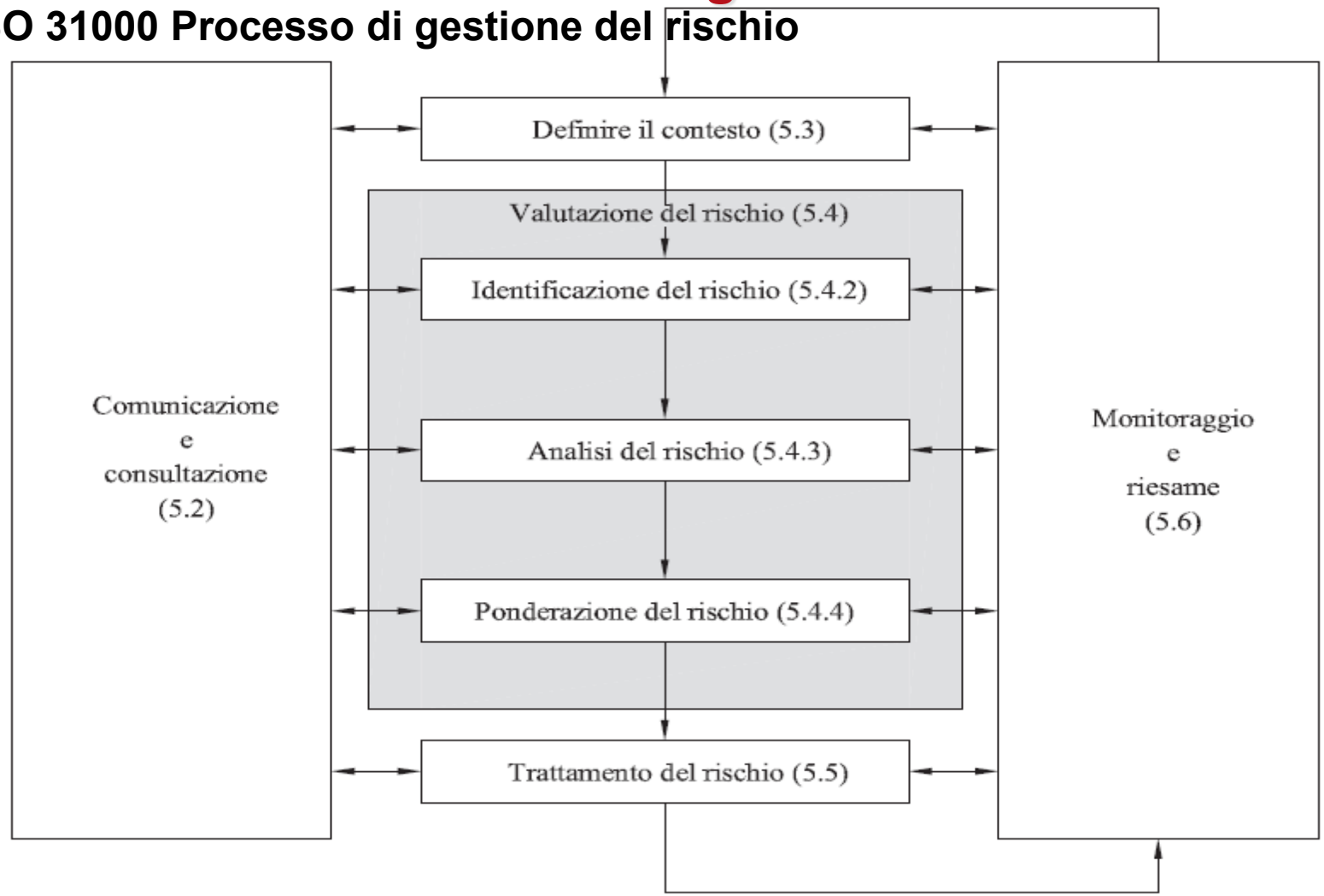
Risk Management

ISO 31000

Definire il contesto

Risk Management

ISO 31000 Processo di gestione del rischio



Risk Management

ISO 31000

Def. "definire il contesto"
Definire il contesto consente di cogliere gli **obiettivi** dell'organizzazione, l'**ambiente** in cui essa persegue tali obiettivi, i relativi **portatori d'interesse** e la diversità dei **criteri di rischio**, elementi che contribuiscono tutti a rivelare e **valutare la natura e la complessità dei propri rischi**.

Risk Management

ISO 31000

Definire il contesto esterno

Il contesto esterno è l'ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obiettivi.

La comprensione del contesto esterno è importante al fine di assicurare che gli obiettivi e le preoccupazioni dei portatori d'interesse esterni siano considerati nello sviluppo dei criteri di rischio. Essa si basa sul contesto relativo a tutta l'organizzazione, ma con specifici dettagli riguardanti i requisiti cogenti, le percezioni dei portatori d'interesse e altri aspetti relativi ai rischi propri del campo di applicazione del processo di gestione del rischio.

Il contesto esterno può comprendere, non limitandosi ad essi:

- l'ambiente sociale e culturale, politico, cogente, finanziario, tecnologico, economico, naturale e competitivo, sia internazionale, nazionale, regionale o locale;
- elementi determinanti e tendenze fondamentali che hanno un impatto sugli obiettivi dell'organizzazione; e
- relazioni con i portatori d'interesse esterni, loro percezioni e valori.

Risk Management

ISO 31000

Definire il contesto interno

Il contesto interno è l'ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi.

Il processo di gestione del rischio dovrebbe essere in linea con la cultura, i processi, la struttura e la strategia dell'organizzazione.

Il contesto interno è qualsiasi cosa, all'interno della stessa organizzazione, che può influenzare il modo in cui un'organizzazione intende gestire il rischio.

Risk Management

ISO 31000
Definire il contesto interno
…
Ciò può comprendere non limitandosi ad essi:*

- governance, struttura organizzativa, ruoli e responsabilità;
- politiche, obiettivi, e le strategie in atto per raggiungerli;
- capacità, intesa in termini di risorse e conoscenza (per esempio capitale, tempo, persone, processi, sistemi e tecnologie);
- sistemi e flussi informativi*, processi decisionali (sia formali sia informali);
- le relazioni con i portatori d'interesse interni, le loro percezioni ed i loro valori;
- la cultura dell'organizzazione;
- norme, linee guida e modelli adottati dall'organizzazione; e
- forma ed estensione delle relazioni contrattuali.

Risk Management

ISO 31000
Definire il contesto del processo di gestione del rischio

Dovrebbero essere stabiliti gli obiettivi, le strategie, il campo di applicazione ed i parametri delle attività dell'organizzazione, o quelle **parti** di essa ove è applicato il processo di gestione del rischio*.
Dovrebbero essere specificate le **risorse** richieste, le **responsabilità** ed autorità, e le **registrazioni** da mantenere attive.
Il contesto del processo di gestione del rischio varia in funzione delle esigenze dell'organizzazione.

Risk Management

ISO 31000

Definire il contesto del processo di gestione del rischio

…

Esso può implicare, non limitandosi a:

- la definizione di traguardi e **obiettivi** delle attività relative alla gestione del rischio;
- la definizione delle **responsabilità** a tutti i livelli del processo di gestione del rischio;
- la definizione del **campo di applicazione**, così come la profondità e l'ampiezza delle attività relative alla gestione del rischio da effettuare, comprese specifiche **inclusioni o esclusioni**;
- la **definizione di attività**, processi, funzioni, progetti, prodotti, servizi o beni in termini di tempo e ubicazione;
- la definizione delle relazioni tra un particolare progetto, processo o attività e altri progetti, processi o attività dell'organizzazione;
- la definizione delle **metodologie di valutazione del rischio**;
- la definizione della modalità con cui sono valutate la **prestazione e l'efficacia della gestione del rischio;**

Risk Management

ISO 31000
Definire il contesto del processo di gestione del rischio

…

- l'identificazione e la specificazione delle decisioni che devono essere prese; e
- l'identificazione, la definizione dell'ambito di applicazione o la formulazione degli **studi necessari**, la loro estensione ed obiettivi, e le **risorse richieste** per tali studi.

Prestare attenzione a questi ed altri fattori pertinenti dovrebbe aiutare ad assicurare che **l'approccio alla gestione del rischio adottato sia appropriato alle circostanze, all'organizzazione ed ai rischi** che influenzano la realizzazione dei propri obiettivi.

Risk Management

ISO 31000
Definire i criteri di rischio

L'organizzazione dovrebbe **definire i criteri da utilizzare per valutare la significatività del rischio*.**
I criteri dovrebbero riflettere i valori, gli obiettivi e le risorse dell'organizzazione.
Alcuni criteri potrebbero essere **imposti o derivare da requisiti cogenti*** e da altri requisiti sottoscritti dall'organizzazione.
I criteri di rischio dovrebbero essere coerenti con la politica per la gestione del rischio, dovrebbero essere definiti all'inizio di qualsiasi processo di gestione del rischio e sottoposti a riesame in modo continuo.

Risk Management

ISO 31000
Definire i criteri di rischio

…

Nella definizione dei **criteri di rischio,** i fattori da considerare dovrebbero comprendere quanto segue:

- la natura e i tipi di cause e conseguenze che possono accadere e come misurarle;
- come viene definita la verosimiglianza (probabilita');
- l'orizzonte temporale della verosimiglianza (probabilita') e/o delle conseguenze (Severita');*
- come viene determinato il livello di rischio;*
- i punti di vista dei portatori d'interesse;
- il livello al quale il rischio diviene accettabile o tollerabile;* e
- se si debba tener conto della combinazione di rischi multipli e, nel caso, come e quali combinazioni dovrebbero essere considerate.

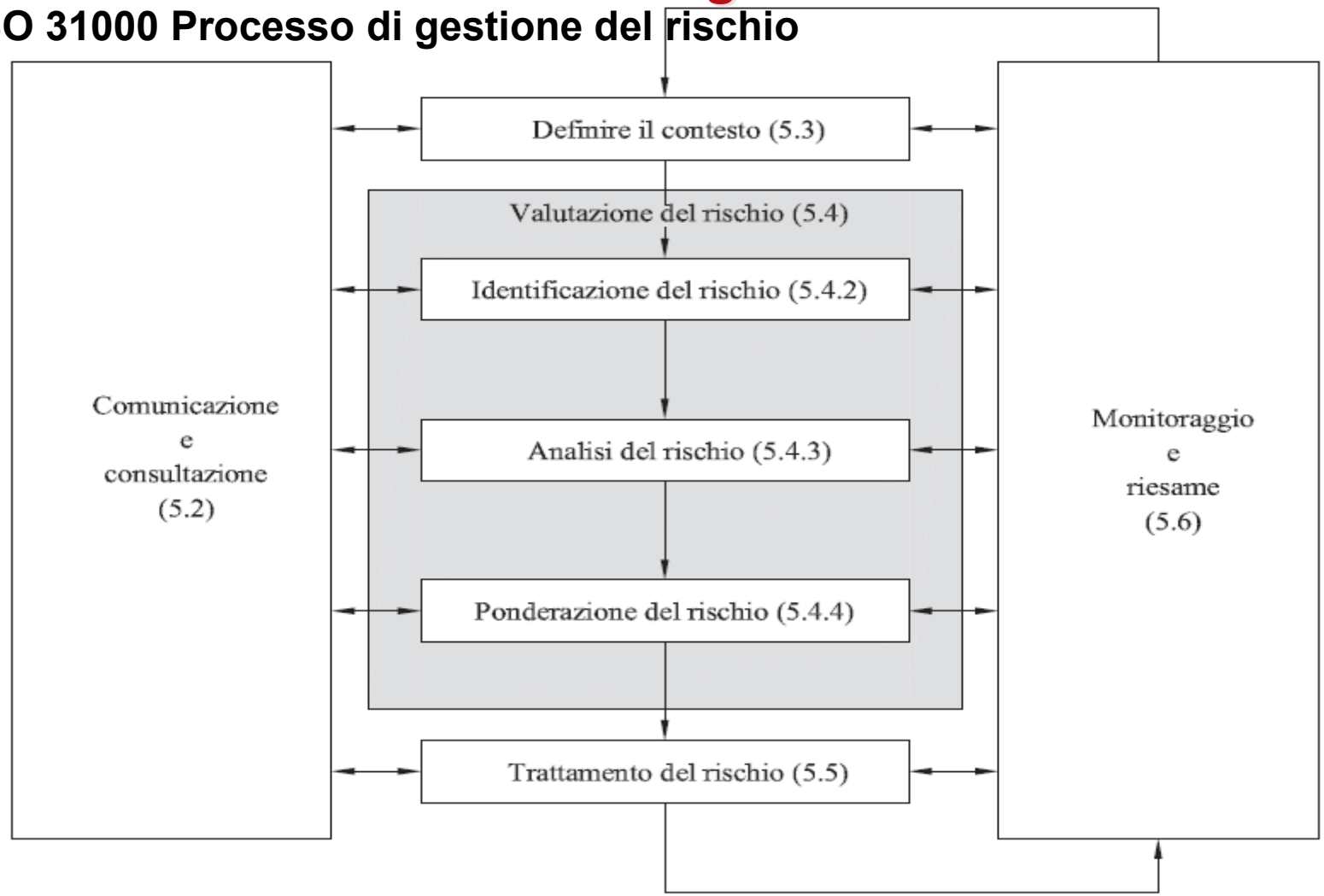
Risk Management

ISO 31000

Valutazione del rischio

Risk Management

ISO 31000 Processo di gestione del rischio



Risk Management

ISO 31000

Valutazione del rischio

Processo complessivo di:

- **identificazione del rischio**
- **analisi del rischio** e
- **ponderazione del rischio**

Risk Management

ISO 31000

Definizioni

Identificazione del rischio

- L'identificazione del rischio implica l'identificazione delle fonti di rischio, degli eventi, relative cause e delle loro potenziali conseguenze.
- 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 dei portatori d'interesse**

Def. rischio: Effetto dell'incertezza sugli obiettivi.

Risk Management

ISO 31000
Identificazione del rischio

L'organizzazione dovrebbe identificare le **fonti di rischio, le aree di impatto, gli eventi** (comprese le modifiche nelle circostanze), **le cause e le potenziali conseguenze** di questi ultimi. L'obiettivo di tale fase è quello di **generare un elenco completo dei rischi** basato su quegli eventi che possono creare, incrementare, prevenire, degradare, accelerare o ritardare il raggiungimento degli obiettivi. È importante identificare i rischi associati al mancato perseguimento di un'opportunità.

L'identificazione globale è critica, poiché un rischio non identificato in questa fase non viene considerato nelle analisi successive.

Risk Management

ISO 31000
Identificazione del rischio

…

Il processo di identificazione dovrebbe includere i **rischi la cui fonte sia sotto il controllo della organizzazione o meno***, anche se la fonte o causa di rischio può non essere manifesta.

La identificazione del rischio dovrebbe comprendere l'esame degli effetti indiretti di particolari conseguenze, inclusi gli effetti a cascata o cumulativi (per esempio "effetto domino").

Essa dovrebbe inoltre considerare un'ampia gamma di conseguenze anche se la fonte o causa di rischio può non essere manifesta.

Oltre a identificare ciò che può accadere, è necessario considerare le possibili cause e scenari che mostrano quali conseguenze possono aver luogo.

Dovrebbero essere considerate tutte le cause e conseguenze significative.

Risk Management

ISO 31000
Identificazione del rischio

…

L'organizzazione dovrebbe applicare strumenti e tecniche d'identificazione* adatti ai propri obiettivi e capacità ed ai rischi cui far fronte.
Nell'identificazione dei rischi e' importante che le informazioni pertinenti ed aggiornate. Queste, ove possibile, dovrebbero comprendere appropriate informazioni derivanti da conoscenze ed esperienze pregresse.
Nell'identificazione dei rischi dovrebbero essere coinvolte persone con appropriate conoscenze.

Risk Management

ISO 31000

Definizioni

Analisi del rischio:

- Processo di comprensione della natura del **rischio** e di determinazione del **livello di rischio**
- L'analisi del rischio fornisce la base per la **ponderazione del rischio** e le decisioni circa il **trattamento del rischio**
- L'analisi del rischio comprende la **misurazione del rischio**.

ISO 31000

Analisi del rischio

L'analisi del rischio implica considerazioni sulle cause e fonti di rischio, le loro conseguenze positive o negative, e la verosimiglianza del loro accadimento.
I fattori che influenzano conseguenze e verosimiglianza dovrebbero essere identificati.
Il rischio è analizzato mediante la determinazione delle conseguenze (SEVERITA') e la relativa verosimiglianza (PROBABILITÀ) e altri attributi del rischio.
Un evento può avere molteplici conseguenze e può avere influenza su più obiettivi.
I controlli (BARRIERE) esistenti e la loro **efficacia ed efficienza** dovrebbero anch'essi essere presi in considerazione.

Risk Management

ISO 31000
Analisi del rischio

…

Il modo in cui le conseguenze e la verosimiglianza sono espresse e la modalità in cui sono combinati per determinare il livello di rischio dovrebbero riflettere il tipo di rischio, le informazioni disponibili e lo scopo per cui i dati in uscita dalla valutazione del rischio devono essere utilizzati. Questi dovrebbero essere tutti coerenti con i criteri di rischio.

È inoltre importante considerare l'interdipendenza tra differenti rischi e relative fonti.

La confidenza nella determinazione del livello di rischio e la sua sensitività a precondizioni ed ipotesi dovrebbero essere considerate nell'analisi e comunicate efficacemente ai responsabili delle decisioni e, quando appropriato, ad altri portatori d'interesse.

Dovrebbero essere specificati, e possono essere evidenziati, fattori quali divergenze di opinioni tra gli esperti, incertezza, disponibilità, qualità, quantità e continua attualità delle informazioni, o limiti nella modellazione.

Risk Management

ISO 31000
Analisi del rischio

…

L'analisi del rischio può essere intrapresa con vari livelli di dettaglio, in funzione del rischio, dello scopo dell'analisi e delle informazioni, dei dati e delle risorse disponibili.
L'analisi può essere qualitativa, semi-quantitativa o quantitativa, o una combinazione di queste, in funzione delle circostanze.
Le conseguenze e la loro verosimiglianza possono essere determinate mediante la modellazione degli esiti di un evento o di un insieme di eventi, o attraverso una estrapolazione da studi sperimentali o dai dati disponibili.
Le conseguenze possono essere espresse in termini di impatti tangibili e intangibili.
In alcuni casi, allo scopo di specificare le conseguenze e la loro verosimiglianza in tempi, luoghi, gruppi o situazioni differenti, è richiesto più di un valore numerico o di un termine descrittivo.

Risk Management

ISO 31000

Definizioni

Ponderazione del rischio:

- Processo di comparazione dei risultati dell'**analisi del rischio** rispetto ai **criteri di rischio** per determinare se il **rischio** e/o la sua espressione quantitativa sia accettabile o tollerabile.
- La ponderazione del rischio agevola la decisione circa il **trattamento del rischio**

Risk Management

ISO 31000

Ponderazione del rischio

L'obiettivo della ponderazione del rischio è di agevolare, sulla base degli esiti dell'analisi del rischio, i processi decisionali riguardo a quali rischi necessitano un trattamento e le relative priorità di attuazione.

La ponderazione del rischio implica il **confronto tra il livello di rischio trovato** durante il processo di analisi ed **i criteri di rischio stabiliti durante l'esame del contesto.*** La necessità di trattamento può essere considerata sulla base di questo confronto.

Le decisioni dovrebbero tenere conto del più ampio contesto riguardante il rischio e comprendere la considerazione della tolleranza dei rischi sopportata dalle parti, diverse dall'organizzazione, che possono trarre benefici dal rischio.

Le decisioni dovrebbero essere prese nel rispetto dei requisiti cogenti e di altro tipo.

Risk Management

ISO 31000
Ponderazione del rischio

…

In alcune circostanze, la ponderazione del rischio può portare ad una decisione d'intraprendere ulteriori analisi.

La ponderazione del rischio può anche portare ad una decisione di non sottoporre ad ulteriore trattamento il rischio, ma limitarsi a mantenere attivi i controlli esistenti.

Questa decisione è influenzata dalla propensione al rischio dell'organizzazione e dai criteri di rischio stabiliti.

Risk Management

ISO 31000

Definizioni

Livello di rischio:
Espressione quantitativa di un **rischio** o combinazione di rischi, espresso in termini di combinazione di **conseguenze (Severità)** e della loro **verosimiglianza (Probabilità)**

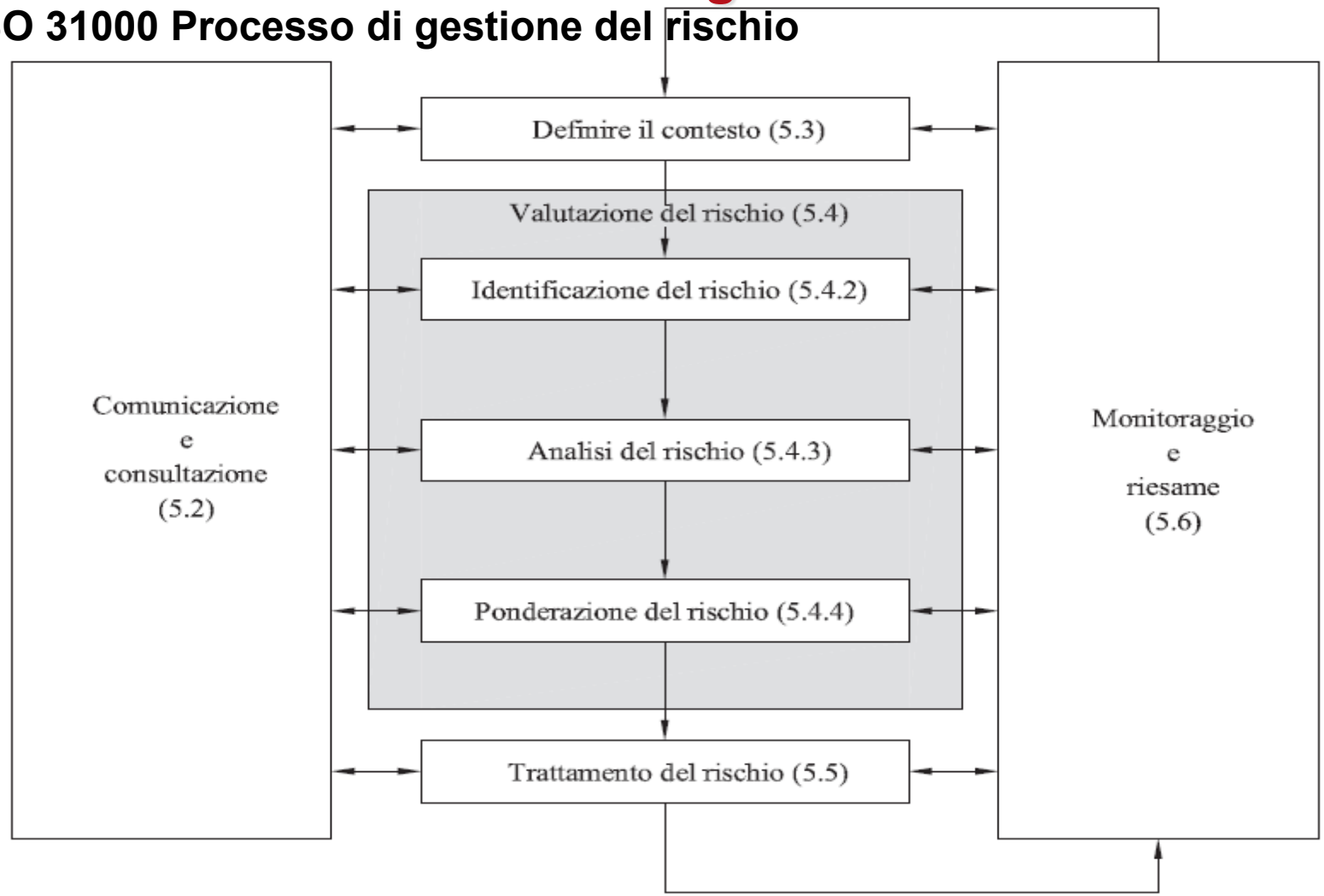
Risk Management

ISO 31000

Trattamento del rischio

Risk Management

ISO 31000 Processo di gestione del rischio



Risk Management

ISO 31000

Trattamento del rischio

Il trattamento del rischio implica la selezione di una o più opzioni per modificare i rischi e l'attuazione di tali opzioni.

Una volta attuati, i trattamenti **forniscono o modificano i controlli**.*

Il trattamento del rischio comporta un processo **ciclico** di:

- **valutazione di un trattamento** del rischio;
- **decisione circa la tollerabilità dei livelli di rischio residuo;**
- **se non tollerabile, generazione di un nuovo trattamento** del rischio; e
- **valutazione dell'efficacia di tale trattamento.**

Risk Management

ISO 31000

Trattamento del rischio

…

Le **opzion**i di trattamento del rischio non sono necessariamente incompatibili tra loro o adatte a tutte le circostanze.

Le opzioni possono comprendere quanto segue:

- **evitare** il rischio decidendo di non iniziare o non continuare l'attività che da origine ad esso;
- **assumere** o **aumentare** l'esposizione al rischio al fine di cogliere un'opportunità;*
- **rimuovere** la **fonte di rischio** *
- **modificare** la **verosimiglianza (probabilità)***
- **modificare** le **conseguenze** *
- **condividere il rischio** con altra(e) parte(i) (compresi contratti e finanziamento del rischio), Assicurazioni
- **ritenere il rischio** con una decisione informata

Risk Management

ISO 31000

Trattamento del rischio

…

I trattamenti del rischio che affrontano conseguenze negative sono talvolta denominati “protezione dal rischio”, “eliminazione del rischio”, **“prevenzione del rischio”,** e **“riduzione del rischio”.**

Il trattamento del rischio può generare nuovi rischi o modificare rischi esistenti.

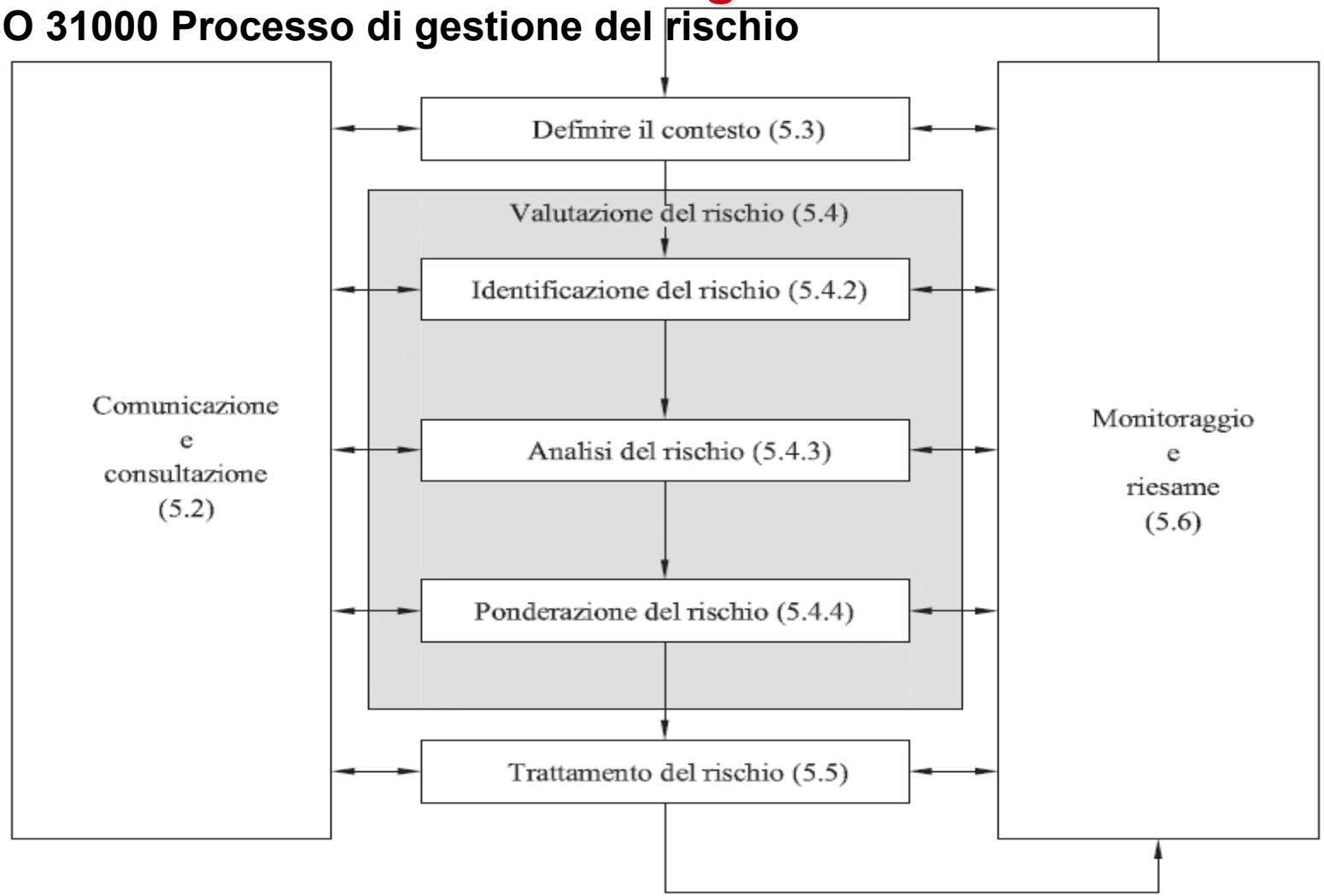
Risk Management

ISO 31000

Monitoraggio e riesame

Risk Management

ISO 31000 Processo di gestione del rischio



Risk Management

ISO 31000

Monitoraggio e riesame

Sia il monitoraggio sia il riesame dovrebbero essere una parte pianificata del processo di gestione del rischio e comportare **verifiche o sorveglianza regolari.***
Detti processi possono essere periodici o *ad hoc*.
Le responsabilità per il monitoraggio e il riesame dovrebbero essere chiaramente definite.

ISO 31000

Monitoraggio e riesame

I processi di monitoraggio e riesame dell'organizzazione dovrebbero comprendere tutti gli aspetti del processo di gestione del rischio allo scopo di:

- assicurare che i controlli siano efficaci ed efficienti sia nella progettazione sia nell'operatività;
- ottenere ulteriori informazioni per migliorare la valutazione del rischio;
- analizzare ed apprendere dagli **eventi** (compresi i near-miss), **cambiamenti, tendenze, successi e fallimenti**;*
- rilevare i **cambiamenti** nel contesto esterno ed interno, comprese le modifiche ai criteri di rischio e al rischio stesso, che possano richiedere revisioni dei trattamenti del rischio e delle priorità; e
- **identificare i rischi emergenti**.*

Risk Management

ISO 31000

Monitoraggio e riesame

…

I progressi nell'attuazione dei piani di trattamento del rischio forniscono una misura della prestazione. I risultati possono essere incorporati all'interno della gestione della prestazione complessiva dell'organizzazione, nelle misurazioni e nelle attività di reporting esterne ed interne.

I **risultati del monitoraggio e riesame dovrebbero essere registrati** e riferiti esternamente ed internamente, come appropriato, e dovrebbero anche essere utilizzati come dati in ingresso al riesame della struttura di riferimento per la gestione del rischio

Risk Management

ISO 31000

Registrazione del processo di gestione del rischio

Risk Management

ISO 31000

Registrazione del processo di gestione del rischio
Le attività di gestione del rischio **dovrebbero essere tracciabili.**
Nel processo di gestione del rischio, le registrazioni forniscono la base per il miglioramento nei metodi e negli strumenti, così come nel processo complessivo.
Le decisioni concernenti **l'elaborazione delle registrazioni** dovrebbe considerare:

- le esigenze dell'organizzazione per l'apprendimento continuo;
- i benefici di ri-utilizzo delle informazioni per scopi relativi alla gestione;
- i costi e gli sforzi che l'elaborazione e la conservazione delle registrazioni comportano;
- **le esigenze, in termini cogenti ed operativi, per le registrazioni**;*
- i metodi di accesso, la facilità nel reperire ed i mezzi di archiviazione;
- **il periodo di conservazione**; e
- **la delicatezza delle informazioni.**


PAUSA