aias academy

L'Accademia su misura per i professionisti HSE

Gestione dei rischi nelle organizzazioni

Carlo Bisio,
24/06/2025

Programma dell’incontro

Introduzione al risk management e alla sua importanza per l'INFN.

- La norma ISO 31000:
- Principi del risk management.
- Framework per la gestione del rischio.
- Processo di risk management.

La norma UNI CEN 31010:

- Cenni sui diversi tipi di valutazione del rischio.
- Metodologie per la valutazione del rischio.

Cenni alla ISO 22316 sulla resilienza organizzativa e ai rischi emergenti

Carlo Bisio

- *Graduate Member of IOSH (Institution of Occupational Health and Safety)*
- *Socio AIAS (Associazione Italiana Ambiente e Sicurezza)*
- *Registrato dal CREE come Ergonomo Europeo (Eur.Erg.) e Socio SIE (Società Italiana di Ergonomia e Fattori Umani)*

- **NEBOSH International Diploma in Occupational Health and Safety** *(UK, 2017)*
- **Master 2° liv. in Ergonomia** *(Parigi, 2013)*
- **Psicologo del lavoro e delle organizzazioni** *(Padova, 1995)*
- ***IEMA Foundation Certificate in Environmental Management*** *(UK, 2020)*

Altre qualificazioni su mindfulness, meditazione.
Attualmente studente di yoga

Collaborazioni universitarie

- Univ. Milano Bicocca *(docente a contratto per oltre 10 anni)*
- Politecnico di Milano
- Università del Molise
- Univ. Statale di Milano
- Altri atenei

Collaborazioni significative con più di 200 aziende in numerosi settori, fra cui:

- Chimico
- Farmaceutico
- Sanità
- Siderurgico
- Meccanico
- Gomma
- Cartario
- Alimentare
- Grande distribuzione
- Telecomunicazioni
- Turismo
- Edilizia
- Ferroviario
- Vetrario


PSICOLOGIA PER LA SICUREZZA SUL LAVORO
Dossier Ambiente n°118
Salute Sicurezza Lavoro
ERGONOMIA
PER LA SALUTE E LA SICUREZZA SUL LAVORO
Dall'Autore di "Psicologia per la Sicurezza sul Lavoro"
Fare Apprendere la Sicurezza
Manuale per la formazione dei formatori per la sicurezza
CARLO BISIO
COMUNICARE IN AZIENDA
Manuale di sopravvivenza per manager
Dossier Ambiente n°106
STRESS LAVORO CORRELATO E BENESSERE ORGANIZZATIVO
13 SocialMente
FATTORE UMANO E SICUREZZA SUL LAVORO
Aspetti psicosociali e interventi nelle organizzazioni
a cura di Carlo Bisio
GIUNTI O.S.
dal 1987
Dossier Ambiente n°126
LA GESTIONE DEL RISCHIO DI VIOLENZE SUL LUOGO DI LAVORO
A cura di Carlo Bisio
CARLO BISIO
COSTRUZIONE DELLA REALTÀ E FORMAZIONE
PROSPETTIVA PSICOSOCIALE E SISTEMICA SUI PROCESSI D'APPRENDIMENTO
40 chiavi di lettura sulla sicurezza
Modelli, tecniche, concetti e approcci che o professionista nel campo della sicurezza e sal dovrebbe conoscere
Carlo Bisio
Gestione della sicurezza nei sistemi sociotecnici
Resilienza, incidenti e complessità nella sicurezza industriale
EPC EDITORE
VALUTARE IN FORMAZIONE
Azioni, significati e valori
a cura di Carlo Bisio
Presentazione di Dante Bellamio
Scritti di: Federico Amietta, Massimo Bellotto, Carlo Bisio, Stefano Gheno, Maurizio Lichtner, Vincenzo Majer, Marco Mariani, Piergiorgio Reggio, Elena Righetti, Alberto Vergani, Leonardo Verdi Vighetti
STUDI E RICERCHE
AV
Associazione Italiana di Valutazione
FrancoAngeli
CARLO BISIO
SICUREZZA, FORMAZIONE E ALTRE VICISSITUDINI
Racconti autobiografici di un consulente
EPC EDITORE
Carlo Bisio
Renata Borgato
MANUALI
FrancoAngeli
La forza della melagrana
Riflessioni per conoscere il gruppo ed esercitazioni per usarlo al meglio

Risk management

Alcune definizioni

Rischio (risk)
L'effetto dell'incertezza sugli obiettivi

Componenti del rischio

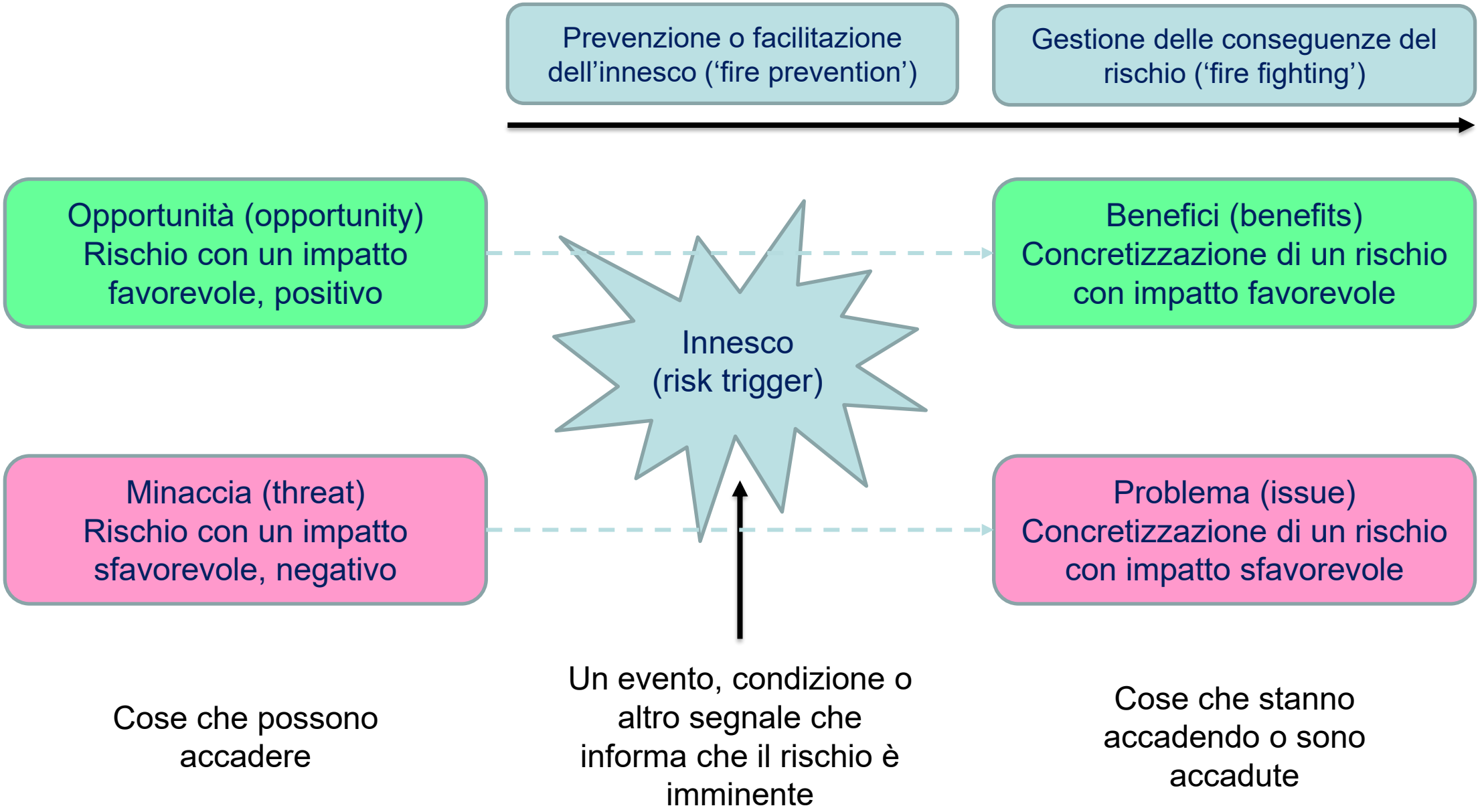
Probabilità (probability, likelyhood, chance)

Conseguenze (impacts, consequeces, costs)

Categorie di rischi

Opportunità (opportunity)
Rischio con un impatto favorevole, positivo

Minaccia (threat)
Rischio con un impatto sfavorevole, negativo


Prevenzione o facilitazione dell'innesco ('fire prevention')
Gestione delle conseguenze del rischio ('fire fighting')
Opportunità (opportunity)
Rischio con un impatto favorevole, positivo
Benefici (benefits)
Concretizzazione di un rischio con impatto favorevole
Innesco
(risk trigger)
Minaccia (threat)
Rischio con un impatto sfavorevole, negativo
Problema (issue)
Concretizzazione di un rischio con impatto sfavorevole
Cose che possono accadere
Un evento, condizione o altro segnale che informa che il rischio è imminente
Cose che stanno accadendo o sono accadute

Una metafora…

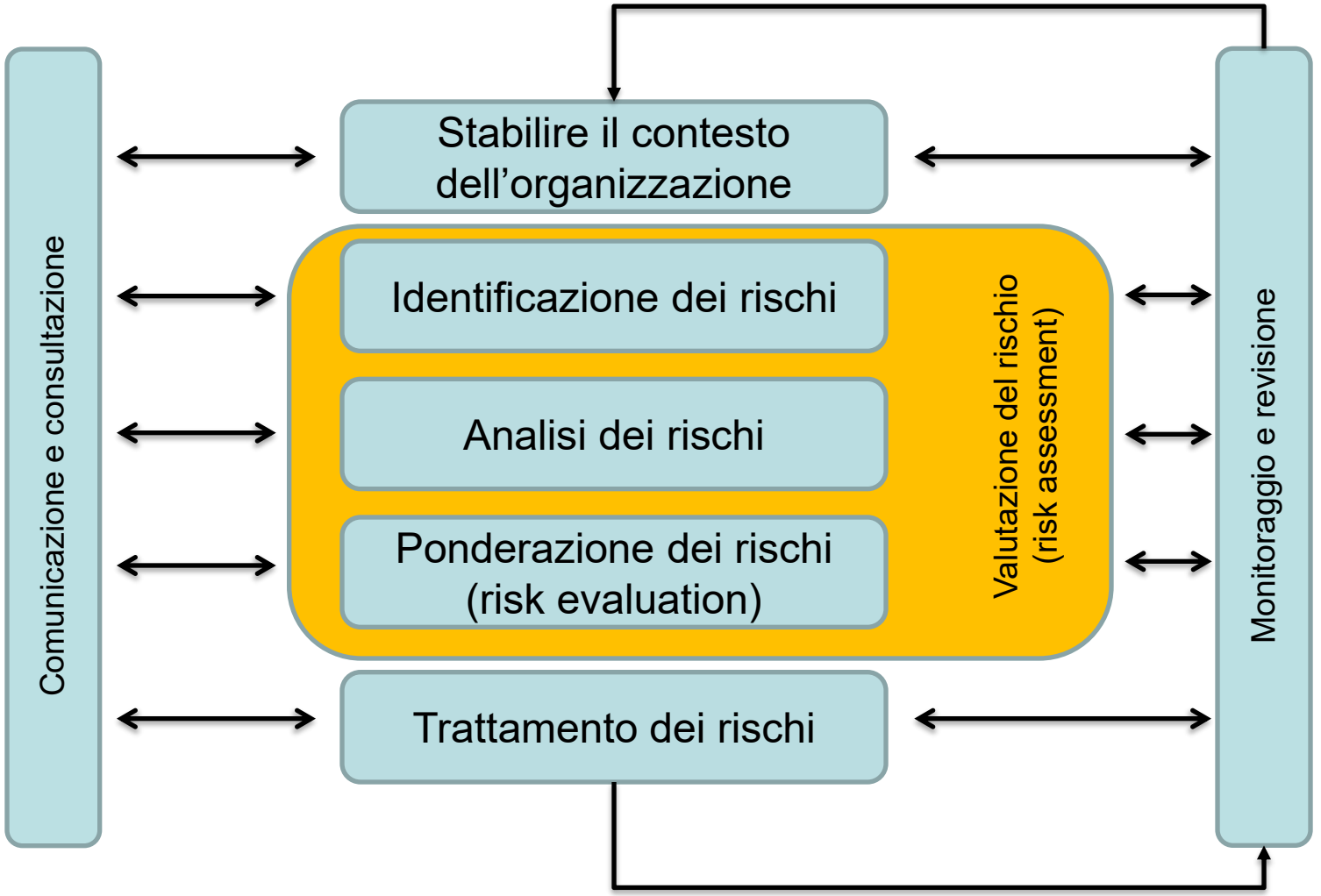
Principi del risk management

- Crea e protegge valore – obiettivo primario di ogni attività di RM
- Integrato nei processi organizzativi, non un add-on
- Strutturato e completo – approccio sistematico e coerente
- Personalizzato sul contesto (mandato, stakeholder, cultura)
- Inclusivo – coinvolge persone con competenze e visioni diverse
- Dinamico – si adatta al cambiamento e anticipa l'incertezza
- Basato sulle migliori informazioni disponibili (dati, esperienza, intuizione)
- Considera fattori umani e culturali – il comportamento conta
- Spinge al miglioramento continuo – learning loop post-evento

Framework di gestione del rischio

- Leadership & Commitment (TOP MANAGEMENT)
  - Definisce obiettivi, risk appetite, risorse
- Integrazione
  - Il RM entra in governance, strategia, operations, HR, acquisti …
- Design del Framework
  - Scopo, contesto, criteri
  - Ruoli, responsabilità, risorse, comunicazione
- Implementazione
  - Attività, processi e strumenti operativi (p.es. Bowtie, LOPA)
- Valutazione
  - Monitoraggio performance, audit, KPI di rischio
- Miglioramento
  - Azioni correttive e di apprendimento continuo (PDCA Loop)

Gestione del rischio nella ISO 31000



Integrazione dei tre aspetti

Livello	Domanda a cui risponde	Scopo/Funzionalità	Messaggio-chiave da trasmettere in aula
Principi	**Perché** facciamo risk management?	- Definiscono i valori che rendono il RM “buono” (crea valore, è inclusivo, dinamico, ecc.). - - Servono come criteri di qualità: se un’attività non rispetta i principi, non è vero RM ISO 31000.	“Sono la bussola etica e culturale: senza principi il RM diventa puro adempimento.”
Framework	**Come** l’organizzazione rende possibile il RM?	- Traduce i principi in governance, ruoli, policy, risorse e reporting. - Garantisce che il RM sia integrato (non un silos) e sostenuto dal top management.	“È l’impianto che collega la vision ai mezzi: se manca, il processo resta sulla carta.”
Processo	**Che cosa** facciamo concretamente e in quale ordine?	- Sequenza operativa (scopo-contesto-criteri → identificare → analizzare → valutare → trattare → monitorare → comunicare). - È la “ricetta” applicabile a ogni rischio, dal piano strategico al singolo cantiere.	“È l’azione quotidiana: senza processo non si vedono risultati misurabili.”

Tecniche di risk assessment

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

Incertezza nel risk management

- **Incertezza aleatoria**: deriva dal fatto che certi fenomeni sono intrinsecamente aleatori e l'incertezza non può essere ridotta tramite ulteriori ricerche (es. lancio di dadi)
- **Incertezza epistemica**: deriva da uno stato di conoscenze non complete, e può essere ridotta da raccolta di dati, affinamento di modelli, miglioramento di campionamento, ecc.
- Altre forme di incertezza dovuti a ambiguità nei **linguaggi** (incertezza linguistica) o nelle **decisioni**, associata a sistemi di valori, giudizi professionali, ecc.

Rischio

- Include gli effetti di ogni forma di incertezza sugli obiettivi. Può portare a conseguenze positive, negative o entrambe
- È spesso descritto in termini di fonti di rischio, potenziali eventi, loro conseguenze, loro probabilità
- Le fonti di rischio possono includere variabilità intrinseche (incertezza aleatoria) dovuta ad es. a fattori umani o eventi nella società

Le tecniche di risk assessment hanno la finalità di aiutare la comprensione dell'incertezza e rischi associati, per supportare decisioni o azioni meglio informate

Implementare una valutazione del rischio

- Pianificare una valutazione del rischio
- Gestire informazioni, sviluppare modelli
- Applicare tecniche di valutazione del rischio
- Riesaminare l’analisi svolta
- Applicare i risultati per supportare decisioni
- Documentare processo ed esiti

Le tecniche di valutazione del rischio
(1 di 3)

- Tecniche per ricavare punti di vista da parti interessate o esperti *(es. braistorming, Delphi, interviste)*
- Tecniche per l'identificazione dei rischi *(es. checklist, classificazioni o tassonomie come SWOT o PESTLE; FMEA/FMECA; HAZOP)*
- Tecniche per determinare fonti, cause e motivi del rischio *(es. fishbone)*

Le tecniche di valutazione del rischio
(2 di 3)

- Tecniche per analizzare i controlli esistenti *(es. bow tie)*
- Tecniche per comprendere conseguenze e probabilità *(es. Event Tree, Fault Tree, Human Reliability Analysis)*
- Tecniche per analizzare dipendenze e interazioni *(es. mappe causali, cross impact analysis)*

Le tecniche di valutazione del rischio
(3 di 3)

- Tecniche per fornire una misura del rischio *(es: risultati di studi tossicologici)*
- Tecniche per valutare la significatività del rischio *(es. ALARP, Pareto, indici di rischio)*
- Tecniche per scegliere tra diverse opzioni *(es: analisi costi benefici)*
- Tecniche per la registrazione e documentazione *(es. risk registers, risk matrix)*

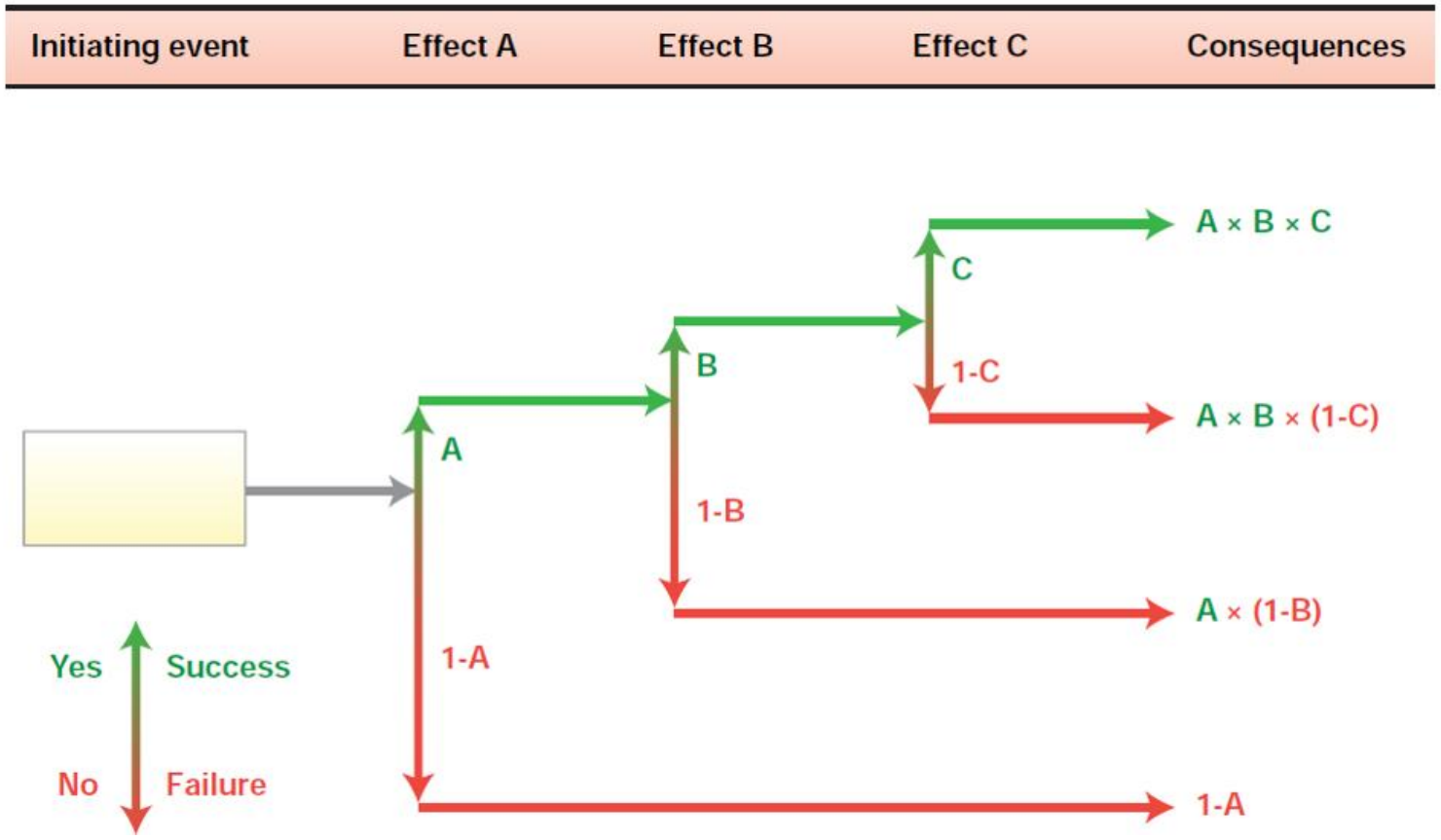
Le tecniche per analizzare i controlli

- Queste tecniche possono essere utilizzate per verificare se i controlli del rischio sono appropriati e adeguati
- LOPA e bow tie identificano le barriere tra una fonte di rischio e le sue possibili conseguenze e possono essere usate per verificare se le barriere sono sufficienti

LOPA (Layers of protection analysis)

- Analizza la riduzione del rischio raggiunta da un insieme di controlli
- Può essere considerata un caso particolare di albero degli eventi
- A volte può essere utilizzata in uno studio HAZOP

Esempio di semplice albero degli eventi



LOPA (Layers of protection analysis)

- Identificazione degli **eventi pericolosi** di interesse
- Identificazione degli **eventi iniziali** (guasti, altre cause), ciascuno dei quali può innescare l'occorrenza dell'evento pericoloso
- Si prende in considerazione ogni **coppia causa-conseguenza**
- Identificazione delle **barriere di protezione indipendenti (IPL)** ciascuno dei quali, se funzionante, può prevenire l'evento pericoloso
- Identificazione di ogni **specifica condizione** richiesta per l'occorrenza dell'evento pericoloso (*conditional modifiers*)

Le barriere indipendenti (IPL)

Un *indipendent protection layer* è **un sistema o un'azione capace di prevenire il fatto che uno scenario proceda verso conseguenze indesiderate**

Ogni IPL:

- dev'essere indipendente sia dall'evento causale che da tutti gli altri IPL associati con lo scenario
- dev'essere auditabile

Tipi di IPL

- Caratteristiche progettuali
- Strumenti di protezione fisica
- Sistemi di *interlock* e di *shutdown*
- Allarmi critici e interventi manuali
- Protezioni fisiche post evento
- Sistemi per la risposta a un'emergenza

Le procedure standard e le ispezioni non aggiungono direttamente barriere, quindi in generale non dovrebbero essere considerate IPL

La valutazione dell'efficacia

- La frequenza dell'occorrenza della conseguenza indesiderata può essere stimata combinando la frequenza della causa iniziale con la probabilità di fallimento di ogni IPL, considerando anche ogni condizione modificatrice (*conditional modifier*)
- Per la frequenza e la probabilità si utilizzano ordini di grandezza della magnitudo

Utilizzi della LOPA

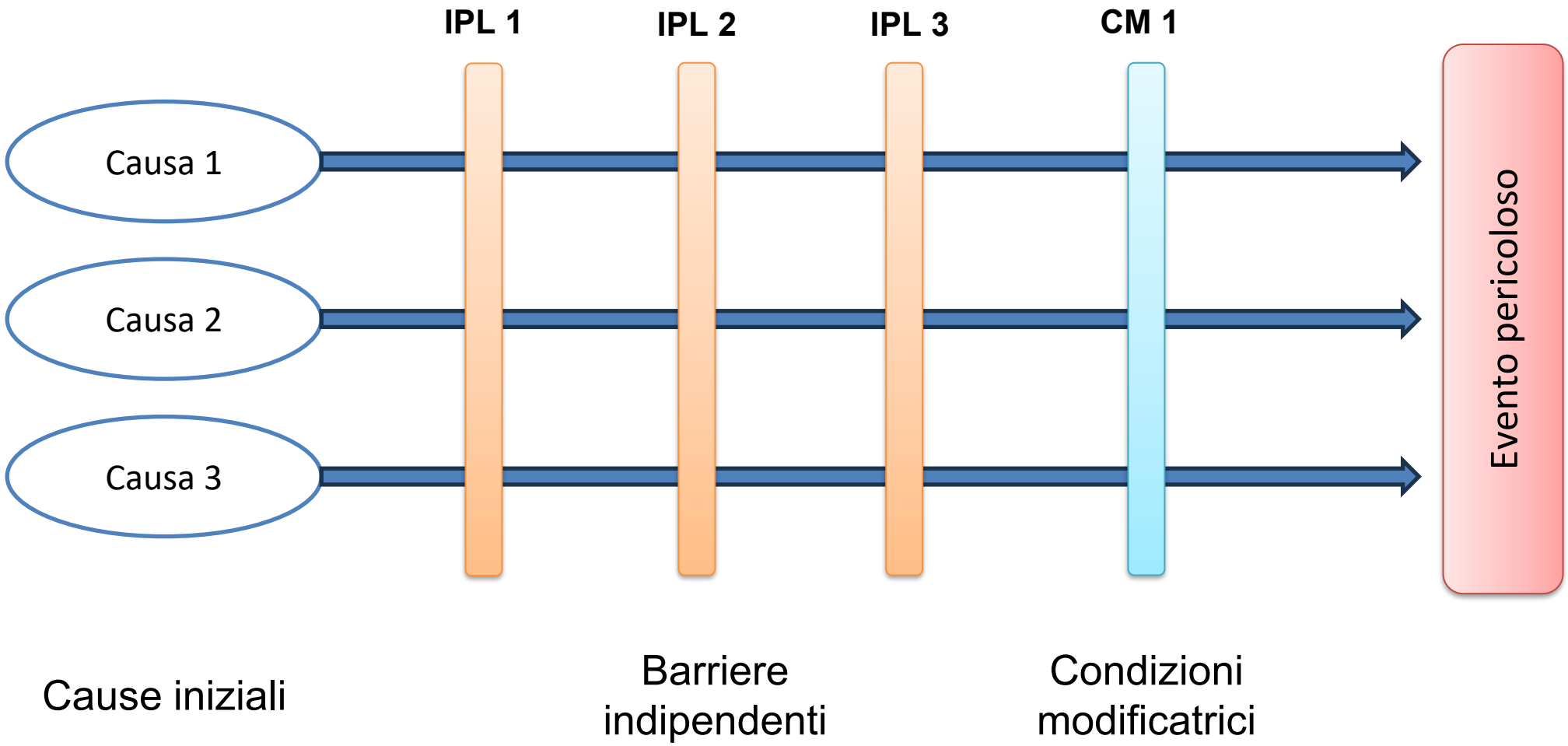
- Utilizzo **qualitativo**: per una revisione delle barriere tra un fattore causale e una conseguenza
- Utilizzo **quantitativo**: per allocare risorse nel trattamento del rischio, analizzando la riduzione del rischio prodotta da ogni barriera di protezione, o per specificare gli IPL e i livelli di sicurezza (*safety integrity level* – SIL) per i sistemi

LOPA: input e output

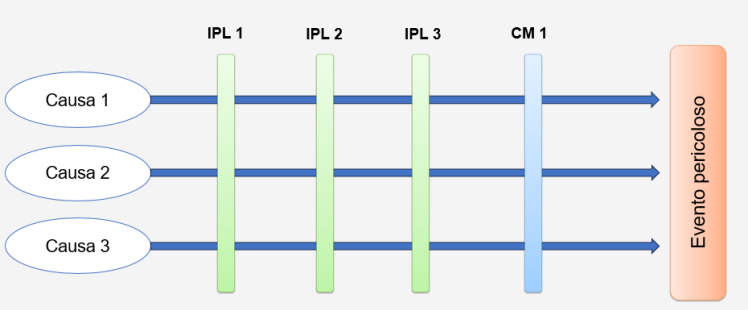
Informazioni sugli eventi, loro fonti, cause e conseguenze
Informazioni sui controlli già adottati o su quelli proposti
Frequenze degli eventi causali e delle probabilità di fallimento di ogni barriera
Quantificazione delle conseguenze
Definizione di rischio tollerabile

Raccomandazioni per futuri trattamenti del rischio
Stima del rischio residuo

LOPA: uno schema



LOPA: esempio di calcolo



	Frequenza della causa (all'anno)	Probabilità di fallimento del IPL 1	Probabilità di fallimento del IPL 2	Probabilità di fallimento del IPL 3	Probabilità della condizione modificatrice	Frequenze intermedie dell'evento
Causa iniziale 1	0,1	0,1	0,2	0,05	0,5	0,00005
Causa iniziale 2	0,2	0,1	0,2	0,05	0,5	0,0001
Causa iniziale 3	0,6	0,1	0,2	0,05	0,5	0,0003
				Frequenza complessiva dell'evento pericoloso		**0,00045**

LOPA: punti di forza

- Richiede meno tempo e risorse di un albero degli eventi o una valutazione pienamente quantitativa, ma è più rigorosa di giudizi soggettivi
- Aiuta a identificare le barriere più critiche e a destinarvi maggiore attenzione e risorse
- Identifica operazioni, sistemi e processi per i quali non ci sono sufficienti barriere
- Si focalizza sulle conseguenze più significative e gravi

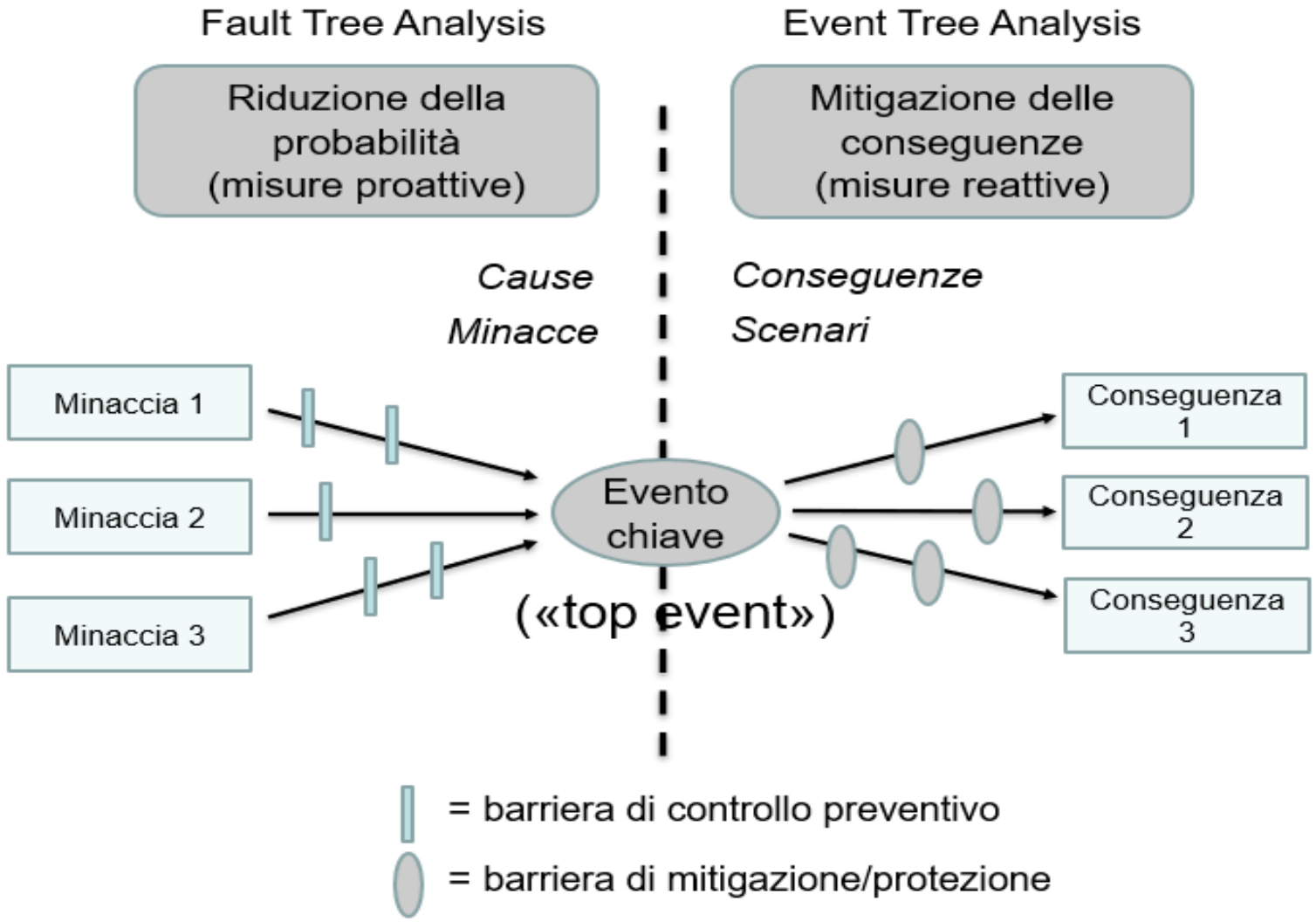
LOPA: limiti

- Non considera le interazioni complesse tra i rischi o tra i controlli (analizza una coppia causa-conseguenza alla volta, e uno scenario alla volta)
- Nell'utilizzo quantitativo, potrebbe non considerare certi tipi di guasti comuni
- Non è applicabile a scenari complessi dove ci sono molte coppie causa-conseguenza o dove ci sono varie conseguenze che hanno impatti su diversi stakeholder

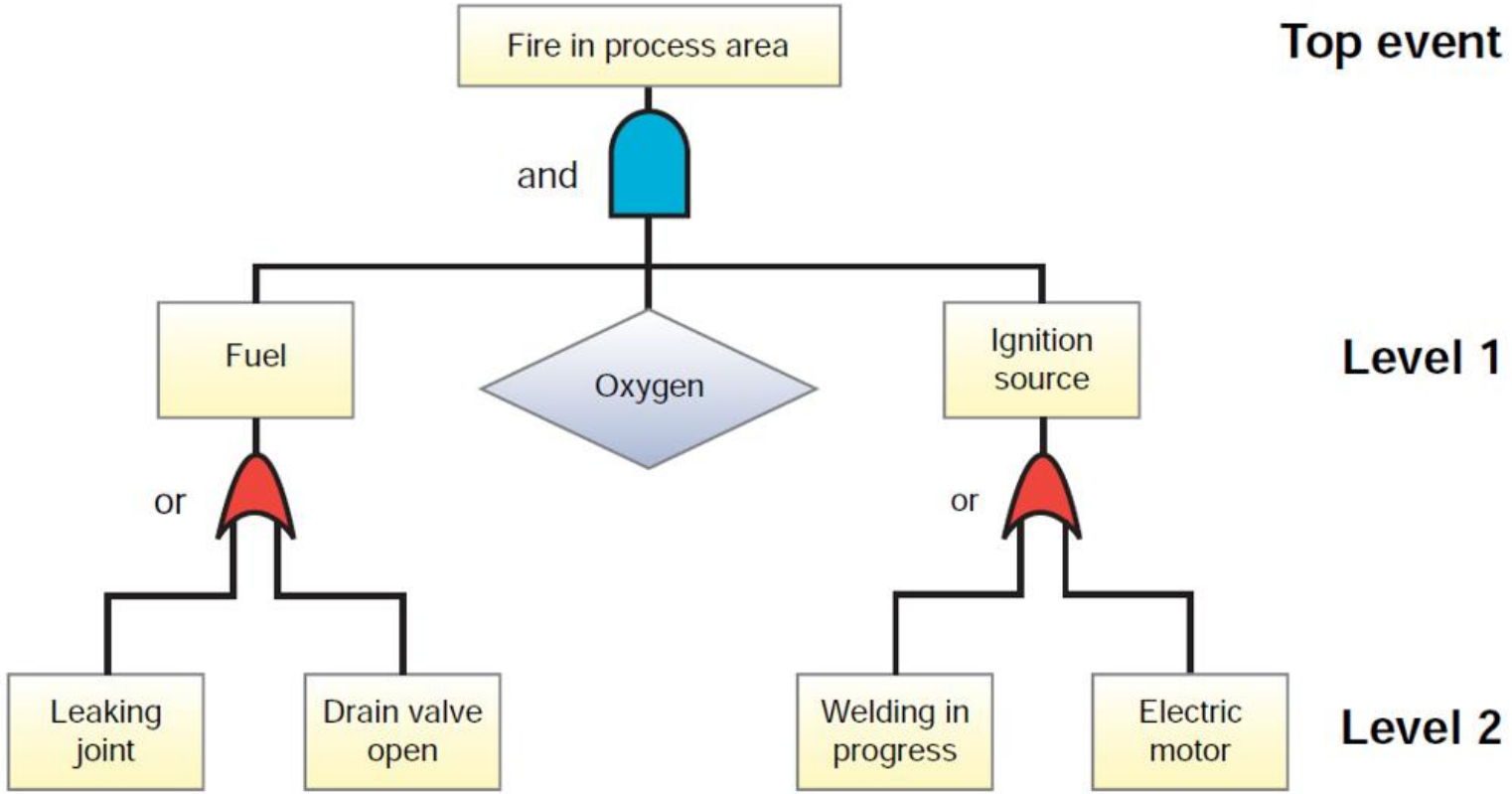
Modello bow tie per l’analisi delle barriere

- Si tratta di una raffigurazione della relazione fra albero dei guasti e l’albero degli eventi
- È stato sviluppato in ambito industriale negli anni ’90
- Si basa sul modello di Reason delle cause degli incidenti (Swiss cheese model)

Schema del modello bow tie



Esempio di semplice albero dei guasti



Usi del bow tie

In modo **qualitativo**

- la rappresentazione grafica consente di visualizzare quanto il rischio è ben controllato
- la valutazione del rischio in questo caso è qualitativa, si basa sul giudizio di esperti

In modo **quantitativo**

- se sono presenti dati a sufficienza per poter costruire l'albero dei guasti e l'albero degli eventi, entrambi in modo quantitativo, si può procedere ad una raffigurazione che contenga le probabilità
- la valutazione del rischio in questo caso è quantitativa, si basa su dati storici o empiricamente ricavati

Resilienza e rischi emergenti

ISO 22316:2017ISO (International Organization for Standardization). (2017). ISO 22316:2017, Sicurezza e resilienza – Resilienza organizzativa – Principi e attributi.
ISO/TS 31050:2023ISO (International Organization for Standardization). (2023). ISO/TS 31050:2023, Gestione del rischio – Linee guida per la gestione di un rischio emergente per migliorare la resilienza.

Come vengono definiti i rischi emergenti
(ISO/TS 31050)

- Sono rischi caratterizzati da novità, dati insufficienti e carenza di informazioni verificabili e di conoscenza necessaria a prendere decisioni su di essi

Esempi di situazioni che possono dare luogo a rischi emergenti

- Cambiamenti non riconosciuti nel contesto organizzativo
- Innovazione o sviluppo sociale e tecnologico
- Nuove fonti di rischio, fonti non precedentemente riconosciute
- Processi, prodotti o servizi nuovi o modificati

Un esempio collegato alla sicurezza e salute è costituito dal punto 8.1.3 della ISO 45001 ***Gestione del cambiamento***

Esempi di cambiamenti nel contesto che possono essere fonti di rischio

- Eventi naturali (eventi estremi)
- Sfide poste dall'Internet of Things
- Resistenza agli antibiotici
- Intelligenza artificiale
- Macchine autonome
- Cambiamenti climatici, transizione energetica

Allegato A, informativo, alla ISO/TS 31050

Esempi di categorie di rischi emergenti

- I rischi emergenti includono:
  - Rischi che non sono stati riconosciuti o esperiti in precedenza da un'organizzazione
  - Rischi familiari ma in un contesto nuovo o non familiare dove la conoscenza esistente non è applicabile
  - Rischi che evolvono in modo significativo
  - Rischi sistemici *(vedi prossima slide)*
  - Nuove combinazioni di rischi

Rischi emergenti: esempi *(1 di 5)*

Rischi che non sono stati riconosciuti o esperiti in precedenza da un'organizzazione

Esempio:

L'utilizzo di una nuova tecnologia di stampa 3D con materiali compositi sconosciuti potrebbe comportare l'esposizione a nanoparticelle o sostanze volatili non ancora classificate come pericolose, con effetti a lungo termine sulla salute dei lavoratori non ancora noti. Questo è un rischio emergente perché l'organizzazione non ha precedenti esperienze con questa tecnologia e i suoi potenziali effetti sulla salute.

Rischi emergenti: esempi *(2 di 5)*

Rischi familiari ma in un contesto nuovo o non familiare dove la conoscenza esistente non è applicabile

Esempio:

Il lavoro da casa, diffusosi durante la pandemia, ha portato a un aumento dei rischi psicosociali, come l'isolamento sociale e la difficoltà nel conciliare lavoro e vita privata. Anche se questi rischi erano già noti in altri contesti, il lavoro da casa ha creato un nuovo ambiente in cui le conoscenze e le strategie di prevenzione precedenti potrebbero non essere efficaci.

Rischi emergenti: esempi *(3 di 5)*

Rischi che evolvono in modo significativo

Esempio:

Il cambiamento climatico sta portando a un aumento degli eventi meteorologici estremi, come ondate di calore, alluvioni e tempeste, che possono avere un impatto significativo sulla sicurezza dei lavoratori, ad esempio nel settore delle costruzioni o dell'agricoltura. Questo è un rischio emergente perché la sua frequenza e intensità stanno cambiando rapidamente, richiedendo nuove misure di prevenzione e adattamento.

Rischi emergenti: esempi *(4 di 5)*

Rischi sistemici

Esempio:

La crescente interconnessione dei sistemi informatici e la dipendenza dalle infrastrutture critiche, come la rete elettrica, rendono le organizzazioni più vulnerabili agli attacchi informatici, che possono causare interruzioni dell'attività, perdite di dati e danni economici. Questo è un rischio emergente perché la sua complessità e le sue potenziali conseguenze sono in continua evoluzione, richiedendo un approccio olistico e multidisciplinare per la sua gestione.

Rischi emergenti: esempi *(5 di 5)*

Nuove combinazioni di rischi

Esempio:

L'introduzione di robot collaborativi (cobot) negli ambienti di lavoro può portare a nuove combinazioni di rischi, come il rischio di collisione tra uomo e macchina, il rischio di stress lavoro-correlato a causa dell'aumento del carico di lavoro mentale e il rischio di perdita di competenze specifiche a causa dell'automazione. Questo è un rischio emergente perché richiede una nuova valutazione dei rischi e l'adozione di misure preventive integrate che tengano conto delle interazioni tra i diversi fattori di rischio.

Rischi sistemici *(allegato C, informativo)*

- Il termine sottolinea la interconnessione tra le minacce
- Sono caratterizzati da:
  - Un alto livello di complessità, dove i processi causali sono difficili da comprendere
  - Sono trasversali ai paesi e ai settori
  - Si sviluppano in modo non-lineare per relazioni causali non-deterministiche
  - Sono caratterizzati da punti di non ritorno, raggiunti i quali il sistema cambia le condizioni di esistenza in breve tempo
  - Generalmente c'è un ritardo nella regolamentazione e nella percezione pubblica degli impatti

Cambiamenti e rischi emergenti

I rischi emergenti sono tipicamente rappresentati da una serie di nuove circostanze o condizioni, precedentemente non riconosciute, o cambiamenti nelle caratteristiche di rischi già identificati.

- I cambiamenti possono essere ad esempio:
  - Nelle norme in vigore nella società
  - Nella cultura organizzativa
  - Nelle percezioni
  - Dati, o informazione interpretate dai dati, circa un rischio o il modo in cui esso evolve

Cambiamenti e rischi emergenti: esempi *(1 di 2)*

Tipo di cambiamento	Esempi di rischi emergenti
Cambiamenti nelle norme in vigore nella società	L'aumento dell'accettazione sociale del lavoro da casa ha portato a nuove sfide per la sicurezza e la salute sul lavoro, come l'isolamento dei lavoratori e la difficoltà nel monitorare le condizioni di lavoro
Cambiamenti nella cultura organizzativa	L'adozione di nuove tecnologie digitali può portare a un cambiamento nella cultura organizzativa, con un'enfasi maggiore sulla velocità e l'efficienza, che può aumentare il rischio di stress e burnout per i lavoratori

Cambiamenti e rischi emergenti: esempi *(2 di 2)*

Tipo di cambiamento	Esempi di rischi emergenti
Cambiamenti nelle percezioni	Una maggiore consapevolezza dei rischi psicosociali, come lo stress e il burnout, può portare i lavoratori a essere più propensi a segnalare questi problemi, il che può farli apparire come rischi emergenti, anche se potrebbero essere sempre stati presenti
Cambiamenti nei dati o nell'informazione interpretata dai dati circa un rischio o il modo in cui esso evolve	L'analisi dei dati raccolti tramite i dispositivi indossabili può rivelare nuove informazioni sui rischi ergonomici associati a determinati compiti lavorativi, portando a una rivalutazione dei rischi e all'adozione di nuove misure preventive

A cosa possono portare i rischi emergenti

- Possono portare ad esempio:
  - Esposizione a pericoli imprevisti e a minacce con esiti incerti
  - Aumento dell'esposizione a pericoli o minacce da fonti già note
  - Opportunità perse o utilizzate

A cosa possono portare i rischi emergenti: esempi *(1 di 3)*

Tipo di rischio emergente	Esempi
Esposizione a pericoli imprevisti e a minacce con esiti incerti	• Esempio 1: L'utilizzo di nuove tecnologie di intelligenza artificiale (IA) nei processi produttivi può comportare l'esposizione a pericoli imprevisti, come algoritmi che prendono decisioni errate o imprevedibili con conseguenze negative per la sicurezza dei lavoratori. • Esempio 2: L'introduzione di nuovi materiali nanotecnologici può comportare l'esposizione a minacce con esiti incerti a lungo termine sulla salute dei lavoratori, a causa della scarsa conoscenza degli effetti a lungo termine di queste sostanze.

A cosa possono portare i rischi emergenti: esempi *(2 di 3)*

Tipo di rischio emergente	Esempi
Aumento dell’esposizione a pericoli o minacce da fonti già note	• Esempio 1: L'intensificazione del lavoro a causa dell'uso di tecnologie digitali può aumentare l'esposizione a pericoli già noti, come lo stress, la fatica e i disturbi muscoloscheletrici • Esempio 2: La diffusione del lavoro da casa può aumentare l'esposizione a minacce da fonti già note, come l'isolamento sociale, la sedentarietà e le difficoltà nell'applicazione delle norme di sicurezza domestica

A cosa possono portare i rischi emergenti: esempi *(3 di 3)*

Tipo di rischio emergente	Esempi
Opportunità perse o utilizzate	• Esempio 1: La mancata adozione di misure preventive per affrontare i rischi emergenti legati all'uso delle tecnologie digitali può portare alla perdita di opportunità di migliorare la produttività e il benessere dei lavoratori. • Esempio 2: L'utilizzo di nuove tecnologie per il monitoraggio e la gestione dei rischi emergenti può portare a un miglioramento delle condizioni di lavoro, a una riduzione degli infortuni e delle malattie professionali e a un aumento della competitività aziendale.

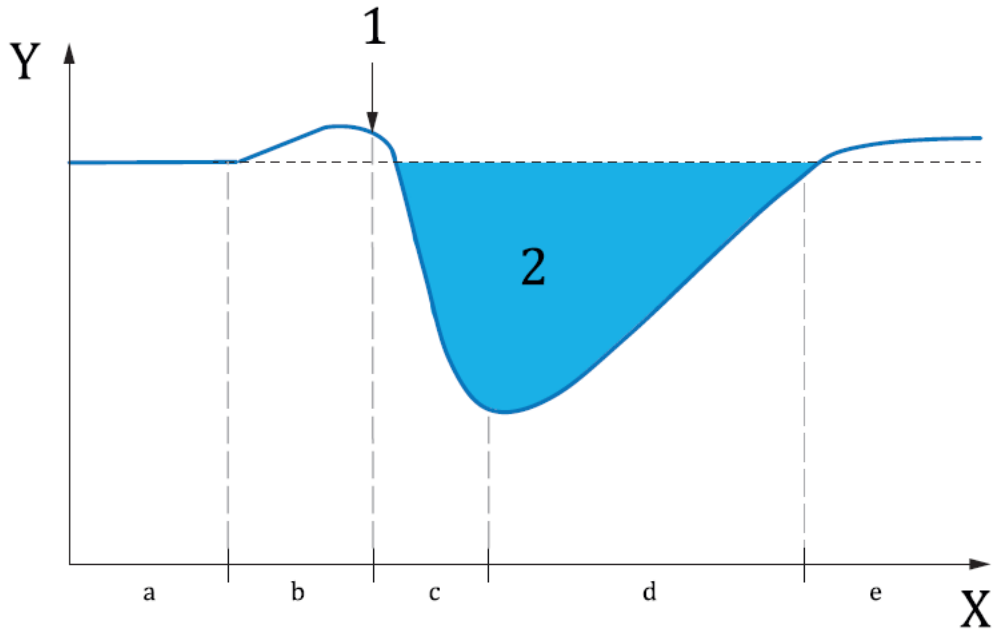
Resilienza Organizzativa *(ISO 22316)*

Abilità di un'organizzazione in un contesto in cambiamento di assorbire i cambiamenti, adattarvisi e recuperare funzionalità

Vi sono 7 principi della resilienza organizzativa. Essa è:

- Aumentata quando i comportamenti sono allineati a scopi e a una visione condivisa
- È sostenuta da una comprensione aggiornata del contesto dell'organizzazione
- È sostenuta dall'abilità di assorbire, adattarsi e rispondere in modo efficace ai cambiamenti
- È sostenuta da una buona capacità di governare e gestire
- È supportata da una varietà di abilità, leadership, conoscenze ed esperienze
- È accresciuta dal coordinamento fra contributi di discipline diverse, dalle aree tecniche a quelle scientifiche
- È sostenuta da un'efficace gestione dei rischi

Un modello per la resilienza organizzativa di fronte a rischi emergenti



Key

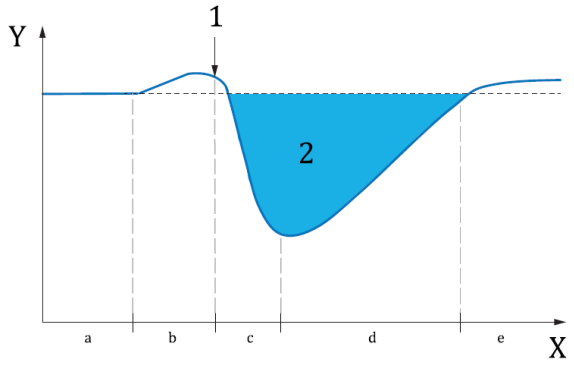
X	scenario time phase
Y	functionality
1	onset of an emerging risk/event/scenario
2	loss of functionality
a	Scanning for emerging risks.
b	Anticipate/prepare.
c	Absorb/withstand.
d	Respond/recover.
e	Adapt/transform.

Figure 2 — Example of an emerging risk development scenario

Immagine tratta dalla ISO/TS 31050

Un modello per la resilienza organizzativa di fronte a rischi emergenti. Esempio *(1 di 4)*

Rischio emergente: carenza di personale qualificato nel settore IT



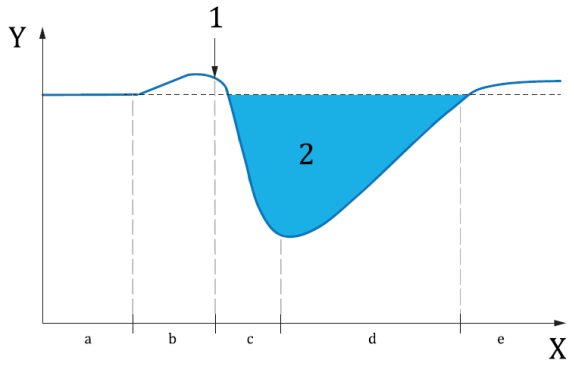
Key

X	scenario time phase
Y	functionality
1	onset of an emerging risk/event/scenario
2	loss of functionality
a	Scanning for emerging risks.
b	Anticipate/prepare.
c	Absorb/withstand.
d	Respond/recover.
e	Adapt/transform.

- **Scanning**: l'azienda monitora il mercato del lavoro e le tendenze del settore IT, notando una crescente difficoltà nel reperire e trattenere personale qualificato.
- **Anticipate/prepare**: l'azienda prevede che la carenza di personale qualificato potrebbe portare a ritardi nei progetti, aumento dei costi e difficoltà nell'innovare. Per prepararsi, l'azienda investe in programmi di formazione interna, crea partnership con università e scuole di formazione professionale e adotta strategie di employer branding per attrarre talenti.

Un modello per la resilienza organizzativa di fronte a rischi emergenti. Esempio *(2 di 4)*

Rischio emergente: carenza di personale qualificato nel settore IT



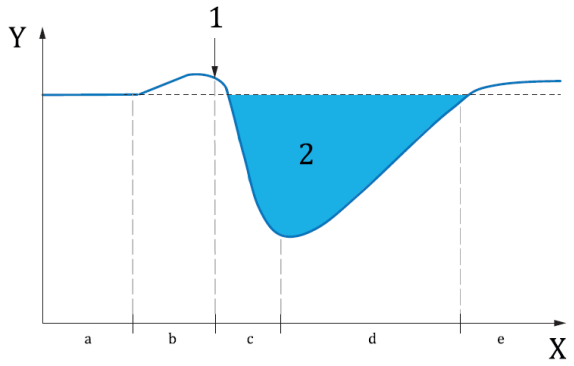
Key

X	scenario time phase
Y	functionality
1	onset of an emerging risk/event/scenario
2	loss of functionality
a	Scanning for emerging risks.
b	Anticipate/prepare.
c	Absorb/withstand.
d	Respond/recover.
e	Adapt/transform.

- **Absorb/withstand**: la carenza di personale inizia a farsi sentire, causando alcuni ritardi nei progetti e un aumento del carico di lavoro per il personale esistente. L'azienda utilizza la sua flessibilità e la sua capacità di adattamento per far fronte alla situazione, ad esempio riorganizzando i team, assegnando priorità ai progetti e ricorrendo a consulenti esterni.

Un modello per la resilienza organizzativa di fronte a rischi emergenti. Esempio *(3 di 4)*

Rischio emergente: carenza di personale qualificato nel settore IT



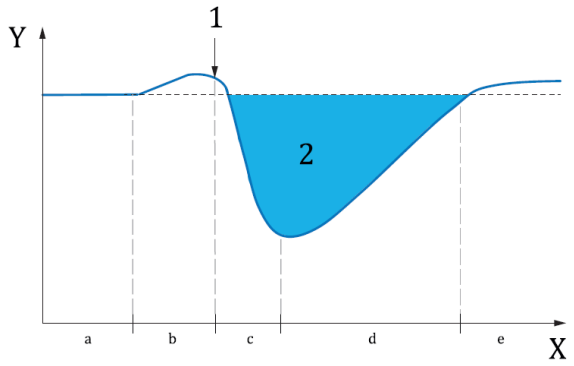
Key

X	scenario time phase
Y	functionality
1	onset of an emerging risk/event/scenario
2	loss of functionality
a	Scanning for emerging risks.
b	Anticipate/prepare.
c	Absorb/withstand.
d	Respond/recover.
e	Adapt/transform.

- **Respond/recover**: l'azienda implementa misure correttive per mitigare l'impatto della carenza di personale, come l'aumento degli stipendi, l'offerta di benefit e l'adozione di modelli di lavoro flessibili. L'azienda cerca anche di accelerare i processi di recruiting e di onboarding per ridurre i tempi di inserimento di nuove risorse.

Un modello per la resilienza organizzativa di fronte a rischi emergenti. Esempio *(4 di 4)*

Rischio emergente: carenza di personale qualificato nel settore IT

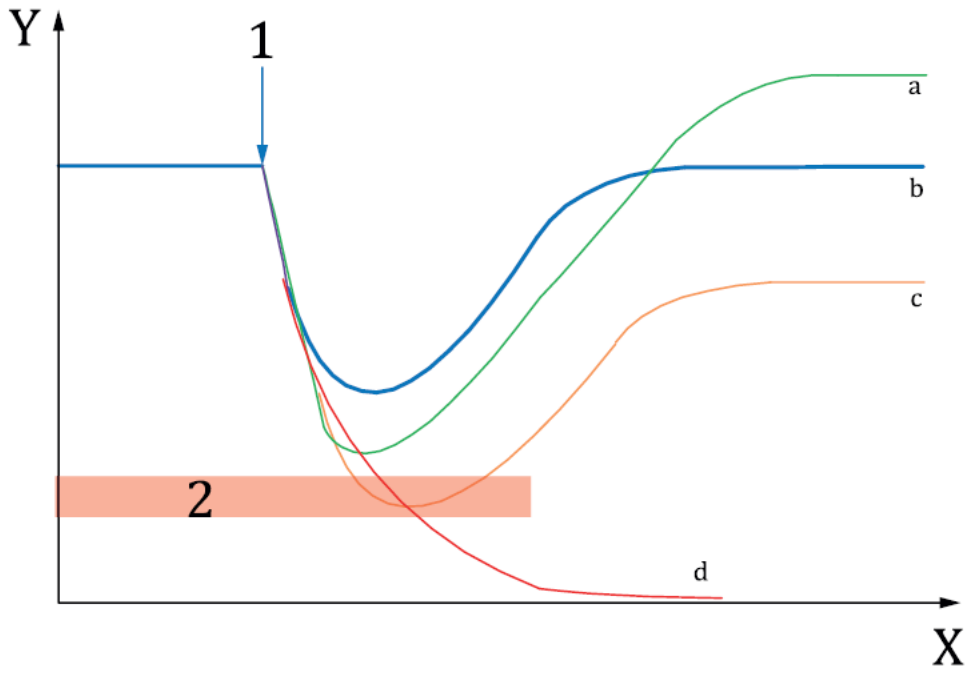


Key

X	scenario time phase
Y	functionality
1	onset of an emerging risk/event/scenario
2	loss of functionality
a	Scanning for emerging risks.
b	Anticipate/prepare.
c	Absorb/withstand.
d	Respond/recover.
e	Adapt/transform.

- **Adapt/transform**: l'azienda riconosce che la carenza di personale qualificato è un problema a lungo termine e adotta una strategia di trasformazione digitale per automatizzare alcune attività, migliorare l'efficienza e ridurre la dipendenza da personale altamente specializzato. L'azienda investe anche in tecnologie di intelligenza artificiale per supportare i processi decisionali e liberare risorse umane per attività a maggior valore aggiunto.

Resilienza: diversi esiti degli eventi sulla funzionalità



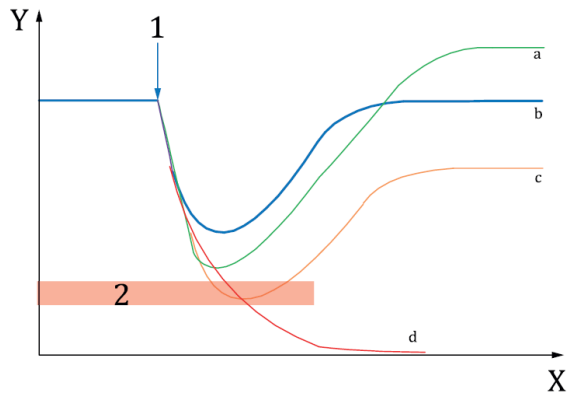
Key

X	scenario time
Y	functionality
1	onset of an emerging risk/event/scenario
2	stress-test limits
a	Functionality better than before.
b	Functionality same as before.
c	Functionality only partially recovered.
d	Functionality completely lost.

Figure 3 — Potential impacts of an incident (event) on functionality

Immagine tratta dalla ISO/TS 31050

Resilienza: diversi esiti degli eventi sulla funzionalità. Scenario a



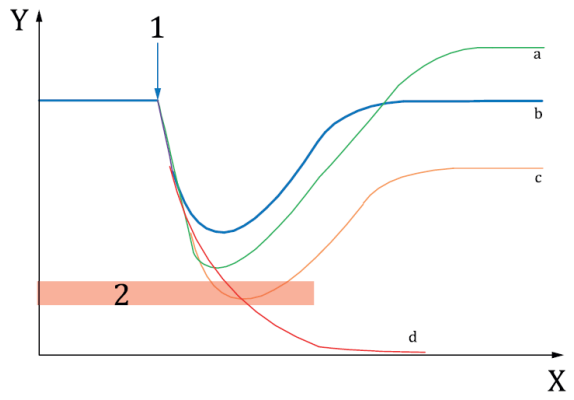
Key

X	scenario time
Y	functionality
1	onset of an emerging risk/event/scenario
2	stress-test limits
a	Functionality better than before.
b	Functionality same as before.
c	Functionality only partially recovered.
d	Functionality completely lost.

Funzionalità migliore di prima. L'organizzazione non solo recupera la funzionalità precedente all'evento, ma la migliora, imparando dall'esperienza e adattandosi al nuovo contesto.

Esempio: Un'azienda farmaceutica, grazie alla pandemia, investe in ricerca e sviluppo, produce un nuovo vaccino efficace e aumenta la sua quota di mercato, migliorando la sua funzionalità rispetto al periodo pre-pandemico.

Resilienza: diversi esiti degli eventi sulla funzionalità. Scenario b



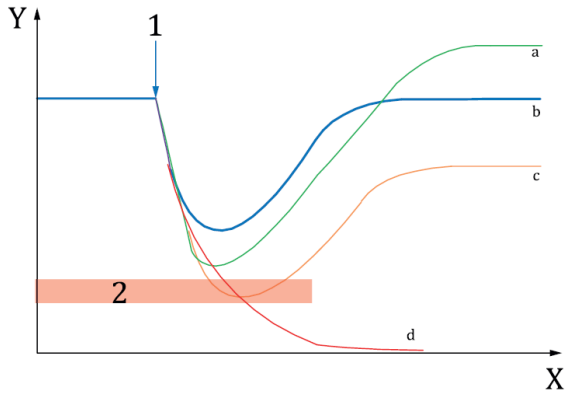
Key

X	scenario time
Y	functionality
1	onset of an emerging risk/event/scenario
2	stress-test limits
a	Functionality better than before.
b	Functionality same as before.
c	Functionality only partially recovered.
d	Functionality completely lost.

Funzionalità uguale a prima. L'organizzazione riesce a recuperare completamente la funzionalità precedente all'evento, tornando allo stato iniziale.

Esempio: Un'azienda di servizi, dopo un periodo di difficoltà durante il lockdown, riesce a ripristinare completamente la sua attività, tornando ai livelli di produttività pre-pandemici.

Resilienza: diversi esiti degli eventi sulla funzionalità. Scenario c



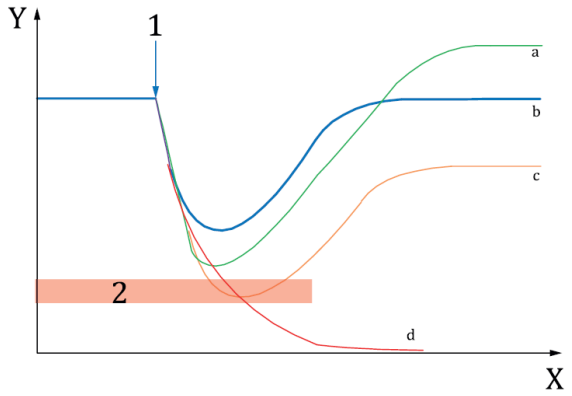
Key

X	scenario time
Y	functionality
1	onset of an emerging risk/event/scenario
2	stress-test limits
a	Functionality better than before.
b	Functionality same as before.
c	Functionality only partially recovered.
d	Functionality completely lost.

Funzionalità parzialmente recuperata. L'organizzazione recupera solo parzialmente la funzionalità precedente all'evento, subendo un danno permanente.

Esempio: Un ristorante, a causa delle restrizioni e del cambiamento delle abitudini dei consumatori, subisce una riduzione permanente del fatturato, riuscendo a sopravvivere ma con una funzionalità ridotta.

Resilienza: diversi esiti degli eventi sulla funzionalità. Scenario d



Key

X	scenario time
Y	functionality
1	onset of an emerging risk/event/scenario
2	stress-test limits
a	Functionality better than before.
b	Functionality same as before.
c	Functionality only partially recovered.
d	Functionality completely lost.

Funzionalità completamente persa. L'organizzazione non riesce a recuperare la funzionalità e cessa di esistere.

Esempio: Un'agenzia di viaggi, fortemente dipendente dal turismo internazionale, non riesce a superare la crisi causata dalla pandemia e fallisce.

Identificare i rischi emergenti

- La modalità chiave per l'identificazione dei rischi emergenti è **l'analisi del contesto**
- 'Comprendere il contesto dell'organizzazione (interno ed esterno) e le aspettative delle parti interessate' è una parte importantissima di ogni sistema di gestione
- Ciò andrebbe fatto in base a processi continui e proattivi per identificare i pericoli
- Monitorare le fonti pertinenti (ad es. EU-OSHA, evoluzione normativa, geopolitica, ambientale)
- Integrare nelle prassi di valutazione del rischio secondo la ISO 31000

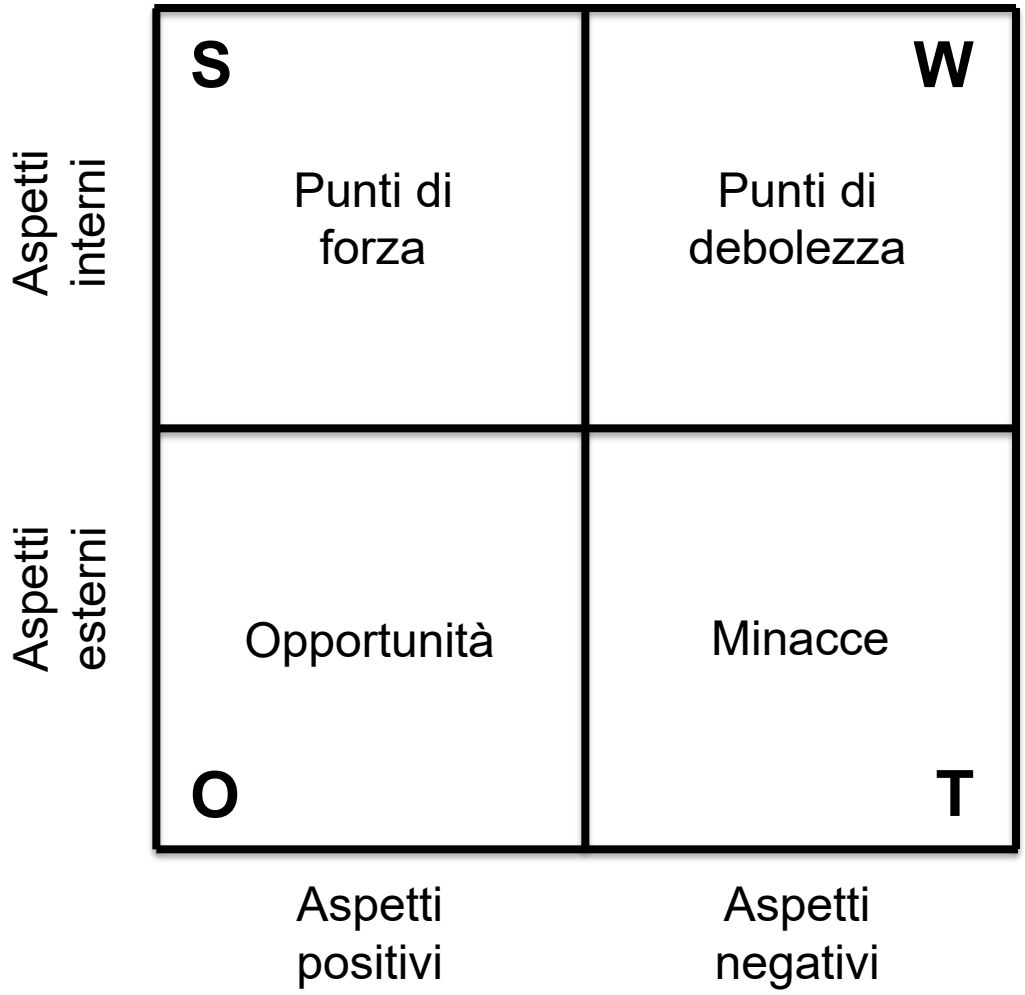
Fare un’analisi del contesto

- Creare un gruppo inter-funzionale per identificare gli aspetti di contesto
- Gestire un’interazione fra i diversi attori, condurre surveys, intervistare le varie funzioni aziendali e stakeholder
- Utilizzare processi di identificazione dei pericoli, valutazione dei rischi
- Considerare le informazioni storiche e attuali
- Esplorare possibili proiezioni future
- Preparare una lista di aspetti contestuali di rilievo
- Identificare i rischi e le opportunità associate agli aspetti contestuali e pianificare azioni di mitigazione

Analisi SWOT

- Analisi del contesto interno ed esterno ad un’organizzazione
- Consente di verificare il posizionamento riguardo a punti di forza, di debolezza, alle opportunità e minacce, con il fine di scegliere le azioni strategiche o operative conseguenti

Analisi SWOT



Analisi PESTLE: cos'è

- Tecnica per analizzare i fattori esterni rilevanti per un'organizzazione
- Ha l'obiettivo di sviluppare adeguate risposte ai cambiamenti
- Gli elementi che emergono costituiscono un quadro di riferimento per la revisione di una strategia aziendale o per una decisione importante
- È denominata anche con altri acronimi leggermente diversi (ad es. PEST), ed è usata spesso in combinazione con l'analisi SWOT

Analisi PESTLE: i fattori

L'analisi PESTLE	
In un'analisi dell'ambiente esterno, occorre tenere conto dei fattori…	
P	Politici
E	Economici
S	Sociologici
T	Tecnologici
L	Legali
E	Ambientali (Environmental)
L'analisi PESTLE dell'ambiente esterno	

Perché gestire i rischi emergenti: i benefici

- I benefici nella gestione dei rischi emergenti sono:
  - Maggiore consapevolezza, con riduzione della probabilità di mancanza di anticipazione dei rischi emergenti
  - Riconoscimento precoce dei rischi emergenti e aumento dei livello di preparazione e di resilienza
  - Disseminazione in tempi brevi di dati e scambio di informazioni tra parti interessate
  - Allineamento delle azioni sui rischi emergenti attraverso tutti gli aspetti del contesto organizzativo

Gestione dei rischi emergenti

- La loro gestione si basa sulla conoscenza e sulla necessita di accumulare dati e informazioni verificabili

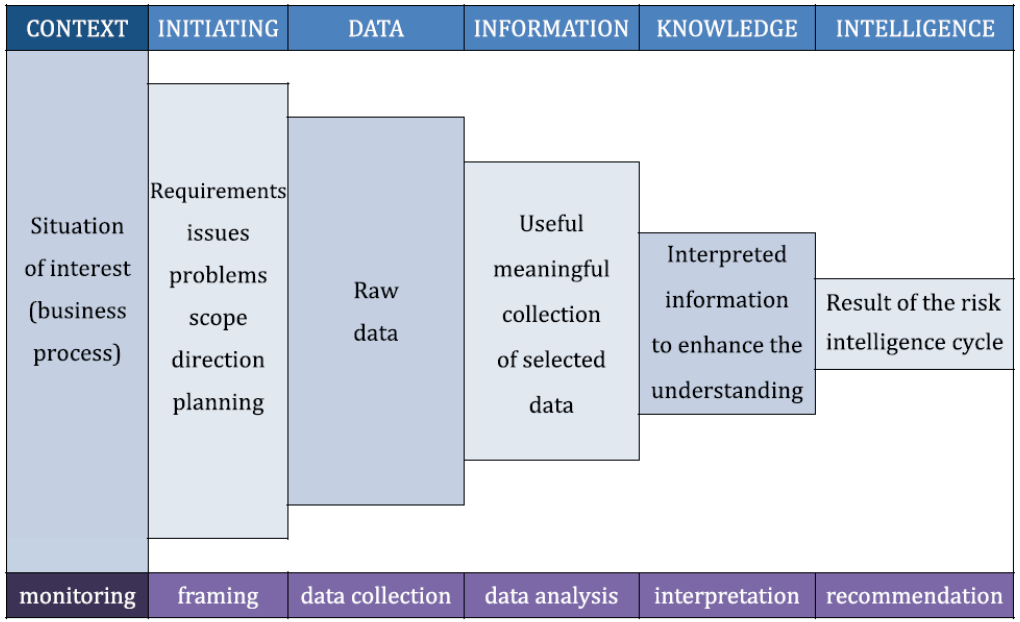


Figure 4 — Data, information, knowledge and intelligence (DIKI) process

Immagine tratta dalla ISO/TS 31050

Il processo DIKI (Data, Information, Knowledge, Intelligence)

- **Monitoraggio**: in questa fase si monitora il contesto per individuare segnali deboli di possibili rischi emergenti.
- **Definizione**: si definisce il problema, l'ambito di interesse e gli obiettivi.
- **Raccolta dati**: si raccolgono dati grezzi sul rischio emergente.
- **Analisi dati**: si analizzano i dati raccolti per estrarre informazioni significative.
- **Interpretazione**: si interpretano le informazioni per comprenderne il significato e le implicazioni.
- **Raccomandazioni**: si formulano raccomandazioni per la gestione del rischio emergente.

Il processo DIKI: esempio

Rischio emergente: Utilizzo di robot collaborativi (cobot) in un'azienda manifatturiera.

Monitoraggio	L'azienda monitora le novità tecnologiche e le tendenze del settore, individuando l'emergere dei cobot come una nuova soluzione per l'automazione
Definizione	L'azienda definisce il problema: valutare i rischi per la sicurezza dei lavoratori derivanti dall'introduzione dei cobot. L'ambito di interesse è l'ambiente di lavoro in cui i cobot saranno utilizzati. L'obiettivo è garantire la sicurezza dei lavoratori
Raccolta dati	L'azienda raccoglie dati grezzi sui cobot, come le specifiche tecniche, le modalità di utilizzo, le norme di sicurezza, gli incidenti e i near miss riportati in letteratura e in altre aziende
Analisi dati	L'azienda analizza i dati raccolti per individuare i pericoli specifici dei cobot, come il rischio di collisione, di schiacciamento, di intrappolamento, di lesioni da movimenti imprevisti
Interpretazione	L'azienda interpreta le informazioni per comprendere la gravità dei pericoli, la probabilità di accadimento, le possibili conseguenze per i lavoratori
Raccomandazioni	L'azienda formula raccomandazioni per la gestione del rischio, come la progettazione di postazioni di lavoro sicure, l'adozione di sistemi di sicurezza, la formazione dei lavoratori, la definizione di procedure di lavoro sicure

Alcuni esempi di elementi da includere nelle registrazioni

- Nome del rischio emergente, sua identificazione
- Descrizione dei possibili scenari, interconnessioni possibili con altri rischi
- Risultati di pre-assessment (es. area di attività impattate, possibili metodi di valutazione del rischio)
- Informazioni di valutazione dei rischi (es. descrizione e gravità delle conseguenze)
- Azioni per monitorare il contesto e aggiornate le informazioni

Allegato B, informativo, alla ISO / TS 31050

Elementi da includere nelle registrazioni – Esempio *(1 di 2)*

- Rischio emergente 1: Utilizzo di robot collaborativi (cobot) in un'azienda manifatturiera
- Nome del rischio emergente: Interazione uomo-cobot in area di assemblaggio.
- Descrizione degli scenari:
  - ✓ Scenario 1: Collisione accidentale tra lavoratore e cobot durante le operazioni di carico/scarico pezzi.
  - ✓ Scenario 2: Intrappolamento degli arti superiori del lavoratore tra il cobot e altre attrezzature.
  - ✓ Scenario 3: Attivazione inaspettata del cobot a causa di un malfunzionamento del sistema di sicurezza.
- Possibili interconnessioni con altri rischi:
  - ✓ Rischio di stress lavoro-correlato a causa dell'aumento del carico di lavoro mentale per la gestione dell'interazione con il cobot.
  - ✓ Rischio ergonomico a causa di posture incongrue durante l'interazione con il cobot.

Elementi da includere nelle registrazioni – Esempio *(2 di 2)*

- Risultati di pre-assessment:
  - ✓ Aree di attività impattate: assemblaggio, manutenzione, programmazione.
  - ✓ Possibili metodi di valutazione del rischio: analisi ergonomica delle postazioni di lavoro, HAZOP.
- Informazioni di valutazione dei rischi:
  - ✓ Gravità delle conseguenze: da lievi (contusioni) a gravi (fratture, lesioni permanenti).
  - ✓ Probabilità di accadimento: da bassa a media, a seconda dello scenario.
- Azioni per monitorare il contesto e aggiornare le informazioni:
- Monitoraggio degli incidenti e dei near miss.
  - ✓ Consultazione periodica dei lavoratori.
  - ✓ Aggiornamento delle valutazioni dei rischi in base alle nuove informazioni e alle modifiche del processo.

Linee guida per la gestione dei rischi emergenti al fine di migliorare la resilienza

- Vengono mutuate le fasi descritte nella ISO 31000, aggiungendo ove pertinenti delle ulteriori considerazioni
- Processo di risk assessment dei rischi emergenti:
  - Identificazione dei rischi emergenti
  - Analisi dei rischi
  - Valutazione dei rischi
  - Trattamento dei rischi
  - Monitoraggio e revisione dei rischi
  - Registrazione e documentazione

Esempi di indicatori di resilienza nella ISO/TS 31050

Categoria di indicatori	Esempi di indicatori
Indicatori time-dependent	Lasso di tempo tra un cambiamento nel contesto e l'identificazione di un rischio emergente
Indicatori di produttività e prestazione	Durata della perdita di funzionalità
Indicatori della resilienza in sé (core resilience indicators)	Misura in cui sono state realizzate opportunità dai rischi emergenti

L’analisi del contesto come cerniera

ISO 31000 (cl. 6.3 “Scope, Context & Criteria”)
Personalizza l’intero processo di risk management partendo da **interno + esterno** (mercato, supply-chain, cultura, governance, ecc.)

ISO 31010
Ribadisce che “stabilire il contesto” è il **primo passo** prima di selezionare le tecniche di valutazione (FMEA, Bowtie, LOPA…) e di interpretarne correttamente gli output

ISO/TS 31050 (Emerging Risk & Resilience)
Estende il concetto: il contesto diventa un **radar dinamico** per intercettare segnali deboli, mutamenti socio-tecnologici e fattori di volatilità che alimentano i rischi emergenti — e da lì rafforzare la resilienza organizzativa.

Dal contesto all'azione: il flusso integrato

Output dell'analisi (1)	*Dove confluisce*	*Beneficio chiave*
Risk Drivers noti (minacce/opportunità mappate)	Processo ISO 31000 (Identifica → Analizza → Valuta → Tratta)	Decisioni sul rischio basate su evidenze
Barriere e controlli attuali	Scelta tecniche ISO 31010 (es. Bowtie, LOPA)	Misura dell'efficacia di sicurezza e compliance
Trend & weak signals (cambiamenti di contesto)	Ciclo di "Risk-Intelligence" ISO/TS 31050	Capacità di **anticipare** nuovi scenari e potenziare la **resilienza**
Gap di resilienza (tolleranza agli shock) (2)	Piani di continuità, esercitazioni IC, modelli di stress test	Ripristino rapido e reputazione salvaguardata

(1) I prodotti concreti che escono dall'attività di analisi del contesto (interno + esterno) prima di passare alle fasi operative del risk management.

(2) Il gap di resilienza è la distanza tra la capacità di resilienza che l'organizzazione richiede (per reggere gli shock plausibili nel proprio contesto) e la capacità di resilienza di cui dispone davvero oggi. In pratica: quanto si è lontani dal livello di "assorbo-adatto-riparto" di cui ci sarebbe bisogno.

Grazie