Analisi e gestione del rischio cyber

Vincenzo Calabrò

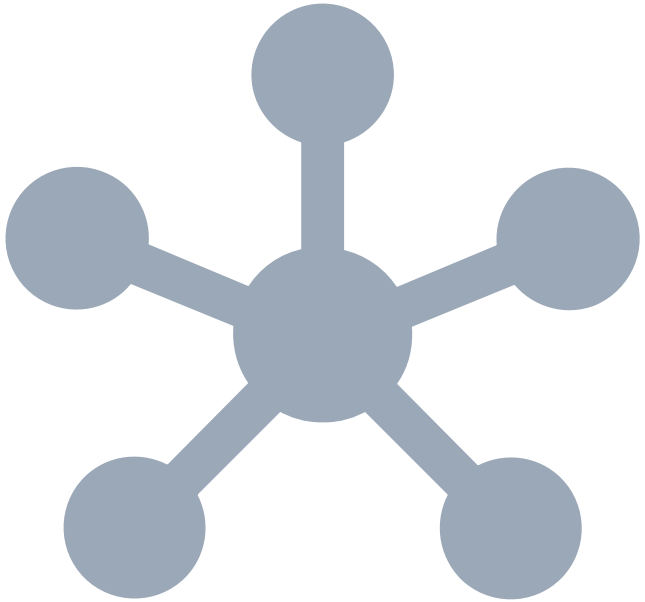
PARTE 1 –
SCALDIAMO
I MOTORI

PARTE 2 –
E' TEMPO
DI 31000

PARTE 3 –
INFORMATION
SECURITY

PARTE 4 –IL
CISO (CHIEF INFORMATION
SECURITY MANAGER)

PARTE 2 – E’ TEMPO DI 31000



Ogni organizzazione, perseguendo i suoi obiettivi, corre molti e diversi rischi.

Il risk management aumenta la possibilità dell'organizzazione di affrontare i rischi in modo migliore, aumentando così la propria possibilità di avere successo.

Il risk management aumenta la razionalità delle decisioni.

Il risk management process aiuta l'organizzazione ad attuare il risk management

La ISO 31000:2018 Risk management — Guidelines standardizza nomenclatura e approccio

ISO 31000:2018

https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

La ISO 31000:2018 ci aiuta a…

… e, inoltre, dobbiamo organizzarci per avere successo

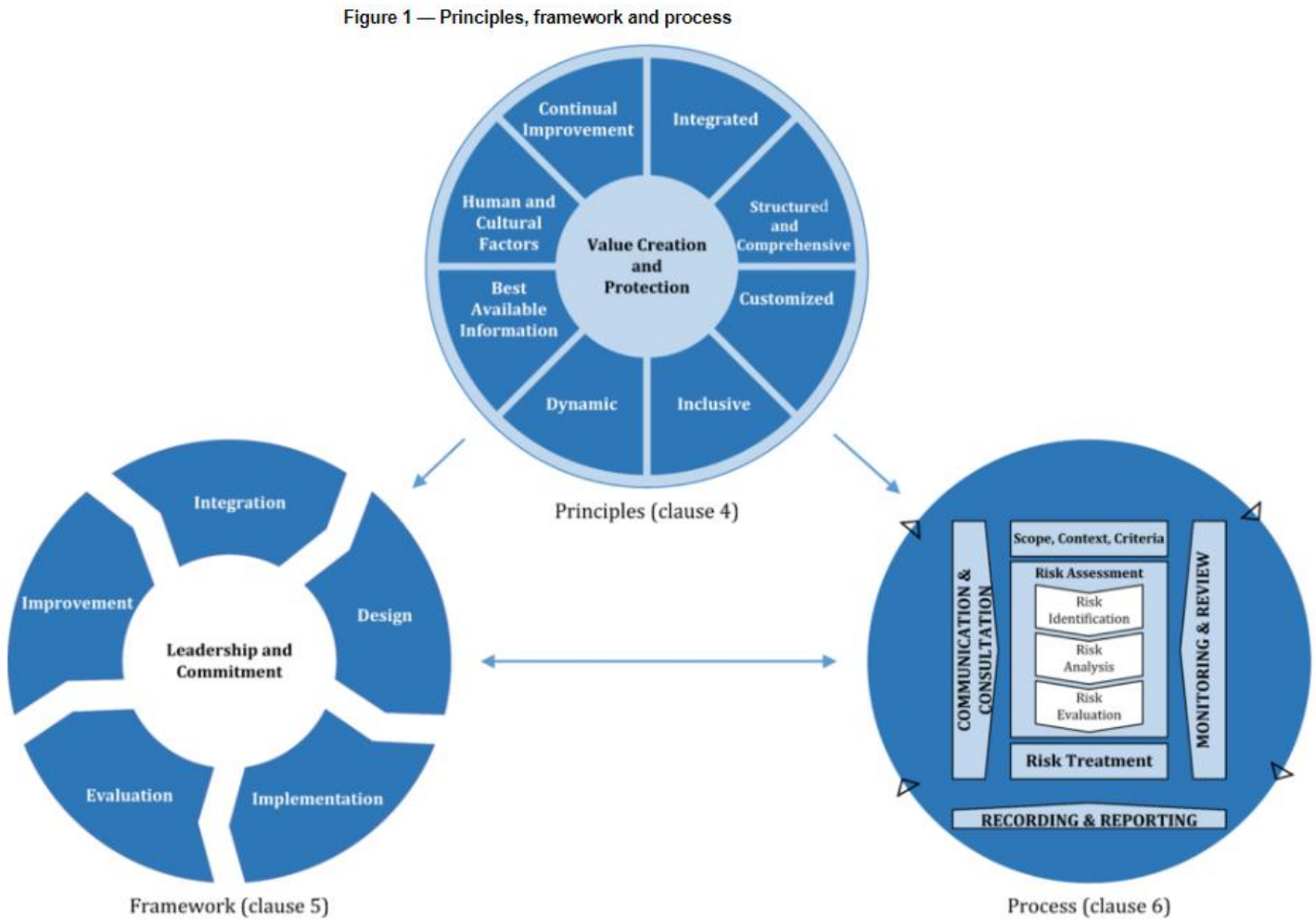
… e prima ancora, di comprendere in che contesto siamo

… ma per farlo abbiamo bisogno di valutarlo

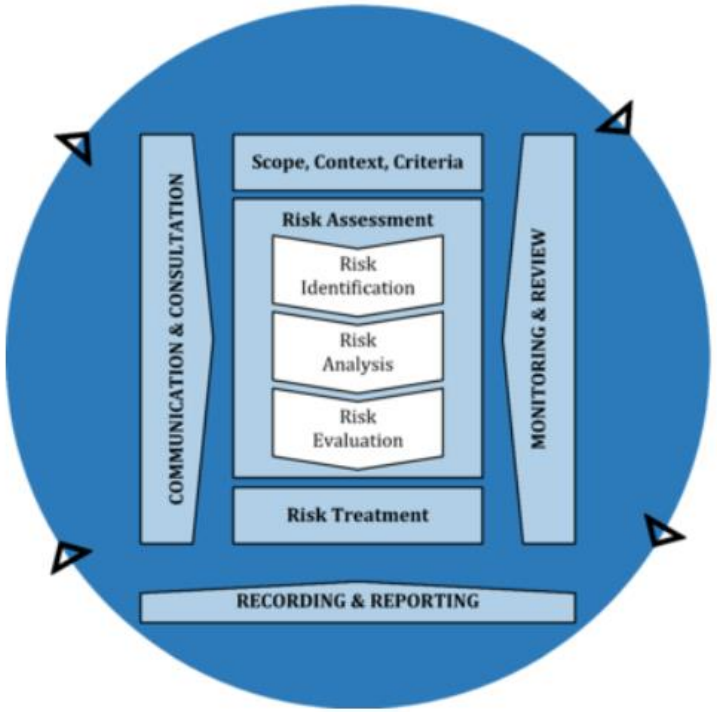
… trattare il rischio

Principi, framework e processo

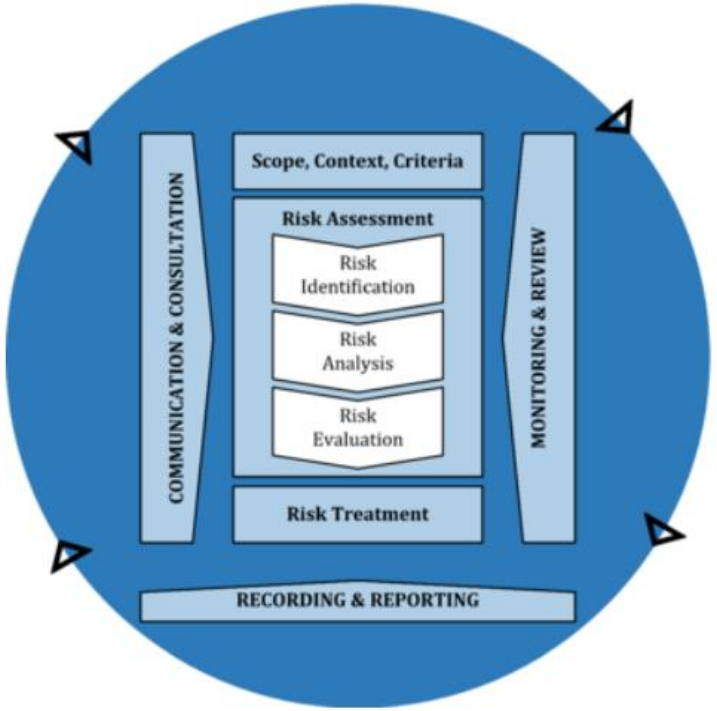
Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.



Risk Management Process as ISO 31000:2018



Cosa sono i 4 triangolini sul perimetro?



Communication and consultation

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Questo processo ha lo scopo di allineare costantemente gli *stakeholders* e ottenere feedback e informazioni utili per prendere le decisioni.

E' un processo cruciale e garantisce nel tempo il commitment aziendale ed è un prerequisito per il successo dell'iniziativa di risk management

Stakeholder (ISO 31000:2018)

DEFINIZIONE

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: The term “interested party” can be used as an alternative to “stakeholder”.

Monitoring and review

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il monitoraggio continuo e le review periodiche hanno lo scopo di assicurare la qualità dell'intero processo di risk management e di migliorarlo nel tempo. In pratica risponde alla domanda «Stiamo facendo bene? Si può migliorare?»

Queste domande bisognerebbe porsele in ogni fase e momento dell'intero processo e bisognerebbe pianificarle e assegnare delle chiare responsabilità di esecuzione. Il risultato di queste analisi dovrebbe essere incorporato nel sistema di gestione delle performance e nel reporting aziendale.

Recording and reporting

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il processo stesso di risk management e i suoi output dovrebbero essere documentati e resi disponibili tramite appropriati meccanismi come, per esempio, la stesura di documenti e la loro archiviazione in modi e luoghi appropriati affinché siano disponibili a chi ne ha o potrebbe avere bisogno. Questi decisioni devono tenere a mente anche gli aspetti di riservatezza e i diversi stakeholder (es. esterni). Lo scopo di questo processo è quello comunicare, fornire informazioni a supporto delle decisioni, migliorare le attività di risk management e interagire con gli stakeholder.

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Scope significa «ambito» ed è molto importante definirlo con chiarezza in anticipo. Lo scope può essere limitato geograficamente (es. le consociate spagnole), secondo il livello (strategico, operativo, progetto, prodotto) o altri criteri

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

E’ importante conoscere e stabilire il contesto interno ed esterno in cui opera l’organizzazione e nel quale essa cerca di raggiungere i propri obiettivi perché creano il contesto entro il quale il processo di risk management deve operare.
Ritroveremo questo tema nel framework – design

Scope context and criteria

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Come abbiamo visto, lo scopo del risk management process è quello di aumentare la razionalità delle decisioni organizzative. In un certo senso, quello di applicare il «metodo scientifico» all'analisi del rischio. Quindi si devono definire criteri e misure il più possibile oggettive e ripetibili nel tempo e da persone diverse per dare istruzioni alle fasi di assessment e treatment che seguono. In questa fase si cerca quindi di definire cose come la risk capacity dell'organizzazione o quando classificare un rischio come alto o basso, eccetera. Si capirà meglio in seguito.

Visto che il risk management ha a che fare con l'incertezza e l'esecuzione del processo stesso fa cambiare nel tempo la maturità aziendale sarà necessario adeguare le decisioni prese in questa fase nel tempo.

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Lo scopo della fase di risk identification è quello di trovare, comprendere e descrivere i rischi. Per farlo è necessario avere delle informazioni rilevanti e aggiornate. Per redigere questa lista si devono considerare molti elementi, come:

— tangible and intangible sources of risk;

— causes and events;

— threats and opportunities;

— vulnerabilities and capabilities;

— changes in the external and internal context;

— indicators of emerging risks;

— the nature and value of assets and resources;

— consequences and their impact on objectives;

— limitations of knowledge and reliability of information;

— time-related factors;

— biases, assumptions and beliefs of those involved.

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

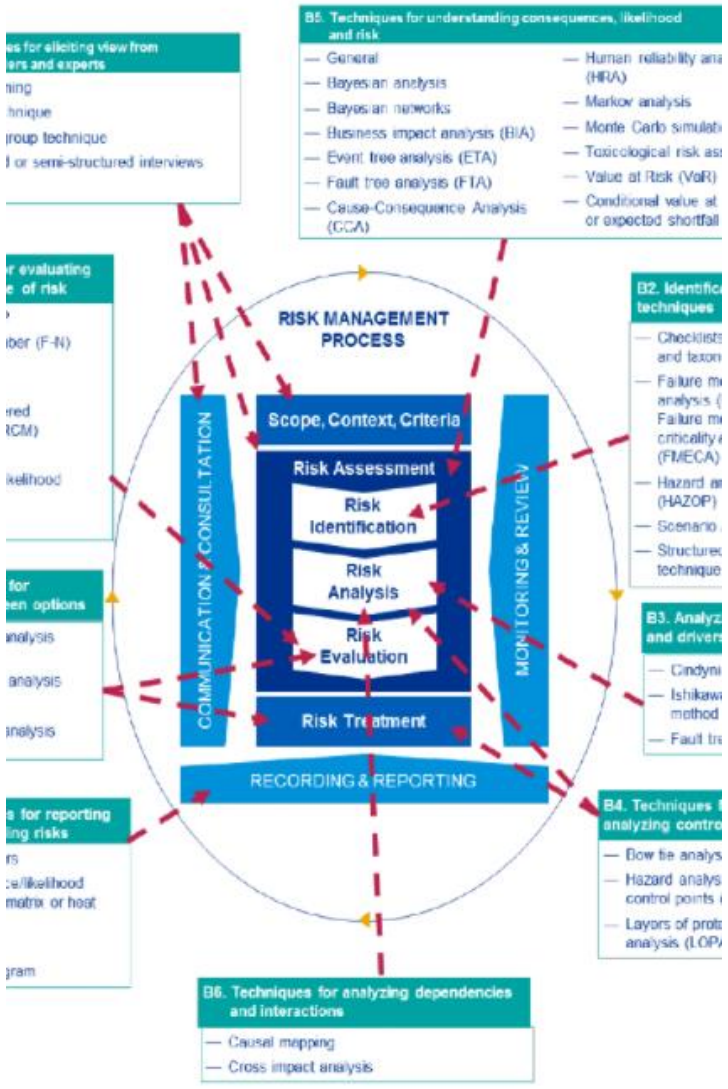
Nella fase di risk analysis si cerca di comprendere la natura del rischio e le sue caratteristiche incluso, se appropriato, il livello di rischio. L'analisi considera gli eventi di rischio (*event*), le risk source, le *conseguenze (consequences)*, le probabilità (*likelihood*), i controlli (*control*) e le relazioni tra eventi che possono avere molteplici cause e conseguenze su diversi obiettivi…

La fase di analisi è prona ad errori (di valutazione, legati alle tecniche di analisi ecc.) e soggetta punti di vista anche molto diversi; quindi è meglio usare molteplici tecniche per valutare rischi con conseguenze gravi.

Lo scopo della fase di analisi è quello di dare informazioni alla fase successiva (evaluation) per decidere se il rischio dovrà essere trattato o meno e come.

Elenco 31 Tecniche di Valutazione del rischio (Tabella A) edizion

1. Brainstorming
2. Structured or semi-structured interviews
3. Delphi
4. Check-lists
5. Primary hazard analysis
6. Hazard and operability studies (HAZOP)
7. Hazard Analysis and Critical Control Points (HACCP)
8. Environmental risk assessment
9. Structure «What if? (SWIFT)
10. Scenario analysis
11. Business impact analysis
12. Root cause analysis
13. Failure mode effect analysis
14. Fault tree analysis
15. Event tree analysis
16. Cause and consequence analysis
17. Cause-and-effect analysis
18. Layer protection analysis (LOPA)
19. Decision tree
20. Human reliability analysis
21. Bow tie analysis
22. Reliability centred maintenance
23. Sneak circuit analysis
24. Markov analysis
25. Monte Carlo simulation
26. Bayesian statistics and Bayes Nets
27. FN curves
28. Risk indices
29. Consequence/probability matrix
30. Cost/benefit analysis
31. Multi-criteria decision analysis (MCDA)



ISO 31010:2019 guida alle tecniche di valutazione del rischio

FONTE: https://www.certifico.com/id/4040

DEFINIZIONE

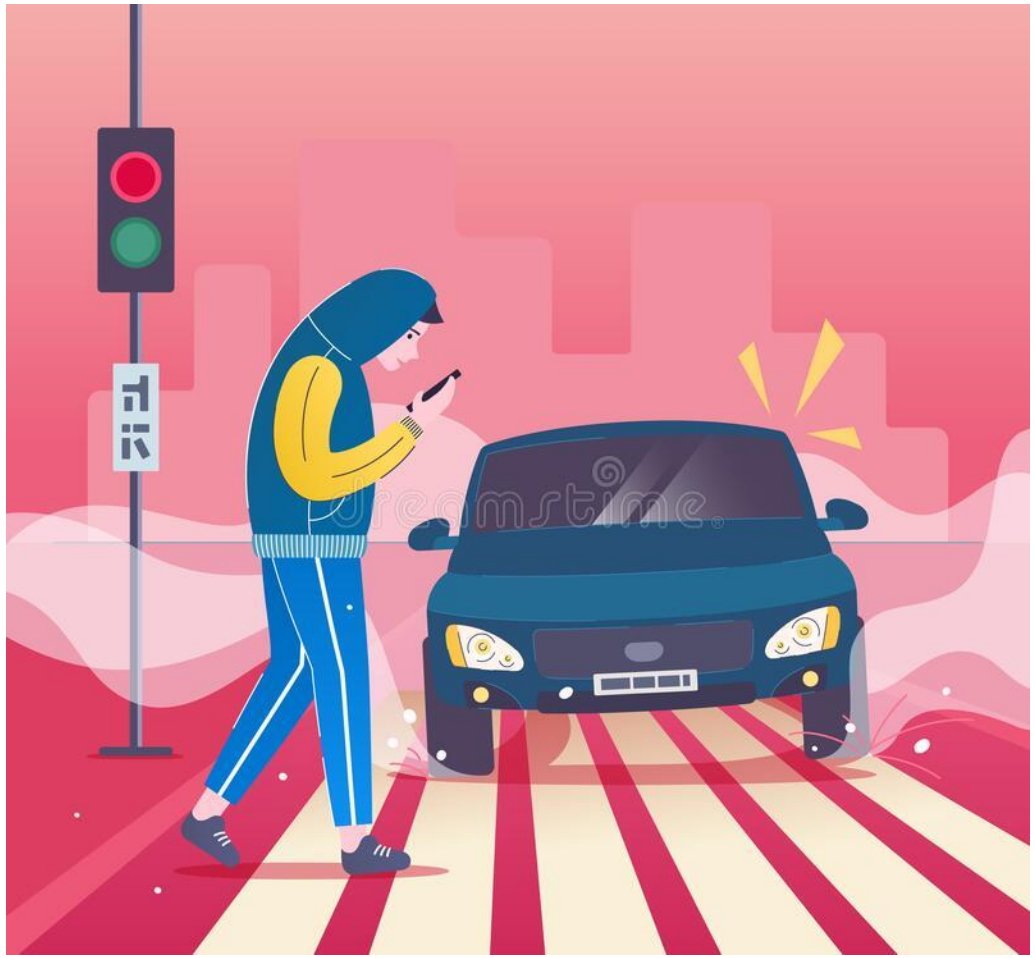
Event (ISO 31000:2018)

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several consequences (3.6).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.



	Pedestrian crossing the road being distracted
1. As a result of <defined cause / causes>,	Come risultato di attraversare la strada guardando il cellulare
2. <this unexpected event> could occur,	Un'automobile potrebbe investirmi
3. which could produce <this effect on targets>	e causarmi morte o ferite e conseguenti costi medici

FONTE:
https://www.dreamstime.com/search.php?securitycheck=3592561f791a84f63f3595d615730338&firstvalue=&lastsearchvalue=&srh_field=pedestrian+accident+vector+illustration+man+smartphone+crosswalk+danger+road+careless+young+dangerous+way+safety+internet+image11892738&s_ph=y&s_il=y&s_video=y&s_audio=y

DEFINIZIONE

Consequence (ISO 31000:2018)

outcome of an event (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

Cosa significa PxI

Considerazioni sulle conseguenze

Visto che si dovranno valutare molti rischi, ognuno con le sue proprie eterogenee conseguenze, per esempio:

- Causare morte o ferite e conseguenti costi medici
- Sversare più di 100.000 litri di inquinante nel fiume
- Comportare un esborso di denaro di 10.000 € per le riparazioni
- Ricevere una multa del 4% del fatturato mondiale annuo
- Apparire nei social con alcuni / molti messaggi negativi per la reputazione

E’ necessario classificare le conseguenze in qualche modo al fine di compararle e ordinare i rischi secondo le conseguenze. La classificazione può essere una misura precisa e quantitativa (esempio denaro perso) oppure per range e qualitativa (esempio lieve / grave).

Definizione dei criteri per la gestione del rischio (un esempio)

L'**Impatto/Danno/Conseguenze (D)** dovute all'evento sfavorevole (incidente), valutata secondo la scala qualitativa.

Impatto/Danno/Conseguenze (D)			
1	Molto basso	Insignificante	Nessun danno alle persone e alla produzione. Basso impatto economico
2	Basso	Basso	Intervento del primo soccorso. Alcune attività bloccate senza danni alla produzione. Medio impatto economico
3	Medio	Moderato	Richiesto intervento medico. Molte attività bloccate con moderati danni alla produzione. Alto impatto economico
4	Alto	Elevato	Danni estesi alle persone. Alcuni processi bloccati con elevati danni alla produzione. Massimo impatto economico anche a livello sistemistico (sistema informatico)
5	Molto alto	Catastrofico	Casi di morte. Rilascio gas tossici con effetti dannosi. Massimo impatto economico a livello sia sistemistico che infrastrutturale

DEFINIZIONE

Likelihood (ISO 31000:2018)

chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

Cosa significa PxI

Considerazioni sulle probabilità

Analogamente alle conseguenze, abbiamo lo stesso bisogno di valutare la probabilità di accadimento e realizzazione di un rischio ai fini di classificazione e ordinamento.

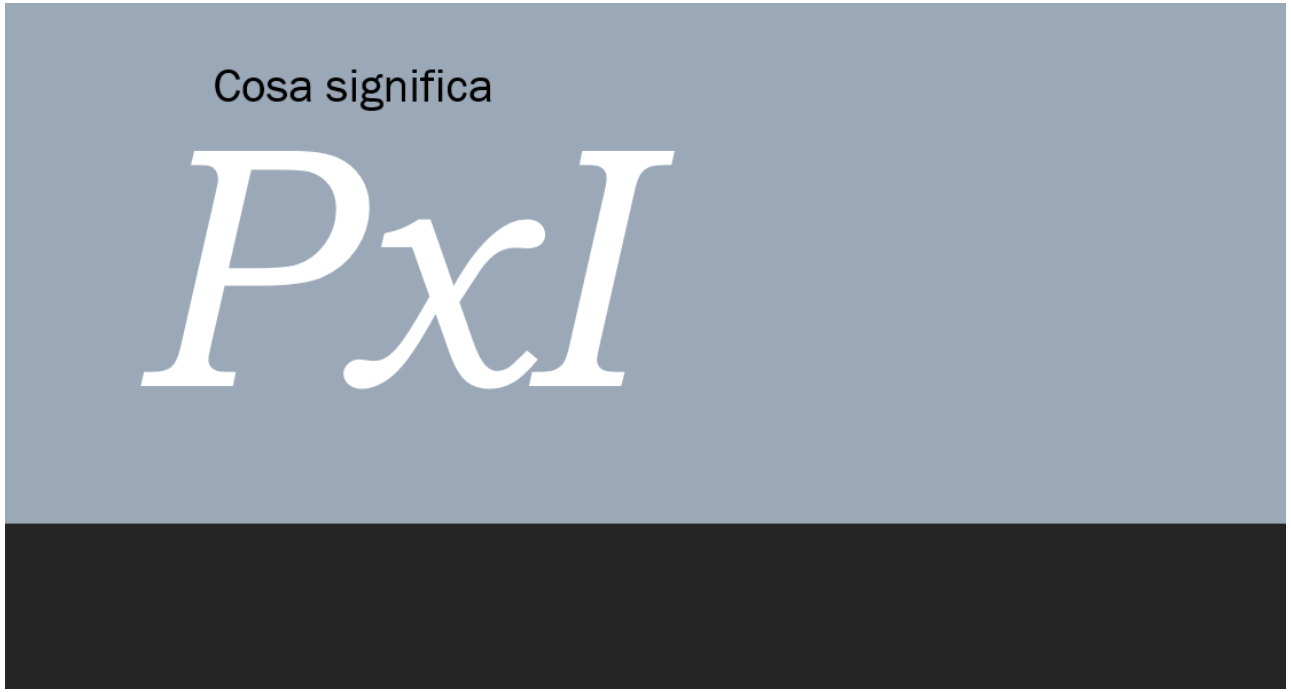
Definizione dei criteri per la gestione del rischio (un esempio)

La **Probabilità** (P) con la quale si manifesta l'evento sfavorevole (incidente), valutata secondo la scala qualitativa.

Probabilità (P)			
1	Molto bassa	Rara	Accade solo in circostanze eccezionali (P<1%)
2	Bassa	Improbabile	È improbabile che accada (1%<P<5%)
3	Media	Moderata	Può accadere in un certo numero di casi (5%<=P<20%)
4	Alta	Probabile	Avviene in una buona parte dei casi (20%< =P<=50%)
5	Molto alta	Quasi certo	Avviene nella maggior parte dei casi (P>50%)

Considerazioni su conseguenze e probabilità

Inoltre ci è sicuramente utile combinare le due valutazioni in un unico indicatore di rischio (livello di rischio).



Level of risk (ISO/IEC 27002:2018)

magnitude of a risk, expressed in terms of the combination of consequences and their likelihood

DEFINIZIONE

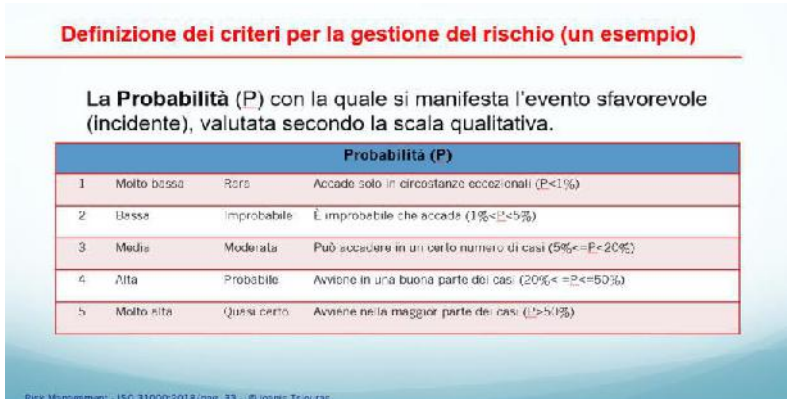
Definizione dei criteri per la gestione del rischio (un esempio)

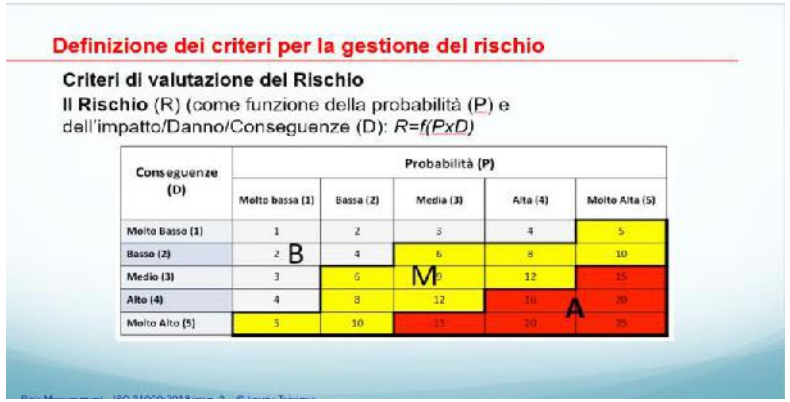
Criteri di valutazione del Rischio

Il **Rischio** (R) (come funzione della probabilità (P) e dell'impatto/Danno/Conseguenze (D): *R=f(PxD)*

Conseguenze (D)	Probabilità (P)				
	Molto bassa (1)	Bassa (2)	Media (3)	Alta (4)	Molto Alta (5)
Molto Basso (1)	1	2	3	4	5
Basso (2)	2 B	4	6	8	10
Medio (3)	3	6	M 9	12	15
Alto (4)	4	8	12	16 A	20
Molto Alto (5)	5	10	15	20	25

Quando si definiscono queste scale e criteri?





Risk assessment

ERAVAMO QUI

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Nella fase di risk analysis si cerca di comprendere la natura del rischio e le sue caratteristiche incluso, se appropriato, il livello di rischio. L'analisi considera gli eventi di rischio (event), le risk source, le conseguenze, le probabilità, i controlli (control) e le relazioni tra eventi che possono avere molteplici cause e conseguenze su diversi obiettivi…

La fase di analisi è prona ad errori (di valutazione, legati alle tecniche di analisi ecc.) e soggetta punti di vista anche molto diversi; quindi è meglio usare molteplici tecniche per valutare rischi con conseguenze gravi.

Lo scopo della fase di analisi è quello di dare informazioni alla fase successiva (evaluation) per decidere se il rischio dovrà essere trattato o meno e come.

Risk assessment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

La valutazione del rischio è un punto di snodo decisionale del processo. Prendendo in input le informazioni prodotte dall'analisi e i criteri di accettabilità (identificati nella fase scope, context and criteria) permette di decidere se e come procedere con il trattamento del rischio.

— do nothing further;

— consider risk treatment options;

— undertake further analysis to better understand the risk;

— maintain existing controls;

— reconsider objectives.

Il risultato della valutazione dovrebbe essere registrato formalmente, comunicato e validato dal management

Risk treatment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

Il rischio può essere trattato in molti modi.

Più specificamente:
- Si può evitare rinunciando all'attività che origina il rischio
- Si può modificare il rischio rimuovendo la fonte di rischio o riducendo la probabilità e l'impatto tramite delle misure
- Si può condividere o trasferire a terzi (es. assicurazione)
- Si può accettare così com'è

Sono scelte complesse che tengono conto dei costi, dei benefici, degli obblighi contrattuali e di legge, della diversa opinione dei diversi stakeholder ecc.

Il trattamento di un rischio può modificare o creare altri rischi che dovranno quindi essere a loro volta gestiti.

Risk treatment

6.2 Communication and consultation

6.3 Scope, context and criteria
- 6.3.2 Defining the scope
- 6.3.3 External and internal context
- 6.3.4 Defining risk criteria

6.4 Risk assessment
- 6.4.2 Risk identification
- 6.4.3 Risk analysis
- 6.4.4 Risk evaluation

6.5 Risk treatment
- 6.5.2 Selection of risk treatment options
- 6.5.3 Preparing and implementing risk treatment plans

6.6 Monitoring and review

6.7 Recording and reporting

I piani di trattamento del rischio specificano come saranno implementate le opzioni scelte di modo che siano ben chiari i compiti di chi è coinvolto e il progresso del piano possa essere monitorato.

I piani dovranno essere integrati nei piani di gestione aziendale e nei relativi processi in accordo con gli stakeholder interessati.

Le informazioni a corredo devono comprendere il perché siano state scelte quelle opzioni di trattamento, i benefici attesi, l'indicazione dei responsabili (approvazione ed esecuzione), le azioni proposte, le risorse disponibili, i criteri di misura del risultato, i vincoli, le regole di reporting, le date previste di svolgimento e completamento del compito).

Control (ISO 31000:2018)

DEFINIZIONE

measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

Considerazioni sui controlli

I controlli possono essere organizzativi o tecnologici, per esempio:

- Ogni sera passare a controllare tutte le porte per verificare che siano chiuse
- Prima di decollare con il parapendio svolgere i 5 controlli del manuale di sicurezza della FIVL
- Installare l'antivirus su ogni nuovo PC consegnato ai dipendenti e rimuovere la password di amministrazione

Parleremo moltissimo dei controlli quando andremo sulla ISO 27000:2018

Risk Management Framework as ISO 31000:2018

Framework = struttura di riferimento

Leadership and commitment

Il top management deve assicurarsi che il risk management sia integrato in tutte le attività dell'organizzazione e dimostrare la propria leadership e il proprio commitment in diversi modi

— customizing and implementing all components of the framework;

— issuing a statement or policy that establishes a risk management approach, plan or course of action;

— ensuring that the necessary resources are allocated to managing risk;

— assigning authority, responsibility and accountability at appropriate levels within the organization.

Il top management è responsabile di gestire il rischio, mentre gli organi di controllo sono responsabili della supervisione della gestione del rischi. In particolare:

— ensure that risks are adequately considered when setting the organization's objectives;

— understand the risks facing the organization in pursuit of its objectives;

— ensure that systems to manage such risks are implemented and operating effectively;

— ensure that such risks are appropriate in the context of the organization's objectives;

— ensure that information about such risks and their management is properly communicated.

Integration

Il risk management deve essere integrato nell’organizzazione, nel suo scopo, nei meccanismi di governo, e nelle operations. Deve essere ovunque e ognuno nell’organizzazione ha la responsabilità di gestire il rischio. Le responsabilità di gestione del rischio e la responsabilità di controllo della gestione del rischio devono essere assegnate con precisione.

Design

Quando si progetta il framework (la struttura di riferimento organizzativa) bisogna fare una serie di cose:

- Comprendere molto bene l'organizzazione e il suo contesto
- Articolare il commitment continuo verso il risk management tramite delle policy (documenti strategici), dichiarazioni o altro spiegandone il bisogno e i meccanismi di funzionamento nell'organizzazione
- Assegnare ruoli organizzativi, autorità, responsabilità e competenze. Evidenziare chi sono i *risk owner*
- Allocare le risorse umane, organizzative, tecnologiche
- Stabilire i meccanismi di comunicazione e di consultazione

Risk owner (ISO Guide 73:2009 Risk management — Vocabulary)

person or entity with the accountability and authority to manage a risk

DEFINIZIONE

Implementation

Durante l’implementazione del risk management framework bisogna sviluppare un piano che includa tempi e risorse, identificare nel dettaglio il processo decisionale e modificare il processo decisionale se necessario e assicurarsi che le disposizioni prese per gestire il rischio siano ben comprese.

Evaluation

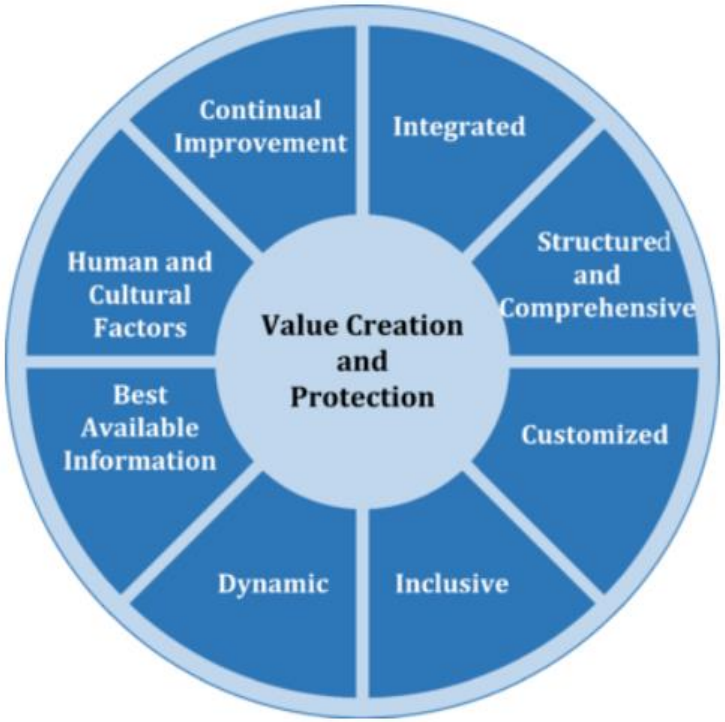
Per valutare l'efficacia del quadro di gestione del rischio, l'organizzazione dovrebbe:

- Misurare periodicamente le prestazioni del risk management framework rispetto al suo scopo, ai piani di implementazione, agli indicatori e al comportamento atteso
- Determinare se rimane adatto a sostenere il raggiungimento degli obiettivi dell'organizzazione

Improvement

In una logica di miglioramento continuo, l’organizzazione deve adattarsi e migliorarsi. Appena vengono identificate delle aree o delle opportunità di miglioramento bisogna sviluppare dei piani e assegnare le responsabilità per la loro esecuzione.

Risk Management Principles as ISO 31000:2018



Principles

a) Integrated: Risk management is an integral part of all organizational activities.

b) Structured and comprehensive: A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) Customized: The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

d) Inclusive: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) Dynamic: Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) Best available information: The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g) Human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement: Risk management is continually improved through learning and experience.

Considerazioni finali sulla ISO 31000:2018

La linea guida aiuta le organizzazioni a strutturare il processo di risk management

Nonostante questa presentazione faccia altrimenti, i principi, il framework e i processi vengono illustrati in quest'ordine

Anche se non si fa esplicito riferimento al PDCA si prevede una continua retroazione (feedback) tra le varie fasi del processo

Visto che il risk management cerca di ridurre i rischi e l'incertezza correlata, è normale che varie decisioni e disposizioni vengano corrette ed emendate nel tempo

Il risk management (di successo) è un processo continuativo che deve accompagnare l'evoluzione organizzativa negli anni; è per sempre