**ANALISI E GESTIONE DEL RISCHIO**

INDICE

* [Che cos’è il rischio?](#rischio)
* [Risk Management](#Risk_Management)

Introduzione

**Clusit:** Associazione Italiana per la sicurezza informatica.

**Rapporto Clusit 2024**: parte da una panoramica degli incidenti di sicurezza più significativi a livello globale del 2023 confrontandoli con i dati dei 4 anni precedenti. È importante per le analisi che svolge e l’opera di informazione verso il pubblico, la stampa e i decision maker.

Il numero di attacchi è in crescita sia a livello globale (12%) che a livello italiano (65%).



**Caso: Colonial Pipeline Cyber Attack**: degli hackers hanno bloccato il più grande oleodotto americano (8850km) che fornisce il 45% del carburante dell’East Coast, impedendo il trasporto di combustibili.

Le aziende hanno smesso di erogare carburante per una decina di giorni subendo danni economici ingenti.

Sono stati richiesti 5 milioni di riscatto.

Biden ha dovuto firmare un ordine esecutivo in appena 3 giorni per rispondere a questo attacco, con gli obiettivi di:

1. Rimuovere le barriere nella condivisione delle informazioni tra governo e settore privato;
2. Modernizzare ed implementare standard di cyber security più forti nel governo generale;
3. Migliora la suppy chain security

Sono intervenute la FBI e la CISA (Cybersecurity and Infrastructure Security Agency), quest’ultima creata appena nel 2018 ma con un budget di più di 3 miliardi.

Si pensa che l’attaccante sia riuscito ad accedere tramite il computer di un dipendente che lavorava da remoto questo mostra come il lavoro da remoto sia un vantaggio ma anche un aumento della superficie d’attacco, bisogna bilanciare il lavoro da remoto con maggiore sicurezza.

L’organizzazione di hacker creò anche Darkside per pubblicizzarsi sul dark web e far comprare i servizi ad altri hacker, si autoproclamano come “etici” non attaccando organi sensibili come scuole, ospedali, organizzazioni no-profit e chiedendo sempre un riscatto non in grado di far chiudere l’azienda.

Nonostante ciò, il 15% delle aziende hackerate (non per forza da Darkside) ha fallito entro un anno dal pagamento del riscatto, a volte i piccoli imprenditori preferiscono chiudere l’azienda ed aprirne un’altra.

**Caso LazioCREA**: un gruppo di hacker ha attaccato il sistema vaccinale del Lazio durante la pandemia. Sono entrati mediante le credenziali di un dipendente di Frosinone ed hanno criptato milioni di dati con un ransomware, richiedendo un riscatto di 5 milione in cryptovalute per la chiave di criptaggio.

Fortunatamente il ransomware non era perfetto e si sono recuperati i dati tramite un backup, ma il sistema è stato bloccato per 6 giorni.

Fasi del furto:

1. Furto delle credenziali VPN
2. Installazione di **Emotnet**: programma malware sviluppato come trojan bancario per accedere ai dispositivi e spiare i dati sensibili. Si nasconde tra gli antivirus ed installa un worm infiltrandosi nei computer di rete. Si diffonde tramite mail spam.
3. Inserimento del ransomware che cripta le informazioni sovrascrivendo i vecchi dati con nuovi e cryptando i vecchi. In questo caso fortunatamente non hanno cryptato il backup.

**Cosa gestiscono i sistemi aziendali?**

Le aziende possono essere di diversi tipi, in questo caso non consideriamo le Pubbliche amministrazioni e onlus.

I dati possono essere strutturati (DataBase) o Destrutturati (documentali).

**Sistemi per la gestione di:**

* **Fornitori**: l’ufficio acquisti tratta i fornitori (vendor) dopo aver raccolto le esigenze interne ordinando i materiali necessari diretti (per la produzione) o indiretti. Tra i documenti troviamo ordine di acquisto (purchase order), richiesta di acquisto RDA (per raccogliere le esigenze) e richiesta di offerta RDO (per chiedere informazioni). I dati principali riguardano le persone giuridiche (**fornitori**), i **prezzi** e le **condizioni di vendita.**
* **Produzione**: molto varia in base al prodotto. Dati: **qualità** e **quantità**, usando in maniera efficiente le risorse.
* **Gestione dei clienti**: possono essere altre aziende (B2B) o clienti (B2C), gestiti dall’ufficio commerciale. Ci sono anche collaboratori esterni come commerciali, agenti, rappresentanti, distributori… retribuiti in base agli obiettivi raggiunti. Di solito il margine è più importante del fatturato, tranne se voglio un fatturato molto alto per comprare la concorrenza. Se i prodotti sono sofisticati si aggiunge una forza di prevendita (assistenza all’acquisto) e di post-vendita (assistenza all’uso). Sistema informatico **CRM** (customer relationship management) che gestisce i contatti, le trattative e gli ordini.
* **Ricerca e sviluppo**: cerca soluzioni buone per il mercato. **Segreti**. Ufficio R&D Research&Development. Documenti: disegni in bozza, disegni tecnici dettagliati, documenti testuali, corrispondenza interna, documenti interni, modelli, prototipi…
* **Marketing**: produce la marca verso il mercato. gestice pubblicità, conferenze, articoli, social networks...I sistemi informativi raccolgono le info e le rendono disponibili.   
  Dati: analisi di mercato, proiezioni di vendita, campagne pubblicitarie…
* **Risorse umane**: si occupa dell’amministrazione e della gestione del personale attraverso tutte le fasi del rapporto di lavoro (dalla candidatura, all’assunzione, alle dimissioni o pensionamento). Si occupa degli stipendi dei lavoratori, dello studio del loro potenziale e della loro formazione. Dati: dipendenti, retribuzione, valutazioni, salute…
* **Amministrazione finanza e controllo**:Tiene la contabilità in partita doppia e redige il bilancio di esercizio composto da conto economico (costi e ricavi), stato patrimoniale (la ricchezza dell’azienda, attivo e passivo) e nota integrativa. Permette di misurare le performance dell’azienda, definisce il budget, tiene i rapporti con le banche, si procura o cede liquidità…
* **Funzione legale**: Le aziende possono avere un ufficio legale per cause, controversie, brevetti... Principalmente documentazione cartacea.

**RID/CIA**: Confidentiality (riservatezza), Integrity (integrità) e Availability (disponibilità).



Marketing in ritardo poco efficace

Copia cartacea

Reputazione?

Bilanci non pronti quando necessari

Bilanci sono pubblici

Mancato/errato pagamento

Leak delle info🡪 perde segretez

Perdo elenco dei clienti

Non posso produrre per tot tempo

Fattura pagata a pers sbagliata

Che cos'è il rischio?

1. [ISO 27000] **effetto dell'incertezza sugli obiettivi.**

L'incertezza è dovuta ad eventi che possono avere effetti negativi o positivi (quasi sempre negativi).

Il rischio è associato alle potenziali minacce che sfruttano le vulnerabilità dell’asset di un’informazione o di un gruppo di informazioni e potrebbe avere conseguenze negative sull’azienda.

**Obiettivi dell’analisi**: riguardano diversi ambiti (economico, sicurezza, salute), possono essere applicati a diversi livelli (strategico, tattico, operativo), possono essere espressi in modi differenti e a parole diverse, in maniera frontale oppure implicita. Possono essere economici-finanziari (fatturato, margine, giacenza di cassa…) e non economico-finanziari (ambiente, salute e sicurezza dei dipendenti, felicità della comunità…).

Gli obiettivi potrebbero essere in contrasto tra di loro.

**Effetto**: deviazione rispetto alle aspettative.

**Incertezza**: deficit della conoscenza del mondo, degli eventi, delle loro probabilità e conseguenze.

Legata alla conoscenza di un evento, di una situazione.

Dipende da due elementi:

1. dall'incertezza, intesa come conoscenza di un evento e del relativo "contorno".
2. dall'esposizione dell'obiettivo all'incertezza, intesa come impatto, magnitudo.

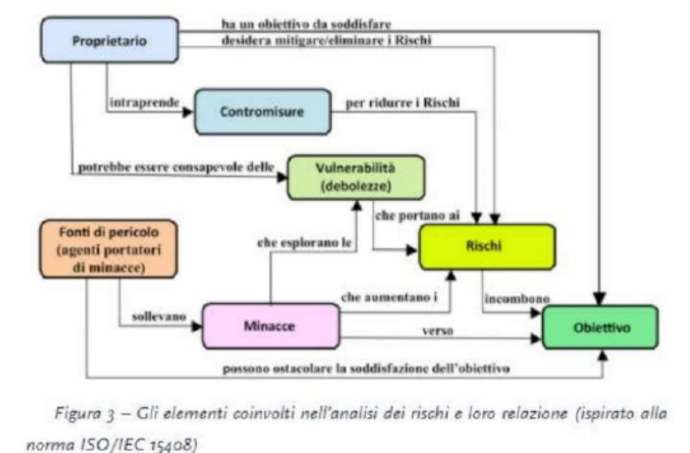
**Effetto dell'incertezza**: corrisponde a mancare l'obiettivo di un piccolo o grande margine.

1. [Fiorito] ***R = P x I***, con P la probabilità che accada l'evento e I l'impatto.

Lo esprime come: "come risultato di una causa, un inaspettato evento ([ISO 31000] il verificarsi o il cambiamento di un particolare insieme di circostanze) può avvenire, il quale produce certi effetti sugli obiettivi".

NB: Gallotti distingue impatto e conseguenza come qualcosa di immediato e qualcosa a breve/medio/lungo termine.

1. [loannis] ***R = f ( P, D)*** con P **probabilità** di incidente, D **impatto** (legato alle conseguenze dell’evento sull’obiettivo( [ISO 31000] conseguenze= risultato di un evento che influisce sugli obbiettivi) e **funzione** che si sceglie per combinare P e D.

**Proprietario di un obiettivo**:ogni individuo ha un proprietario (introdotto da Ioannis)

* Responsabilità del raggiungimento dell’obiettivo
* Responsabilità del controllo della situazione
* Attribuire valore all’obbiettivo (l’unico che può farlo)
* Decide la strada per raggiungerlo.
* Fonte di pericolo (agenti portatori di minacce) e misure (controlli intrapresi dal proprietario per ridurre rischi a livelli accettabili.

1. In sicurezza informatica, rischio è espresso come effetto dell’incertezza sugli obiettivi della sicurezza informatica.
2. [ISO 31000] viene espresso in termini di fonti di pericolo e di potenziali eventi.

Es: rischi di contagio da covid, rischio di credito insoluto e rischio di perdita di un asset.

Risk Management

Risk management: processo di gestione del rischio; la ISO 31000 ne definisce principi e linee guida.

Obiettivo: evitare che l’incertezza impedisca il raggiungimento degli obiettivi.

“insieme di attività che servono per indirizzare e controllare l’organizzazione rispetto al rischio”.

**Risk manager process**: applicazione sistematica delle regole policies che l’azienda si dà.

Per farlo applico sistematicamente politiche, procedure e pratiche alle attività di comunicazione, consultazione e identificazione, analisi, trattamento e monitoraggio dei rischi 🡪Come le aziende fanno risk manager. Descritto nella ISO 31000.

**Certificazioni professionali**: strumento con cui dimostrare la propria competenza in un certo sensore al di là o a rafforzamento delle referenze individuali.

**Classificazioni dei rischi secondo l’impatto**:

* **Strategici**: Sono legati agli aspetti strategici dell’azienda come mission, vision e obiettivi aziendali. Sono di altissimo livello e quindi comprensibili anche dal «pubblico» (stakeholder esterni).

Es: margine, fatturato, salute dei clienti, tasso di cambio, mancanza di acqua e materie prime…

* **Operazionali** (processi e procedure): Sono legati agli aspetti di processo e procedurali dell’azienda. Per essere identificati e compresi richiedono la conoscenza di dettaglio dei processi e/o procedure

Es: far aprire un conto corrente alla persona sbagliata.

* + **Processi**: set di attività legate tra loro che usano degli inputs per arrivare al risultato atteso. 🡪attività per raggiungere un goal
  + **Procedure**: modo specifico per mandare aventi un’attività o processo. 🡪passaggi da seguire per un task.
* **Progetti**: relativi ai progetti di ogni tipo, inclusi quelli di realizzazione/integrazione di software. Per essere identificati e compresi richiedono la conoscenza del progetto, ma alcune caratteristiche sono comuni. Temporaneo: ha un inizio e una fine. Obiettivi specifici. Utilizzano risorse limitate ed un budget. Gestiti da project manager.
* **Prodotti**: Sono legati alla progettazione, produzione, commercializzazione e manutenzione di prodotti materiali o immateriali. L’enfasi è sulla realizzazione di qualcosa che verrà prodotto in grandi quantità

5 fasi del Risk Management:

1)Comprensione del contesto, ambito e criterio;

2)Risk Assessment;

3)Trattamento del rischio;

4)Monitoraggio e riesame; 🡪continua nel tempo.

5)Comunicazione e consultazione. 🡪continua nel tempo.

1. **Comprensione del contesto, ambito** (o campo di applicazione) **e criterio**:

Contesto di un’organizzazione [ISO 9000:2015]: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e sul raggiungimento degli obiettivi di un’organizzazione.

>Fattori interni: struttura organizzativa, caratteristiche principali del sistema informativo, rapporti con il personale interno e le loro abilità informatiche.

>Fattori esterni: potenziali concorrenti, normative applicabili, clima politico e sociale nelle zone in cui opera l’organizzazione e posizione del mercato.

>Esigenze degli stakeholder [ISO 31000]: tutte le persone o organizzazione che possono essere impattate o si sentono impattate dalle decisioni o attività dell’azienda; possono essere interni o esterni.

È necessario stabilire:

* il **campo di applicazione** o ambito in cui effettuare la valutazione del rischio: definisce i confini del dominio entro il quale si ha intenzione di applicare il risk management.   
  ES: confini di un appartamento.
* i **criteri per la gestione dei rischi**: valori di riferimento rispetto ai quali il rischio è ponderato. ([ISO 27000])

Criteri:

* + **di valutazione delle conseguenze**: definiscono qualitativamente le conseguenze dell’evento verificabile
  + **di valutazione delle probabilità**: definiscono qualitativamente la probabilità dell’evento
  + **di valutazione dei rischi**: si appoggia all’utilizzo della Matrice dei Rischi, che viene creata utilizzando le scale definite in precedenza: per un criterio di valutazione qualitativo si assegnano dei punteggi ad ogni livello.
  + **per accettazione dei rischi**: si definiscono gli intervalli entro i quali a)accettare i rischi, b)ridurli o c)ridurli immediatamente.

Si definisce la risk capability che coincide con la quantità massima di danno che l’organizzazione può subire senza intaccare i suoi obiettivi,

1. **Risk Assessment:** processo complessivo di identificazione, analisi e ponderazione del rischio. [ISO 27000].

Insieme di attività volte a identificare i rischi, calcolarne il livello e decidere se sono accettabili.

Un **metodo i valutazione del rischio** valido deve avere:

* Completezza: considerati tutti gli asset, tutte le minacce e tutte le vulnerabilità.
* Ripetibilità: valutazioni condotte nello stesso contesto devono dare gli stessi risultati.
* Comparabilità: valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere il cambiamento e le modalità di cambiamento del rischio.
* Coerenza.

**Risk Owner:**  persona o entità con la responsabilità e il potere di gestire un rischio.

Richiesto dalla ISO 27000/1 durante la valutazione dei rischi.

* Potere di spesa
* Spesso coincide con la Direzione
* Responsabile ultimo del rischio: decide quali controlli di sicurezza attuare e mantenere.

Tre fasi del Risk Assesment: identificazione, analisi e valutazione del rischio.

* 1. **Identificazione del rischio**: processo di individuazione, riconoscimento e descrizione del rischio

Si individuano e descrivono gli asset, le minacce, le vulnerabilità e i Risk owner.

Si può utilizzare il diagramma di Bow-Tie.

Asset [ISO 27000]: qualsiasi cosa abbia valore per l’organizzazione e possono essere di diverso tipo.

* Informazioni (primi asset da identificare): per identificarle si parte dai processi dell’organizzazione (es: info clienti, fornitori…) e si coinvolgono i responsabili delle aree dell’organizzazione (**referenti per le informazioni**) che devono identificare le informazioni create ed utilizzate dalla propria area.
* Server, applicazioni, pc fissi e non, rete informatica, personale interno ed esterno, fornitori, documenti e archivi cartacei, sede, organizzazione nel suo complesso.

**Minacce** [ISO 27000]: causa potenziale di un incidente che può comportare danni a un sistema o all’organizzazione.

L’indentificazione delle minacce può essere svolta su diversi livelli di dettaglio: prima un’analisi poco dettagliata e poi viene migliorata successivamente con riesami periodici.

L’analisi del rischio relativo alla sicurezza delle informazioni richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni. Prima si individuano gli **agenti di minaccia** (entità responsabile del manifestarsi della minaccia, es: malintenzionati, natura, strumenti tecnici...) e poi si individuano le **tecniche di minaccia.**

Viene elaborata una lista delle vulnerabilità o dei controlli di sicurezza per rendere sistematica l’identificazione e la valutazione.

**>Vulnerabilità** [ISO 27002]: debolezza di un asset o di un controllo di sicurezza che può essere sfruttata dalle minacce.

**>Controlli di sicurezza** [ISO 27000]: misura attua alla modifica del rischio, contrasta la minaccia. Possono essere di prevenzione, recupero o rilevazione.

Risultato:

* Descrizione degli asset;
* Elenco delle categorie degli asset;
* Elenco di minacce con parametri RD pertinenti;
* Elenco di controlli di sicurezza o di vulnerabilità;
* Tabella di relazione Categorie di Asset 🡪Minacce;
* Tabella di relazione Categorie di Asset 🡪 Controlli di sicurezza/Vulnerabilità;
* Tabella di relazione Minacce 🡪 Controlli di sicurezza/Vulnerabilità;
  1. **Analisi del rischio** [ISO 27000]: processo di comprensione della natura del rischio e di determinazione del livello di rischio.

Attività di stima del rischio senza alcun tipo di giudizio.

Per determinare il livello di rischio bisogna **assegnare valori agli asset** (termini di RID), **alle minacce e alle vulnerabilità** (assegnazione/evaluation), i valori devono essere oggettivi e ripetibili (giustificare i valori con fonti consultate).

Si stima la probabilità dei **rischi** parziali, cioè la probabilità con la quale una minaccia può esplorare/sfruttare una vulnerabilità e creare un evento sfavorevole provocando un incidente con impatto negativo sulla soddisfazione degli obiettivi. Una vulnerabilità🡪1/+ minacce.

**Rischio intrinseco (puro)**: combinazione tra il valore degli asset e la probabilità dell’accadimento di una minaccia (senza considerare vulnerabilità o controlli). Si effettuano controlli ideali sulla base del rischio intrinseco di ogni asset e si valuta il suo discostamento dal valore dei controlli di sicurezza ideali in modo da attribuire un valore rispetto all’adeguatezza e conformità.

Controllo non progettato come quello ideale 🡪Controllo **non adeguato**.

Controllo di sicurezza adeguato ma non attuato 🡪Controllo **non conforme**.

1. **Valutazione del rischio** [ISO 27000]:processo di comparazione dei risultati dell’analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
2. **Trattamento del rischio** [ISO 27000]: processo per modificare il rischio.

Processo ciclico con le seguenti fasi:

* 1. Selezione delle opzioni per il trattamento dei rischi;
  2. Identificazione delle misure esistenti;
  3. Identificazione delle misure da implementare se si è deciso di mitigare/eliminare il rischio;
  4. Calcolo dei rischi residui: +riduzione rischi = +misure da adottare = +costo.  
     Rischio residuo accettabile: soglia minima al di sopra del quale il rischio dev’essere ridotto. Se Rischio Residuo > Rischio Residuo Accettabile (RR>RRA) 🡺servono altre misure.
  5. Preparazione del **Piano Trattamento dei Rischi**

Per trattare il rischio si sceglie una delle seguenti opzioni:

->Evitare/eliminare il rischio (non iniziare o interrompere l’attività)

->Aumentare il rischio (iniziare l’attività ignorando il rischio).

->Modificare la probabilità della minaccia (aggiunge/migliora i controlli per ridurre vulnerabilità).

->Modificare le conseguenze (aggiungi controlli per ridurre i danni).

->Condividere il rischio (trasferirlo a terze parti)

->Mantenere il rischio (non fare nulla)

**What-if analysis**: determinazione dei valori previsti per asset, minacce e vulnerabilità per ottenere il livello di rischio presunto in caso si concluda l’azione.

Azioni incoerenti: introducono disomogeneità inutili.

Bisogna calcolare anche la fattibilità economica e rischi introdotti dai nuovi controlli.

Una volta scelte le azioni vanno pianificate riportando: il responsabile dell’azione, la data di chiusura prevista dell’azione, le risorse necessarie e le modalità di verifica dell’efficacia.

1. **Monitoraggio e riesame**: bisogna effettuare altri controlli perché possono esserci cambiamenti nel tempo e bisogna mantenere aperti i canali di comunicazione con le parti interessate per favorire segnalazioni tempestive.
2. **Comunicazione e consultazione.**

Otto principi del risk Management

Principi identificati dalla norma ISO 31000 per guidare l’organizzazione verso il miglioramento delle prestazioni e l’efficacia e efficienza del risk management.

1. **Dinamicità**: i rischi possono emergere, cambiare o scomparire, la gestione del rischio deve riconoscere e rispondere a tali cambiamenti in modo tempestivo.
2. **Inclusività**: coinvolgimento delle parti interessate per prendere in considerazione le loro conoscenze, opinioni e percezioni 🡪 maggiore consapevolezza e gestione del rischio.
3. **Personalizzazione**: Risk management personalizzato per allinearlo alla realtà del contesto.
4. **Migliori informazioni disponibili**: le informazioni devono essere tempestive, chiari e disponibili perché su di esse si basano gli input per la gestione del rischio.
5. **Fattori umani e culturali** che influenzano la gestione del rischio.
6. **Migliorativo**: emergono sempre nuovi rischi.
7. **Integrativo**: Il RM è un’attività integrata con processi e struttura di governo dell’organizzazione.
8. **Approccio strutturato e completo** alla gestione del rischio che contribuisce a risultati coerenti e comparabili.

Rischi strategici: rischi legati agli aspetti strategici dell’azienda come vision (ambizione futura), mission (modo in cui opera per raggiungere gli obiettivi) e obiettivi aziendali.

Sono di alto livello quindi comprensibili anche al pubblico degli stakeholder.

**Rischi operazionali**: legati a processi e procedure.

* **Processi**: set di attività correlate o interagenti tra loro che usa l’input per consegnare il risultato inteso (output, prodotto o servizio). Più processi insieme possono essere considerati un unico processo. L’output di un processo può essere l’input di un altro.
* **Procedure**: modo corretto di svolgere un’attività o procedura. Singoli step da seguire. Può essere documentato o no.

**Rischi relativi al progetto**: relativi a progetti di ogni tipo inclusi i progetti per realizzazione ed integrazione softwares.

* **Progetto**: rischio temporaneo per raggiungere uno o più obiettivi definiti.
  + Hanno un obiettivo specifico da raggiungere.
  + Limitati nel tempo con data di inizio e di fine.
  + Utilizzano risorse.
  + Hanno un budget e limiti di spesa.

**Rischi di prodotto:** Sono legati alla progettazione, produzione, commercializzazione e manutenzione di prodotti materiali o immateriali.

* **Risk management di prodotto**: per gestire il rischio di prodotto, già dalla fase di design bisogna focalizzarsi su difetti del processo di produzione e del prodotto raccogliendo feedback dai vari stakeholder.

**Classificazione dei rischi**: non c’è una tassonomia fissa, possiamo avere ad esempio:

* **R. di credito:**
* **R. di mercato:**
* **R. relativo a risorse umane:**
* **R. legale:**
* **R. ambientale:**
* **R. sociali:**
* **R. di compliance:**
* **R. di salute e sicurezza sul lavoro:**

**ISO 31000**

ISO 31000:2018: “Risk management – guideline standardizzata, nomenclatura e approccio”.

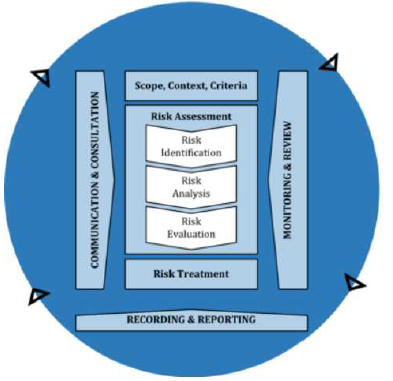
**Risk management:** aumenta la possibilità dell’organizzazione di affrontare i rischi in modo migliore, aumentando la possibilità di successo e la razionalità delle decisioni.

**Risk management process**: aiuta l’organizzazione ad attuare il risk management.

ISO 31000:2018:

* Per uso delle persone che creano e proteggono il valore nelle aziende gestendo il rischio, prendendo decisioni, fissando e soddisfacendo obiettivi e migliorando le performance
* Organizzazioni di tutti i tipi e dimensioni affrontano fattori ed influenze interne ed esterne che rendono incerto il raggiungimento degli obiettivi.
* Affrontare il rischio è iterativo e assistere le organizzazioni in: strategie, obiettivi e decisioni.
* Gestire il rischio è parte di governance e leadership (contribuisce al miglioramento dei sistemi di gestione) e fa parte di tutte le attività associate con un’organizzazione.
* Gestire il rischio considera sia il contesto interno che quello esterno all’organizzazione.

Organizzarsi per il successo 🡪 comprendere il contesto 🡪valutazione rischi 🡪trattamento rischi.



I triangoli indicano che è un ciclo in continuo sviluppo

6.2: **comunication and consultation**: consultazione con gli stakeholders per allinearli ed ottenere un feedback. Continua in tutto il processo. Cruciale per il successo e garantisce il commitment.

* **Stakeholder**: tutte le persone o organizzazioni che possono impattare, essere impattate o sentirsi impattate su/da una decisione o attività dell’azienda.

6.6: **Monitoring and review**: monitoraggio continuo e review periodiche per assicurare la qualità del processo di risk management e discutere i possibili miglioramenti. Molto importante e va svolto in ogni fase del processo.

6.7: **Recording and reporting**: documentazione del processo e archiviazione tenendo a mente la privacy degli stakeholder. Serve per comunicare, fornire informazioni a supporto delle decisioni, migliorare il risk management e interagire con gli stakeholder.

6.3: **Scope, context and criteria:**

.2: **Scope**: ambito dell’applicazione, il compito dell’azienda. Dev’essere chiaro l’ambito su cui si fa l’analisi del rischio.

.3: **Contesto interno ed esterno**: il contesto interno riguarda l’azienda (obiettivo, lavoratori…), quello esterno riguarda sindacati, contesto politico, guerre, scioperi…

.4:  **Risk criteria**: criteri e misure oggettive e ripetibili nel tempo anche da persone diverse per dare istruzioni alle fasi di assesment e treatment. Definisce quando un rischio è da considerare alto o basso. Va adattato nel tempo.

6.4: **Risk assessment**:

.2: **Risk identification**: serve per trovare, comprendere e descrivere i rischi. Servono informazioni rilevanti e aggiornate e richiede di analizzare molte informazioni come:

* + Sorgenti di rischio tangibili/intangibili
  + Cause ed eventi
  + Minacce ed opportunità
  + Vulnerabilità e capacità
  + Cambiamenti di contesto interno-esterno

.3: **Risk analysis:** analisi per comprendere la natura, le caratteristiche ed il livello del rischio. Considera gli eventi di rischio, le risk source, le conseguenze, le probabilità (likelihood), i controlli e le reazioni tra eventi.

**Events**: cambiamento o accadimento di un particolare insieme di circostanze.

Ha diverse cause e conseguenze e può essere aspettato o inaspettato.

Un evento può essere ricorrente nel tempo e una sorgente di rischio.

**Consequence**: outcome di un evento che ha effetto sugli obiettivi.

Può essere: certo/incerto, positivo/negativo e diretto/indiretto.

Le conseguenze possono essere espresse in termine quantitativo o qualitativo e possono avere effetti cumulativi a cascata.

A volte sono difficili da quantificare come nel caso di morti o inquinamento.

**Criteri per gestione del rischio:**

**🡪Classificazione dei rischi:** la gravità in termini economici dipende dalla grandezza dell’azienda.

1)Molto basso (insignificante): nessun danno a persone e produzione. Basso impatto economico.

2) Basso: primo soccorso e alcune attività bloccate ma basso danno alla produzione e impatto economico.

3)Medio (moderato): richiesto intervento medico e danni moderati.

4)Alto (elevato): danni estesi a persone, processi bloccati, danni alla produzione elevati e massimo impatto economico.

5)Molto alto (catastrofico): morti e danni a livello sistemistico/infrastrutturale.

**🡪Likelihood**: possibilità che qualcosa accada

🡪**Probabilità**: probabilità con la quale si manifesta un evento sfavorevole.

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

**Livello di rischio**: Rischio = funzione di probabilità (P) e impatto (D) = f(P\*D).

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

**.4 Risk Evaluation:** La valutazione del rischio .

Input = informazioni prodotte da analisi e i criteri di accettabilità 🡪 decidere se/come procedere con il trattamento del rischio.

* + Rischio basso: non faccio nulla o ricalcolo se non sono sicuro.
  + Rischio alto: considero opzioni di trattamento rischi
  + Rischio altissimo: riconsidero gli obiettivi e cambio attività.

6.5: **Risk treatment**:

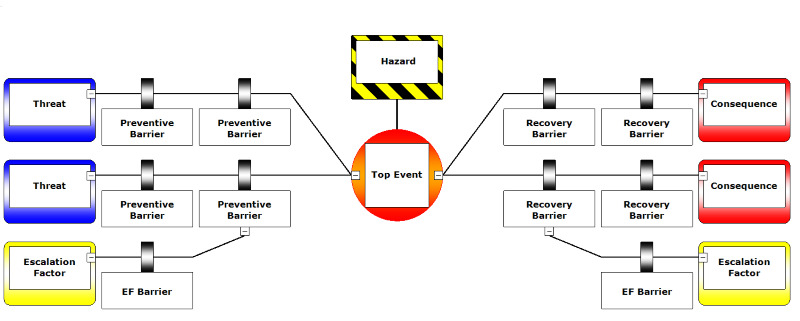
.2: **Select of treatment options**: analizzo i modi in cui posso trattare il rischio: evitare, rinunciare/rimuovere, trasferire ad altri, condividere (assicurazioni), accettare…

.3 Preparing and implementing risk treatment plans: i piani di trattamento specificano come saranno implementate le opzioni scelte (secondo quanto scelto nel punto precedente). I piani devono essere integrati nei piani di gestione dell’azienda e devo specificare le motivazioni delle scelte.

**Controllo**: misura che mantiene e/o modifica un rischio. Include processi, policies, dispositivi… e azioni/condizioni per mantenere o modificare il rischio.

Possono essere organizzativi o tecnologici e possono risentire di errori umani.

**Bow-tie analysis**



ISO 31010 definisce linee guida delle tecniche.

**Bow-tie analysis**: tecnica di analisi del rischio /analisi dei controlli.

Modo schematico per descriver e percorsi dalla fonde del rischi ai risultati per rivedere i controlli.

Particolarmente efficace per interpretazione e gestione dei rischi nell0ambito delle realtà organizzative complesse, grazie al carattere intuitivo e fortemente comunicativo della relativa notazione grafica che risulta potentemente parlata sia agli addetti ai lavori che agli stakeholders.

Non necessita di grande sforzo o competenze tecniche.

Elementi tipici:

**Punto di partenza** (alto) = pericolo = attività, operazione o circostanza con l'intrinseca potenzialità di fare danno -->dev'essere identificato, analizzato e gestito.

**Top Event** (centrale): evento principale che fa perdere il controllo.

**Minacce** (sx): fattori che possono generare la perdita di controllo (top event), ogni causa deve poter generare autonomamente il top event.

**Conseguenze** (dx): eventi che si possono generare a causa del top event. Carattere ecnomico, vite umane, sociale, ambientale... Tenere conto di impatti diretti e indiretti (immagine, reputazione).

Definizione e focalizzazione sui controlli (barriere).

**Barriera** = misura di controllo o livello di protezione di natura tecnica o organizzativo-gestionale che può prevenire lo sviluppo di una causa in un quasi indiciente o prevenire per impedire l'accadimento della conseguenza. Mai efficaci al 100%.

Barriere preventive (sx): operano prima.

Barriere mitigative (dx) operano dopo.

È possibile associare il Bow-tie con gli strati di protezione come LOPA che valuta le barriere per determinare l’affidabilità e capacità di ridurre il rischio, permette anche di calcolare il rischio residuo.

Input: frequenza della cause. Probabilità di fallimento su barriere PFD.

Output: frequenze top event e conseguenze.

Framework di ISO 31000:2018

**Leadership and commitment:** Il top manager gestisce il rischio e dimostra il “commitment” (impegno):

* Personalizzando e implementando i componenti framework
* Stabiliendo l’approccio, i piani e le azioni al rischio
* Assicurando la presenza delle risorse necessarie
* Assegnando authority, responsabilità e accountability ai livelli appropriati.

Gli organi di controllo supervisionano:

* Assicurandosi che i rischi vengano considerati adeguatamente
* Comprendendo le difficoltà nel raggiungerli
* Immagine che contiene testo, cerchio, logo, Carattere

  Descrizione generata automaticamenteAssicurandosi che i sistemi di gestione dei rischi siano implementati e funzionanti, che i rischi siano appropriati e che le informazioni siano comunicate.

**Integration**: Il risk management deve essere integrato in ogni fase dell’organizzazione.

**Improvement**: miglioramento continuo adattandosi per migliorare

**Implementation**: durante l’implementazione bisogna sviluppare un piano per gestire tempi e risorse, identificare il processo decisionale e assicurarsi la chiarezza delle disposizioni prese.

**Evaluation**: valutare l’efficacia della nostra gestione di frequente con misurazioni.

**Design**: fin dalla progettazione del framework bisogna pensare al rischio tramite policies, definizione dei **risk owner** (persona o entità con autorità e accountability per gestire un rischio), assegnazione di risorse e meccanismi di comunicazione

Principi di ISO 31000:2018

Immagine che contiene testo, compact disk, cerchio, Carattere

Descrizione generata automaticamente

Risk management in **continuo miglioramento**

Il risk management è influenzato da **fattori umani e culturali**

Input per gestire il rischio basati sulle **migliori info disponibili al momento**

Rischi **dinamici:** possono cambiare, emergere o scomparire in base al contesto esterno

**Include gli stakeholders** coinvolgendoli in modo appropriato e tempestivo

Framework e processi **personalizzati**

**Approccio** alla gestione del rischio **strutturato** e **comprensivo**

Rischio **integrato** in ogni parte del processo di gestione del rischio

**Information security**: “preservazione di confidenzialità, integrità e disponibilità delle informazioni”. vocabolario ISO 27.000

**Dati**: insieme di singoli fatti, immagini e impressioni.

**Informazioni**: dati organizzati e significativi.

**Conoscenza**: informazioni recepite e comprese da un singolo individuo.

**Sapienza**: conoscenze tra loro connesse che permettono di prendere decisioni.

Le informazioni sono trasmesse (mail, posta, telefono...) e archiviate su dei supporti digitali o analogici, anche l’essere umano è un supporto analogico.

Quali sono le proprietà della information security?

Integrità, riservatezza e confidenzialità, ma anche autenticità, accountability (responsabilità e

possibilità di attribuire la responsabilità di un evento a un’entità), non-repudio e affidabilità.

**Sistema di gestione** (management system) : modo in cui l'azienda si organizza per raggiungere gli obbiettivi. Insieme di elementi interagenti necessari per stabilire policies, obiettivi ed i processi per raggiungerli.

I sistemi servono per tutelare gli interessi privati dell’azienda, a differenza delle norme che tutelano il bene collettivo. Anche la gestione ambientale viene vista come modo per farsi pubblicità.

Secondo le norme ISO: “Sistema di gestione” comprende tutti i sistemi di gestione implementati nelle organizzazioni nei settori in cui operano.

* **ISO 9001**: sistemi di gestione della qualità.
* ISO 14001: sistemi di gestione ambientale.
* ISO 50000: sistemi di gestione dell'energia.
* ISO 45001: sistemi di gestione della sicurezza e della salute nei luoghi di lavoro.
* SA 8000: impatto sull'etica e sul sociale (emessa dal SAI).
* **ISO 27001**: sistemi di gestione della sicurezza delle informazioni.
* ISO 19600: sistemi di gestione della conformità (legislativa).

**Cosa ci dicono i sistemi di gestione?**

Per una certa disciplina (es: qualità, ambiente…), oppure per più ambiti, suggeriscono, dando linee guida generali (non dettagliate), cosa fare

* in termini organizzativi
* di ruoli
* di responsabilità
* in merito alla pianificazione
* riguardo alle operazioni

Un sistema può essere certificato, ma non sei obbligato a certificarti.

Es: Gallotti aiuta ad implementare i sistemi, ma potrei anche farlo ai miei clienti senza bisogno di certificarmi. Se lo faccio però tanto vale certificarlo già che ci sono.

**ISO 27001:** standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI).

È una norma breve, quindi ad alto livello parla del contesto dell'organizzazione e di come gestirlo e "personalizzarlo" in base alla situazione, ad esempio l’identity management viene liquidato in una riga, poi nel 27002 ogni controllo verrà approfondito in almeno una pagina.

Il sistema di gestione richiede il commitment direzionale 🡪commitment = “tutti quei comportamenti di impegno, motivazione, senso del dovere, di appartenenza e di responsabilità degli individui nei confronti della propria azienda, quindi un'identificazione forte con l'organizzazione e i suoi obiettivi”.

Ha molte similiarità con la 31.000 sulla struttura e alcuni argomenti trattati.

Annex A: lista di controlli che vengono usati dall'auditor quando viene richiesta la certificazione da parte di un'azienda. sono un bel po' di pagine di controlli da fare.

In America al posto della ISO 27000 si usano le norme NIST (National Institute of Standards and Technology), quelle norme invece sono reperibili gratuitamente perché il NIST è un’agenzia del governo degli USA, quindi è a servizio dei cittadini.