**Che cos’è il rischio?**

Nell’**ISO 27000** viene definito come “**l’effetto dell’incertezza sugli obiettivi**”, dove l’incertezza (mancanza di conoscenza assoluta) è dovuta ad eventi positivi o negativi e con “effetto” si intende la variazione dagli obiettivi.

Il rischio è associato alle potenziali minacce che sfruttano le vulnerabilità dell’asset.

Gli obiettivi dell’analisi possono riguardare diversi ambiti (economico, sicurezza o salute), essere su diversi livelli (strategico, operativo e tattico), possono essere espressi in modo implicito o esplicito.

Con **Fiorito** abbiamo studiato la formula come **R=P\*I** dicendo che “Come risultato di una causa, un inaspettato evento può avvenire, il quale produce certi effetti sugli obiettivi.” e **Gallotti** distingue impatto (breve termine) e conseguenza (medio/lungo termine).

**Ioannis** invece preferisce **R=f(P,D)** dove questa volta l’impatto è D e introduce la figura del **proprietario di un obiettivo**, cioè una figura che ha le responsabilità del raggiungimento di esso e del controllo della situazione, attribuisce valore, decide la strada per raggiungerlo e studia le **fonti di pericolo** (agenti) e le **misure** per ridurlo.

Il calcolo del livello di rischio comprende tre elementi: minaccia, asset e vulnerabilità

**Classificazione dei rischi – (31.000)**

Tra i possibili rischi di cui un’azienda deve tenere conto troviamo:

**Rischio di credito** (o **rischio di insolvenza**): il rischio che, nell'ambito di un'operazione creditizia, il debitore non assolva anche solo in parte ai suoi obblighi di rimborso del capitale e/o al pagamento degli interessi al suo creditore.

Comprende il **rischio di inadempimento** se il cliente non paga una fattura e il **rischio paese** se riguarda la situazione economico-politica di altri paesi. I crediti non pagati si chiamano “**crediti insoluti**”.

**Gestione del rischio**: gestione preventiva analizzando **l’affidabilità creditizia** dei potenziali clienti, valutando la **potenziale perdita** e creando un **piano di intervento** come lo stabilimento di una soglia massima di credito.

**Rischio di mercato:** rischio che il valore di un investimento diminuisca a causa dei cambiamenti nelle variabili del mercato che comprendono i tassi di interesse, variazione nei tassi di copertura, fluttuazione nei prezzi delle materie prime e movimenti nei mercati azionari.

Comprende il **rischio di tasso di interesse** e il **rischio di cambio** e vengono misurati con strumenti come la varianza e la deviazione standard.

**Gestione del rischio**: gestione preventiva attraverso **diversificazione del portafoglio,** cioè, distribuire gli investimenti in diversi asset per ridurre gli impatti negativi, la **copertura** (hedging) che consiste nell’utilizzare strumenti finanziari per proteggersi da eventi esterni e l’**asset allocation dinamica** per regolare la composizione di un portafoglio in base alle condizioni di mercato.

**Rischio relativo a risorse umane**: rischio che fattori legati al personale di un’organizzazione possano influire negativamente sulla capacità di operare efficacemente e raggiungere gli obiettivi strategici.

Questo rischio non contenuto può influire sia l’**economia** che la **reputazione** di un’azienda.

**Gestione del rischio**: assunzione di un **Human Resource Manager** specializzato nella gestione della forza lavoro.

**Rischio legale**: rischio di subire perdita economica o di non ottenere un vantaggio a causa di una inadeguata gestione di aspetti legali che possono coinvolgere la propria attività o l’azienda.

Gestire questo rischio assicura un **risparmio** in termini di **spesa e di tempo** e una migliore efficienza dell’organico e delle risorse investite.

**Gestione del rischio**: tramite controllo ed implementazione dei documenti contrattuali, formando i dipendenti per rendere effettiva l’applicazione dei codici e delle scritture interne e **controllando i comportamenti di dipendenti e responsabili**.

**Rischio ambientale**: rischio di produrre, gestire o distribuire beni, servizi o prodotti di processi industriali che, in caso di incidente, possono avere effetti sulla popolazione, sugli animali e sul territorio.

Si parla di **emergenza ambientale** quando un evento mette a repentaglio le matrici ambientali (acqua, aria e suolo) e richiede misure straordinarie urgenti per gestire le conseguenze minimizzando i danni e favorendo il ripristino delle condizioni normali dell’ambiente.

**Gestione del rischio**: evitare sprechi, utilizzare fonti di energia rinnovabili e svolgendo un adeguato smaltimento dei rifiuti.

**Rischio sociale**: rischio che eventi, azioni o condizioni legate a dinamiche sociali, culturali o comunitarie possano influenzare negativamente un’organizzazione, progetto o operazione.

Tra le possibili conseguenze troviamo: conflitti con la comunità, impatto negativo sulla reputazione e disuguaglianza sociale.

**Gestione del rischio**: coinvolgimento degli **stakeholder** tramite un dialogo trasparente e collaborativo che risponde alle loro preoccupazioni, sviluppando politiche e programmi che dimostrano l’**impiego dell’azienda verso pratiche socialmente responsabili** e svolgendo l’**analisi di impatto sociale**.

**Rischio di compliance** (o non conformità): rischio di non essere in linea con regolamenti, leggi e norme che garantiscono che l’azienda operi in modo etico, proteggendo la sicurezza dei clienti e rispettando i diritti dei lavoratori.

La non conformità può derivare da fattori come la **mancanza di conoscenza** delle norme e delle regolamentazioni e le conseguenze possono essere gravi come multe, sanzioni, perdita di reputazione e danni all’immagine dell’azienda che può scoraggiare i partener commerciali.

**Gestione del rischio**: gestione tramite **formazione e sensibilizzazione** dei dipendenti su norme e regolamenti, **controlli interni, audit e monitoraggio**.

**Rischio di salute e sicurezza sul lavoro**: rischio che si verifichino eventi indesiderati o imprevisti che possono avere conseguenze negative o dannose sulla salute dei lavoratori.

Il lavoratore è sia destinatario di tutele che responsabile in quanto veste un ruolo attivo partecipando direttamente o tramite rappresentanti alla realizzazione del sistema di sicurezza.

**Gestione del rischio**: svolta seguento il **Documenti di Valutazione Rischi** che garantisce la sicurezza sul lavoro identificando i rischi e individuando le misure di sicurezza da adottare per prevenire **infortuni sul lavoro** e **malattie professionali**.

**L’analisi dei rischi**

**Analisi dei rischi**: attività attraverso la quale, sulla base di una situazione, si valutano le probabilità degli eventi e le conseguenze sugli obiettivi. Si organizzano tutte le potenziali vulnerabilità e minacce di tipo fisico-ambientale, organizzativo e logico.

Secondo Gallotti abbiamo due metodi di analisi: i **metodi quantitativi** valutano il potenziale danno economico dovuto a perdita di RID mentre quelli **quantitativi** usano scale come basso/medio/alto.

Nei metodi quantitativi la raccolta dei dati è onerosa e non sono sempre affidabili.

La probabilità delle minacce, ad esempio, da una parte può essere una % mentre dall’altra un valore di una scala.

Entrambi sono soggettivi, ma i primi permettono più operazioni, di solito con i quantitativi si usa max().

Nei casi di studio, “Passaggio a livello” è l’unico caso di analisi qualitativa, mentre gli altri sono di analisi quantitava, che si dividono in un approccio event-based se calcolano il rischio come “probabilità dell’evento per le conseguenze” come nel caso “Persone chiave” e “Mensa” o asset-based se calcolano il rischio come effetto di P(m), P(v) e I(a) come nei casi del “Tesoretto” e .

**Rischio parziale:** una stessa vulnerabilità può essere usata da più minacce creando ulteriori incidenti.

**Rischi aggregati**: combinazione di rischi parziali tramite media pesata o tramite media aritmetica 🡪dà idea della situazione dell’azienda.

Abbiamo due punti decisionali in cui è utile riunire l’azienda:

1**)Prima del trattamento dei rischi** bisogna fare un riesame dei risultati del Risk assessment, in caso di scostamenti dai risultati attesi si fa il confronto con ciò che è stato stabilito durante l’analisi del contesto 🡪tutti i rischi sono identificati?

2)Il proprietario dei rischi rivede ed approva le misure proposte e i conseguenti **Rischi residui** registrando le condizioni associate all’approvazione.

Si ha un **rischio residuo** quando gli amministratori introducono misure inadeguate ma che gestiscono comunque parte del rischio; quindi, si calcola quanto rischio rimane scoperto.

Se il rischio residuo è > del rischio residuo accettabile allora bisogna introdurre altre misure per ridurre i rischi, il rischio residuo accettabile può variare (ad esempio in base agli stakeholder) ed in questo caso bisogna riesaminare il rischio residuo.

**Intervento esterno a piacere - CISO**

L’intervento è stato tenuto dall’ingegnere Lorenzo Mori, CISO di GVM Care&Research.

**GVM Care & Research** è uno dei principali gruppi ospedalieri italiani con strutture sanitarie d'eccellenza presenti in Italia e all'estero come Francia, Polonia e Ucraina e fornisce alta specializzazione in particolare in ambito cardiovascolare.

GVM fornisce un ecosistema eterogeneo per la salute ed il benessere che comprende sanificazione ospedaliera, parafarmacie, telemedicina e molto altro.

GVM è una società molto complessa perché comprende tante realtà diverse e tante tecnologie ma favorisce interoperabilità, integrazione e alta affidabilità.

L’ospedale in particolare è un sistema complesso che si basa su: interconnessione, eterogeneità dei sistemi e necessità di privacy e riservatezza, inoltre è un’infrastruttura critica perché riguarda il mantenimento delle funzioni cruciali della società e dell'economia e su alcuni dispositivi non è possibile installare alcun antivirus.

**Sicurezza e sanità secondo CLUSIT**.

Il settore sanitario è uno dei più colpiti da cybercrime e le minacce informatiche sono in aumento e diventano più sofisticate, viene scelto perché tratta informazioni sensibili con un alto valore sul mercato nero e che hanno una lunga durata (a differenza delle carte di credito).

Le vulnerabilità del settore sono: dispositivi medicali difficili da aggiornare e connessi fra loro e la mancanza di risorse da investire per la sicurezza informatica.

Il **CISO** (Chief Information Security Officer) è il responsabile della protezione dei dati e dei sistemi informatici di un’azienda dalle minacce informatiche. Si occupa di:

* Sviluppo e implementazione di una strategia di sicurezza informatica
* Gestione del rischio informatico: sviluppa piano di risposta e disaster recovery
* Definizione di politiche e procedure di sicurezza
* Monitoraggio e risposta agli incidenti di sicurezza
* Promozione della consapevolezza della sicurezza informatica
* Assicura la conformità alle normative.
* Gestisce il budget per la sicurezza informatica.

Il CISO non lavora isolato ma collabora con diverse figure come:

* **Consiglio di amministrazione (CdA)** che aggiorna su stato della sicurezza informatica e i rischi.
* **Direttore dei Sistemi informatici (CIO)** per integrare e garantire la sicurezza.
* **Direttore tecnico (CTO)** per implementare le soluzioni di sicurezza.
* **Area legale e di compliance** per garantire la conformità alle normative sulla privacy e per implementare politiche e procedure di sicurezza.
* **Risorse umane** per formare e sensibilizzare i dipendenti sulla sicurezza informatica.
* **Marketing** per garantire la sicurezza delle campagne online e la privacy dei clienti.

Il CISO deve affrontare diverse sfide come tenersi al passo con l’evoluzione delle minacce, garantire conformità alle normative, promuovere consapevolezza, proteggere ambienti IT complessi e gestire la carenza di personale qualificati, i rischi legati a terzi ed il budget per la sicurezza.

**Quale libro ti è piaciuto di più? Ioannis 🡪ISO 31.000**

Per affrontare il rischio il normatore **ISO** (Internation Organization for Standardization) ha emesso delle norme come la **ISO 31000:2018** “Risk management – Guidelines” applicabile ad ogni organizzazione o entità che gestisce i rischi.

La norma ISO 31000 è una **linea guida**, fornisce indicazioni senza approfondimenti e non può essere usata per audit o certificazioni.

L’**ISO 31000** definisce i principi e le linee guida del **Risk management**, cioè l’insieme di attività che servono per indirizzare e controllare l’organizzazione rispetto al rischio, l’obiettivo è evitare che l’incertezza impedisca il raggiungimento degli obiettivi.

Il **risk management process** consiste nell’applicazione sistematica di policies, procedure e pratiche che l’azienda si dà.

I rischi, a seconda dell’impatto, possono essere classificati in:

* **Strategici** se legati agli aspetti strategici dell’azienda come mission, vision e obiettivi (es: margine, fatturato…),
* **Operazionali** se legati a **processi** (set di attività legate fra loro che usano un input per arrivare all’output) o a **procedure** (ordine di passaggi per mandare avanti un’attività o processo).
* **Relativi a progetti**: relativi a progetti di ogni tipo, richiedono la conoscenza specifica del progetto e alcune caratteristiche comuni. I progetti sono temporanei, hanno obiettivi specifici, usano risorse limitate ed un budget. Sono gestiti da un project manager.
* **Di prodotto**: legati alla progettazione, produzione, commercializzazione e manutenzione di prodotti materiali o immateriali. Il prodotto è il risultato di un progetto.

**Processo del risk management**: 5 fasi cicliche.

**1)Scope, context and criteria.**

Contesto di un’organizzazione: combinazione di fattori interni come la struttura organizzativa, il sistema informativo, conoscenze, competenze, obiettivi ed il personale e fattori esterni come concorrenti, normative, stakeholder e il clima politico e sociale.

Bisogna considerare le esigenze dell’ambito/scope (dominio in cui applicare il risk management, cioè il compito dell’azienda) e i criteri.

Tra i criteri abbiamo quelli di valutazione delle conseguenze, delle probabilità, dei rischi (con matrice) e i criteri per accettazione dei rischi.

**2)Risk assessment**: processo di identificazione, analisi e ponderazione del rischio (ISO 27000).

Si valuta un rischio attraverso un metodo completo, ripetibile, comparabile e coerente.

Può essere analitico se usa la somma (minaccia + vulnerabilità) o empirico se usi delle matrici.

Il risk assessment si divide in:

I)**Identificazione** del rischio: consiste nell’individuare le **minacce** (cause di un potenziale incidente), le **vulnerabilità** (debolezza di un asset o di un controllo), il **risk owner** (persona con responsabilità e potere di gestire il rischio) e gli **asset** (ciò che ha valore per l’organizzazione).

Si effettuano anche dei controlli di sicurezza.

II)**Analisi** del rischio: comprensione della natura del rischio e di assegnazione del livello di rischio che deve essere oggettivo e ripetibile. Si stimano i rischi parziali e quelli puri.

III)**Valutazione** del rischio: processo di comparazione dei risultati dell’analisi rispetto ai criteri di rischio per determinare se il rischio è accettabile.

**3)Risk treatment**: processo ciclico per modificare il rischio basato sulla selezione delle opzioni, identificazione delle misure già esistenti e da implementare, calcolo del rischio residuo e paragone con il rischio accettabile ed infine preparazione del Piano di Trattamento dei Rischi.

Per trattare il rischio si può: evitarlo, rimuovere la sorgente, accettarlo/aumentarlo, modificare le probabilità o le conseguenze o condividerlo.

Si determinano i valori previsti tramite **what-if analysis**.

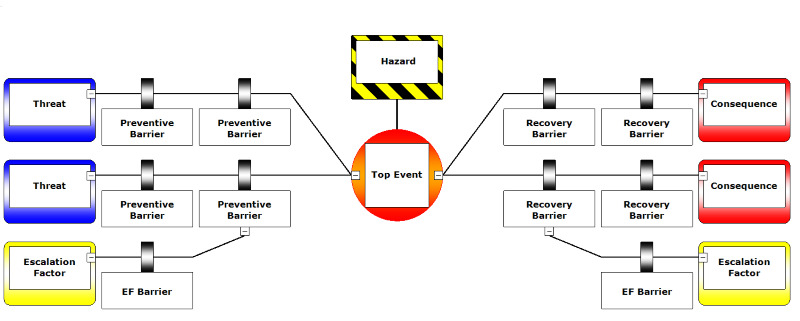
**-)Recoding and reporting**: documentazione del processo e archiviazione dei documenti.

**-)Monitoring and review**: controlli periodici per osservare i cambiamenti, avviene per tutto il processo.

**-)Comunicazione e consultazione** degli stakeholder, avviene per tutto il processo.

Il risk management si basa su 8 principi per guidare l’organizzazione verso il miglioramento delle prestazioni: **dinamicità** (adattarsi ai cambiamenti dei rischi), **inclusività** (coinvolgere gli stakeholder), **personalizzazione**, **informazioni** tempestive, chiare e disponibili, **fattori umani e culturali**, **migliorativo**, **integrativo** e fornito di **approccio strutturato e completo**.

**Intervento di studenti a piacere: Bow-tie analysis**



Tecnica di analisi del rischio e dei controlli che usa un modo schematico per descrivere percorsi dalla fonte dei rischi (minaccia) ai risultati (conseguenze).

Al centro troviamo il **top event**, cioè l’evento principale che fa perdere il controllo.

Sopra di esso troviamo il **Punto di partenza**, cioè il pericolo che consiste in un’attività, operazione o circostanza con la potenzialità di arrecare danno.

A sinistra troviamo le **minacce**, cioè i fattori che possono generare perdita di controllo (top event), e le **barriere preventive** che riducono le possibilità che la causa diventi un incidente.

A destra abbiamo le **conseguenze**, eventi (solitamente negativi) che possono essere generati dal top event e sono preceduti da **barriere mitigative** che riducono il danno.

**Semplicistico rispetto alle realtà perché mancano collegamenti tra cause**.

**Quale libro ti è piaciuto di più? Ioannis 🡪Tesoretto**

Famiglia: il capofamiglia (proprietario) conserva un tesoretto di 40.000€ nell’appartamento.

Obiettivo: conservare il tesoretto integro.

Contesto esterno: l’appartamento si trova nella periferia nord di una città settentrionale, al primo piano di una palazzina da 8 appartamenti.

La famiglia al piano terra (appartamento 2) ha due figli di cui il maggiore ha precedenti penali.

Portatori di interesse esterni: negozi che vorrebbero avere il capofamiglia come cliente.

Potenziali minacce esterne: malviventi della zona e il figlio dell’appartamento 2.

Contesto interno (stakeholder): nucleo familiare di capofamiglia, moglie e figlio 22enne, i genitori lavorano ma il figlio no. 🡪unici a conoscenza del tesoretto.

Immagino: tesoretto in un cassetto senza lucchetto in una stanza con finestra.

Scala di impatto: 1)Molto basso: 10k€ < 2)Basso: 20k€ < 3)Medio: 30k€ < 4)Alto: 40k€ < 5)M. alto 50k€.

Scala probabilità: 1)Molto basso < 2)Basso < 3)Medio < 4)Alto < 5)Molto alto.

Si potrebbe analizzare la situazione con tecniche di brainstorming, check-list o interviste.

Vulnerabilità:

1. V1: Porta del salone in cui è custodito il tesoretto.
2. V2: Porta d’ingresso dell’appartamento
3. V3: Finestra del salone affacciata sull’esterno.

Poi bisognerebbe fare un’analisi per vedere se ci sono agenti portatori di minacce come ladri che vogliono impossessarsi del tesoretto, ma anche agenti meno evidenti come umidità o incendi.

Minaccia M1: figlio del capofamiglia disoccupato 🡪 prelievo del tesoretto totale o parziale (75% - 30.000€) 🡪v1.

Minaccia M2: famiglia al primo piano che viene a conoscenza del tesoretto 🡪furto totale (D=40.000€) e uso di V2 o V3.

Combinazioni: (M1, V1)🡪D13=30k€ o (M2, V2) o (M2, V3)🡪D4=40k€.

Probabilità: P1\_1(M1, V1)=5, P2\_2(M2,V2)=4, P2\_3(M2,V3)=3.

Rischi parziali:

R1=f(P1\_1,D1)=5\*3=15; R2=f(P2\_2,D2)=4\*4=16; R3=f(P2\_3,D2)=3\*4=12.

**Rischio aggregato** tramite media aritmetica: 15+16+12=43/3=14 🡪rischio complessivo medio.

Il capofamiglia decide se intervenire spostando il tesoretto (cambiando tuti i rischi) o di lasciarlo lì e lavorare sui singoli rischi parziali che lo compongono.

Operazioni possibili: modificare, accettare, evitare o condividere/trasferire i rischi.

Evitare i rischi (trasferirli): portarli in banca. Modificare i rischi: introdurre misure adeguate.

Accettare i rischi non è percorribile (livello medio di Ragg e Medio/Alto di Rp).

Ridurre i rischi parziali:

1. Immagine che contiene testo, schermata, numero, Carattere

   Descrizione generata automaticamenteR1: figlio: rimuovere la vulnerabilità (serratura alla porta o cassaforte) o allontanare la minaccia spingendolo a trovarsi un lavoro. Misure: c1 (lavoro), C2 (cassaforte), C3 (porta del salone chiusa a chiave), C4 (sensibilizzare il figlio).
2. R2: malviventi attraverso la porta: C2 (cassaforte), C5 (porta blindata all’ingresso).
3. R3: malviventi dalla finestra: C2 (cassaforte), C6 (finestra).

C5 (porta blindata) è già implementata 🡪riduce valore di R2 di quantità R2\_g2c5.

Rischio residuo parziale R1: R1=15, se applico tutte le misure (C1, C2, C3, C4) scende da liv 15 a liv 1.

RR1=R1-RG1=15-14=1.

Rischio residuo parziale R2: R2=16, applicando C2 e C5 scende a 1. RR2=R2-RG2=16-15=1.

Rischio residuo parziale R3: R3=12, applicando C2 e C6 scende a 1. RR3=R3-RG3=12-11=1.

🡺Rischio residuo aggregato: RRaggr=1.

Il proprietario approva il Piano di Trattamento Rischi e approva i Rischi Parziali Residui: RR1=1, RR2=1, RR3=1, RRaggr=1. Tutti i rischi parziali residui RRi sono sotto il livello di accettazione.

In seguito, il proprietario deve approvare i RRi e procedere implementando le contromisure stabilite nel piano provvedendo all’investimento delle competenze, alle risorse e ad ogni altro supporto.

**Framework di ISO 31000:2018**

Un **Framework** (o struttura) è l'insieme di elementi fondamentali che guidano l'organizzazione nell'implementazione, nel mantenimento e nel miglioramento continuo della **gestione del rischio** e supporta l’approccio ciclico **plan-do-check-act**.

Plan: individuare attività, processi e strumenti da utilizzare per conseguire i risultati previsti. Avviene a livello strategico (attività a lungo termine e caratteristiche generali), tattico (miglioramenti dei processi) e operativo (attività quotidiane necessarie). 🡪Do: realizzare ciò che hai pianificato. 🡪 Check: controllare se l’esito è quello aspettato. 🡪Act: agire se il controllo mostra carenze.

Il **leader** gestisce il rischio e dimostra “commitment” personalizzando/implementando il framework, stabilendo cosa fare, assicurandosi della presenza di risorse e assegnando autorità e responsabilità.

Inoltre, il leader deve **definire i criteri e livelli di accettazione rischi**, condurre **esami periodici** e **promuovere il miglioramento continuo**.

Gli **organi di controllo** si assicurano che i rischi vengano considerati adeguatamente, che i rischi siano appropriati e che la gestione dei rischi sia implementata e funzionante.

Altre componenti del framework:

Immagine che contiene testo, cerchio, logo, Carattere

Descrizione generata automaticamente**Integration**: il RM deve essere integrato in ogni fase dell’organizzazione.

**Design**: bisogna tenere conto dei rischi fin dalla progettazione definendo il risk owner e le policies e assegnando le risorse.

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

**Evaluation**: valutare spesso l’efficacia della gestione con misurazioni.

**Improvement**: miglioramento ed adattamento continuo.

Immagine che contiene testo, compact disk, cerchio, Carattere

Descrizione generata automaticamente**Principi:**

-Rischio **integrato** in ogni parte del processo.

-Approccio **strutturato e comprensivo** al RM.

-Framework e processi sono **personalizzati**.

-**Inclusivo degli stakeholder**: coinvolgendoli in modo appropriato e tempestivo.

-Rischi **dinamici**: tenere conto che possono cambiare in base al contesto.

-Usa le **migliori informazioni disponibili al momento**.

-Influenzato da fattori umani e culturali.

-Il RM è in **continuo miglioramento**.

**Quale libro ti è piaciuto di più? Ioannis 🡪Passaggio a livello.**

Premessa: in questo caso, per la natura della situazione, non è possibile seguire in modo rigoroso il processo del risk management 🡪 impossibile raccogliere dati o compiere analisi.

Le uniche analisi sono qualitative basate sui ragionamenti del momento (soggettive).

**Evento**: un uomo deve andare in ufficio a piedi impugnando una borsa con documenti e laptop.

Deve arrivare puntuale (almeno 15 min prima) 🡪Passaggio a livello chiuso.

**Obiettivo**: attraversare il passaggio a livello per arrivare in orario e non essere investito.

Creiamo delle scale di probabilità e di conseguenze da 1 a 5 e ordiniamo le azioni per priorità crescente di rischio (priorità = rischio basso).

Il **contesto** offre le seguenti opzioni:

1. Attraversare comunque i binari 🡪rischio di essere investito
2. Usufruire del ponte sopraelevato 🡪+400m di strada, pioggia e borsa in mano 🡪rischio di farsi male e ritardo 15-30 min.
3. Cambiare strada allungando il percorso 🡪ritardo 15-30 min.
4. Aspettare che passino tutti i treni e si alzino le sbarre 🡪ritardo >30 min.

R1: rischio = essere investito dal treno🡪D=5 \* P=5 🡪R=25.

R2: farsi male sul ponte di ferro 🡪 P=4 \* D=5 🡪R=20.

R3: ritardo cambiando strada 🡪 P=3 \* D=1 🡪R=3.

R4: ritardo per aspettare il passaggio a livello 🡪P=5 \* D=1 🡪R=5. (Io metterei D=2).

Le scelte migliori sono R3 e R4 🡪meglio R3 perché il ritardo di D4 è meno prevedibile.

Una volta deciso il da farsi: chiamare il collega per avvisare del ritardo, tracciare il nuovo percorso e avviarsi attraverso esso.

Monitoraggio continuo: controllare il tempo ed il percorso mentre si cammina avvisando in ufficio per ulteriori ritardi.

Per migliorare la situazione per le prossime volte: partire prima (soprattutto se piove), informarsi sugli orari di chiusura del passaggio a livello, chiedere di non pianificare le riunioni importanti al mattino presto e considerare la possibilità di una riunione con collegamento da remoto.

**Quale libro ti è piaciuto di più? Gallotti 🡪ISO 27.000**

**Dati**: insieme di singoli fatti, immagini o espressioni 🡪**Informazioni**: dati organizzati e significativi.

**Conoscenza**: informazioni recepite da 1 individuo🡪**Sapienza**: conoscenze connesse che permettono di prendere decisioni.

**Proprietà della information security**: integrità, confidenzialità e disponibilità + **autenticità,** **accountability/tracciabilità** (attribuire ad una persona la responsabilità di un evento), **non-ripudio**, **completezza** ed **affidabilità**.

**ISO 27001:** standard internazionale che descrive le **best practices** per un **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI) ed è alla base del più importante schema per la **certificazione** dei processi. Usa il termine “verosimiglianza” e non “probabilità” perché non sono solo analisi quantitative.

È una norma **breve** di **alto livello** che parla di come gestire e organizzare l’organizzazione, poi nel 27002 descrive i controlli più dettagliatamente.

Definisce il “**risk owner**” come persona/entità con responsabilità e potere per gestire un rischio e coincide spesso con la Direzione.

Il sistema di gestione richiede un commitment direzionale, cioè tutti “i comportamenti di impegno, motivazione e senso del dovere, di appartenenza e responsabilità nei confronti dell’azienda”.

**Annex A**: lista di controlli usati dall’auditor quando viene richiesta la certificazione da un’azienda.

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.

L’annex A divide i controlli di sicurezza in strategici, fisici, tecnologici e di persone.

**Statement of applicability** (dichiarazione di applicabilità): documento chiave nell'ambito della norma ISO/IEC 27001.

Elenca i controlli di sicurezza **nell’Annex A** della ISO 27.001 e indica quali sono applicati e quali no con le relative motivazioni. Poco apprezzato e si rischia che diventi un elenco di caselle spuntate.

**Controlli di sicurezza**: misure che modificano il rischio includono processi, politiche, dispositivi, partiche…Non sempre potrebbero ottenere l’effetto atteso o previsto di modifica del rischio.

Tipologie: preventivi, di recupero e di rilevazione.

Relazioni tra controlli: alternativi (o uno o l’altro, entrambi = sicurezza del più debole), compensativi (meno efficaci in sostituzione a quelli ideali), complementari (possono essere usati insieme) e correlati (devono essere usati insieme 🡪es: concerto).

L’annex A contiene 4 sezioni e i loro controlli:

* Organizzativi: legati alla gestione e governance della sicurezza delle informazioni. Es: politica per documenti sensibili in zone ad accessibili solo a personale autorizzato.
* Sulle persone: formazione e gestione del personale (limitati dalla legge). Es: corso su sicurezza informatica.
* Fisici: per proteggere gli asset fisici. Es: antincendio.
* Tecnologici: per sicurezza delle informazioni e dell’IT. Es: antivirus e back-up.

**Assets:** qualsiasi bene che abbia valore per l’azienda, tra cui le informazioni.

Le informazioni vanno: identificate trovando il responsabile, classificate ed etichettate indicando il livello di riservatezza ed in base ad esso vanno trattate (conservate, copiate, distrutte).

Si possono usare programmi automatici di **data loss prevention** per controllare il rispetto delle regole e **tecniche di mascheramento** per sostituirle o cambiarle o **di anonimizzazione**.

Gli asset vanno identificati e censiti indicandone le proprietà e bisogna controllare gli accessi limitandoli alle persone **autorizzate** seguendo i principi Need to know, minimum privilege e segregation of duties, inoltre le informazioni possono essere protette tramite cifratura conservando adeguatamente le **chiavi crittografiche**.

**Conduzione dei sistemi informatici**: esercizio/gestione dei sistemi IT, comprendendo i sistemi poco intelligenti come quelli che costituiscono la IoT che sono da trattare con particolare attenzione.

È importante documentare perché, anche in presenza di un massimo esperto, lui potrebbe assentarsi o lasciare l’azienda, quindi bisogna scrivere dei manuali per l’installazione, l’uso e la gestione dei problemi.

La configurazione sicura dei sistemi critici (**hardening**) e dovrebbe includere un blocco per le connessioni non sicure e l’istallazione di softwares da parte degli utenti, installazioni e aggiornamenti di antivirus e firewall, back-up, crittografia, disconnessione per inattività ed altre misure di sicurezza o per aumentare l’efficienza (ad esempio risparmiando memoria).

Bisogna tenere conto dei **cambiamenti** che possono riguardare HW, SO, applicazioni, cloud… e comprendono chiusure, modifiche, introduzione di nuovi dispositivi (vulnerabilità) e correzioni.

Ogni cambiamento comporta nuovi possibili rischi e vulnerabilità, quindi deve seguire lo schema:

richiesta e requisiti 🡪 autorizzazione 🡪 pianificazione (plan) 🡪 progetto e sviluppo (do) 🡪riesami, verifiche e test (check e act) 🡪rilascio.

I cambiamenti possono essere registrati tramite un sistema informatico di “**ticketing**”.

Altre misure di sicurezza sono: utilizzo di **antivirus**, **backup**, monitoraggio dei **log**, controllo del grado di utilizzo elle memorie **RAM** e **CPU**, controllo dei **dispositivi portatili** e **cancellazione dei dati** una volta scaduto il tempo di conservazione.

**Fornitori**: sono una forma di condivisione del rischio e si dividono in 3 tipi: di prodotti HW/SW, di servizi non informatici e di servizi informatici. La fornitura viene divisa in 3 fasi: stabilire i requisiti 🡪verificare che i fornitori possano garantirli🡪 decidere se accettare i requisiti non garantiti 🡪contratto 🡪verificare il rispetto del contratto.

Negli accordi bisogna stabilire: riservatezza, sicurezza, continuità operativa, monitoraggio, audit, canali di comunicazione…

Nei casi di servizi informatici è importante specificare le modalità d’uso, responsabilità, normative…

Bisogna tenere conto della continuità operativa del fornitore: se manca 🡪cambiare fornitore, averne più di uno, poterlo fare da soli.

**Business continuity** (Continuità operativa): capacità di un’organizzazione di continuare a fornire prodotti o servizi a un livello accettabile predefinito, dopo un incidente di disturbo.

Il Business continuity Management System fa sia da prevenzione (identificando rischi e stabilendo strategie) che da risposta al rischio di interruzione dell’attività

Nella sicurezza delle informazioni è necessario occuparsi della disponibilità delle informazioni (usando le ridondanze) e della continuità dei processi di sicurezza delle informazioni.

Necessarie: business impact analysis (tempi max, risorse necessarie in caso di emergenza…), valutare il rischio relativo alla continuità operativa (cause di indisponibilità), stabilire obiettivi e strategie di ripristino (**recovery time, recovery point**), impostare piani di continuità…

Utilizzare delle **strategie** (Gallotti) come un sito di appoggio che fa da disaster recovery (back-up o servizio sostitutivo temporaneo) e piani come crisis plan, incident plan e emergency plan.

**Tecniche di minaccia**:

Le possibili minacce sono molte: intrusione nella sede o nel sistema informatico, frodi, furti d’identità, danneggiamenti fisici, furti informatici, documenti, malware, usi non autorizzati di servizi informatici, esaurimento delle risorse (DOS e scioperi), intercettazioni…

Autorizzazioni: operazioni che può effettuare una persona su un sistema informatico o sui dati o gli accessi ad ambienti fisici.

Principi: **minimum privilege** (fornire solo le autorizzazioni minime), **need to know** (accesso concesso solo a chi ha la necessità di conoscere quei dati) e **segregation of duties** (separazione dei ruoli).

**Audit**: processo sistematico, indipendente e documentato volto all’ottenimento di prove, al fine di valutarle per determinare quanto i criteri di audit (politiche, procedure e requisiti) sono soddisfatti.

-Interni (1° parte): svolti dall’organizzazione stessa, i criteri sono le procedure interne.

-esterni (2° parte): svolti da parte interessata (cliente) presso un’organizzazione, criteri=accordi tra parti.

-di certificazione (3° parte): svolti da organismi indipendenti e i criteri vengono concordati dall’organizzazione con l’organismo di certificazione.

Gli auditor possono commettere errori o essere malintenzionati, quindi devono essere trattati come ospiti ed accedere ai dati solo in modalità di sola lettura.

L’auditor è da considerare come: ospite (trattarlo bene), partner (essere sinceri), fornitore (non subire passivamente) e un auditor (fare prove prima).

In caso di non-conformità grave si aggiunge un **audit straordinario** qualche settimana dopo per controllare che il problema sia stato risolto, altrimenti si procede con gli audit periodici.

**Non conformità**: mancato soddisfacimento di un requisito. ES: backup ogni 2 mesi invece di 1.

Bisogna reagire eliminandole e affrontando le conseguenze.

Può provenire da un servizio fornito o ricevuto che risulta diverso dal contratto, un errore di esecuzione o un output diverso da quello atteso.

Possiamo effettuare azioni preventive (eliminare le possibili cause🡪rischi) o correttive.

**Sistema di gestione**: modo in cui l’azienda si organizza per raggiungere gli obiettivi. Insieme di elementi interagenti necessari per policies, obiettivi e processi. Tutelano gli interessi dell’azienda non del collettivo.

I “sistemi di gesitone” comprendono tutti i sistemi di gestione come: qualità (9001), ambientale (14001), informazioni (27001) e altri come energia, sicurezza sul lavoro…

I **sistemi di gestione** ci dicono, per ogni disciplina, cosa fare in termini organizzativi, di ruoli, di responsabilità, di pianificazione…

**Sistemi aziendali e debolezze.**

**C.I.A.**: la sicurezza delle informazioni si basa su tre proprietà principali:

-**Integrità** (integrity): proprietà di accuratezza e completezza dei dati.

-**Disponibilità** (availability): proprietà di accessibilità ai dati in ogni momento.

-**Riservatezza** (confidentiality): proprietà di non accessibilità alle informazioni sensibili da parte di individui non autorizzati o malintenzionati.

**Sistema per la gestione di…**

**Fornitori:** l’ufficio acquisti tratta i fornitori (vendor) ordinando i materiali necessari diretti o indiretti.

Producono documenti come l’ordine di acquisto, la richiesta di acquisto (RDA) per esprimere le esigenze e la richiesta di offerta (RDO) per richiedere informazioni.

**Vulnerabilità**: **INTEGRITA’**: errori nella scelta del fornitore più conveniente, nella spedizione o nel ritiro della merce e errori di pagamento che possono essere indirizzati ad un’altra persona.

**Produzione:** sistema che gestisce la catena produttiva dei prodotti o servizi venduti e dati come la qualità o quantità delle materie prime utilizzate.

**Vulnerabilità: DISPONIBILITA’**: impossibilità di controllare le scorte (ordinando l’acquisto di altre) e del processo produttivo, ritardi nelle decisioni aziendali e blocco temporaneo dalla produzione e di conseguenza dei guadagni.

**Clienti**: le aziende possono lavorare per altre aziende (B2B) o per clienti privati (B2C), in ogni caso sono gestiti dall’ufficio commerciale e da altri collaboratori esterni come commerciali o rappresentanti pagati in base agli obiettivi.

Si utilizza un sistema informatico **CRM** che gestisce i contatti, le trattative e gli ordini.

**Vulnerabilità: DISPONIBILITA’**: mancata assistenza dei clienti, impossibilità nella personalizzazione delle interazioni, riduzione della produttività e blocco temporaneo dalla vendita di beni ed erogazione di servizi.

**Ricerca e sviluppo**: ufficio R&D con informazioni estremamente private sul futuro dell’azienda come disegni in bozza, dettagli tecnici, corrispondenza interna, documenti, modelli, prototipi…

**Vulnerabilità: RISERVATEZZA**: un leak dei dati di R&D può influenzare negativamente l’immagine dell’azienda facendola passare come poco affidabile nella gestione delle informazioni, può esporre dati sensibili su partners e collaboratori, far perdere il vantaggio commerciale e portare ad un furto di proprietà intellettuale da parte della concorrenza.

**Marketing**: produce la marca verso il mercato e gestisce pubblicità, conferenze, articoli e social networks. I sistemi informativi raccolgono informazioni come analisi di mercato, proiezioni di vendita e campagne pubblicitarie e le rendono disponibili.

**Vulnerabilità: DISPONIBILITA’**: perdita di dati in tempo reale che porta a rimandare operazioni in periodi meno efficaci, difficoltà di efficienza del marketing, perdita di fidelizzazione dei clienti e perdita di occasioni difficilmente ripetibili. + **riservatezza**.

**Amministrazione, finanza e controllo**:si occupa di tenere la contabilità in partita doppia, di redigere il bilancio di esercizio composto da CE, SP e nota integrativa e di misurare le performance dell’azienda ad esempio definendo il budget.

**Vulnerabilità: DISPONIBILITA’**: ritardi nella chiusura del libri contabili, difficoltà nella pianificazione del budgeting, temporaneo blocco delle operazioni finanziarie e **pubblicazione tardiva delle scritture contabili** con **perdita di fiducia** degli stakeholder e **sanzioni.**

**Legale**: presenza di un ufficio legale per cause, controversie o brevetti.

**Vulnerabilità: RISERVATEZZA**: conseguenze legali per negligenza, violazione di accordi di non divulgazione (NDA), perdita di fiducia, danni reputazionali e **esposizione di informazioni sensibili**.

+ disponibilità.

**Verticali: Cloud.**

Le aziende iniziarono ad utilizzare i cloud quando non li comprendevano a pieno e non c’era chiarezza sul significato, poi la NIST diede una definizione di cloud e la BCE stabilì delle linee guida ribadendo l’importanza dell’analisi del rischio. Cloud più famosi: Azure, Google, AWS, Oracle, Aruba…

Gli elementi del cloud si dividono in tre categorie:

* **Service model**: l’infrastruttura può essere:
  + **Software as a Service (SaaS)**: il consumer può usare le applicazioni da diversi dispositivi ma non controlla l’infrastruttura cloud o le applicazioni.
  + **Platform as a Service (PaaS)**: il consumer non controlla l’infrastruttura ma può caricare delle applicazioni su cui ha controllo.
  + **Infrastructure as a Service (IaaS)**: il consumer può processare, salvare i dati, usare le risorse… Il client gestisce tutto come SO, dati e applicazioni. Più costoso.
  + Casi estremi: On-Prem (gestisci tutto tu) e BusinesProcess-aas (tutto il provider).
* **Deployment model**: modelli di distribuzione.
  + **Cloud privato**: infrastruttura per una singola organizzazione con i dipendenti come consumer 🡪non sfrutta l’economia di scala 🡪costosa.
  + **Community cloud**: cloud ad uso di una comunità di persone che condividono una mission (es: gruppo di aziende o banche) e può essere gestito da membri, terzi o misto.
  + **Cloud pubblico**: può aderire chiunque.
  + **Hybrid cloud**: insieme di 2 infrastrutture di tipo diverso.
* **Essential characteristics**:
  + **On-demand self-service**: il consumatore può comprare ciò che vuole senza interazioni umane con ogni provider 🡪veloce.
  + **Accesso a banda larga**: favorisce l’uso di piattaforme diverse (tablet, smartphone, pc).
  + **Resource pooling**: non compri un intero server ma esattamente le risorse che ti servono
  + **Rapid elasticity**: puoi modificare la quantità di risorse cloud quando vuoi.
  + **Measured service**: il prezzo personalizzato in base a quanto compri.

Perché viene scelto il cloud:

1. **Risparmio**: è difficile decidere il valore monetario del cloud, conta come spesa a breve termine e richiede delle competenze, ma permette il pay as you go e fornisce un esperto per l’assistenza clienti. Il cloud risparmia comprando in grandi quantità.
2. **Capacità di calcolo**: il cloud performa meglio di un sistema tradizionale grazie al resource pooling e alla rapid elasticity. Si basa sulla virtualizzazione.
3. **Acquisizione di servizi e applicazioni innovative**: servizi già pronti (make or buy).
4. **Maggiore sicurezza**: l’economia di scala provvede maggiore sicurezza, sia fisica del datacenter che dei dati tramite crittografia.

Bisogna tenere conto dei rischi/opportunità riguardo gli obiettivi, il percorso e quelli intrinseci del cloud, il coud aumenta la complessità del governo per via della perdita di controllo diretto e di competenze, delle giurisdizioni con sistemi legali differenti, della supply-chain opaca e della Shadow IT.

**Rischi**: data breach (🡪crypt), problemi con API/interfacce, minacce interne, APT, DOS, uso malevolo, lock-in (difficoltà a esportare i dati), perdita di governance (no controllo), chiusura o acquisizione del cloud, shadow IT (prendere un server cloud senza chiedere all’IT) e supply-chain opaca.

**Non si può negoziare con EULA**, possiamo solo accettare ma dobbiamo informarci per conoscere le nostre tutele, l’incomprensione del modello di responsabilità è la causa principale di incidenti.

**Audit:** esame della capacità di soddisfare gli accordi come fornitori di servizi.

**Gallotti**: non reputa il rischio cloud particolarmente grave o nuovo e lo paragona al trasferimento di dati via e-mail, critica il falso mito dei server in paesi indefinibili, i fornitori di cloud sono certificati, ma bisogna leggere attentamente i contratti per conoscere le proprie responsabilità.

Un cloud si può a sua volta appoggiare a servizi terzi, si potrebbero combinare le infrastrutture come un fornitore SaaS (dropbox) che usa un cloud Iaas (AWS) o usare modelli ibridi, questo permette di essere più specializzati e ridurre i costi.

Un servizio di e-mail, ad esempio, è un SaaS perché viene fornito tramite software pronto da utilizzare senza preoccuparsi del server, ma in casi in cui è uno strumento per sviluppatori e aziende che lo usano per integrare le loro applicazioni allora è un PaaS.

**Quale libro ti è piaciuto di più? Fiorito**

**Risk management**: processo per identificare, analizzare, valutare, prioritizzare e gestire i rischi prevenendo che eventi con effetti dannosi influenzino i nostri goal e riducendone impatto o probabilità.

Gestire i rischi permette di prendere decisioni più efficienti con le informazioni a disposizione facilitando il raggiungimento degli obiettivi e migliorando le performance.

Il risk management è personale e dipende dal **risk profile**, cioè la capacità di sopportare una perdita tornando ai propri obiettivi e l’appetito verso i rischi.

I profili di rischio si dividono in conservativi, moderati e aggressivi e sono influenzati da caratteristiche personali come vita ed età ma anche dalla situazione economica e dalla conoscenza del mercato.

Le persone che prendono decisioni possono essere: impulsive, compliant, evitanti, deleganti, bilanciate, riflessive o con priorità.

Secondo la teoria del **cigno nero** le persone sovrastimano le spiegazioni razionali nei dati passati e sottostimano il peso della casualità dei dati. L’autore sostiene che chi prende decisioni deve essere esposto al mondo reale e che, se non vede gli effetti dei rischi non sarà motivato a fare la scelta corretta da qui la frase “se ti va bene, hai vinto, se va male è colpa del cigno nero”.

Teoria del **Mental accounting**: trattiamo il denaro diversamente in base a fattori come le sue origini avendo una diversa propensione alla spessa 🡪gratta e vinci.

**The effect of sunk costs:** i costi irrecuperabili ci portano spesso a correre più rischi in determinate decisioni rispetto a quelli che avremmo preso o considerato se non avessimo sostenuto tali spese.

ES: compriamo 2 esperienze una da 2000$ e una migliore da 1000$ ma sono lo stesso giorno, razionalmente dovremmo fare la 2, ma la 1 costa di più quindi ci sembra di buttare meno soldi. Se spendiamo soldi o abbiamo una perdita tendiamo a prendere più rischio sperando di recuperare.

**Endowment effect**: le persone tendono a valutare di più gli asset che loro possiedono rispetto agli stessi asset ma che non possiedono. Li overvalutano perché sono loro.

Vediamo questo effetto quando i proprietari di aziende per evitare il rischio di perderle corrono rischi ancora più alti perché sovrastimano il valore. Il prezzo a cui vendiamo è sempre più alto del prezzo a cui compreremmo.

Casi particolari: decisoni collettive e decisioni dei giovani.

Per un paese è necessario considerare **rischi sia interni che esterni**, ad esempio se l’obiettivo è “ridurre la povertà e la fame”, un rischio esterno è la contrazione dell’economia, un rischio interno è l’inflazione. Uno stato deve considerare anche il rischio sovrano, cioè la possibilità che uno stato non adempia agli impegni e obblighi finanziari ed il rischio paese che include la probabilità che lo stato limiti i pagamenti in valuta estera. L’appetito per il rischio dipende anche dalla cultura, paesi come il Giappone sono propensi al rischio (92) perché abituati a catastrofi naturali, noi siamo al 70, mentre la Cina a 30 perché è capace di adattarsi.

Quando analizziamo un problema dobbiamo considerare i “5 why”, cioè, ci chiediamo quale sia il motivo e ci chiediamo 5 volte perché avvenga.

**Risk map**: strumento per identificare, valutare, monitorare e riportare il livello di rischio di un’organizzazione. Viene rappresentato il livello di rischio sia nei rischi finanziari che in quelli non finanziari nei colori verde, giallo, rosso, ciò permette di rappresentare i rischi più gravi (rischi top) e quelli emergenti che si verificano a causa di innovazioni.

Si utilizzano le metriche **Key risk indicators** per determinare potenziali eventuali rischi e le azioni da intraprendere per anticiparl.

**Controlli (31000)**: azioni per mitigare i rischi e migliorare la probabilità di soddisfare gli obiettivi. I rischi che rimangono dopo i controlli sono chiamati rischi **residui**. Riguardo il controllo dobbiamo porci 5 domande: Chi? Cosa? Come? Quando? Perché?

Le caratteristiche del controllo: preventive, detective, corrective, automatic/manual.

Mancanze dei controlli: design deficiency (assenti o non disegnati correttamente), execution def., control def. (meno grave, il controllo non permette di trovare quell’errore), significant def e material def. (grave, mancanza di controlli porta a evento imprevisto con conseguenze gravi).

**Glossario**

* **Information data:** conoscenza o insieme di dati che hanno valore per un individuo o un’organizzazione. (27.000)
* **Sicurezza delle informazioni (Information security):** preservazione di riservatezza, integrità e disponibilità delle informazioni + accountability, non ripudio e affidabilità. (27.000-27.001).
* **Sistema di gestione** (management system): modo in cui l’azienda si organizza per raggiungere gli obiettivi. Insieme di elementi interagenti necessari per policies, obiettivi e processi.
* **Evento relativo alla sicurezza delle informazioni** (27.000)**:** occorrenza dello stato di un sistema, servizio o rete che identifica una possibile violazione delle policies o un errore nei controlli o una situazione sconosciuta significativa.
* **Obiettivo**: risultato da raggiungere. Può essere strategico, tattico o operativo, può essere applicato in molti modi e devono essere SMART (Specifici, misurabili, achivable, relevant e time-bound (scadenza)).
* **Asset** (27.000): qualsiasi bene che abbia valore per l’azienda come informazioni, personale, competenze, softwares…
* **Minaccia** (27.000): causa potenziale di un incidente che può comportare danni a un sistema o all’organizzazione. La minaccia è potenziale, l’evento è accaduto. Chiamata “risk source”.
* **Conseguenza:** effetti di un rischio a breve, medio e lungo termine. Gli impatti sono immediati. Possono essere anche positive (opportunità).
* **Processo** (27.000): insieme di attività tra loro interrelate o interagenti che trasforma elementi in input in elementi in output. Devono essere tenuti sotto controllo.
* **Procedura** (27.002)**:** un modo specifico per effettuare un’attività o un processo.
* **Controlli** (31000-27000): azioni per mitigare i rischi e migliorare la probabilità di soddisfare gli obiettivi.
* **Vulnerabilità** (27.002): debolezza di un asset o di un controllo di sicurezza che può essere sfruttata da una o più minacce.
* **HLS:** High level structure: standard per la scrittura degli standard, pubblicato nell’Annex SL delle ISO, tutti gli standard adesso lo seguono. Inizialmente era stato creato come guida ma venne pubblicato come direttiva. Su quello si basa ISO 27.001.
* **Stakeholder** (9000): persona o organizzazione che può impattare, che viene impattata o crede di esserlo dalla decisione o attività di un’azienda.
* **Business continuity** (22300)**:** capacità di un’organizzazione di continuare a fornire prodotti o servizi a un livello accettabile predefinito, dopo un incidente di disturbo.
* **CLUSIT**: associazione italiana per la sicurezza informatica (ci lavora il prof) nata per pormuovere la politica e cultura della sicurezza in Italia.
* **NIST**: agenzia del governo degli USA che si occupa della gestione delle tecnologie di diverse discipline.
* **Verosimiglianza**: chance che qualcosa accada.
* **Politica**: intenzioni e indirizzi di un’organizzazione espressi formalmente da parte della Direzione.

**ISO 27000 vs 31000**

|  |  |
| --- | --- |
| **ISO 27.000 (Gallotti)** | **ISO 31.000 (Ioannis)** |
| requisiti per la gestione della sicurezza delle informazioni. | linee guida per la gestione dei rischi in generale |
| Normativo, con requisiti e controlli specifici (es. ISO 27001 per certificazione). | **Flessibile**, basato su principi e linee guida generali. |
| La famiglia ISO 27000 include norme **certificabili** (es. ISO 27001). | Non certificabile; fornisce solo una guida per i processi di gestione del rischio. |
| Basata su information security management system | Basato su un framework per la gestione del rischio senza requisiti obbligatori o controlli dettagliati. |
| |  | | --- | | Entrambe promuovono un approccio sistematico e continuo alla gestione (ciclo PDCA - Plan, Do, Check, Act). |  |  | | --- | |  | | |

**Standard verificabili**: norme con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente; usano il verbo imperativo shall (deve);

**Linee guida**: manuali o raccolte di best practice al fine di raggiungere un certo obiettivo; si riconoscono perché sono usano i verbi al condizionale should/can/may (dovrebbe/può/potrebbe).

Altri standard ISO:

* **19.600**: conformittà legislativa.
* 27.000: vocabolario gratuito.
* 27.001: requisiti per il SGSI, comprende Annex A per SoA e Annex SL con HLS.
* 27.002: fornisce una serie di linee guida (non certificabile) per implementare i controlli di sicurezza elencati nell'**Annex A** della ISO/IEC 27001. Ultima revisione nel 2022.
* 27.003: guida all’interpretazione della 27001
* 27.004: guida per misurazione e monitoraggio di un SGSI
* 27.005: guida per gestione del rischio
* 27.017 e 27018: controlli di sicurezza e di privacy dei cloud.
* 27.019: controlli nel settore energetico.
* **27.701**: requisiti del GDPR.
* **27.799**: controlli nel settore della sanità.
* 31.001: linee guida per la gestione dei rischi in generale
* **31.010**: inidicazioni utili delle tecniche per l’analisi del rischio (brainstorming e farfallino).
* 9.001: norma certificabile relativa alla qualità dei processi. Comprende diversi requisiti come il contesto, la leadership e la pianificazione ed è focalizzata sul cliente.
* 15.408: **common criteria**: standard per valutare e certificare la sicurezza dei prodotti IT. Nacquero perché le procedure di valutazione e certificazione erano lunghe e da ripetere. I costi di valutazione sono alti a causa della lunghezza del processo, per questo motivo i Common Criteria sono in continua evoluzione. In assenza di documentazione precisa si può solo valutare ad un basso livello di garanzia.