Gestione e analisi del rischio

Massimo Battaglioni
Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
massimo.battaglioni@unimc.it

A.A. 2023/2024

Come definire il rischio?

- Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi (cfr. Norma UNI 11230)

Come definire il rischio?

- **Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi** (cfr. Norma UNI 11230).

- Potenzialità che un'azione o un’attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile (cfr. Wikipedia).

Come definire il rischio?

- **Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi** (cfr. Norma UNI 11230).
- Potenzialità che un'azione o un’attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile (cfr. Wikipedia).

- Il rischio è la possibilità che si verifichi un evento indesiderato o negativo. È una valutazione delle conseguenze negative o danni che possono derivare da un'attività o un evento, e della probabilità che tali conseguenze si verifichino (cfr. pizzagpt 2023)

- Il rischio è la possibilità che si verifichi un evento negativo, che può portare a perdite o danni. Nell'ambito della gestione dei rischi, esso è comunemente definito come la combinazione della probabilità di un evento e delle sue conseguenze (ChatGPT 4 13/03/2024)

Come definire il rischio?

- **Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi** (cfr. Norma UNI 11230).
- Potenzialità che un'azione o un’attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile (cfr. Wikipedia).
- Il rischio è la possibilità che si verifichi un evento negativo, che può portare a perdite o danni. Nell'ambito della gestione dei rischi, esso è comunemente definito come la combinazione della probabilità di un evento e delle sue conseguenze (ChatGPT 4 13/03/2024)

✓ Il termine "rischio" viene più frequentemente usato quando vi è la possibilità di conseguenze negative.

Come definire il rischio?

- **Insieme della possibilità di un evento e delle sue conseguenze sugli obiettivi** (cfr. Norma UNI 11230).
- Potenzialità che un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile (cfr. Wikipedia).
- Il rischio è la possibilità che si verifichi un evento negativo, che può portare a perdite o danni. Nell'ambito della gestione dei rischi, esso è comunemente definito come la combinazione della probabilità di un evento e delle sue conseguenze (ChatGPT 4 13/03/2024)
- ✓ Il termine "rischio" viene più frequentemente usato quando vi è la possibilità di conseguenze negative.
- ✓ Il concetto di rischio implica la "combinazione della probabilità di un evento e della entità delle sue conseguenze".

Come definire il rischio?

- **Insieme della possibilità di un evento e delle sue conseguenze sugli obiettivi** (cfr. Norma UNI 11230).
- Potenzialità che un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile (cfr. Wikipedia).
- ✓ Il termine "rischio" viene più frequentemente usato quando vi è la possibilità di conseguenze negative.
- ✓ Il concetto di rischio implica la sua dimensione e cioè la "combinazione della probabilità di un evento e della entità delle sue conseguenze".

- ✓ In alcuni settori, per esempio in quello finanziario, al concetto di rischio viene associato anche quello di "conseguenza positiva". Più in generale, si fa riferimento al binomio rischio-rendimento, nel senso che maggiore è la dimensione del rischio a cui ci si espone e maggiore dovrebbe essere il rendimento.

Quanto si è disposti a rischiare?

Terminologia

- **Risk Management (Gestione del rischio):** Processo messo in atto nelle aziende per identificare i rischi e sviluppare strategie per evitarli e governarne il controllo.

Terminologia

- **Risk Management (Gestione del rischio):** Processo messo in atto nelle aziende per identificare i rischi e sviluppare strategie per evitarli e governarne il controllo.

- **Risk Assessment (Valutazione del rischio):** Esame di tutti i rischi presenti in azienda finalizzato a pianificare l'attuazione delle misure volte alla loro «eliminazione» o riduzione a livello accettabile.

Terminologia

- **Risk Management (Gestione del rischio):** Processo messo in atto nelle aziende per identificare i rischi e sviluppare strategie per evitarli e governarne il controllo.
- **Risk Assessment (Valutazione del rischio):** Esame di tutti i rischi presenti in azienda finalizzato a pianificare l'attuazione delle misure volte alla loro «eliminazione» o riduzione a livello accettabile.

- **Risk Analysis (Analisi del rischio):** Parte dall'identificazione dei beni da proteggere per poi valutare le possibili minacce in termini di probabilità di occorrenza e relativo danno potenziale (gravità).

Rischi ed eventi collegati

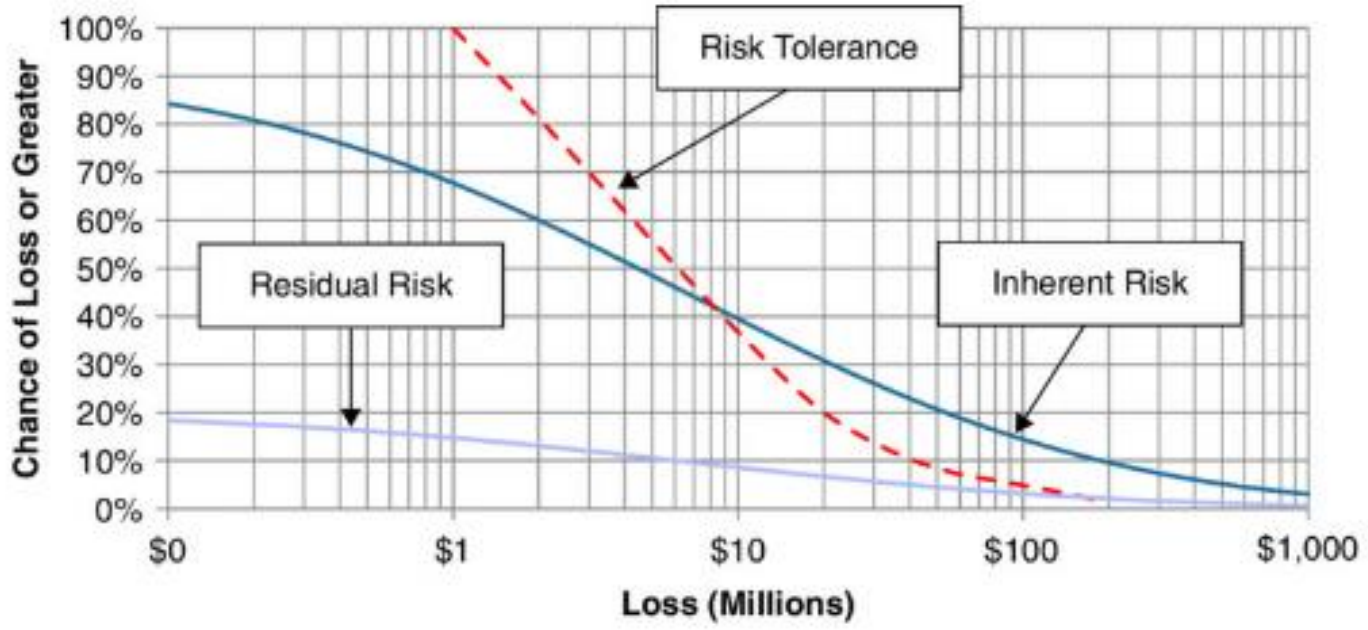
Rischi	Possibili eventi
Naturali	Alluvioni, uragani, terremoti
Sociali	Criminalità, terrorismo
Finanziari	Andamento del mercato, variazione delle condizioni praticate da clienti e fornitori
Competitivi	Contraffazione, Sabotaggio
Cyber	Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware
Fisici	Incidenti sul lavoro, accessi non autorizzati ad aree protette
Data Protection	Furto, corruzione, perdita, divulgazione di informazioni
Compliance	Violazione di leggi o regolamenti
Etici	Comportamenti non etici

Termini e definizioni (UNI11230)

Rischio	Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi
Obiettivo	Risultato da raggiungere
Evento	Accadimento di una serie di circostanze
Conseguenza	Esito di un evento
Probabilità	Misura o stima della possibilità che un evento ha di verificarsi
Controllo	Misura che mantiene e/o modifica il rischio
Minaccia	Causa o origine di un danno o perdita potenziali
Vulnerabilità	Debolezza di un asset o controllo che può essere sfruttata da una o più minacce

- Definizioni simili si trovano nelle norme ISO 31000:2018 e ISO 27000:2018.

Valutazione dell'impatto economico



CCDF (Complementary Cumulative Distribution Function)

= **Probabilità di perdere una cifra maggiore di quella indicata**

Rischio intrinseco = CCDF con il profilo attuale

Tolleranza al rischio (Rischio tollerabile) = CCDF ammissibile per l'organizzazione

Rischio residuo = CCDF con il profilo target

Risk management

- La gestione del rischio (risk management) è nata come modello gestionale all'inizio del secolo scorso nel mondo finanziario (anche se nel 1100 i banchieri già gestivano il rischio di credito).

Risk management

- La gestione del rischio (risk management) è nata come modello gestionale all'inizio del secolo scorso nel mondo finanziario (anche se nel 1100 i banchieri già gestivano il rischio di credito).

- Con gli anni è stata introdotta nel mondo assicurativo e delle costruzioni, fino ad assumere un ruolo più centrale e globale all'inizio degli anni '90 con l'Entreprise Risk Management (ERM).

Risk management

- La gestione del rischio (risk management) è nata come modello gestionale all'inizio del secolo scorso nel mondo finanziario (anche se nel 1100 i banchieri già gestivano il rischio di credito).

- Con gli anni è stato introdotto nel mondo assicurativo e delle costruzioni, fino ad assumere un ruolo più centrale e globale all'inizio degli anni 90 con l'Entreprise Risk Management (ERM).

- Ultimo caso è quello del General Data Privacy Regulation (GDPR): il Regolamento Europeo 679/2016 fonda la sua struttura sulla gestione del rischio: nel corpo del testo di legge, infatti, la parola «rischio» compare circa 70 volte.

Risk management

- La gestione del rischio (risk management) è nata come modello gestionale all'inizio del secolo scorso nel mondo finanziario (anche se nel 1100 i banchieri già gestivano il rischio di credito).

- Con gli anni è stato introdotto nel mondo assicurativo e delle costruzioni, fino ad assumere un ruolo più centrale e globale all'inizio degli anni 90 con l'Entreprise Risk Management (ERM).

- Ultimo caso è quello del General Data Privacy Regulation (GDPR): il Regolamento Europeo 679/2016 fonda la sua struttura sulla gestione del rischio: nel corpo del testo di legge, infatti, la parola «rischio» compare circa 70 volte.

- Nel 2009 tutti i concetti inerenti al risk management sono stati formalizzati nello standard ISO 31000:2009 per poi evolversi dando luce l'ultima versione pubblicata a maggio 2018.

Lo standard ISO 31000:2018

- **Lo standard ISO 31000:2018** sul risk management si pone l'obiettivo di mettere ogni organizzazione nelle condizioni di individuare, prevenire e gestire tutti i rischi incombenti nell'ambito della propria attività, attraverso un approccio strutturato.


INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

ISO

Reference number
ISO 31000:2018(E)

Lo standard ISO 31000:2018

- **Lo standard ISO 31000:2018** sul risk management si pone l'obiettivo di mettere ogni organizzazione nelle condizioni di individuare, prevenire e gestire tutti i rischi incombenti nell'ambito della propria attività, attraverso un approccio strutturato.

- A prescindere dal settore in cui operano, i principi ISO 31000 possono essere utilizzati come *framework* di gestione del rischio per qualsiasi azienda. Tali standard facilitano l'implementazione sistematica dei piani di gestione del rischio.

Lo standard ISO 31000:2018

- **Lo standard ISO 31000:2018** sul risk management si pone l'obiettivo di mettere ogni organizzazione nelle condizioni di individuare, prevenire e gestire tutti i rischi incombenti nell'ambito della propria attività, attraverso un approccio strutturato.

- A prescindere dal settore in cui operano, i principi ISO 31000 possono essere utilizzati come *framework* di gestione del rischio per qualsiasi azienda. Tali standard facilitano l'implementazione sistematica dei piani di gestione del rischio.

- Contrariamente ad altri standard, la norma ISO 31000 **non è destinata alla certificazione**.

Lo standard ISO 31000:2018

- La norma è destinata a coloro che creano e proteggono valore nelle organizzazioni avendo cura di gestire rischi, prendere decisioni, fissare e conseguire obiettivi e migliorare le prestazioni.


INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

ISO

Reference number
ISO 31000:2018(E)

Lo standard ISO 31000:2018

- La norma è destinata a coloro che creano e proteggono valore nelle organizzazioni avendo cura di gestire rischi, prendere decisioni, fissare e conseguire obiettivi e migliorare le prestazioni.
- Fornisce linee guida per gestire i rischi che le organizzazioni affrontano e può essere utilizzata durante tutta la vita dell'organizzazione, oltre a poter essere applicata a qualsiasi attività, compreso il processo decisionale a tutti i livelli.


INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

ISO

Reference number
ISO 31000:2018(E)

Lo standard ISO 31000:2018

- La norma è destinata a coloro che creano e proteggono valore nelle organizzazioni avendo cura di gestire rischi, prendere decisioni, fissare e conseguire obiettivi e migliorare le prestazioni.
- Fornisce linee guida per gestire i rischi che le organizzazioni affrontano e può essere utilizzata durante tutta la vita dell'organizzazione, oltre a poter essere applicata a qualsiasi attività, compreso il processo decisionale a tutti i livelli.
- L'approccio comune suggerito dal documento è idoneo a gestire qualsiasi tipo di rischio, non è dedicato ad un particolare settore o industria e può essere adattato a qualunque organizzazione e al suo contesto.


INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

ISO

Reference number
ISO 31000:2018(E)

ISO 31000:2018 – Premesse

- La gestione del rischio è una procedura iterativa che assiste le organizzazioni nel definire le strategie, raggiungere gli obiettivi e prendere decisioni informate.

ISO 31000:2018 – Premesse

- La gestione del rischio è una procedura iterativa che assiste le organizzazioni nel definire le strategie, raggiungere gli obiettivi e prendere decisioni informate.
- La gestione del rischio è parte integrante delle azioni di governance e di leadership e la sua efficacia dipende fortemente dalle modalità con cui l'organizzazione è gestita a tutti i livelli. Essa contribuisce al miglioramento complessivo dei sistemi di gestione dell'organizzazione.

ISO 31000:2018 – Premesse

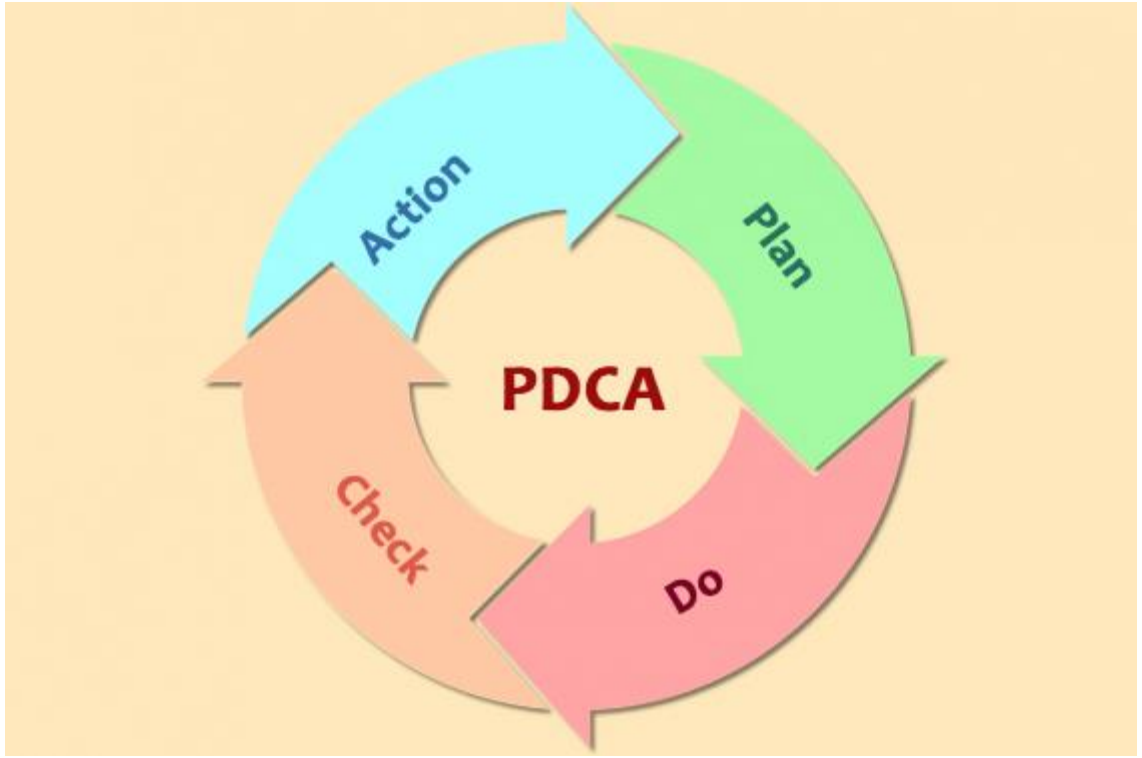
- La gestione del rischio è una procedura iterativa che assiste le organizzazioni nel definire le strategie, raggiungere gli obiettivi e prendere decisioni informate.
- La gestione del rischio è parte integrante delle azioni di governance e di leadership e la sua efficacia dipende fortemente dalle modalità con cui l'organizzazione è gestita a tutti i livelli. Essa contribuisce al miglioramento complessivo dei sistemi di gestione dell'organizzazione.
- La gestione del rischio entra in tutte le attività dell'organizzazione ed include l'interazione con tutti i soggetti interessati (stakeholder).

ISO 31000:2018 – Premesse

- La gestione del rischio è una procedura iterativa che assiste le organizzazioni nel definire le strategie, raggiungere gli obiettivi e prendere decisioni informate.
- La gestione del rischio è parte integrante delle azioni di governance e di leadership e la sua efficacia dipende fortemente dalle modalità con cui l'organizzazione è gestita a tutti i livelli. Essa contribuisce al miglioramento complessivo dei sistemi di gestione dell'organizzazione.
- La gestione del rischio entra in tutte le attività dell'organizzazione ed include l'interazione con tutti i soggetti interessati (stakeholder).
- La gestione del rischio considera il contesto interno ma anche esterno all'organizzazione, includendo il comportamento umano ed i fattori culturali.

Ciclo di Deming

- La norma ISO 31000 prevede un processo di miglioramento continuo. Utilizzando il modello di Deming, il sistema può migliorare continuamente.



ISO 31000:2018 - Processo di gestione del rischio

- La norma **ISO 31000:2018** *Risk management — Guidelines* definisce tutte le attività **concrete** necessarie per sviluppare una metodologia efficiente per la gestione del rischio
- Il processo è iterativo, piuttosto che sequenziale

1° STEP – Context Establishment

- Definire le informazioni di base necessarie per la gestione del rischio:
  - lo scopo, gli obiettivi, i risultati attesi
  - l'approccio, gli strumenti e le tecniche per valutare il rischio
  - i criteri di accettazione del rischio

2° STEP – Risk Assessment

- È il processo di identificazione, stima e prioritizzazione dei rischi relativi alla sicurezza delle informazioni
- Lo scopo è quello di quantificare o descrivere qualitativamente i rischi così da dare priorità a determinate azioni in base ai criteri stabiliti nel 1° step

3° STEP – Risk Treatment

- Consiste nel definire un piano di trattamento tramite un elenco di controlli per affrontare i rischi
- Il piano di trattamento coinvolge misure per ridurre, conservare o evitare i rischi, oltre a misure per la valutazione dell'effettiva efficacia delle misure di trattamento messe in atto

4° STEP – Risk Acceptance

- Consiste nella decisione di accettare i rischi e nella definizione delle responsabilità correlate
- L'organizzazione stabilisce un elenco di rischi consapevolmente accettati, con un'eventuale giustificazione per i rischi che non soddisfano i criteri di accettazione del 1° step

5° STEP – Risk Communication

- È di cruciale importanza che le informazioni riguardo i rischi vengano scambiate e condivise tra chi gestisce i processi di gestione del rischio e tutte le altre parti interessate
- Tutti i risultati del processo dovrebbero anche essere ben documentati con metodologie prestabilite

6° STEP – Risk Monitoring and Review

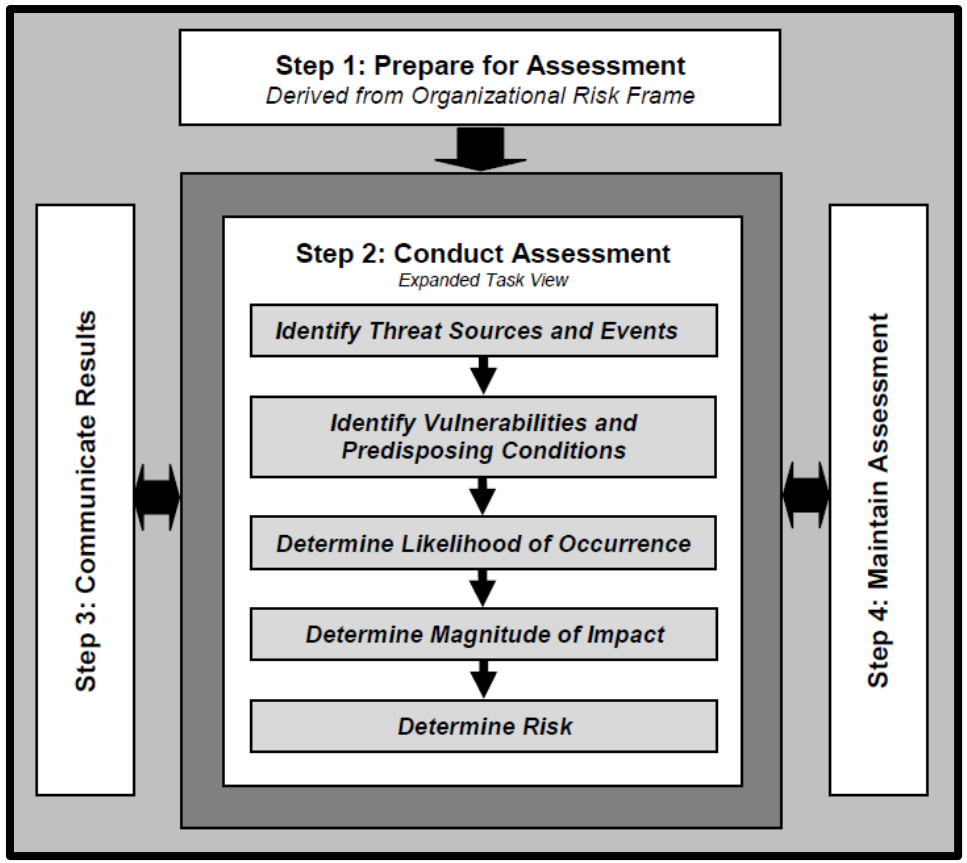
- Lo scopo è quello di testare e di migliorare la qualità e l'efficacia del processo di gestione del rischio. Il monitoraggio e la revisione includono pianificare, raccogliere e analizzare le informazioni, registrare i risultati e fornire feedback
- Il monitoraggio e la revisione dovrebbero avvenire in tutte le fasi del processo

Risk Assessment: una premessa

- Il risk assessment non usa strumenti di misurazione precisi e riflette:
  - i **limiti** delle metodologie, degli strumenti e delle tecniche di valutazione specifiche utilizzate;
  - la **soggettività**, la qualità e l'affidabilità dei dati utilizzati
  - l'**interpretazione** dei risultati della valutazione;
  - le **capacità** e le **competenze** delle persone o dei gruppi che conducono le valutazioni.

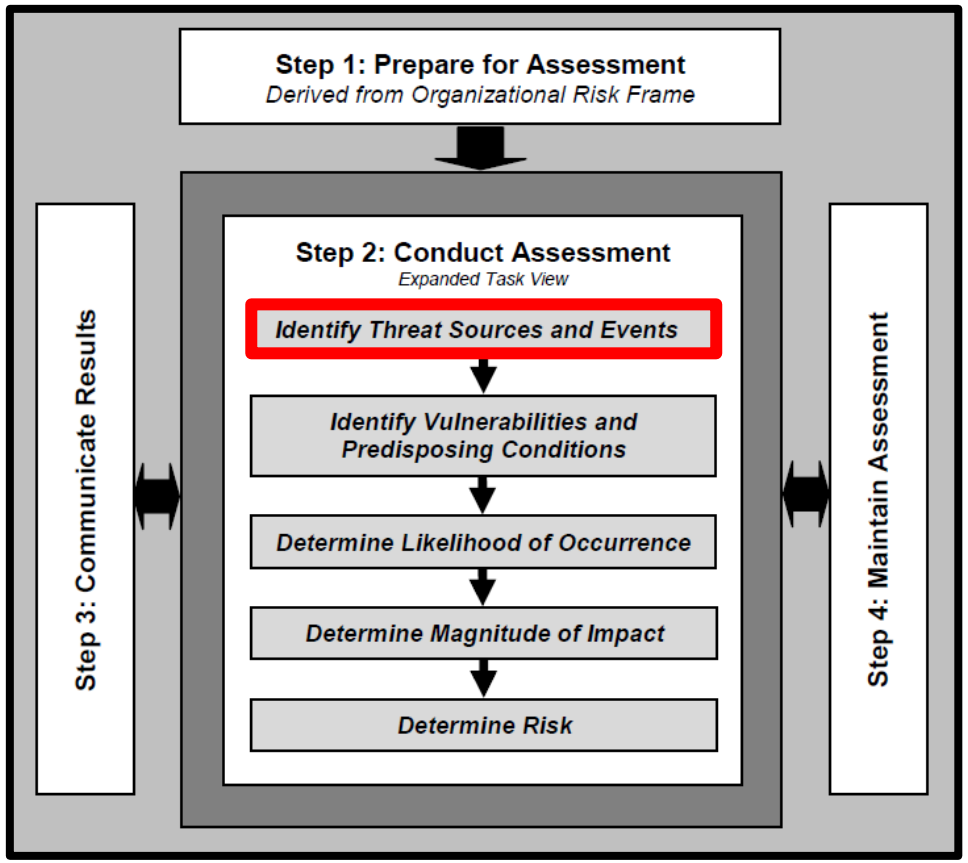
Risk Assessment

- Valutare il rischio significa analizzare le **minacce** e le **vulnerabilità** dell'infrastruttura in esame con lo scopo di determinare la **probabilità** che si verifichino eventi che potrebbero avere un **impatto** negativo sull'organizzazione



NIST SP 800-30r1, Guide for Conducting Risk Assessments

Risk Assessment

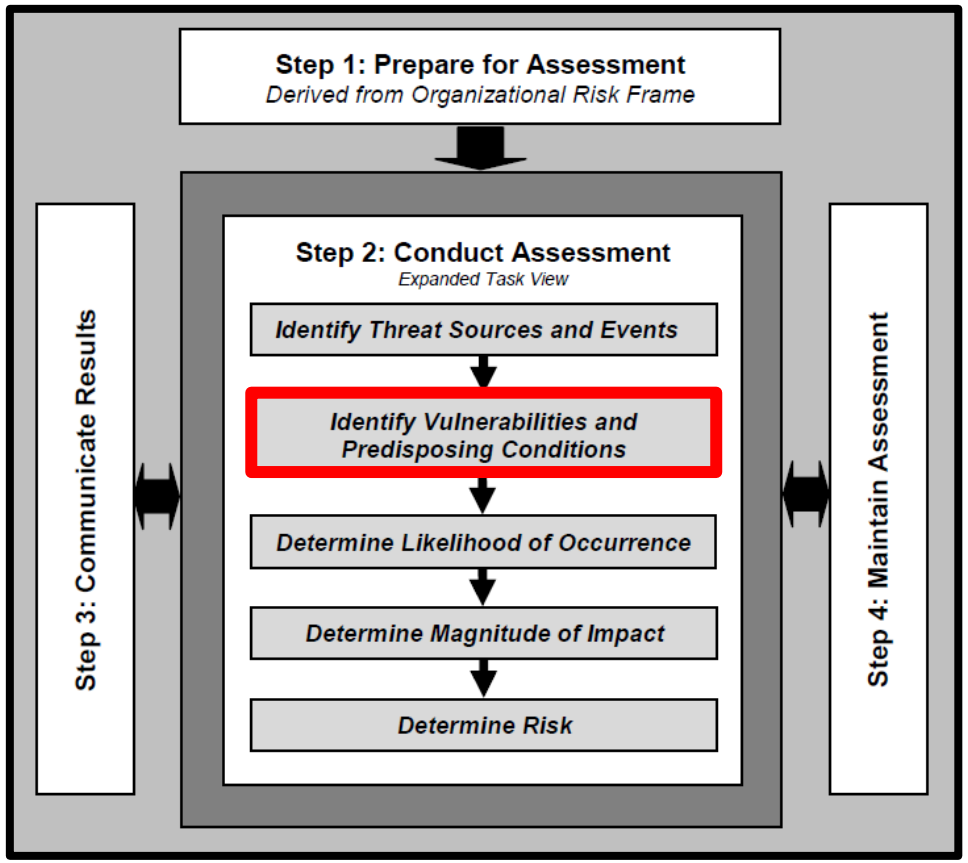


NIST SP 800-30r1, Guide for Conducting Risk Assessments

1. Identificare le minacce

- È richiesto di stilare una lista di tutte le possibili minacce che l'organizzazione può incontrare
- La minaccia è la *causa scatenante*, è l'elemento che potenzialmente innesca un rischio
- Le minacce sono eventi spesso non controllabili

Risk Assessment

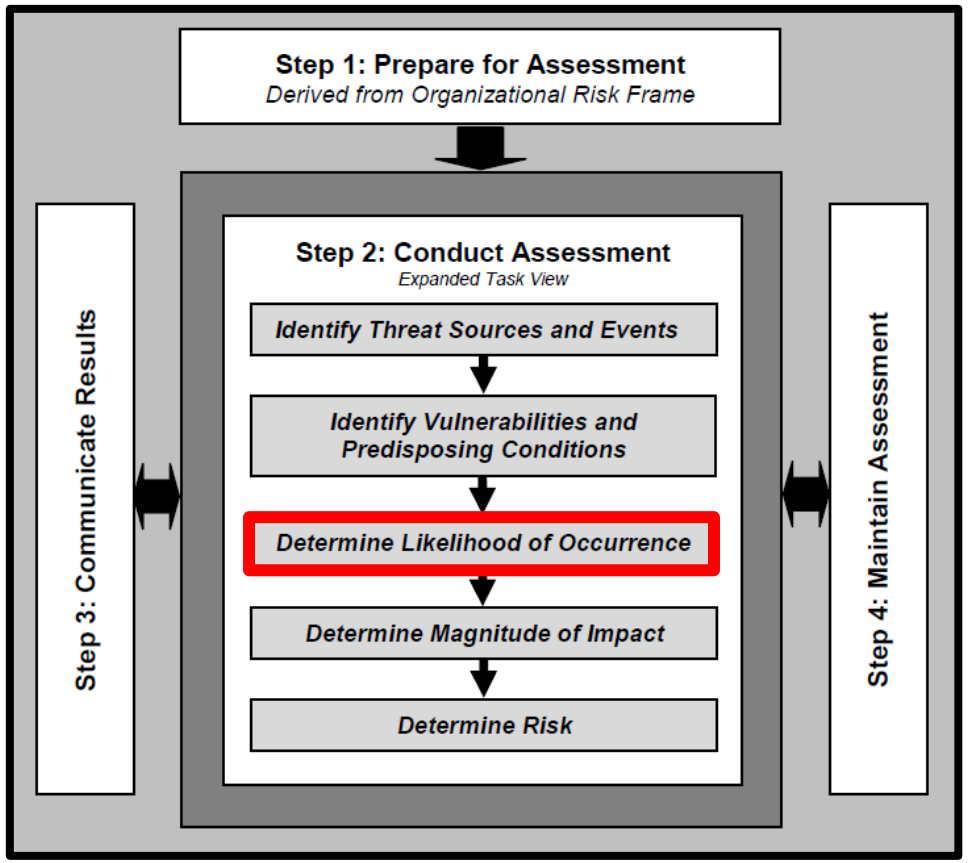


NIST SP 800-30r1, Guide for Conducting Risk Assessments

2. Identificare le vulnerabilità e i fattori predisponenti

- Elencare tutte le vulnerabilità di un'organizzazione
- Una vulnerabilità è una *debolezza interna all'infrastruttura tecnologica* di un'organizzazione che può essere utilizzata da una minaccia per causare un danno all'organizzazione
- Solitamente, le vulnerabilità sono controllabili

Risk Assessment

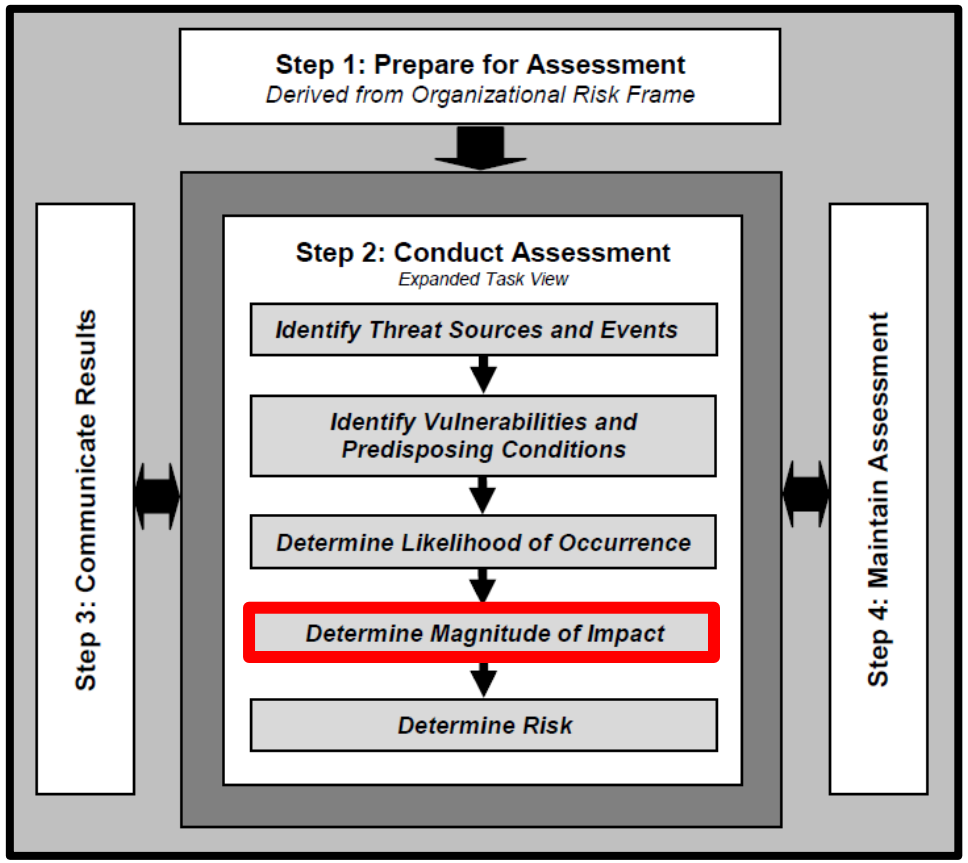


NIST SP 800-30r1, Guide for Conducting Risk Assessments

3. Determinare la probabilità di accadimento

- Significa stimare la probabilità con cui una determinata minaccia si verificherà in un periodo di tempo
- La stima della probabilità di accadimento va ripetuta **per ogni minaccia** identificata al 1° step, tenendo in considerazione le vulnerabilità evidenziate al 2° step

Risk Assessment

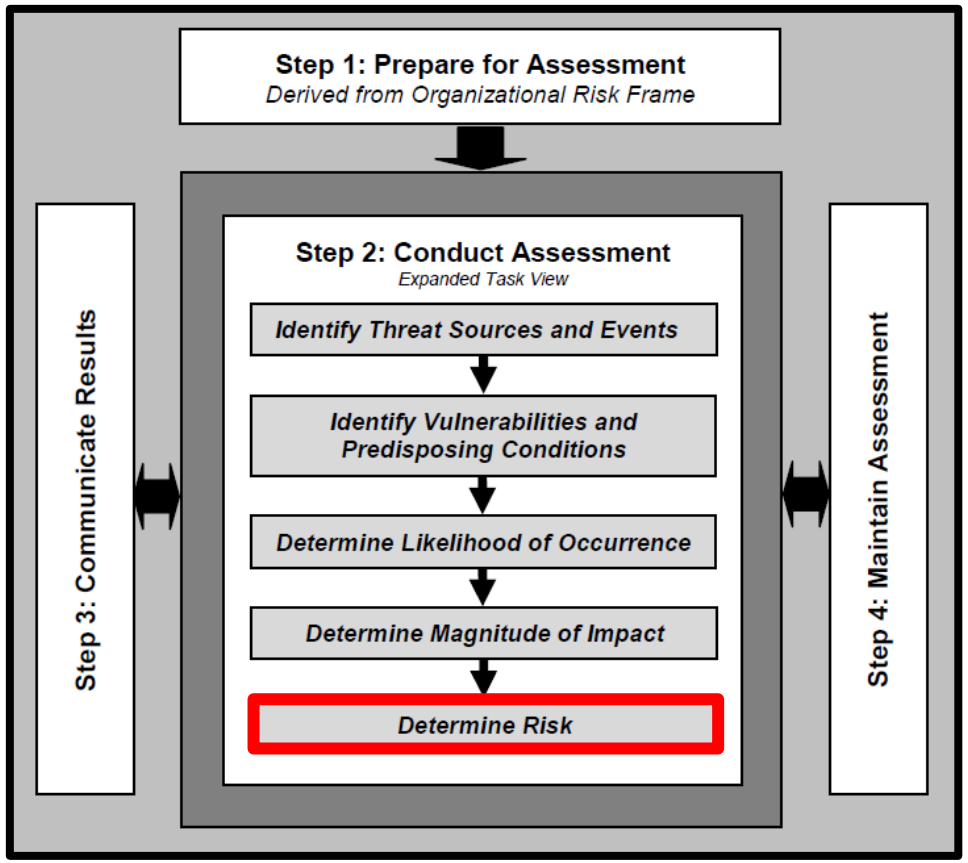


NIST SP 800-30r1, Guide for Conducting Risk Assessments

4. Determinare l'entità dell'impatto

- Significa stimare l'entità e la gravità delle conseguenze, in termini di perdite economiche, che l'organizzazione deve affrontare nel caso in cui una minaccia accada
- Anche la stima degli impatti va ripetuta per ogni minaccia identificata al primo step

Risk Assessment



NIST SP 800-30r1, Guide for Conducting Risk Assessments

5. Determinare il rischio

- L'ultimo step è determinare effettivamente il rischio
- Il rischio è definito come una combinazione della probabilità di accadimento e dell'impatto

$$R=P\times I$$

Analisi del rischio

- Il rischio è una combinazione di probabilità e di gravità:

$$R = P \times Vu \times Val$$

P = Probabilità dell'attacco

Vu = Vulnerabilità all'attacco

Val = Valore del danno provocato nel caso in cui l'attacco abbia successo

Come fare?

- La valutazione del rischio può essere effettuata attraverso molti approcci differenti
- Le norme e gli standard forniscono delle indicazioni su come, in generale, valutare i rischi **MA** non forniscono degli strumenti per farlo
- Molti strumenti sono stati sviluppati sia da enti nazionali e internazionali, sia nella letteratura scientifica
  - Generalmente questi strumenti possono essere divisi in QUALITATIVI o QUANTITATIVI

Metodi QUALITATIVI

- La *valutazione qualitativa* utilizza tipicamente una serie di metodi, principi o regole basati su categorie o livelli non numerici per la valutazione del rischio

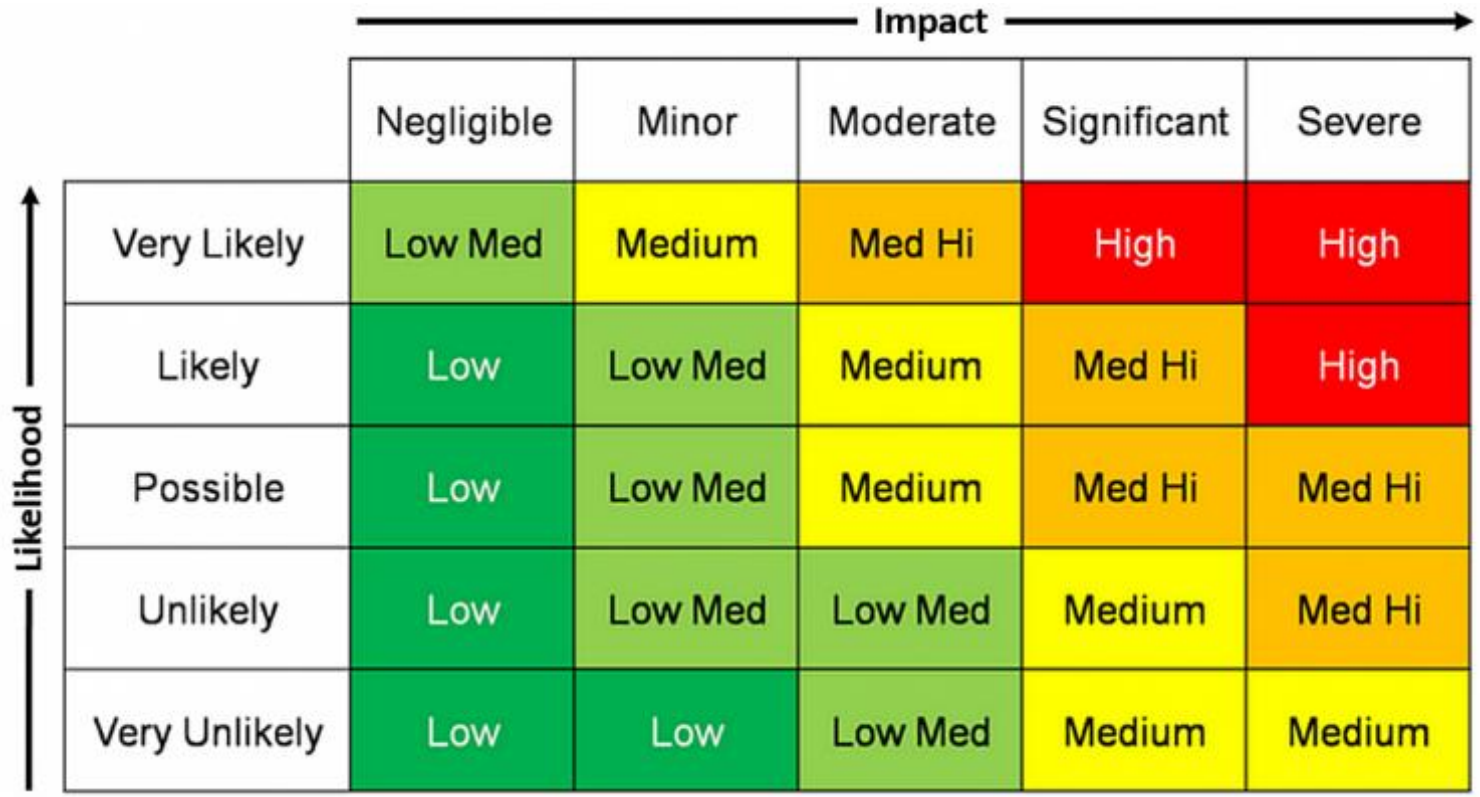
PRO

- Efficienti in termini di tempo e costi, poiché non richiedono la stima di valori esatti
- Possono essere utilizzati per identificare facilmente le possibili aree di miglioramento

CONTRO

- Esperti diversi potrebbero produrre risultati significativamente diversi
- Riprodurre o confrontare i risultati può essere difficile, spesso impossibile

Matrici di rischio



Metodi QUANTITATIVI

- La *valutazione quantitativa* utilizza tipicamente una serie di metodi, principi o regole per la valutazione del rischio basati sull'uso di numeri

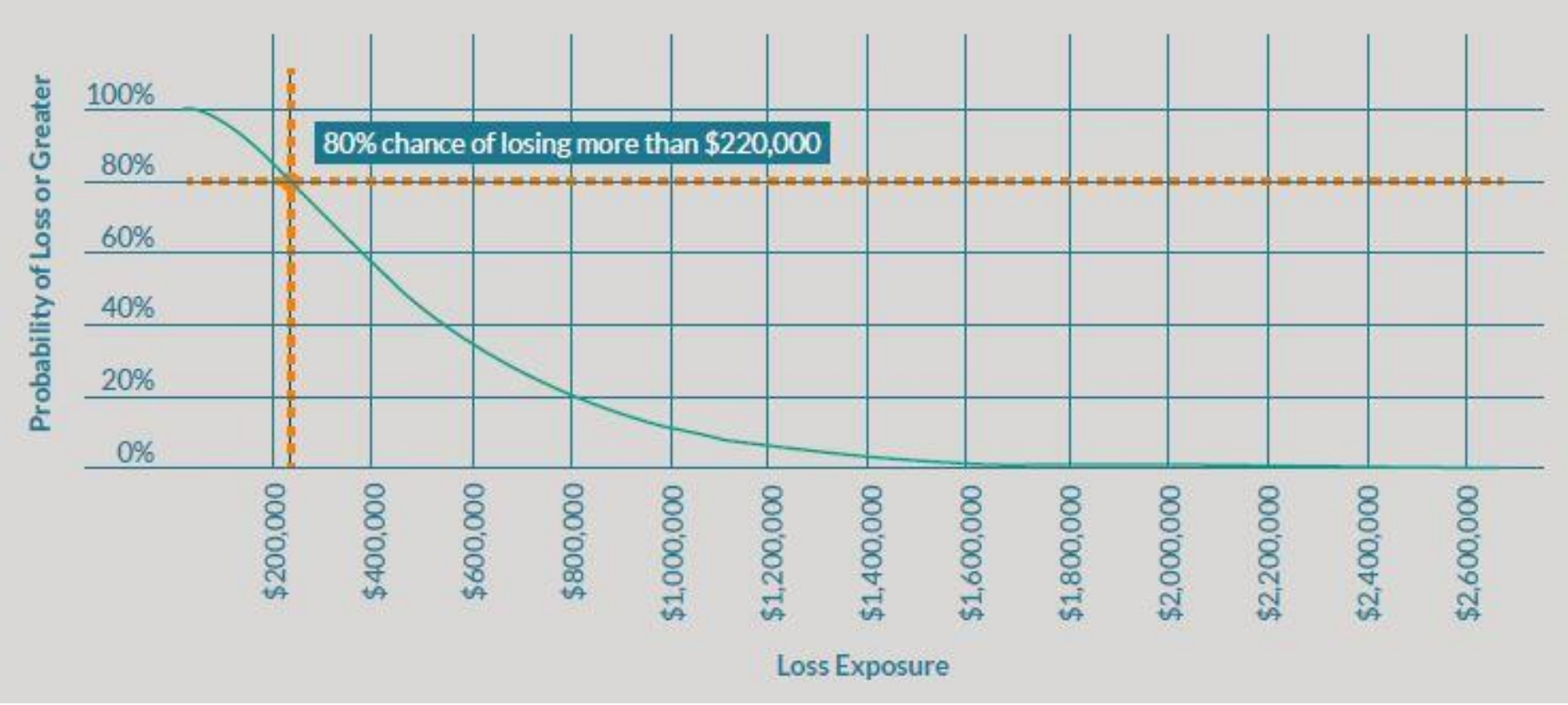
PRO

- I risultati della valutazione quantitativa sono rigorosi, ripetibili e riproducibili
- La stima delle probabilità e degli impatti degli eventi può essere confrontata in modo diretto e oggettivo

CONTRO

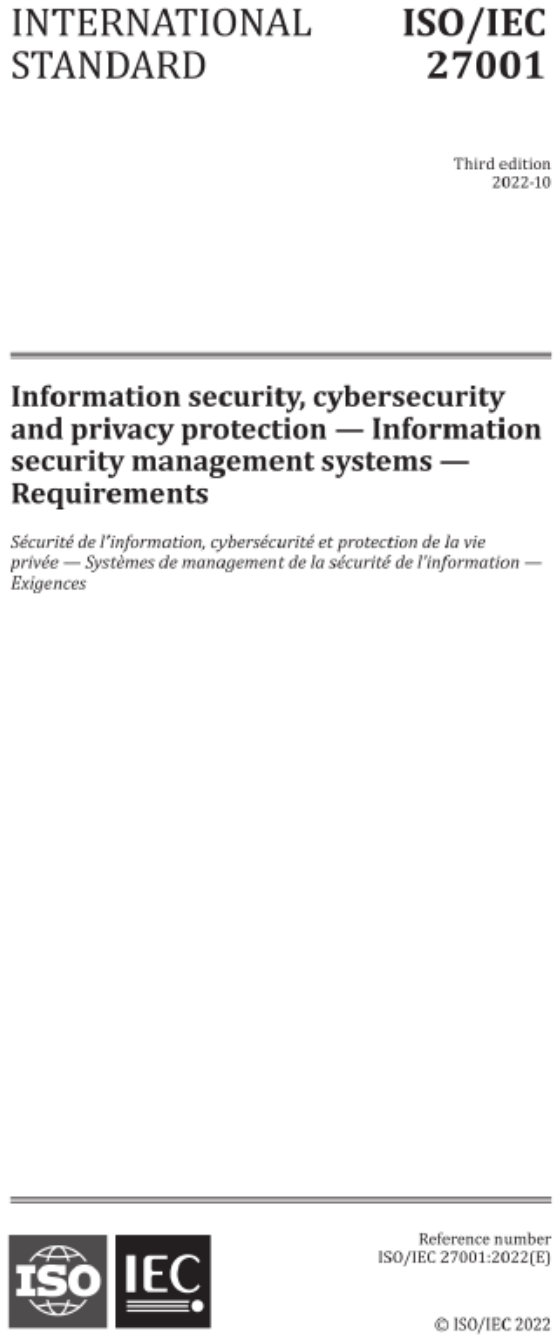
- La stima delle probabilità e degli impatti è molto impegnativa e i risultati potrebbero non essere sempre chiari
- I benefici possono non essere bilanciati dai costi e dalla possibilità di disporre di strumenti per effettuare le necessarie valutazioni

Curve di perdita



Serie di norme ISO 27000

- La ISO/IEC 27001:2022 è uno **standard internazionale** che presenta determinati requisiti per la creazione, la manutenzione e lo sviluppo dei **sistemi di gestione della sicurezza delle informazioni** (ISMS - Information Security Management System).


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

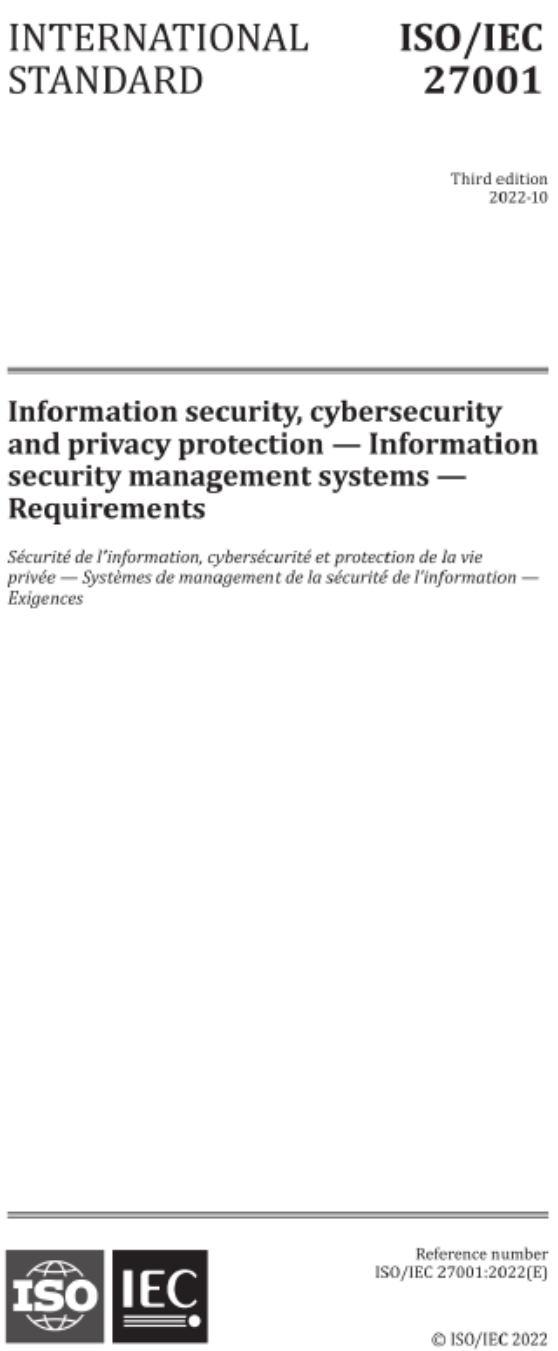
ISO IEC

Reference number
ISO/IEC 27001:2022(E)

Serie di norme ISO 27000

- La ISO/IEC 27001:2022 è uno **standard internazionale** che presenta determinati requisiti per la creazione, la manutenzione e lo sviluppo dei **sistemi di gestione della sicurezza delle informazioni** (ISMS - Information Security Management System).

- La ISO 27001 è applicabile a tutte le organizzazioni, indipendentemente dalla loro dimensione, tipo o natura e si concentra sulla protezione di tre aspetti chiave delle informazioni: riservatezza (**c**onfidentiality), integrità (**i**ntegrity) e disponibilità (**a**vailability).


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

Serie di norme ISO 27000

- La presenza di un robusto sistema Information Security Management System (ISMS), che rappresenta una piattaforma aziendale d'importanza cruciale, aiuta a proteggere i sistemi informativi di un'azienda dagli attacchi cyber, che costituiscono una crescente minaccia per qualsiasi organizzazione provvista di un data center o anche, semplicemente, collegata alla rete Internet.


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

Serie di norme ISO 27000

- La norma ISO 27002:2022 è una raccolta di *best practices* adottabili per soddisfare i requisiti della norma ISO 27001:2022, al fine di proteggere le risorse informative.


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number
ISO/IEC 27002:2022(E)

Serie di norme ISO 27000

- La norma ISO 27002:2022 è una raccolta di *best practices* che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2022, al fine di proteggere le risorse informative.

- ISO 27001 è il documento normativo di certificazione al quale l'organizzazione deve fare riferimento per costruire un ISMS che possa essere certificato da un ente indipendente, mentre la norma ISO 27002 non è certificabile in quanto è una raccolta di raccomandazioni.


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number
ISO/IEC 27002:2022(E)

Controlli CIS (Center for Internet Security)

- I controlli CIS sono un insieme di azioni che costituiscono una serie di best practices difensive che mitigano gli attacchi più comuni contro i sistemi e le reti.

Controlli CIS (Center for Internet Security)

- I controlli CIS sono un insieme di azioni che costituiscono una serie di best practices difensive che mitigano gli attacchi più comuni contro i sistemi e le reti.

- Queste attività assicurano che i controlli CIS siano una serie di azioni prioritarie e altamente focalizzate che siano riconosciute valide dalla comunità così da renderle implementabili, utilizzabili, scalabili e conformi a tutti i requisiti richiesti sia a livello industriale che governativo.

Controlli CIS (Center for Internet Security)

- I controlli CIS sono un insieme di azioni che costituiscono una serie di best practices difensive che mitigano gli attacchi più comuni contro i sistemi e le reti.

- Queste attività assicurano che i controlli CIS siano una serie di azioni prioritarie e altamente focalizzate che siano riconosciute valide dalla comunità così da renderle implementabili, utilizzabili, scalabili e conformi a tutti i requisiti richiesti sia a livello industriale che governativo.

- I controlli CIS sono stati sviluppati sulla base di attacchi reali e su comprovate difese efficaci; questi riflettono la combinazione di conoscenza di esperti provenienti da ogni parte dell'ecosistema, da ogni profilo professionale, da ogni settore, che si sono uniti per creare, adottare e supportare i controlli.

Controlli CIS (Center for Internet Security)

- CIS raccomanda i *Gruppi di Implementazione*, nuove linee guida per dare priorità nell'utilizzo dei Controlli CIS, incentrate sul bilanciamento dei vincoli delle risorse e sull'efficace riduzione del rischio.

Controlli CIS (Center for Internet Security)

- CIS raccomanda i *Gruppi di Implementazione*, nuove linee guida per dare priorità nell'utilizzo dei Controlli CIS, incentrate sul bilanciamento dei vincoli delle risorse e sull'efficace riduzione del rischio.

- I *Gruppi di Implementazione* dei Controlli CIS (*IGs*) sono categorie autovalutate dalle organizzazioni in base agli attributi di cybersecurity pertinenti. Ogni IG identifica un sottoinsieme dei Controlli CIS adeguati al profilo di rischio di un'organizzazione e le relative risorse da impiegare per attuarli.

Controlli CIS

- I criteri utilizzati dalle organizzazioni per identificare la loro categoria organizzativa si basano su:

- Sensibilità dei dati e criticità dei servizi offerti dall'organizzazione.
- Livello atteso di competenza tecnica dimostrato dal personale.
- Risorse disponibili e dedicate alle attività di cybersecurity.

Controlli CIS

- Ogni IG si basa su quello precedente.
- Pertanto, IG2 include IG1 e IG3 include tutti i sotto-controlli CIS in IG1 e IG2.
- CIS raccomanda alle organizzazioni di dare la priorità alla loro attuazione dei controlli seguendo le IG.
- Le organizzazioni dovrebbero implementare i sotto-controlli in IG1, seguiti da IG2 e quindi IG3.
- I sotto-controlli contenuti in IG1 sono quelli essenziali.
- L'implementazione di IG1 dovrebbe quindi essere considerata tra le prime cose da fare nell'ambito di un programma di cybersecurity.

Controlli CIS

- **Gruppo di Implementazione 1**
  - Un'organizzazione IG1 è di dimensioni medio-piccole con competenze IT e di cybersecurity limitate che può dedicare alla protezione delle risorse poco personale.

Controlli CIS

- **Gruppo di Implementazione 1**
  - Un'organizzazione IG1 è di dimensioni medio-piccole con competenze IT e di cybersecurity limitate che può dedicare alla protezione delle risorse poco personale.
  - La principale preoccupazione di queste organizzazioni è di mantenere l'operatività a causa della limitata tolleranza dei tempi di fermo.

Controlli CIS

- **Gruppo di Implementazione 1**
  - Un'organizzazione IG1 è di dimensioni medio-piccole con competenze IT e di cybersecurity limitate che può dedicare alla protezione delle risorse poco personale.
  - La principale preoccupazione di queste organizzazioni è di mantenere l'operatività a causa della limitata tolleranza dei tempi di fermo.
  - La sensibilità dei dati che stanno cercando di proteggere è bassa e limitata principalmente alle informazioni finanziarie e dei dipendenti.

Controlli CIS

- **Gruppo di Implementazione 1**
  - Un'organizzazione IG1 è di dimensioni medio-piccole con competenze IT e di cybersecurity limitate che può dedicare alla protezione delle risorse poco personale.
  - La principale preoccupazione di queste organizzazioni è di mantenere l'operatività a causa della limitata tolleranza dei tempi di fermo.
  - La sensibilità dei dati che stanno cercando di proteggere è bassa e limitata principalmente alle informazioni finanziarie e dei dipendenti.
  - I sub-controlli previsti al livello IG1 dovrebbero essere implementabili con competenze di cybersecurity limitate e mirati a contrastare attacchi generici non mirati.

Controlli CIS

- **Gruppo di Implementazione 2**
  - Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.

Controlli CIS

- **Gruppo di Implementazione 2**
  - Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.
  - Queste organizzazioni supportano più dipartimenti con profili di rischio diversi in base alla funzione lavorativa e alla missione.

Controlli CIS

- **Gruppo di Implementazione 2**
  - Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.
  - Queste organizzazioni supportano più dipartimenti con profili di rischio diversi in base alla funzione lavorativa e alla missione.
  - Le organizzazioni IG2 spesso archiviano ed elaborano le informazioni sensibili dei clienti o dell'azienda e possono resistere a brevi interruzioni del servizio.

Controlli CIS

➢ **Gruppo di Implementazione 2**

- Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.
- Queste organizzazioni supportano più dipartimenti con profili di rischio diversi in base alla funzione lavorativa e alla missione.
- Le organizzazioni IG2 spesso archiviano ed elaborano le informazioni sensibili dei clienti o dell'azienda e possono resistere a brevi interruzioni del servizio.
- Una delle maggiori preoccupazioni è la perdita della fiducia dell'utenza in caso di violazione.

Controlli CIS

➢ **Gruppo di Implementazione 2**

- Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.
- Queste organizzazioni supportano più dipartimenti con profili di rischio diversi in base alla funzione lavorativa e alla missione.
- Le organizzazioni IG2 spesso archiviano ed elaborano le informazioni sensibili dei clienti o dell'azienda e possono resistere a brevi interruzioni del servizio.
- Una delle maggiori preoccupazioni è la perdita della fiducia dell'utenza in caso di violazione.
- I sub-controlli selezionati per IG2 aiutano i team di sicurezza ad affrontare una maggiore complessità operativa.

Controlli CIS

➢ Gruppo di Implementazione 2

- Un'organizzazione IG2 impiega persone responsabili della gestione e della protezione dell'infrastruttura IT.
- Queste organizzazioni supportano più dipartimenti con profili di rischio diversi in base alla funzione lavorativa e alla missione.
- Le organizzazioni IG2 spesso archiviano ed elaborano le informazioni sensibili dei clienti o dell'azienda e possono resistere a brevi interruzioni del servizio.
- Una delle maggiori preoccupazioni è la perdita della fiducia dell'utenza in caso di violazione.
- I sub-controlli selezionati per IG2 aiutano i team di sicurezza ad affrontare una maggiore complessità operativa.
- Alcuni controlli secondari dipenderanno dalla tecnologia, dal livello aziendale e dalle competenze necessarie per le installazioni e le configurazioni.

Controlli CIS

- **Gruppo di Implementazione 3**
- Un'organizzazione IG3 impiega esperti di sicurezza specializzati nei diversi aspetti della cybersecurity (ad es. gestione dei rischi, test di penetrazione, sicurezza delle applicazioni).

Controlli CIS

- **Gruppo di Implementazione 3**
  - Un'organizzazione IG3 impiega esperti di sicurezza specializzati nei diversi aspetti della cybersecurity (ad es. gestione dei rischi, test di penetrazione, sicurezza delle applicazioni).
  - I sistemi e i dati IG3 contengono informazioni sensibili o funzioni soggette a controllo regolamentate da norme.

Controlli CIS

- **Gruppo di Implementazione 3**
  - Un'organizzazione IG3 impiega esperti di sicurezza specializzati nei diversi aspetti della cybersecurity (ad es. gestione dei rischi, test di penetrazione, sicurezza delle applicazioni).
  - I sistemi e i dati IG3 contengono informazioni sensibili o funzioni soggette a controllo regolamentate da norme.
  - Un'organizzazione IG3 deve occuparsi della disponibilità dei servizi e della riservatezza e integrità dei dati sensibili.

Controlli CIS

- **Gruppo di Implementazione 3**
  - Un'organizzazione IG3 impiega esperti di sicurezza specializzati nei diversi aspetti della cybersecurity (ad es. gestione dei rischi, test di penetrazione, sicurezza delle applicazioni).
  - I sistemi e i dati IG3 contengono informazioni sensibili o funzioni soggette a controllo regolamentate da norme.
  - Un'organizzazione IG3 deve occuparsi della disponibilità dei servizi e della riservatezza e integrità dei dati sensibili.
  - Gli attacchi riusciti possono causare danni significativi all'interesse pubblico.

Controlli CIS

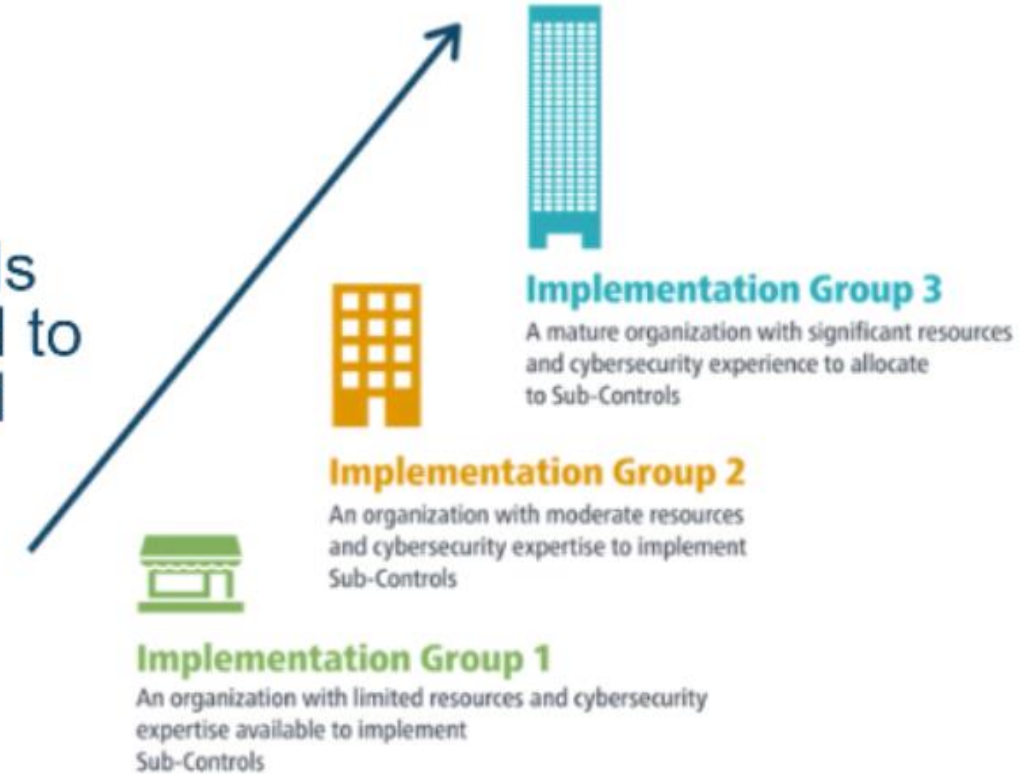
➢ **Gruppo di Implementazione 3**

- Un'organizzazione IG3 impiega esperti di sicurezza specializzati nei diversi aspetti della cybersecurity (ad es. gestione dei rischi, test di penetrazione, sicurezza delle applicazioni).
- I sistemi e i dati IG3 contengono informazioni sensibili o funzioni soggette a controllo regolamentate da norme.
- Un'organizzazione IG3 deve occuparsi della disponibilità dei servizi e della riservatezza e integrità dei dati sensibili.
- Gli attacchi riusciti possono causare danni significativi all'interesse pubblico.
- I sotto-controlli selezionati per IG3 devono ridurre gli attacchi mirati da un avversario sofisticato.

Controlli CIS

Building Groups

The number of Sub-Controls an organization is expected to implement increases based on which group an organization falls into



Controlli CIS

1. *Inventario e Controllo delle Risorse Aziendali* - Gestire attivamente (inventariare, tracciare e correggere) tutte le risorse aziendali (dispositivi dell'utente finale, mobili e portatili inclusi, dispositivi di rete, dispositivi non informatici/ Internet of Things – IoT e server) connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette in azienda. Ciò aiuterà anche nell'identificare quelle non autorizzate e non gestite, da rimuovere o aggiornare.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
1.1	**Stabilire e Mantenere un Inventario Dettagliato delle Risorse Aziendali** Stabilire e mantenere un inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati, includendo: dispositivi dell'utente finale (compresi portatili e mobili), dispositivi di rete, dispositivi non informatici/IoT e server. Assicurare che l'inventario registri l'indirizzo di rete (se statico), l'indirizzo hardware, il nome del computer, il proprietario della risorsa aziendale, il reparto per ogni risorsa e se la risorsa è stata approvata per la connessione alla rete. Per i dispositivi mobili degli utenti finali, gli strumenti di tipo MDM possono supportare questo processo. Questo inventario include le risorse connesse all'infrastruttura fisica, virtuale, remota e quelle all'interno di ambienti cloud. Include inoltre le risorse che sono regolarmente connesse all'infrastruttura di rete dell'impresa, anche se non sono sotto il suo controllo. Rivedere e aggiornare l'inventario di tutte le risorse aziendali semestralmente o più frequentemente.	Dispositivi	Identificare	●	●	●
1.2	**Trattare le Risorse non Autorizzate** Assicurare la presenza di un processo per trattare le risorse non autorizzate su base settimanale. L'azienda può scegliere di rimuovere la risorsa dalla rete, bloccarne la connessione remota o metterla in quarantena.	Dispositivi	Rispondere	●	●	●
1.3	**Utilizzare uno Strumento di Rilevamento Attivo** Utilizzare uno strumento di rilevamento attivo per identificare le risorse connesse alla rete aziendale. Configurarlo per l'esecuzione quotidiana o più frequente.	Dispositivi	Rilevare		●	●
1.4	**Utilizzare i log del Protocollo Dinamico di Configurazione Host (DHCP)** Utilizzare i log su tutti i server DHCP o altri strumenti di gestione degli indirizzi IP (Internet Protocol) per aggiornare l'inventario delle risorse aziendali. Rivedere ed utilizzare i registri per aggiornare l'inventario delle risorse settimanalmente o più frequentemente.	Dispositivi	Identificare		●	●
1.5	**Utilizzare uno Strumento di Rilevazione Passiva** Utilizzare uno strumento di rilevazione passiva per identificare le risorse connesse alla rete aziendale. Rivedere e utilizzare le scansioni per aggiornare l'inventario delle risorse almeno una volta alla settimana o più frequentemente.	Dispositivi	Rilevare			●

Controlli CIS

2. *Inventario e Controllo delle Risorse Software* - Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.

Controlli CIS

2. *Inventario e Controllo delle Risorse Software* - Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.
3. *Protezione dei dati* - Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.

Controlli CIS

2. *Inventario e Controllo delle Risorse Software* - Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.
3. *Protezione dei dati* - Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.
4. *Configurazione sicura delle risorse aziendali e del software* - Stabilire e mantenere la configurazione sicura delle risorse aziendali (dispositivi dell'utente finale, inclusi portatili e mobili, dispositivi di rete, dispositivi non informatici / IoT, server) e software (sistemi operativi e applicazioni).

Controlli CIS

2. *Inventario e Controllo delle Risorse Software* - Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.
3. *Protezione dei dati* - Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.
4. *Configurazione sicura delle risorse aziendali e del software* - Stabilire e mantenere la configurazione sicura delle risorseaziendali (dispositivi dell'utente finale, inclusi portatili e mobili, dispositivi di rete, dispositivi non informatici / IoT, server) e software (sistemi operativi e applicazioni).
5. *Gestione degli account* - Utilizzare procedure e strumenti per assegnare e gestire l'autorizzazione a risorse e software aziendali, per gli account utente, inclusi quelli amministrativi e di servizio.

Controlli CIS

6. *Gestione del controllo degli accessi* - Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.

Controlli CIS

6. *Gestione del controllo degli accessi* - Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.
7. *Gestione continua delle vulnerabilità* - Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.

Controlli CIS

6. *Gestione del controllo degli accessi* - Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.
7. *Gestione continua delle vulnerabilità* - Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.
8. *Gestione dei log di controllo* - Raccogliere, avvisare, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o rimediare in seguito ad un attacco.

Controlli CIS

6. *Gestione del controllo degli accessi* - Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.
7. *Gestione continua delle vulnerabilità* - Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.
8. *Gestione dei log di controllo* - Raccogliere, avvisare, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o rimediare in seguito ad un attacco.
9. *Protezione della Posta Elettronica e del Browser Web* - Migliorare le protezioni ed il rilevamento delle minacce provenienti dalle e-mail e da vettori web, che danno l'opportunità agli aggressori di manipolare il comportamento umano sfruttandone il diretto coinvolgimento.

Controlli CIS

10. *Difesa dal Malware* - Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.

Controlli CIS

10. *Difesa dal Malware* - Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.
11. *Recupero dei dati* - Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.

Controlli CIS

10. *Difesa dal Malware* - Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.
11. *Recupero dei dati* - Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.
12. *Gestione dell'infrastruttura di rete* - Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.

Controlli CIS

10. *Difesa dal Malware* - Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.
11. *Recupero dei dati* - Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.
12. *Gestione dell'infrastruttura di rete* - Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.
13. *Monitoraggio e difesa della rete* - Adottare processi e strumenti per stabilire e mantenere un monitoraggio completo della rete e una difesa contro le minacce alla sicurezza dell'infrastruttura di rete aziendale e agli utenti.

Controlli CIS

10. *Difesa dal Malware* - Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.
11. *Recupero dei dati* - Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.
12. *Gestione dell'infrastruttura di rete* - Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.
13. *Monitoraggio e difesa della rete* - Adottare processi e strumenti per stabilire e mantenere un monitoraggio completo della rete e una difesa contro le minacce alla sicurezza dell'infrastruttura di rete aziendale e agli utenti.
14. *Sensibilizzazione e formazione sulle competenze di sicurezza* - Stabilire e mantenere un programma di sensibilizzazione alla sicurezza per istruire il personale affinché sia consapevole ed adeguatamente preparato per ridurre i rischi di sicurezza informatica aziendali.

Controlli CIS

15. Gestione dei service provider - Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.

Controlli CIS

15. *Gestione dei service provider* - Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.
16. *Sicurezza degli applicativi* – Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull’azienda.

Controlli CIS

15. *Gestione dei service provider* - Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.
16. *Sicurezza degli applicativi* – Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull'azienda.
17. *Gestione e risposta agli incidenti* - Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad esempio criteri, piani, procedure, ruoli definiti, formazione e comunicazioni) per prepararsi a rilevare e rispondere rapidamente ad un attacco.

Controlli CIS

15. *Gestione dei service provider* - Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.
16. *Sicurezza degli applicativi* – Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull'azienda.
17. *Gestione e risposta agli incidenti* - Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad esempio criteri, piani, procedure, ruoli definiti, formazione e comunicazioni) per prepararsi a rilevare e rispondere rapidamente ad un attacco.
18. *Test di penetrazione* - Verificare l'efficacia e la resilienza delle risorse aziendali identificando e sfruttando i punti deboli nei controlli (persone, processi e tecnologia) e simulando obiettivi ed azioni di un utente malintenzionato.