Cyber Risk Management

Iniziamo questo capitolo facendoci una prima domanda fondamentale: “**Perchè un’organizzazione dovrebbe implementare un piano di Risk Management?**”"Un’organizzazione dovrebbe implementare un piano di Risk Management, perchè negli ultimi anni gli attacchi informatici sono cresciuti sia in termini **numerici**, sia in termini di **gravità d’impatto** che possono avere sull’organizzazione → un’organizzazione, quindi, non deve più farsi la domanda: “**Se** cadrò mai vittima di un attacco informatico”, bensì si deve fare la domanda: “**Quando** cadrò vittima di un attacco informatico”. → questo ha come conseguenza diretta, il fatto che l’organizzazione non può più adottare un approccio, in cui essa decide di investire denaro (per proteggersi dagli attacchi informatici) solamente quando diventa vittima di un attacco informatico, bensì l’organizzazione deve adottare un **approccio pro-attivo**, il quale (ovvero l’approccio pro-attivo) si traduce effettivamente nell’avere un piano di gestione del rischio, che va a:

- **identificare** quali sono:
  - le **minacce**, che possono colpire l’organizzazione;
  - le **vulnerabilità** dell’organizzazione;
- **definire un piano** (ovverosia una serie di misure, che l’organizzazione deve adottare), che possa controllare (ovverosia limitare) l’impatto che le minacce e le vulnerabilità individuate, possono avere sull’organizzazione.

Il secondo importante motivo per cui un’organizzazione dovrebbe implementare un piano di gestione del rischio, è che quest’ultimo consente di definire **DOVE** andare ad investire, ovverosia come l’organizzazione deve spendere il budget a disposizione per proteggersi dagli attacchi informatici → senza fare un piano di gestione del rischio, un’organizzazione potrebbe rischiare di investire risorse economiche e di personale, per implementare misure di protezione verso attacchi che:

- hanno una bassa probabilità di avere un impatto negativo sull’organizzazione;
- hanno di per sè un impatto negativo limitato.

e conseguentemente non investire risorse (economiche e di personale) verso attacchi, che invece potrebbero avere un forte impatto negativo sull’organizzazione.

(In realtà, a seconda di dove opera l’azienda, quest’ultima ha un obbligo di adottare un obbligo di gestione del rischio, andando a rispettare determinati standard richiesti nello specifico settore in cui opera l’azienda → un esempio di ciò è DORA, ovverosia uno standard introdotto per tutte le aziende operanti nel settore finanziario).

“**Com’è strutturato un processo di Risk Management?**” Un processo di Risk Management è articolato in cinque attività principali:

1. **Frame Risk** → in cui viene stabilito il contesto in cui opera l’organizzazione. Questo significa, che i soggetti incaricati di implementate il piano di gestione del rischio all’’interno dell’organizzazione, deve capire:
    a. quali sono le missione, gli scopi, gli obiettivi e le priorità dell'organizzazione;
    b. quali sono le aree chiave e critiche dell'attività dell'organizzazione;
    c. identificare i responsabili e le responsabilità delle decisioni in materia di gestione del rischio e di sicurezza informatica;
    d. identificare i rischi accettabili e i rischi da cui ci si vuole proteggere;
    e. identificare i requisiti legali, statutari, normativi, di conformità o contrattuali che l'organizzazione deve soddisfare.
2. **Assess Risk** → lo scopo di questa fase è di identificare:

- le minacce alle organizzazioni (ad esempio, operazioni, beni o individui);
- le vulnerabilità interne ed esterne alle organizzazioni;
- l'impatto negativo che può verificarsi a causa delle potenziali minacce che sfruttano le vulnerabilità;
- la probabilità che si verifichi un danno.

3. **Responde to Risk** → l’input a questa terza fase è una lista di rischi ordinati secondo un livello di rischio ed è per questo, che questa fase prevede l'analisi e la definizione delle priorità dei rischi e la presa di decisioni su come gestirli. Per ognuno di questi rischi, vi sono quattro possibili strategie da implementare:
    a. accettare il rischio;
    b. evitare il rischio;
    c. trasferire il rischio, andando a stipulare una polizza assicurativa con un’assicurazione, in modo tale che la polizza copre l’azienda in tutti quei costi imputabili all’impatto negativo causato dagli attacchi informatici;

d. trattare il rischio, andando a definire le misure di protezione che riportino il livello di rischio sotto una soglia accettabile. In particolare, possiamo avere quattro tipologie di misure di protezione:

   i. **sicurezza procedurale** → controlli di sicurezza che cercano di mitigare o trattare i rischi identificati attraverso politiche, procedure, processi o linee guida;

   ii. **sicurezza fisica** → controlli che cercano di mitigare o trattare i rischi identificati attraverso la protezione fisica di beni quali edifici, strutture, apparecchiature informatiche e personale;

   iii. **sicurezza del personale** → misure messe in atto per mitigare o trattare i rischi derivanti dagli utenti autorizzati dei sistemi informatici, ad esempio campagne di selezione, formazione e sensibilizzazione alle minacce;

   iv. **sicurezza tecnica** → misure integrate nel sistema informatico per mitigare o trattare i rischi identificati, ad esempio firewall, configurazione sicura, controlli di accesso, software anti-malware, aggiornamenti e patch del software.

4. **Communicate the Risk** → una volta che si è fatto un piano su come trattare tutti i possibili rischi, si deve comunicare i risultati e le raccomandazioni, attraverso un report, al decisore o al gruppo di decisori appropriati all'interno dell'organizzazione (dove per decisori, intendiamo i soggetti all’interno dell’organizzazione, che decidono come investire il budget riservato a gestire gli attacchi informatici). Da notare, che le comunicazioni devono essere significative e adeguate al pubblico in termini di livello di dettaglio e formato utilizzato.

5. **Implement and assure Risk** → in questa ultima fase, si va a:

   a. attuare i controlli di sicurezza raccomandati e conseguentemente si deve mantenere la fiducia, che i controlli e le misure applicate funzionino, e continuino a funzionare, in modo efficace e come previsto. In questo senso, si deve confermare costantemente che i controlli in atto sono appropriati e proporzionati in termini di gestione del rischio di sicurezza informatica ed è quindi opportuno:

      i. sviluppare parametri e indicatori di performance per misurare l'efficacia dei controlli (e che quindi i controlli mantengono il livello di rischio sotto una soglia accettabile);

ii. rivedere le valutazioni e le analisi del rischio quando si verificano cambiamenti significativi;

iii. rivedere se vi sono nuove superfici di attacco nell'organizzazione e di conseguenza delle nuove vulnerabilità.

b. formare le persone che utilizzano, gestiscono e mantengono i sistemi e i servizi, richiedendo loro la formazione e le competenze necessarie per svolgere il proprio lavoro in modo sicuro;

c. assicurarsi che la tecnologia e i processi utilizzati dall'organizzazione siano stati progettati tenendo conto della sicurezza;

d. effettuare test di sicurezza su servizi e dispositivi prima della loro implementazione e durante il loro funzionamento, monitorando e verificando il loro utilizzo.

Vi sono diverse metodologie per implementare un piano di gestione del rischio e per implementare la seconda fase del Risk Management, ovverosia la fase di Assess Risk. Alcune di queste metodologie sono gratuite e sono abbastanza facili da implementare, dato che vi sono molte guide sull'implementazione (un esempio di ciò è lo standard del NIST 800-37). Vi sono, naturalmente, anche altre metodologie a pagamento, le quali richiedono all'organizzazione di investire sia risorse economiche sia risorse umane, le quali devono essere istruite e formate (un esempio di metodologia a pagamento è lo standard ISO 31000).

Anche per quanto riguarda, invece, il Risk Assessment abbiamo diverse metodologie di implementazioni, le quali si suddividono (anche in questo caso) in gratuite oppure a pagamento. In particolare, noi ci focalizzeremo sulla metodologia del NIST, la quale prevede quattro componenti fondamentali:

1. **Risk Assessment Process** → ovverosia gli step che devono essere eseguiti per identificare i rischi e valutare i relativi livelli di rischio;
2. **Risk Model** → definisce quali sono i fattori utilizzati per valutare il livello di rischio;
3. **Assessment Approach** → definisce come possono essere combinati i vari fattori per valutare il livello di rischio risultante. In particolar modo, possiamo avere approcci:
    a. **quantitativi** → assegnano alla probabilità e all'impatto un valore numerico. Essi hanno il vantaggio, che nel momento in cui abbiamo diversi livello di rischio e diverse misure di protezione per tali livelli di rischio, possiamo fare

rapidamente e facilmente un confronto tra di essi (ovvero tra i livelli di rischio);

b. **qualitativi** → identificano i valori della probabilità e all'impatto attraverso dei livelli (come per esempio: molto basso, basso, medio e alto). Essi hanno il vantaggio di essere facilmente comprensibili, soprattutto per i soggetti che devono decidere su quale misura di protezione investire per proteggere l'organizzazione. Lo svantaggio, è che se i livelli assegnati alla probabilità e all'impatto non sono ben definiti, non consentono di confrontare i diversi livelli di rischio;

c. **semi-quantitativo** → ai valori di probabilità e di impatto, gli vengono assegnati un valore di una scala (che va ad esempio da 1 a 10), oppure gli viene assegnato un valore di un range (che va ad esempio da 1 a 100).

4. **Analysis Approach** → quando dobbiamo identificare le componenti del rischio, possiamo utilizzare diversi approcci, ovvero:

   a. possiamo partire ad identificare gli scenari di attacco e poi identificare quali sono le vulnerabilità e le categorie di attaccanti interessati a sfruttare le vulnerabilità;

   b. possiamo partire ad identificare gli assets dell'organizzazione e successivamente capire come tali assets possono essere compromessi e quali sono i possibili scenari di attacco;

   c. possiamo partire ad identificare le vulnerabilità e successivamente, per ogni vulnerabilità, vanno a considerare tutti i possibili scenari di attacco che possono sfruttare tale vulnerabilità e tutte le possibili tipologie di attaccanti.

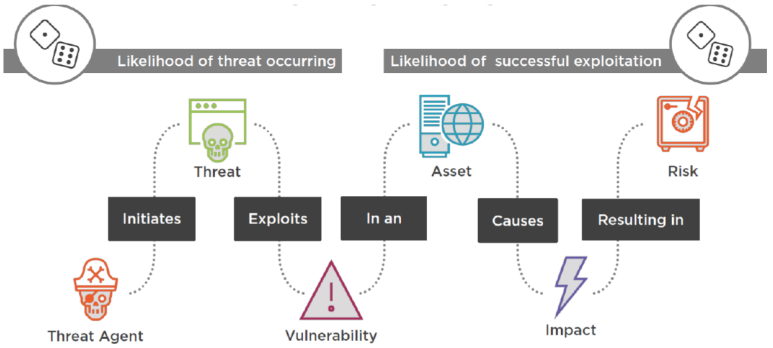
> 💡 Da notare, che non vi è una definizione univoca di rischio, ma quella maggiormente utilizzata è: **Il rischio è la probabilità che un evento abbia un impatto negativo per l'organizzazione**.

Sorge a questo punto spontanea la domanda: "**Come facciamo a valutare questo impatto negativo?**" Per valutare l'impatto negativo utilizziamo il Risk Model, il quale va a definire:

- gli assets → con assets intendiamo le risorse critiche per l'operatività dell'azienda (ovvero per il conseguimento degli obiettivi di business dell'azienda). Gli assets, quindi, ad esempio possono essere: informazioni,

proprietà intellettuale e brevetti → ognuna di questi esempi è una “risorsa” che ha un valore per l’organizzazione e di conseguenza è da proteggere;

- i threat (ovvero gli attacchi) → possono compromettere la confidenzialità, l’integrità, la riservatezza e/o la disponibilità degli assets. I threat possono sfruttare una o più vulnerabilità presenti nel sistema utilizzato per gestire gli assets. Le vulnerabilità, inoltre, possono essere sfruttate dai **threat actors** (ovverosia gli attaccanti), che decidono di iniziare determinati attacchi sfruttando le vulnerabilità del sistema;
- i vari threat che possono essere associati con la probabilità che l’evento threat venga iniziato dagli attaccanti e dobbiamo considerare, anche l’impatto negativo che l’evento threat ha sugli assets aziendali;
- la relazione che c’è tra i concetti descritti sopra. Abbiamo, cioè, un attaccante che inizia un thread, il quale sfrutta delle vulnerabilità presenti negli assets aziendali e che risulta in un impatto negativo per l’organizzazione. L’impatto negativo insieme alla probabilità che l’attacco viene iniziato e che risulti in un impatto negativo, risulta in un livello di rischio.



Vediamo a questo punto, un esempio di metodologia semi-quantitativa utilizzata da OWASP per valutare i rischi associati allo sfruttamento delle vulnerabilità presenti nell’organizzazione. Tale metodologia considera il **rischio** come il prodotto tra:

Probabilità (che l’attaccante inizi l’attacco) x Impatto negativo

e per valutare il valore della probabilità e dell’impatto negativo, vengono utilizzate una serie di metriche (ovvero una serie di fattori), ai quali viene assegnato un valore da una scala da 1 a 9. In particolare, per calcolare il valore della probabilità vengono utilizzati due gruppi di metriche:

1. un gruppo di metriche è relativo all’**attaccante**;

2. il secondo gruppo di metriche è relativo alle **vulnerabilità** sfruttate dall'attaccante.

In particolare, le metriche relative al primo gruppo (ovverosia quelle relative all'attaccante) utilizzate per calcolare il valore della probabilità sono:

- **livello di competenza (Skill Level)** → quanto è tecnicamente competente l'attaccante? Nessuna competenza tecnica (1), alcune competenze tecniche (3), utente avanzato di computer (5), competenze di rete e programmazione (6), competenze di penetrazione della sicurezza (9);
- **motivo** → quanto è motivato l'attaccante a trovare e sfruttare questa vulnerabilità? Ricompensa bassa o nulla (1), ricompensa possibile (4), ricompensa elevata (9);
- **opportunità** → quali risorse e privilegi sono necessarie a all'attaccante per trovare e sfruttare questa vulnerabilità? È richiesto un accesso completo o risorse costose (0), è richiesto un accesso o risorse speciali (4), è richiesto un certo accesso o risorse (7), non è richiesto alcun accesso o risorse (9);
- **dimensione** → quanto è grande questo gruppo di attaccanti? Se è composto da soli sviluppatori (2), amministratori di sistema (2), utenti intranet (4), partner (5), utenti autenticati (6), utenti anonimi di Internet (9).

Invece, le metriche relative al secondo gruppo (ovverosia quello relativo alle vulnerabilità sfruttate dall'attaccante) sono:

- **facilità di scoperta** → quanto è facile per l'attaccante scoprire questa vulnerabilità? Praticamente impossibile (1), difficile (3), facile (7), sono disponibili strumenti automatizzati (9);
- **facilità di sfruttamento** → quanto è facile per l'attaccante sfruttare effettivamente questa vulnerabilità? Teorico (1), difficile (3), facile (5), strumenti automatizzati disponibili (9);
- **consapevolezza** → quanto è nota questa vulnerabilità all'attaccante? Sconosciuta (1), nascosta (4), ovvia (6), di dominio pubblico (9);
- **rilevamento delle intrusioni** → quanto è probabile che un exploit venga rilevato? Rilevamento attivo nell'applicazione (1), registrato e revisionato (3), registrato senza revisione (8), non registrato (9).

> 💡 Una volta che si è dato un valore a tutte queste metriche, per calcolare il valore finale della probabilità, vengono sommati tutti i valori e viene fatta la media.

Per calcolare il valore dell'impatto negativo, anche in questo caso, ci sono due gruppi di metriche:

1. un gruppo di metriche che quantifica l'impatto dell'attacco rispetto alle **proprietà di sicurezza standard** (che ricordiamo essere: riservatezza, integrità e disponibilità);
2. il secondo gruppo di metriche che quantifica l'impatto negativo rispetto al **business dell'azienda**.

In particolare, le metriche utilizzate nel primo gruppo (ovvero quello relativo alle proprietà di sicurezza) sono:

- **perdita di riservatezza** → quanti dati potrebbero essere divulgati e quanto sono sensibili? Dati minimi non sensibili divulgati (2), dati minimi critici divulgati (6), dati estesi non sensibili divulgati (6), dati estesi critici divulgati (7), tutti i dati divulgati (9);
- **perdita di integrità** → quanti dati potrebbero essere danneggiati e quanto sono danneggiati? Dati minimi leggermente corrotti (1), dati minimi gravemente corrotti (3), dati estesi leggermente corrotti (5), dati estesi gravemente corrotti (7), tutti i dati totalmente corrotti (9);
- **perdita di disponibilità** → quanto servizio potrebbe essere perso e quanto è vitale? Servizi secondari minimi interrotti (1), servizi primari minimi interrotti (5), servizi secondari estesi interrotti (5), servizi primari estesi interrotti (7), tutti i servizi completamente persi (9);
- **perdita di responsabilità** → le azioni degli attaccanti sono riconducibili a un individuo? Completamente rintracciabile (1), possibilmente rintracciabile (7), completamente anonimo (9).

Le metriche, invece, utilizzate nel secondo gruppo (ovvero quello relativo al business dell'azienda) sono:

- **danno finanziario** → a quanto ammonta il danno finanziario derivante da un exploit? Inferiore al costo per risolvere la vulnerabilità (1), effetto minore sul profitto annuale (3), effetto significativo sul profitto annuale (7), fallimento (9);

- **danno alla reputazione** → un exploit comporterebbe un danno alla reputazione che danneggerebbe l'azienda? Danno minimo (1), perdita di importanti clienti (4), perdita di avviamento (5), danno al marchio (9);
- **non conformità** → qual è il grado di esposizione della non conformità? Violazione minore (2), violazione evidente (5), violazione di alto profilo (7);
- **violazione della privacy** → quante informazioni di identificazione personale potrebbero essere divulgate? Un singolo individuo (3), centinaia di persone (5), migliaia di persone (7), milioni di persone (9).

> 💡 Una volta che si è dato un valore a tutte queste metriche, per calcolare il valore finale dell'impatto, vengono sommati tutti i valori e viene fatta la media.

Successivamente viene assegnata un'etichetta alla probabilità e all'impatto, in base al loro valore finale:

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

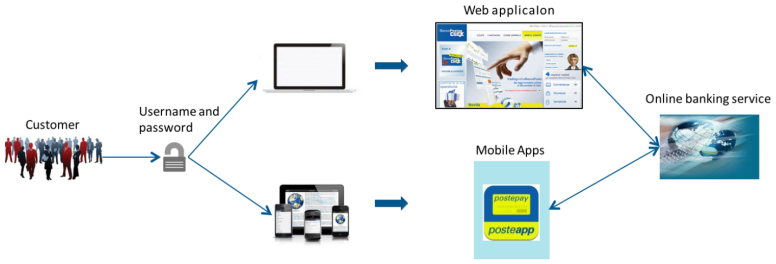
Infine, per trovare il valore finale del rischio viene utilizzata una **Matrice del Rischio**, la quale ha:

- sulle **righe**, i possibili valori **dell'impatto**;
- sulle **colonne**, i possibili valori della **probabilità**

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

L'intersezione tra le righe e le colonne, mostra il valore finale del rischio.

Per capire effettivamente come viene fatto un Risk Assessment, consideriamo uno scenario a noi famigliare, ovvero quello dell'Online Banking:



Immaginiamoci, quindi, che la banca mette a disposizione dei propri clienti un servizio, mediante il quale i clienti possono accedere al loro conto bancario e svolgere altre operazioni correlate, tramite un'applicazione per lo smartphone, oppure tramite un'applicazione Web. In entrambi i casi, gli utenti accedono ai servizi tramite autenticazione mediante username e password e l'obiettivo dell'organizzazione è valutare i rischi associati a questo servizio.

Il processo di Risk Assessment del NIST consiste principalmente in quattro step:

1. **Prepararsi alla valutazione del rischio** → consiste nel raccogliere le informazioni, che consentono agli analisti di comprendere il contesto in cui opera l'azienda. Quindi, l'obiettivo di questa prima fase è quello di stabilire un contesto per la valutazione del rischio e di conseguenza comprende i seguenti compiti:
    a. identificare lo scopo della valutazione;
    b. identificare l'ambito della valutazione;
    c. identificare le ipotesi e i vincoli associati alla valutazione;
    d. identificare il modello di rischio, l'approccio di valutazione e l'approccio di analisi da utilizzare nella valutazione del rischio.
2. **Condurre la valutazione del rischio** → in questa fase si vanno a definire quali sono i possibili scenari di attacco e per ciascuno andiamo a definire la probabilità, l'impatto e conseguentemente il livello di rischio. L'obiettivo di questa seconda fase, quindi, è quello di produrre un elenco di rischi per la sicurezza informatica dell'azienda e di conseguenza comprende i seguenti compiti:
    a. identificare le c**ategorie di attaccanti**, che destano preoccupazione per l'azienda. In particolar modo, mostriamo un elenco di categorie di attaccanti (**avversari**, **accidentali**, **strutturali** e **di ambiente**):

Type of threat source	Descriptions	Characteristics
ADVERSARIAL Outsider Insider Competitor Supplier Nation State	Individuals, groups, organizations, or states that seek to exploit the organization' dependence on cyber resources	Capability, Intent, Targeting
ACCIDENTAL User Privileged User	Erroneous actions taken by individuals	Range of effects
STRUCTURAL IT Equipment Environmental Controls Software	Failure of equipment, environmental controls, or software	Range of effects
ENVIRONMENTAL Natural or Man-Made Disaster Infrastructure Failure	Natural disasters and failures of critical infrastructures on which the organization depends	Range of effects

In questo compito, quindi, dobbiamo chiederci per gli attaccanti avversari (ovverosia gli attaccanti che hanno un intento malevolo):

- quanto è tecnicamente competente l'attaccante?
- quanto è motivato l'attaccante a sfruttare una vulnerabilità?
- qual è l'asset preso di mira dall'attaccante?

Per le altre tipologie di attaccante, invece, dobbiamo chiederci:

- qual è l'effetto dell'attaccante?

(Nel nostro esempio dell'Online Banking, gli attaccanti avversari possono essere le gang Cybercriminali oppure degli attivisti, le quali hanno tipicamente elevate competente tecniche. Le gang Cybercriminali oppure gli attivisti attaccano l'applicazione Web o i Server per motivi economici).

b. identificare i **possibili scenari di attacco** (nel nostro esempio, gli attivisti possono compiere un attacco di Denial of Service e di richiedere un riscatto, mentre le gang cybercriminali possono utilizzare dei ransomware per compiere degli attacchi, andando a sfruttare le vulnerabilità presenti nelle macchine utilizzate nell'organizzazione);

c. identificare le **vulnerabilità che possono sfruttare gli attaccanti** (nel nostro esempio, i malware sfruttano vulnerabilità di Remote Code Execution, mentre gli attacchi di Denial of Service sfruttano la No Load Balancing);

d. determinare la **probabilità che l'attacco si verifichi** → il NIST prevede, che per ciascun scenario di attacco vengano determinate due probabilità, ovvero:

   i. la probabilità che l'attacco venga effettivamente iniziato dall'attaccante → per calcolare tale probabilità, dobbiamo considerare:

      1. le capacità dell'attaccante;

2. le motivazioni dell'attaccante;
3. quanto sia difficile sfruttare la vulnerabilità.

Una volta considerati questi tre aspetti e di conseguenza bilanciando questi tre aspetti, il NIST mette a disposizione una tabella per determinare la probabilità con cui l'attacco possa essere iniziato dall'attacccante. Tale tabella fornisce delle etichette (molto bassa, bassa, moderata…):

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

ii. la probabilità che l'attacco risulti in un impatto negativo per l'organizzazione → per calcolare tale probabilità, dobbiamo considerare quali sono le misure di protezione implementate dall'organizzazione. Anche in questo caso, il NIST ci fornisce una tabella molto simile a quella precedente:

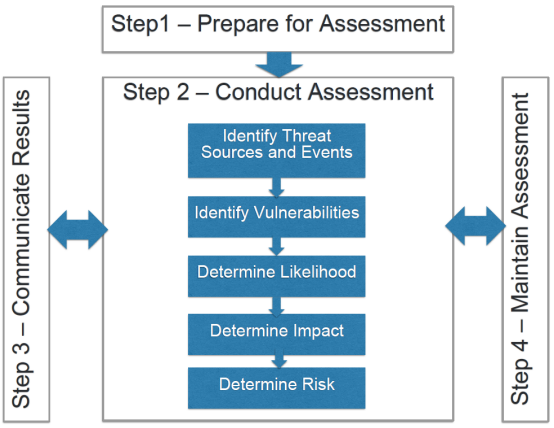
Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

e. **determinare l'impatto negativo** sull'organizzazione. In particolare, il NIST considera varie tipologie di impatto negativo:
   i. sulla nazione;
   ii. sulle altre organizzazioni;
   iii. sui clienti o sugli impiegati dell'organizzazione e conseguentemente sull'immagine dell'organizzazione;
   iv. sugli assets;
   v. sull'operatività ed economici.

(Nel nostro esempio, abbiamo un impatto negativo sull'operatività della banca, economici, sui clienti e di immagine).

f. **determinare il rischio**, che ricordiamo essere la combinazione di probabilità e impatto. Per determinare il rischio, quindi, utilizziamo la Matrice del Rischio.

3. **Comunicare i risultati** → in questa fase, quindi, si vanno a comunicare i risultati della valutazione e condividere le informazioni relative ai rischi, ovvero si va a comunicare i risultati ai decisori dell'organizzazione per supportare le risposte al rischio. Inoltre, si va a condividere le informazioni relative al rischio prodotte durante la valutazione del rischio con il personale organizzativo appropriato;
4. **Mantenere la valutazione dei rischi** → in cui si valuta continuamente i fattori, che possono influenzare la strategia utilizzata dall'organizzazione per mitigare i rischi individuati.



Riassumendo tutto, possiamo dire che: La gestione del rischio (**Risk Management**) è il processo di prioritizzazione dei rischi identificati in termini di probabilità di accadimento, quindi di sforzi coordinati per minimizzare, monitorare e controllare l'impatto di tali rischi.
La valutazione del rischio (**Risk Assessment**) è il processo di identificazione e valutazione del livello di rischio affrontato da un'organizzazione.