Gestione e valutazione del rischio cyber

Processo di gestione del rischio

- La norma **ISO 31000:2018** *Risk management — Guidelines* definisce tutte le attività necessarie per sviluppare una metodologia efficiente per la gestione del rischio

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

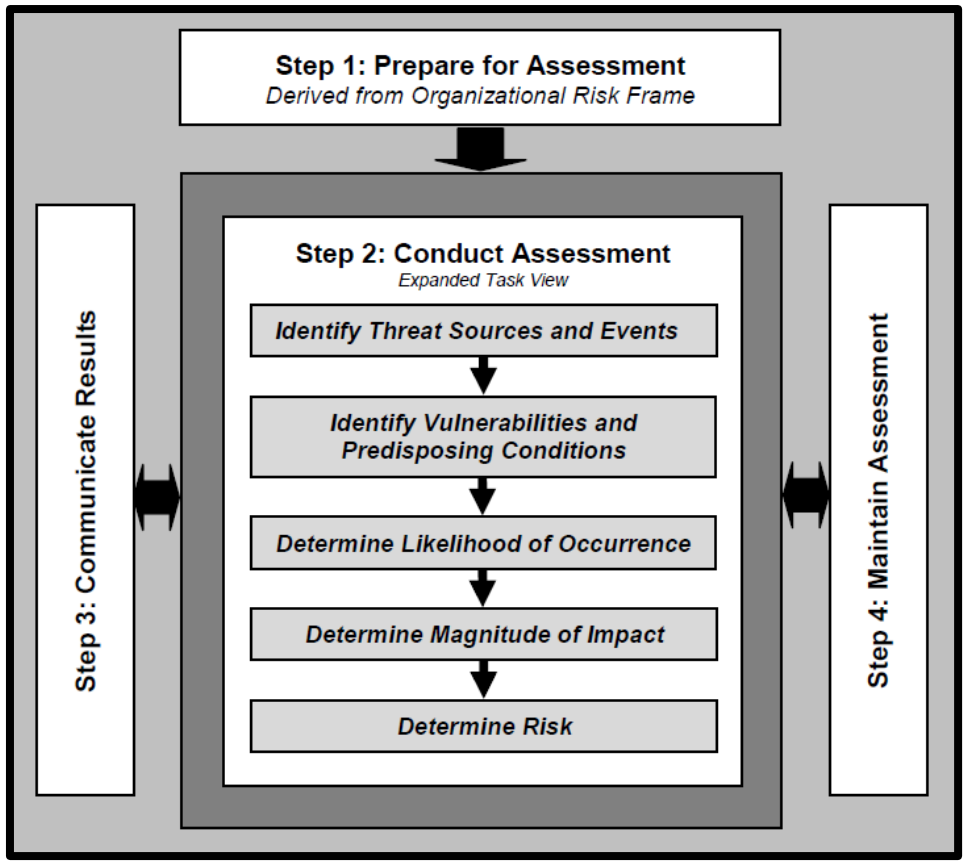
- Lo scopo è quello di testare e di migliorare la qualità e l'efficacia del processo di gestione del rischio. Il monitoraggio e la revisione includono pianificare, raccogliere e analizzare le informazioni, registrare i risultati e fornire feedback
- Il monitoraggio e la revisione dovrebbero avvenire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

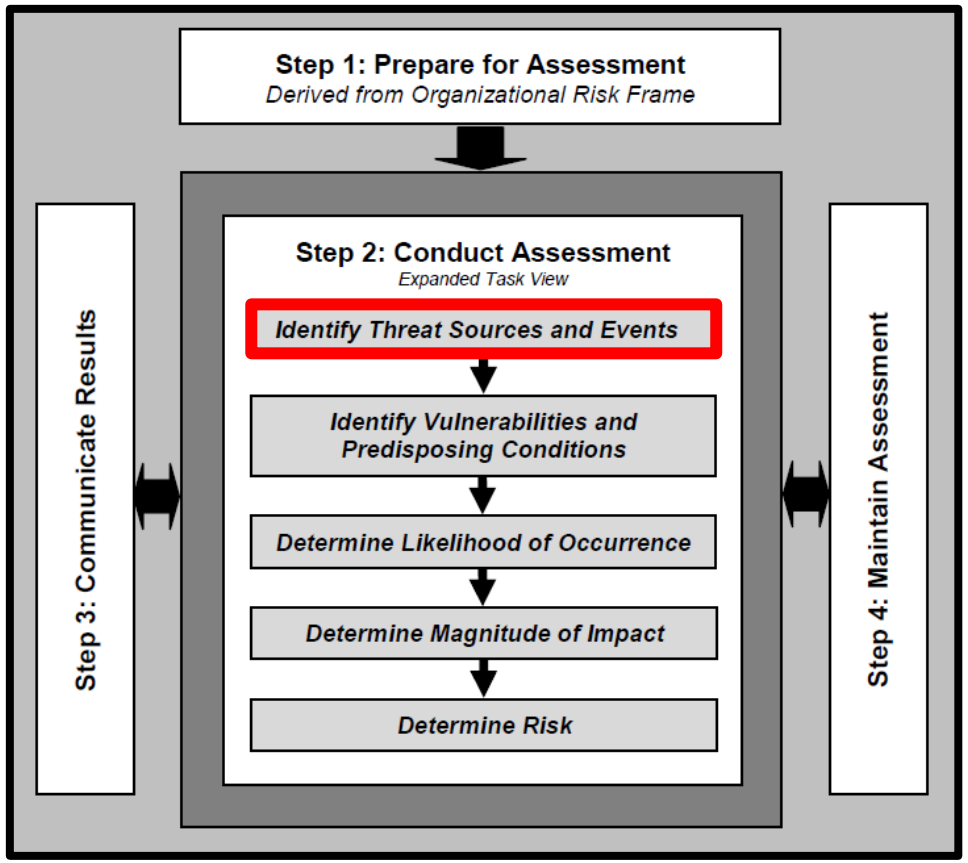
Risk Assessment

- 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

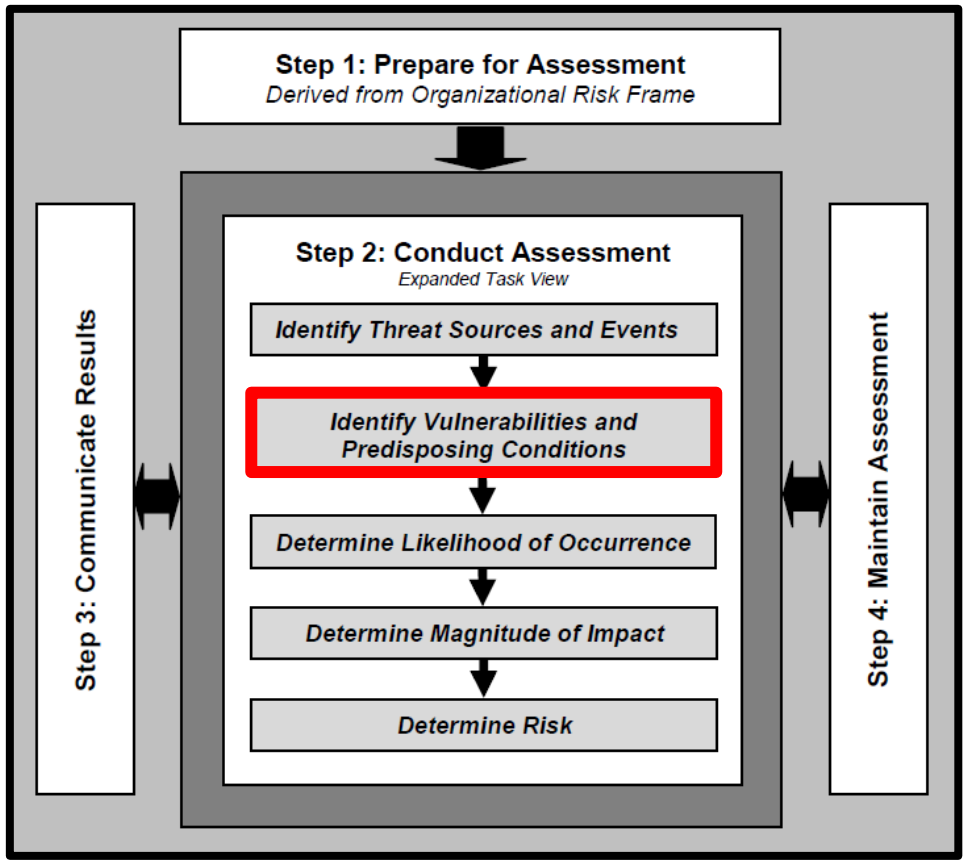


NIST SP 800-30r1, Guide for Conducting Risk Assessments

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

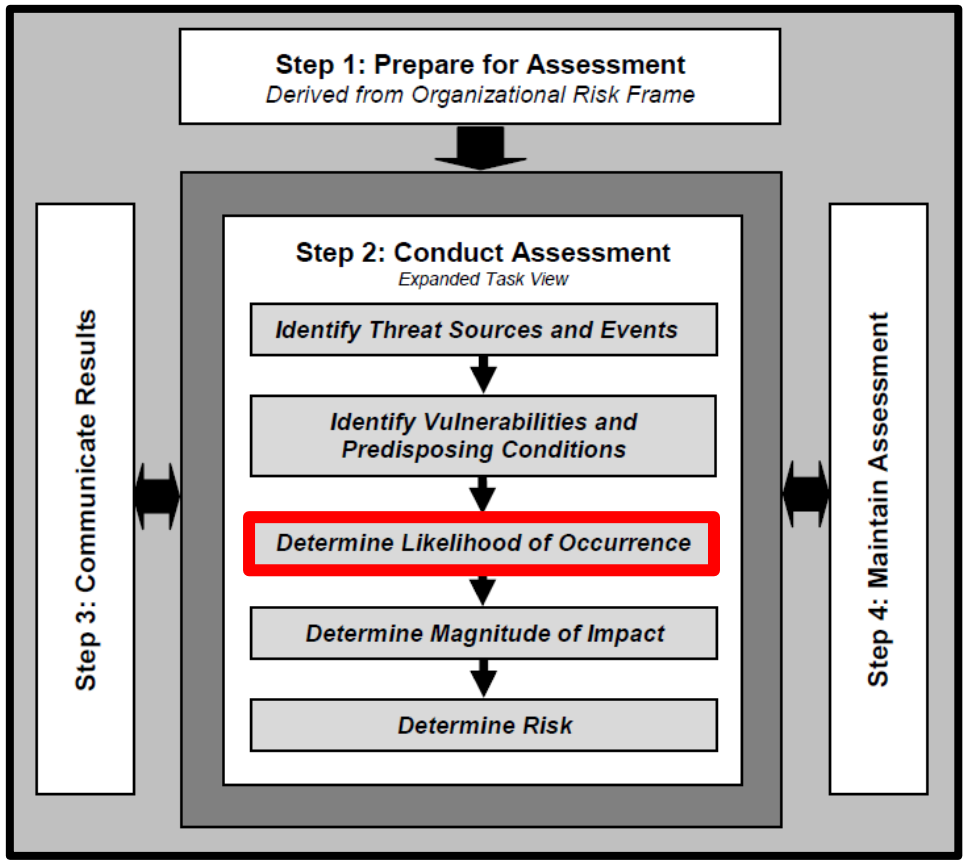


NIST SP 800-30r1, Guide for Conducting Risk Assessments

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

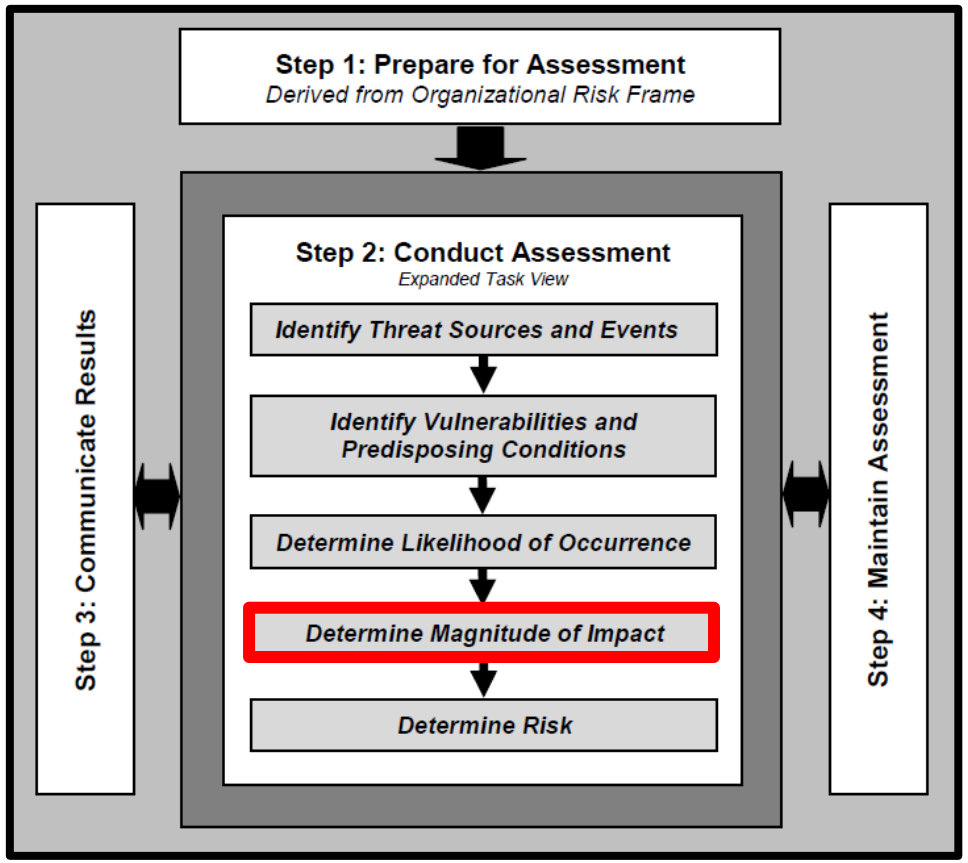


NIST SP 800-30r1, Guide for Conducting Risk Assessments

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

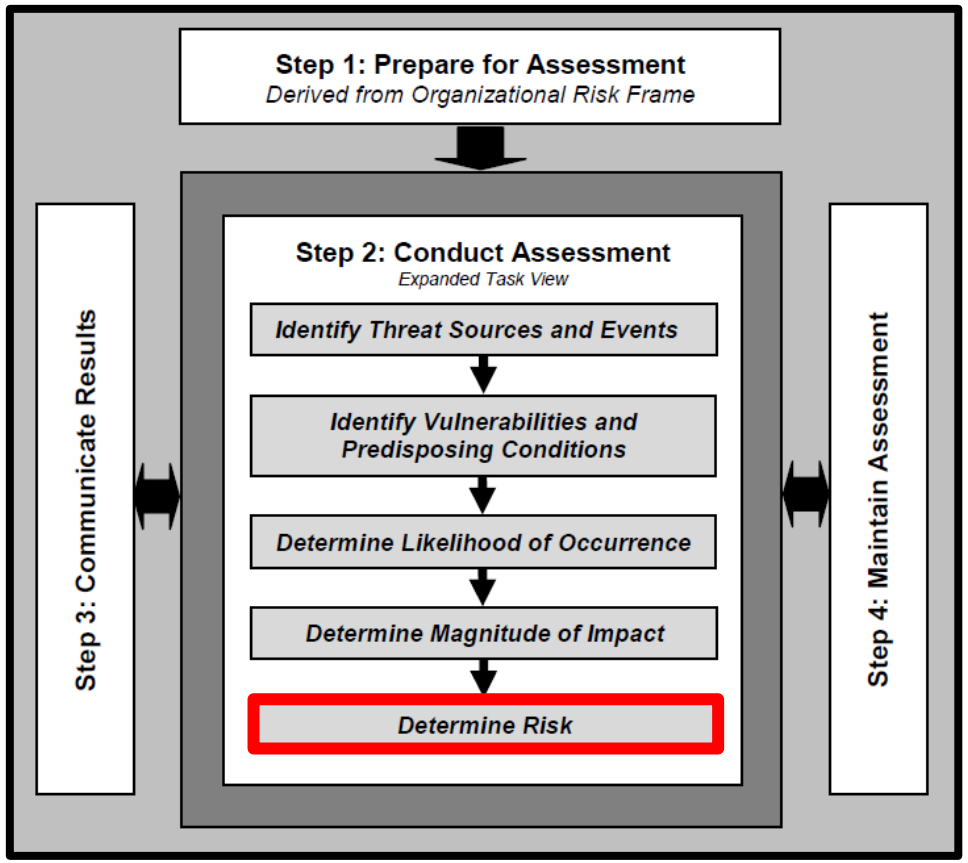


NIST SP 800-30r1, Guide for Conducting Risk Assessments

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

Metodi per la valutazione del rischio cyber

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

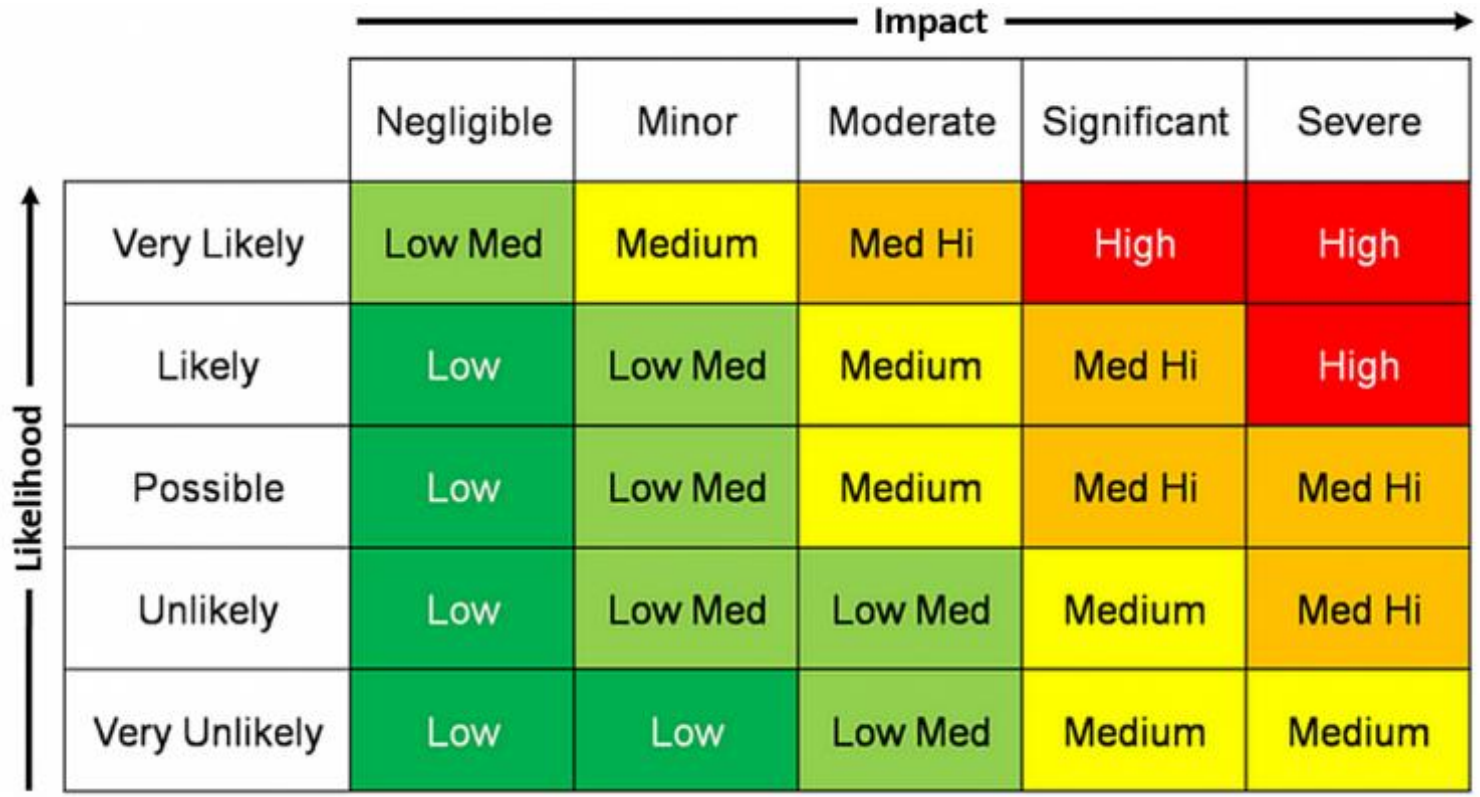
PRO

- 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

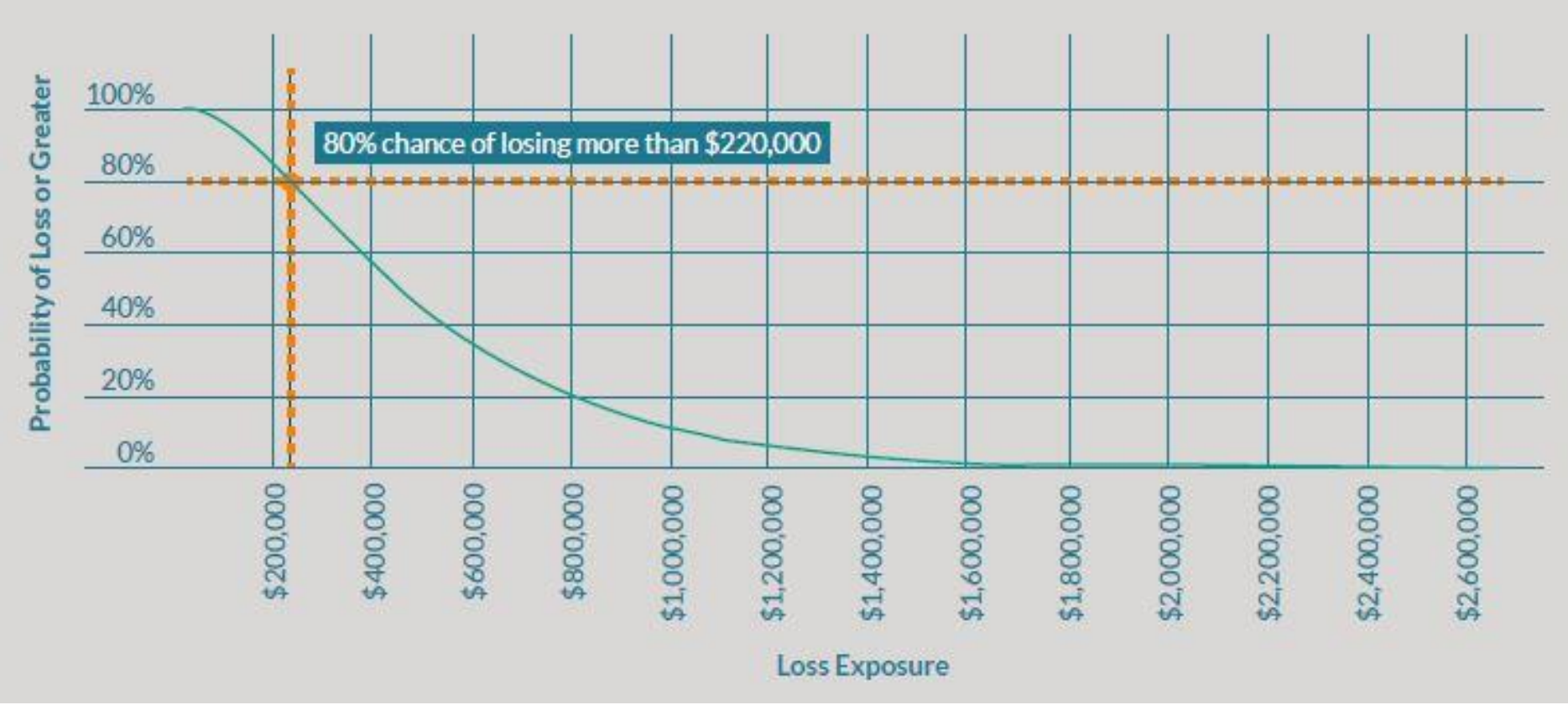
PRO

- 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



Metodi SEMI - QUANTITATIVI

- La *valutazione semi-quantitativa* impiega tipicamente una serie di metodi, principi o regole per la valutazione del rischio, utilizzando intervalli, scale o numeri rappresentativi.

PRO

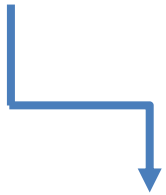
- Si può passare dalla rappresentazione quantitativa a quella qualitativa (ereditando i PRO dei metodi qualitativi)
- Tramite la rappresentazione quantitativa, i confronti numerici sono possibili

CONTRO

- La combinazione e l'interpretazione dei risultati può essere difficile, a causa delle diverse scale di valutazione

Metodo HTMA

- Il metodo **HTMA** ("How To Measure Anything in cybersecurity risk" [1]) è un metodo *quantitativo* di valutazione del rischio basato sulla Simulazione Monte Carlo



un tipo di algoritmo che utilizza una *campionatura casuale* ripetuta un *elevato numero di volte* per ottenere la probabilità del verificarsi di un intervallo di risultati

[1] D. Hubbard e R. Seiersen, How to Measure Anything in Cybersecurity Risk, Wiley, 2016

Simulazione Monte Carlo

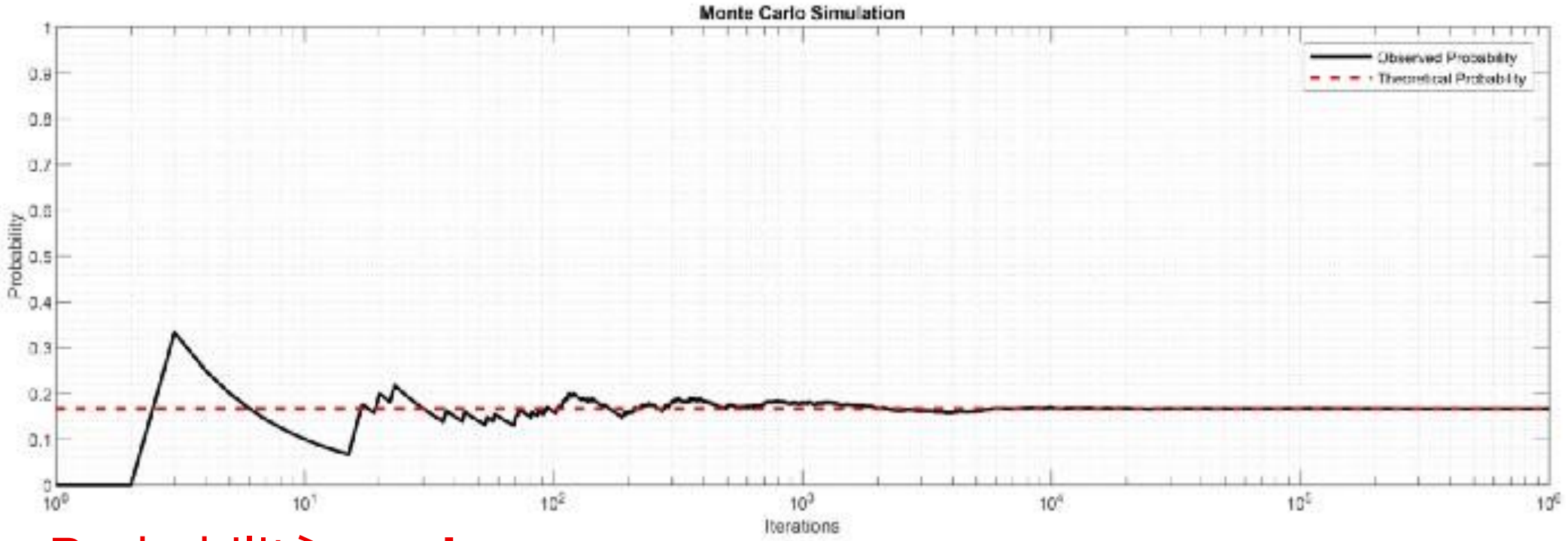
- Qual è la probabilità che, lanciando un dado, io ottenga un 4?

$$\text{probabilità} = \frac{\text{casi favorevoli}}{\text{casi possibili}} \quad \Rightarrow \quad p = \frac{1}{6} \cong 0.17$$

- Quindi, lanciando un dado 6 volte, sicuramente un 4 una volta?

- La probabilità che si verifichi un evento coincide solo con il valore teorico quando l'esperimento viene eseguito infinite volte

Simulazione Monte Carlo



Probabilità **teorica**

Metodo HTMA

- Il metodo **HTMA** ("How To Measure Anything in cybersecurity risk" [1]) è un metodo *quantitativo* di valutazione del rischio basato su Simulazioni Monte Carlo

- HTMA si compone di quattro passaggi:

1. Definizione *della lista degli eventi* (minacce) cyber di cui si vuole valutare il rischio
2. Stima della *probabilità di accadimento* e dell'*impatto* di ciascun evento
3. Generazione degli scenari attraverso la *simulazione Monte Carlo*
4. Interpretazione dei *risultati*

[1] D. Hubbard e R. Seiersen, How to Measure Anything in Cybersecurity Risk, Wiley, 2016

Metodo HTMA

1. Definizione della lista degli eventi cyber di cui si vuole valutare il rischio

- Il rischio è definito come “uno stato di incertezza in cui alcune delle possibilità comportano una perdita, una catastrofe o un altro esito indesiderato”
- Nella lista devono quindi essere elencati degli eventi che comportano un rischio cyber
- Il numero e la natura degli eventi da elencare sono a discrezione di chi sta conducendo l’analisi: si possono considerare i rischi associati a una singola vulnerabilità, a un sistema, a un’unità di business o all’intera organizzazione

Metodo HTMA

2. Stima della probabilità di accadimento e dell'impatto di ciascun evento

Per ogni evento elencato nella lista, si devono stimare:

- *La probabilità di accadimento*: è la probabilità che l'evento si verifichi in un intervallo temporale dato. Ad ogni evento si associa una probabilità compresa tra 0 e 1

- L'*impatto* ad esso associato nel caso in cui l'evento si verifichi: è la perdita monetaria associata al verificarsi dell'evento in un intervallo temporale dato. L'impatto si stima attraverso un intervallo di confidenza (un intervallo di valori plausibili) del 90%, individuato da un limite inferiore (LB) e da un limite superiore (UB)

Metodo HTMA

2. Stima della probabilità di accadimento e dell'impatto di ciascun evento

Minaccia	Probabilità	LB	UB
e_1	p_1	LB_1	UB_1
e_2	p_2	LB_2	UB_2
…	…	…	…
e_N	p_N	LB_N	UB_N

Metodo HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo

Gli eventi elencati nella lista, con le rispettive probabilità di accadimento e i rispettivi impatti, vengono usati come input per la simulazione Monte Carlo

Attraverso la simulazione, l'obiettivo è quello di stimare il rischio totale annuale derivante dagli eventi cyber elencati nella lista, espresso in termini di perdita monetaria

Il valore del rischio totale annuale corrisponde alla somma degli impatti degli eventi che si sono verificati, e dipende quindi, in ogni scenario, da quali eventi si verificano e dall'entità della perdita ad essi associata

Metodo HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo

All'interno di un singolo scenario:

- Va simulata l'occorrenza di ciascun evento (si è verificato o non si è verificato) compatibilmente con la probabilità di accadimento che gli è stata assegnata
- Per gli eventi che non si sono verificati il rispettivo *impatto* viene posto *pari a 0*
- Per ogni evento che si è verificato va generato un impatto compatibile con il range individuato dal suo intervallo di confidenza del 90%
- Gli impatti di tutti gli eventi che si sono verificati vanno sommati, in modo da ottenere l'impatto totale che corrisponde al rischio totale annuale

Metodo HTMA

3. Generazione degli scenari attraverso la simulazione Monte Carlo

La simulazione va poi ripetuta per un numero elevato di volte, così da affinare la stima ed ottenere un valore di rischio che sia il più vicino possibile alla realtà

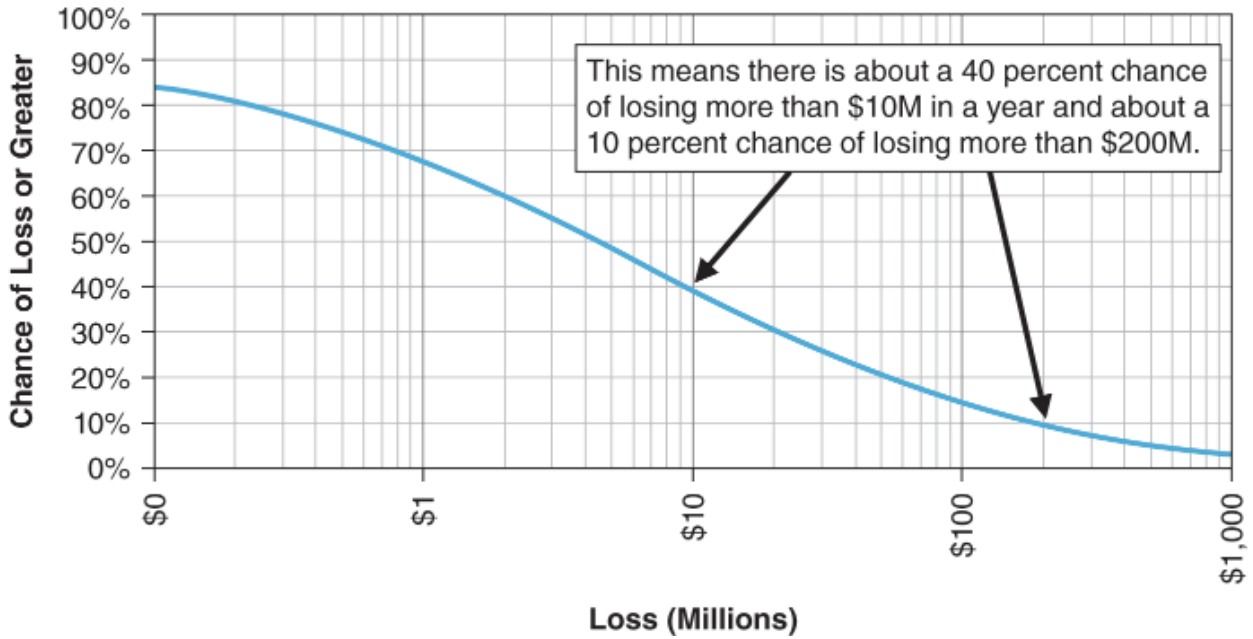
Scenario	Annualized Loss Expectancy
1	ALE_1
2	ALE_2
3	ALE_3
…	…
t	ALE_t

Somma di tutti gli impatti degli eventi che sono accaduti

Metodo HTMA

4. Interpretazione dei risultati

I risultati ottenuti con la simulazione Monte Carlo vengono usati per costruire la Loss Exceedance Curve (LEC), che rappresenti le perdite annuali



HTMA – FAIR – MIX METHOD

https://cegisa.shinyapps.io/qrisk_mix/

Metodo FAIR

- Il metodo **FAIR** ("Factor Analysis of Information Risk" [2]) è un metodo *quantitativo* di valutazione del rischio basato su un'Ontologia del Rischio e su Simulazioni Monte Carlo

- FAIR si compone di quattro passaggi:

1. Definizione *dello scenario* sotto esame e decomposizione in sotto-scenari
2. Stima dei *parametri* per ogni sotto-scenario
3. Generazione dei framework attraverso la *simulazione Monte Carlo*
4. Interpretazione dei *risultati*

[2] J. Freund and J. Jones, Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, 2014.

Metodo FAIR

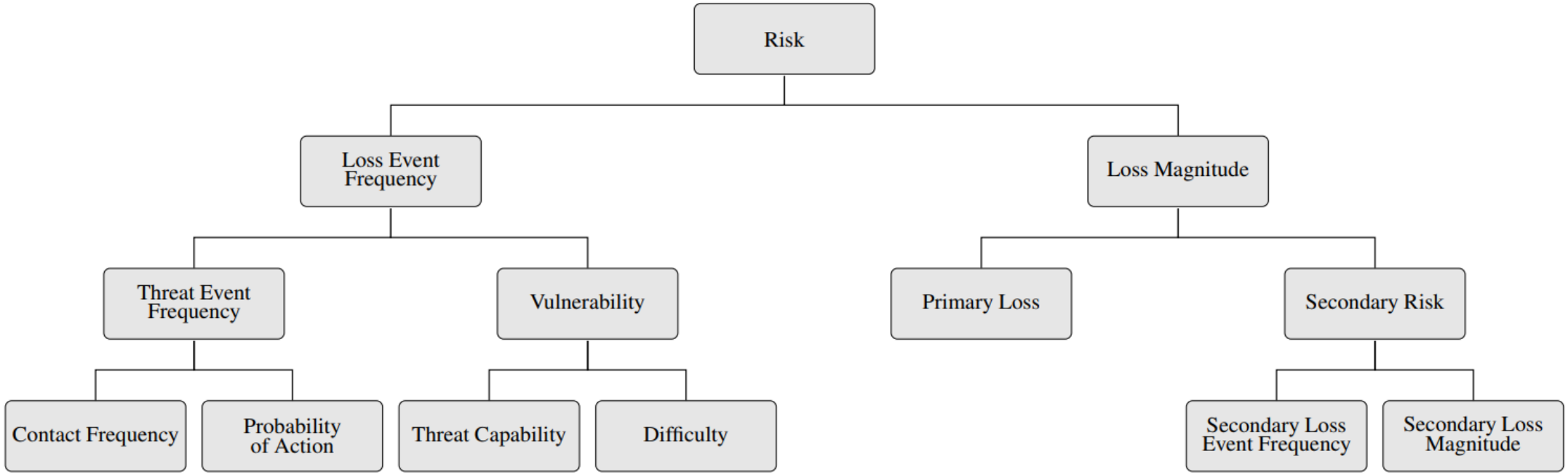
1. Definizione dello *scenario* sotto esame e decomposizione in sotto-scenari

- Scenario: situazione che espone l'organizzazione al rischio cyber
- Sotto-scenari: ottenuti dagli scenari in base a
  - *L'asset a rischio* - risorsa che ha valore per l'organizzazione
  - *Gli agenti responsabili della minaccia* - TCom (Threat Community)
  - *La tipologia di minaccia* - natura della minaccia
  - *L'effetto* - natura della perdita

Metodo FAIR

2. **Stima dei *parametri* per ogni sotto-scenario**

Fondata su un'ontologia del rischio, che definisce i fattori



Metodo FAIR

3. **Generazione degli scenari attraverso la simulazione Monte Carlo**

Attraverso la simulazione Monte Carlo, si stimano:

- Frequenza della perdita primaria
- Entità della perdita primaria per un singolo evento
- Frequenza della perdita secondaria
- Entità della perdita secondaria per un singolo evento
- Entità totale annuale della perdita

Metodo FAIR

4. **Interpretazione dei risultati**

I risultati sono solitamente presentati tramite:

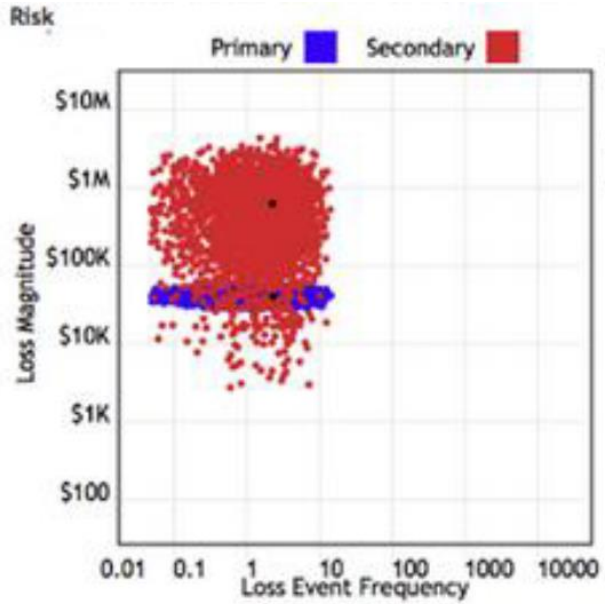
- Grafici a dispersione: riportano frequenza e entità della perdita primaria e secondaria per ciascuno scenario generato con la simulazione Monte Carlo

- Tabelle riassuntive: riportano i valori minimo, medio, più verosimile e massimo ottenuti con la simulazione Monte Carlo per ciascuna delle variabili di interesse

- Percentili: rappresentano il 10° e il 90° percentile della perdita totale

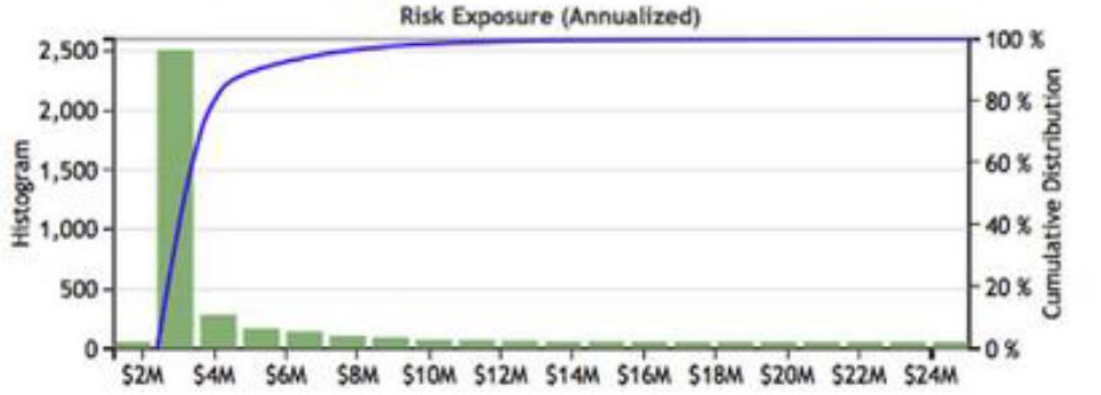
Metodo FAIR

4. **Interpretazione dei risultati**



	Minimum	Average	Most Likely	Maximum
Primary				
Loss Events / Year	0.05	2.36	0.26	14.66
Loss Magnitude	$26,553.00	$39,193.00	$39,259.00	$56,906.00
Secondary				
Loss Events / Year	0.05	2.31	0.26	14.32
Loss Magnitude	$2,682.00	$607,907.00	$16,775.00	$4,207,045.00
Total Loss Exposure	$2,879.00	$1,484,558.00	$98,037.00	$23,072,668.00

Percentiles	10 %	$94,559.28	90 %	$3,785,278.25



Organization

Risk Level	Loss Exposure
High	$9,000,000.00
Medium	$1,000,000.00
Low	$0.00

Department

Risk Level	Loss Exposure
High	$1,000,000.00
Medium	$250,000.00
Low	$0.00

Export to Excel | Export to PDF / Word | Re-run Simulation | Compare Results