UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Risk Assessment in SOMACIS SPA

Daniele Gatto

IT Department Somacis SPA

daniele.gatto93@gmail.com

Martedì 19 Settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione

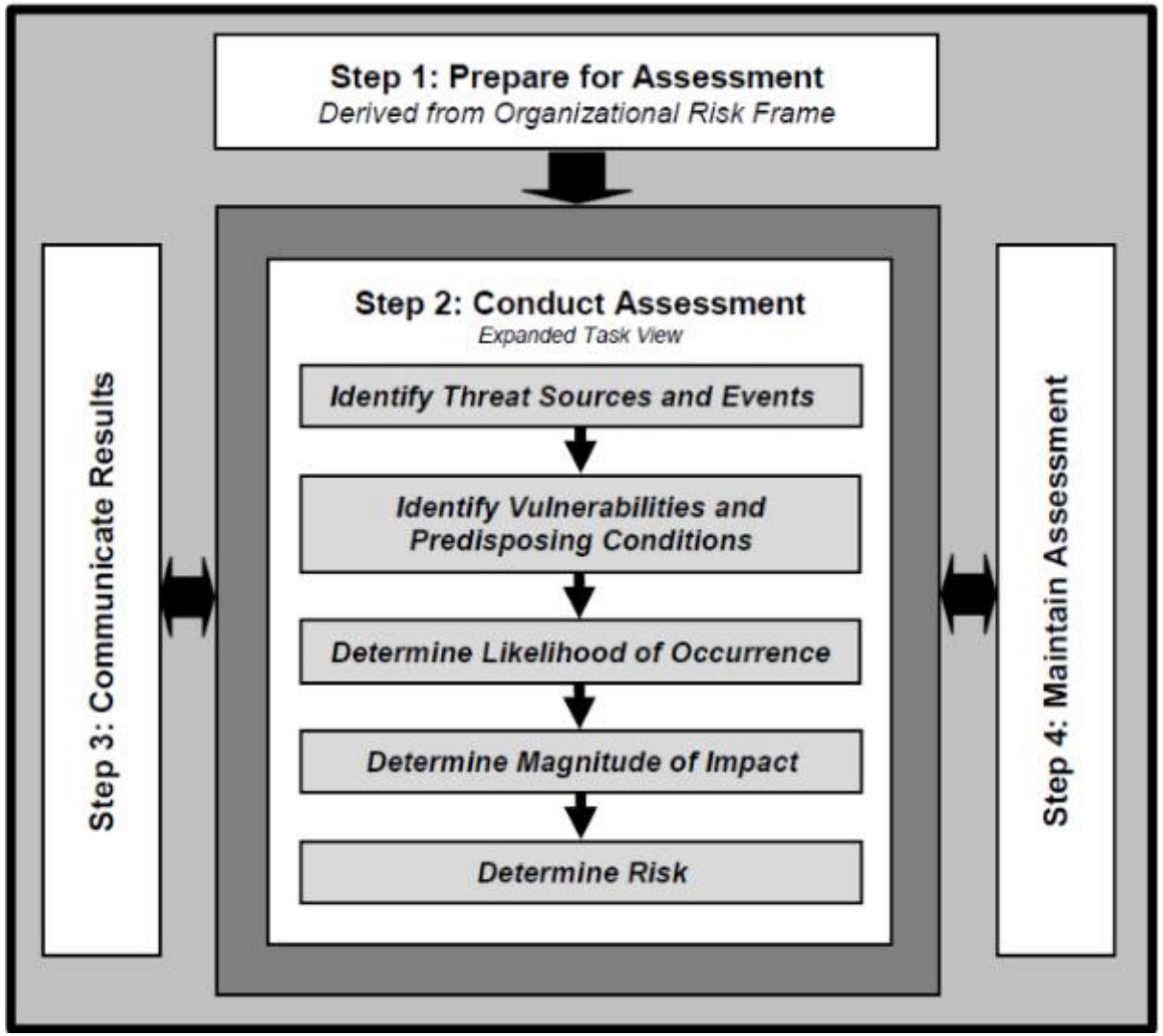
Strumenti e metodi

Norma ISO 31000:2018 Risk management

- Linee guida per una valutazione e gestione del rischio cyber

Risk Assessment

- Analizzare le minacce e le vulnerabilità dell'infrastruttura
- Determinare la probabilità che quegli eventi si verifichino impattando negativamente sull'azienda
- Stimare il costo di tale evento per l'azienda

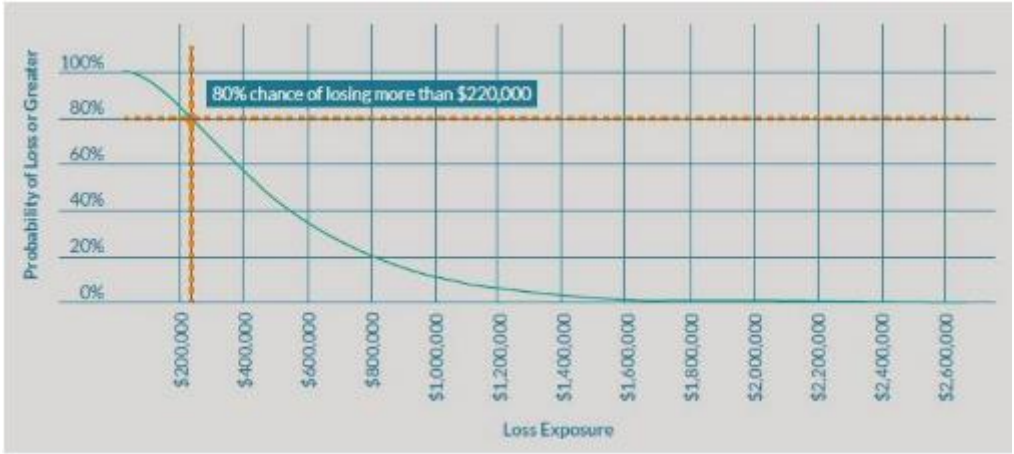


Come stimiamo in concreto questi valori?

- Metodi Qualitativi
  - Veloci
  - Non oggettivi e non confrontabili

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

- Metodi Quantitativi
  - Rigorosi e confrontabili
  - Onerosi e difficili da produrre



Magic

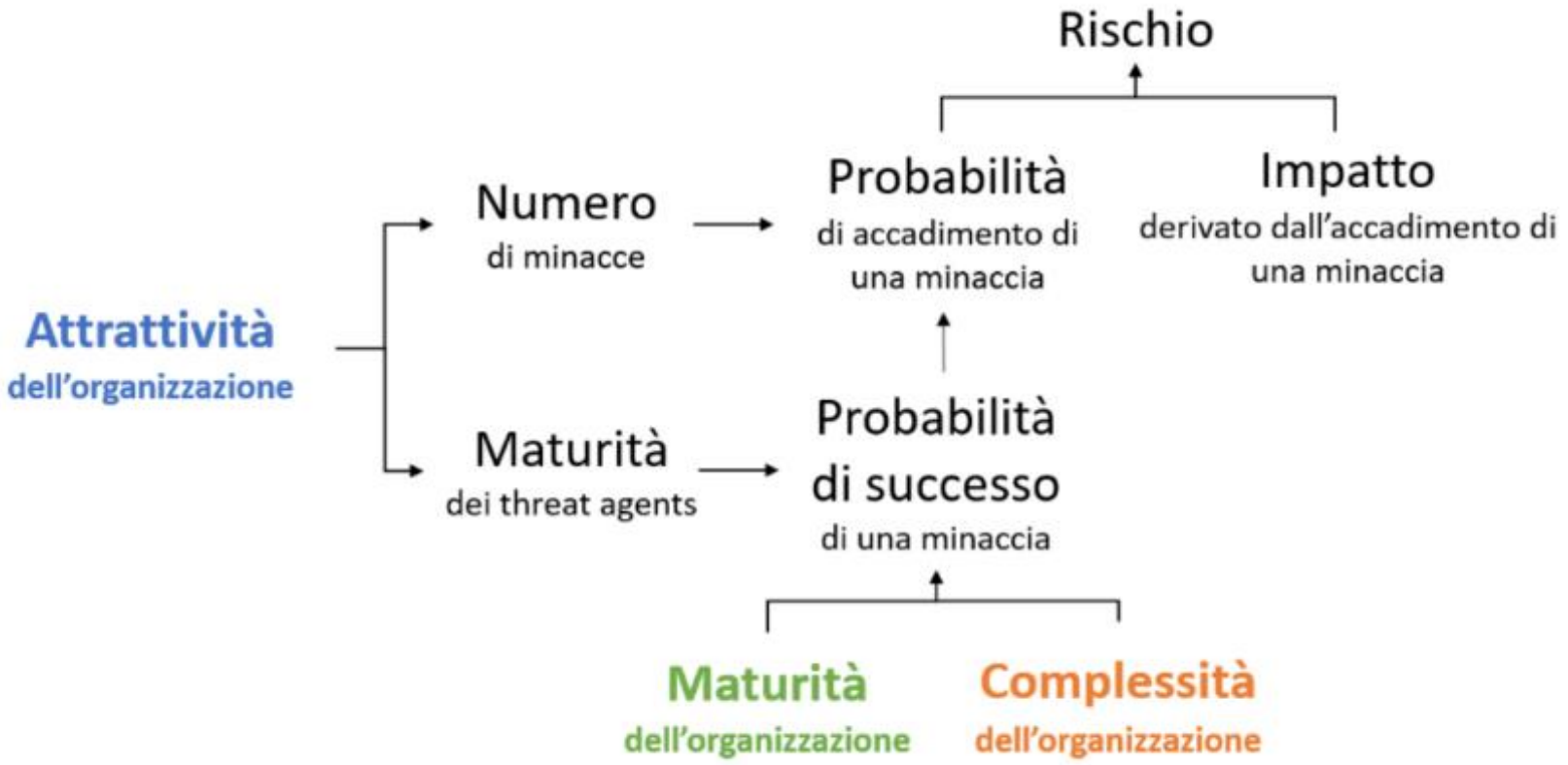
Method for **A**ssessin**G** cyber **I**ncidents o**C**currence

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Metodo quantitativo Magic

- M. Battaglioni, G. Rafaiani, F. Chiaraluce and M. Baldi, "MAGIC: A Method for Assessing Cyber Incidents Occurrence," in IEEE Access, vol. 10, pp. 73458-73473, 2022, doi: 10.1109/ACCESS.2022.3189777.
- G. Rafaiani, M. Battaglioni, M. Baldi, F. Chiaraluce, G. Libertini, L. Spalazzi, and G. Cancellieri, “A functional approach to cyber risk assessment,” in Proceedings AEIT 2021 International Annual conference, 2021
- G. Rafaiani, M. Battaglioni, M. Baldi, and F. Chiaraluce, “Cyber risk assessment: a pragmatic approach,” in Proceedings ICITEE 21, 2021

- Metodo semplice per la valutazione del rischio cyber



Applicazione MAGIC

Others	>>	Attrattività	**Media**
		Peso attrattività	0.8

Informazioni generali	Inserisci:	*Note*
Numero totale di dipendenti	**250**	
Numero complessivo di postazioni di lavoro (PdL)	**150**	
Numero totale di server, compresi i server virtuali	**35**	
Numero complessivo delle istanze dei vari DBMS	**8**	
Numero totale di FTE addetti tecnici al sistema informatico (dipendenti + eventuali esterni a contratto)	**5**	
Numero totale di FTE dedicato al supporto postazioni di lavoro (dipendenti + eventuali esterni a contratto)	**5**	

Indice di maturità medio	**9.33**

Profilo complessità *(per categoria)*	Livello di complessità	Complessità pesata
Reti e infrastruttura	*Bassa*	3.75
Tecnologie su reti IP	*Bassa*	3.75
Applicazioni	*Bassa*	3.55
Servizi online	*Minima*	1.67
Reparto IT	*Bassa*	2.96
Complessità media	***Bassa***	***3.14***
Complessità media pesata	***Bassa***	***3.34***

1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	Sì
2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.	Sì
3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	In parte
4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.	Sì
5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.	Sì
6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	Sì
7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	Sì
8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.	Sì
9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	Sì
10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato,...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.	Sì
11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.	Sì
12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.	Sì
13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).	Sì
14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.	Sì
15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.	In parte

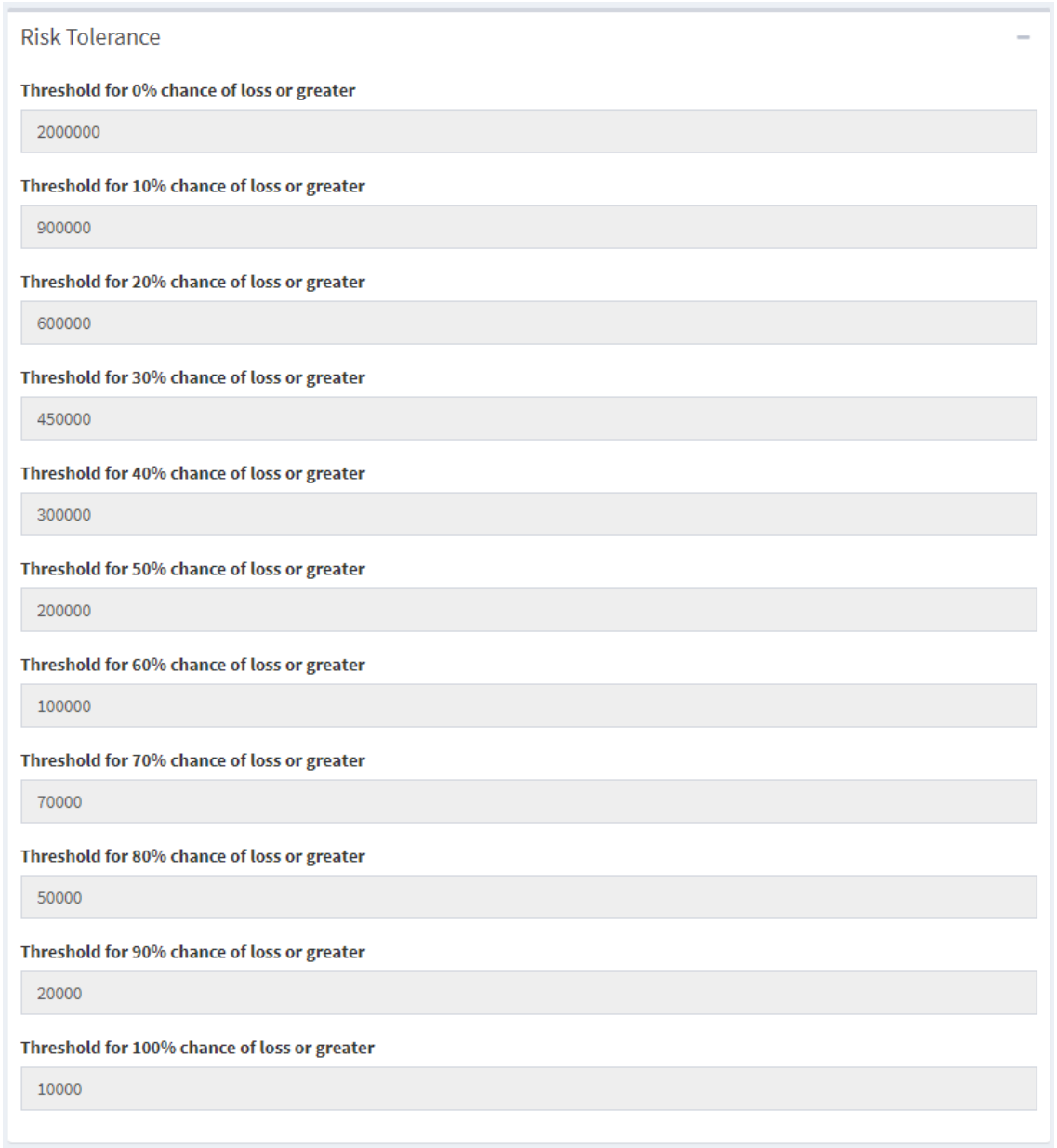
MAGIC – HTMA

- Simulazione HTMA

Table 1: Monte Carlo Simulation input (Risk List)

Event	Probability	LB 90% CI	UB 90% CI
Phishing	0.50	€100	€50,000
SPAM	0.80	€150	€20,000
Furto	0.10	€1,000	€500,000
Eventi Naturali	0.01	€3,000	€1,500,000
Ransomware	0.10	€5,000	€500,000
Perdita Dati	0.20	€2,000	€1,300,000
Perdita di Reputazione	0.04	€50,000	€1,000,000
DDos	0.07	€100,000	€800,000

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



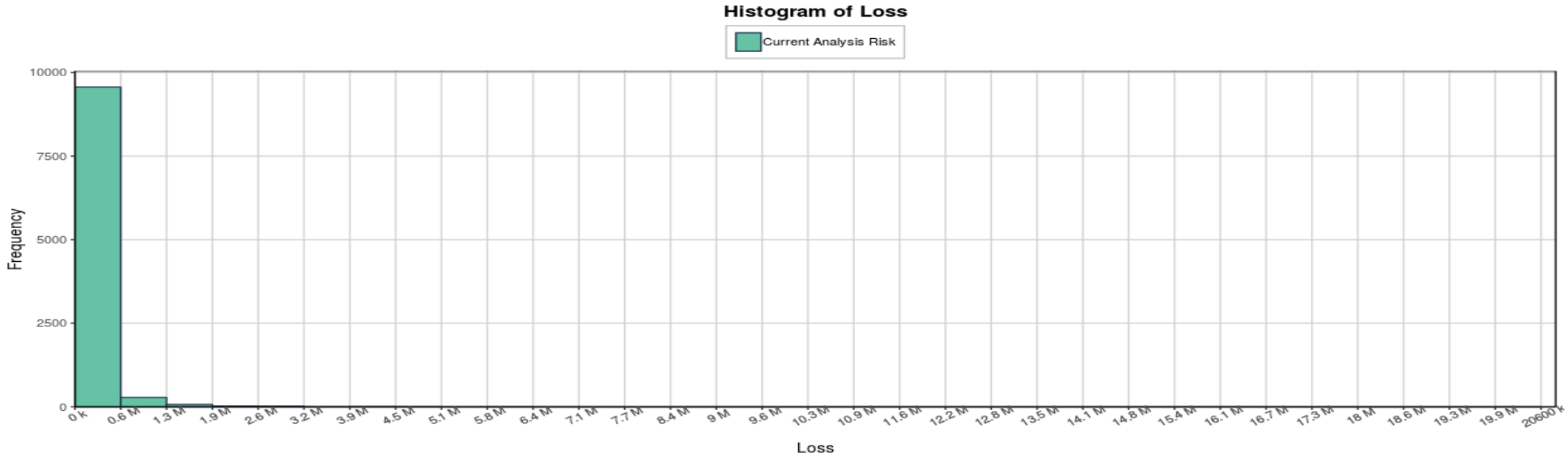
MAGIC – Simulazione HTMA – Risultati 1/2

Table 3: Summary table for Loss

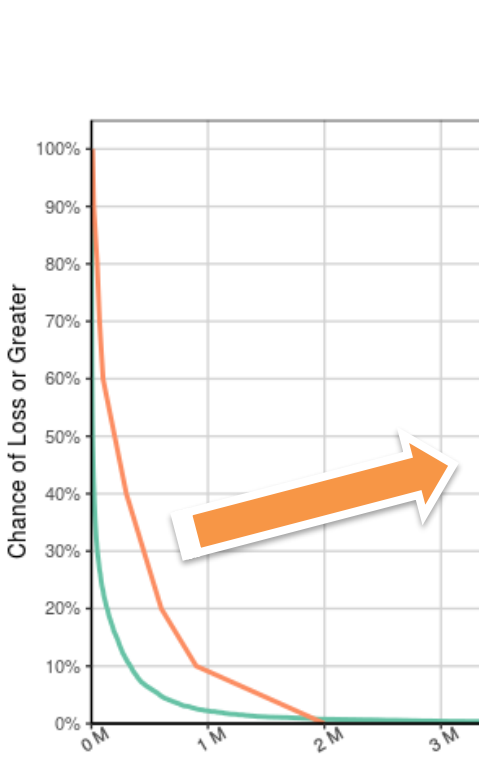
	Min	Avg	Max	Iterations
Current Analysis Risk	€0	€135,555	€20,557,303	10,000

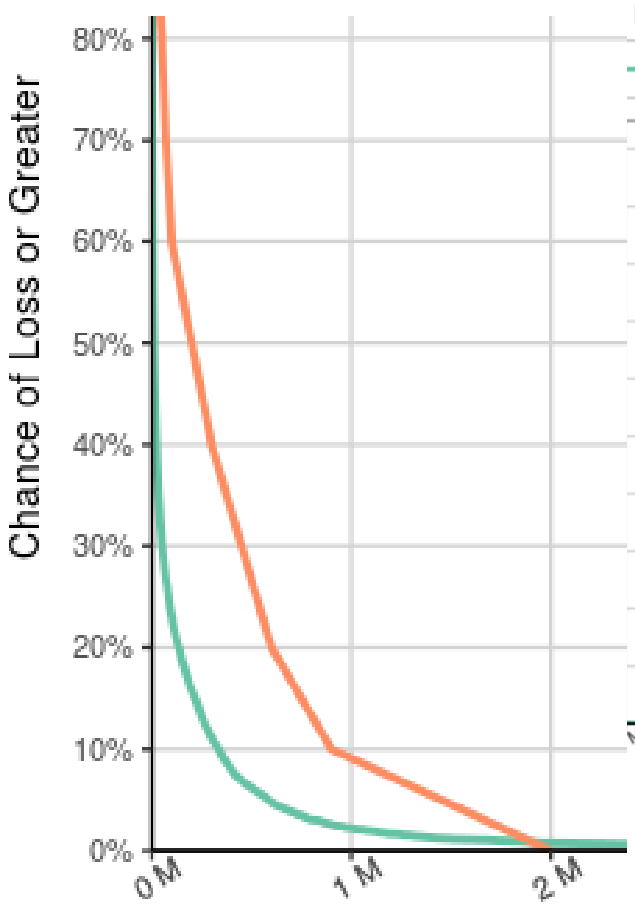
Table 4: Loss percentiles

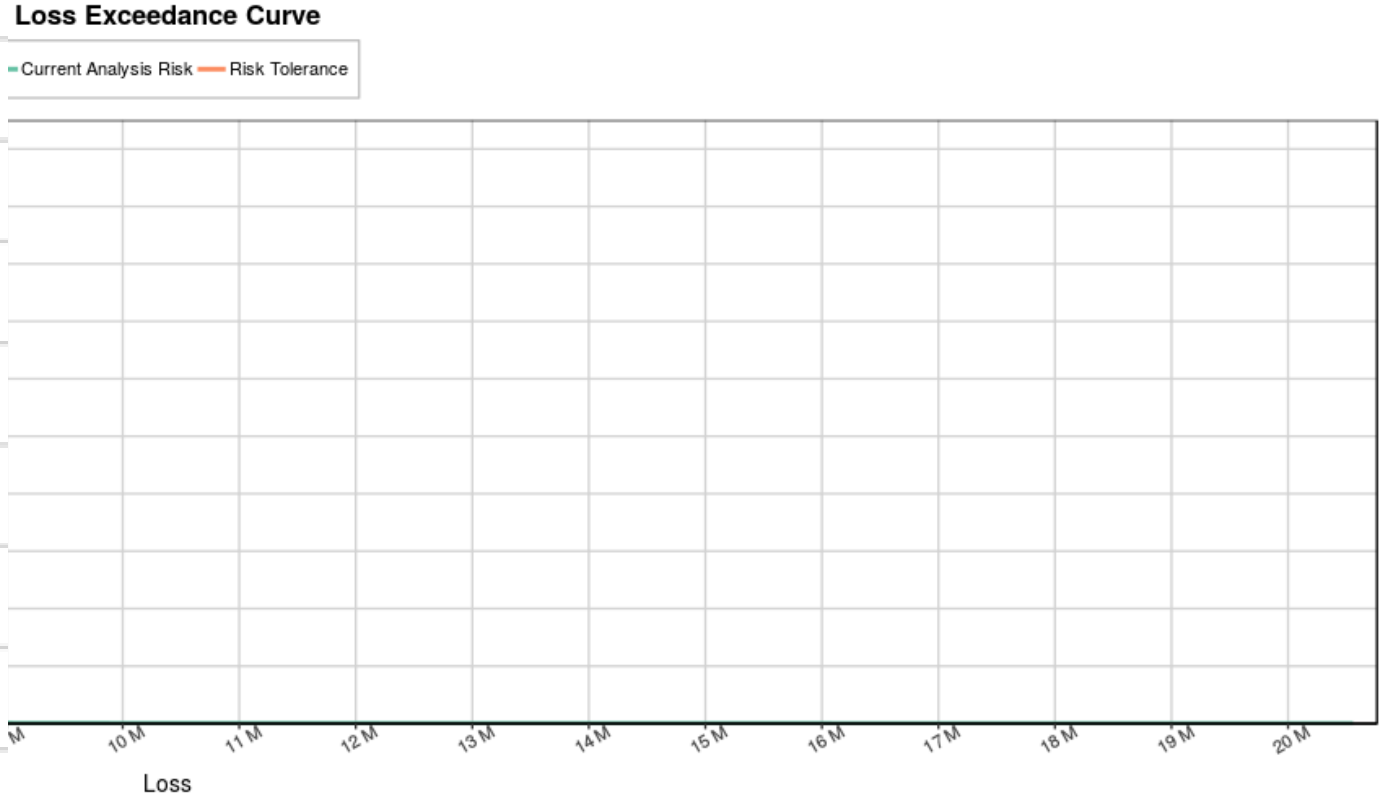
	10%	25%	50%	75%	90%	Iterations



MAGIC – Simulazione HTMA – Risultati 2/2







GRAZIE DELL'ATTENZIONE

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection