UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

A.C.M.E. Spa un caso d'uso del tool MAGIC

Ing. Sergio Martellini

Consulente libero professionista

sergiomartellini@gmail.com +39 3351315403

Con la collaborazione Ing. Giulia Rafaiani e Ing. Massimo Battaglioni

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione

- Sicuramente saprete come negli ultimi anni il meccanismo del M&A (Merge and Acquisition e le loro **Due Diligence**) sta irrompendo nella nostra realtà marchigiana, coinvolgendo in special modo le PMI più appetibili ;
- Mi occupo di consulenza direzionale da oltre 10 anni , in ambito Organizzazione e ICT e lavoro sul nostro territorio. Quindi ho pensato di portare la mia esperienza e calarla in modo operativo in questo lavoro di fine corso;
- **Vorrei analizzare una specifica tipologia di azienda perché credo possa essere di stimolo e interessante per tutti gli operatori del settore cybersec .**

Introduzione

- Tramite l'analisi di questo caso d'uso avremo la possibilità di valutare l'applicazione di un metodo quantitativo ad una classe specifica di aziende;
- Infatti il problema della bassa percezione da parte della proprietà del rischio cyber e del valore ad esso associato sarà il tema principale di questo lavoro ;
- **Mostriamo quindi uno strumento, che ci consenta con dei numeri, di attirare l'attenzione della proprietà e di sviluppare meglio il nostro lavoro in azienda.**

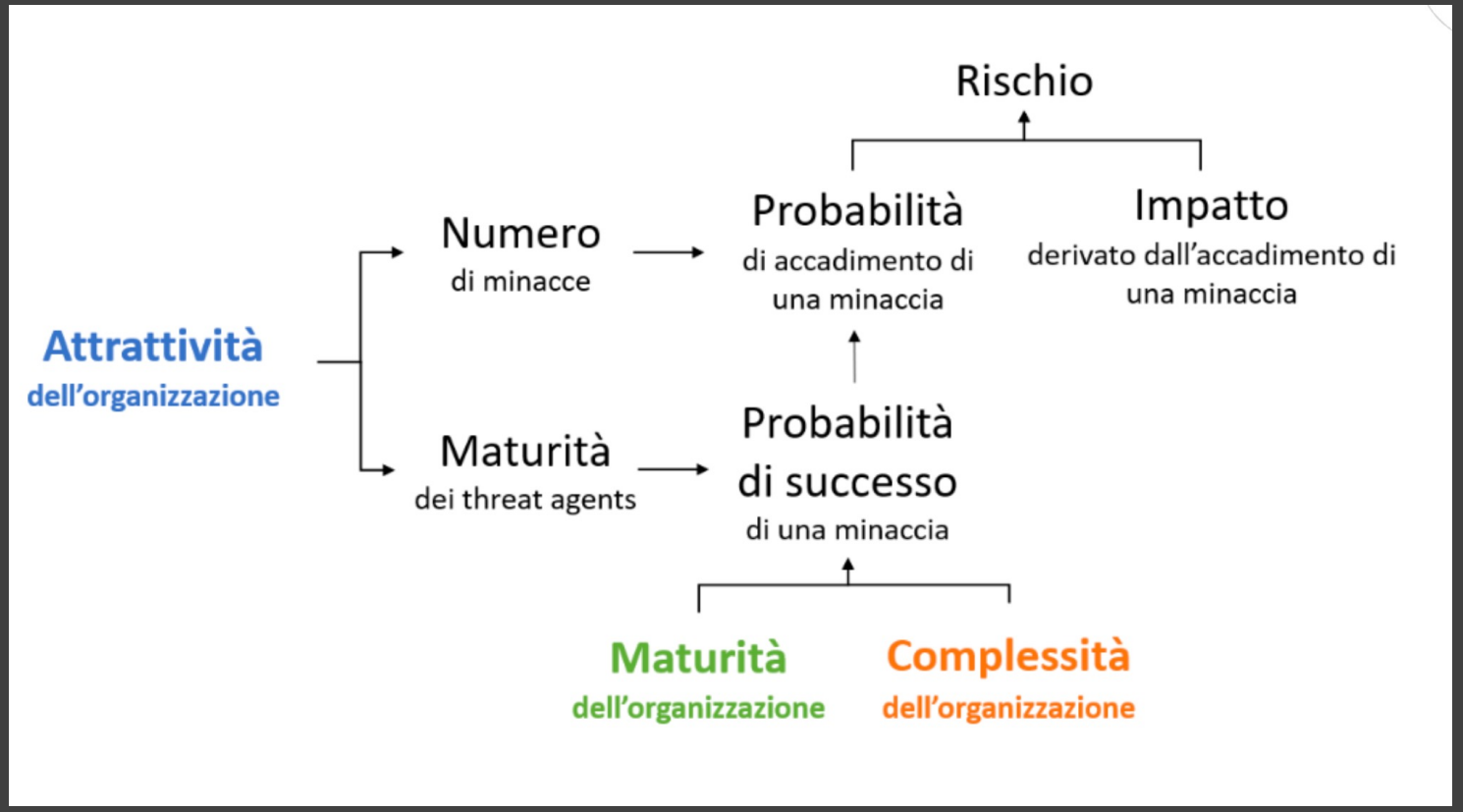
N1 Assunzioni per impostare modello

- Nello specifico ho considerato un’azienda target che ne sintetizza tre che sto seguendo in questo momento;
- I settori manifatturieri sono :
  - Fashion (Conceria e Calzaturificio)
  - Arredo (Componenti per Cucine)
- L’azienda modellizzata ha già una sua struttura e dei controlli implementati così come quelle reali prese ad esempio;
- Le minacce sono state customizzate escludendone alcune a priori e valutando le altre per le esperienze reali e dai report dei sistemi di sicurezza implementati.

N1 ACME spa Struttura Organizzativa e ICT

N2 Utilizzo del metodo di assessment MAGIC

Numero totale di dipendenti	**200**
Numero complessivo di postazioni di lavoro (PdL)	**140**
Numero totale di server, compresi i server virtuali	**25**
Numero complessivo delle istanze dei vari DBMS	**5**
Numero totale di FTE addetti tecnici al sistema informatico (dipendenti + eventuali esterni a contratto)	**1**
Numero totale di FTE dedicato al supporto postazioni di lavoro (dipendenti + eventuali esterni a	**1**



N2 Utilizzo del metodo di assessment MAGIC

Determinazione della Complessità

Valutazione Complessità

Profilo complessità *(per categoria)*	Livello di complessità	Complessità pesata	Num. quesiti	Peso %
Reti e infrastruttura	***Moderata***	***4,16***	11	37,93%
Tecnologie su reti IP	***Moderata***	**5,50**	4	13,79%
Applicazioni	***Bassa***	**3,70**	5	17,24%
Servizi online	***Significativa***	**6,67**	3	10,34%
Reparto IT	***Bassa***	**2,00**	6	20,69%
Complessità media	***Moderata***	***4,41***	**tot**	**tot**
Complessità media pesata	***Moderata***	***4,08***	**29**	**100,00%**

Grafico

N2 Utilizzo del metodo di assessment MAGIC

Controlli ESSENZIALI di cybersecurity		score	weight
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	Sì	1	1
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	1	0,9
Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	In parte	0,5	0,9
È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.	No	0	0,8
Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.	In parte	0,5	0,95
Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	In parte	0,5	1
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).	In parte	0,5	1
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.	In parte	0,5	1
Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	In parte	0,5	1
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.	In parte	0,5	0,9
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	1	1
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.	In parte	0,5	0,8
Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).	Sì	1	0,95
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.	In parte	0,5	0,9

Impostazione dei Controlli

Indice di Maturità

Indice di maturità medio	6,10

N2 Utilizzo del metodo di assesment MAGIC

Set minacce selezionate

Minacce	Probabilità di SUCCESSO	Inserisci questi dati: t	delta_t	n_avg
Malware	12%	365	1	48
Web-based attacks	8%			0
Phishing	10%			30
Web application attacks	8%			0
Spam	6%			30
DDoS	6%			0
Identity theft	8%			1
Data breach	12%			0
Insider threat	13%			1
Botnets	6%			0
Physical manipulation, damage, theft and loss	12%			1
Information leakage	20%			1
Ransomware	8%			75
Cyberespionage	8%			0
Cryptojacking	3%			0
Supply chain	12%			2

Probabilità di ACCADIMENTO
99%
0%
95%
0%
85%
0%
9%
0%
13%
0%
13%
19%
100%
0%
0%
23%

A	B	C	D
Minacce	**Probabilita di ACCADIMENTO**	**LB**	**UB**
Malware	**0.99**	400 €	30.000 €
Phishing	**0.95**	500 €	5.000 €
Spam	**0.85**	500 €	5.000 €
Identity theft	**0.09**	1.000 €	20.000 €
Insider threat	**0.13**	2.000 €	100.000 €
Physical manipulation, damage, theft and loss	**0.13**	500 €	10.000 €
Information leakage	**0.19**	1.000 €	100.000 €
Ransomware	**1.00**	400 €	150.000 €
Supply chain	**0.23**	5.000 €	500.000 €

Valorizzazione €

N3 Utilizzo del metodo di assessment MAGIC

- Abbiamo individuato una tabella di tolleranza del rischio a valore min e max;
- Abbiamo individuato il valore indicativo di un evento di medio bassa entità accaduto realmente e preso questo valore come accettabile dall'azienda 15.000€ ;
- Abbiamo eseguito simulazione con situazione corrente ;
- Poi abbiamo agito sui controlli massimizzando la maturità aziendale e andando poi a ri-simulare per poter comparare;

N3 Risultati simulazione

Table 2: Risk Tolerance

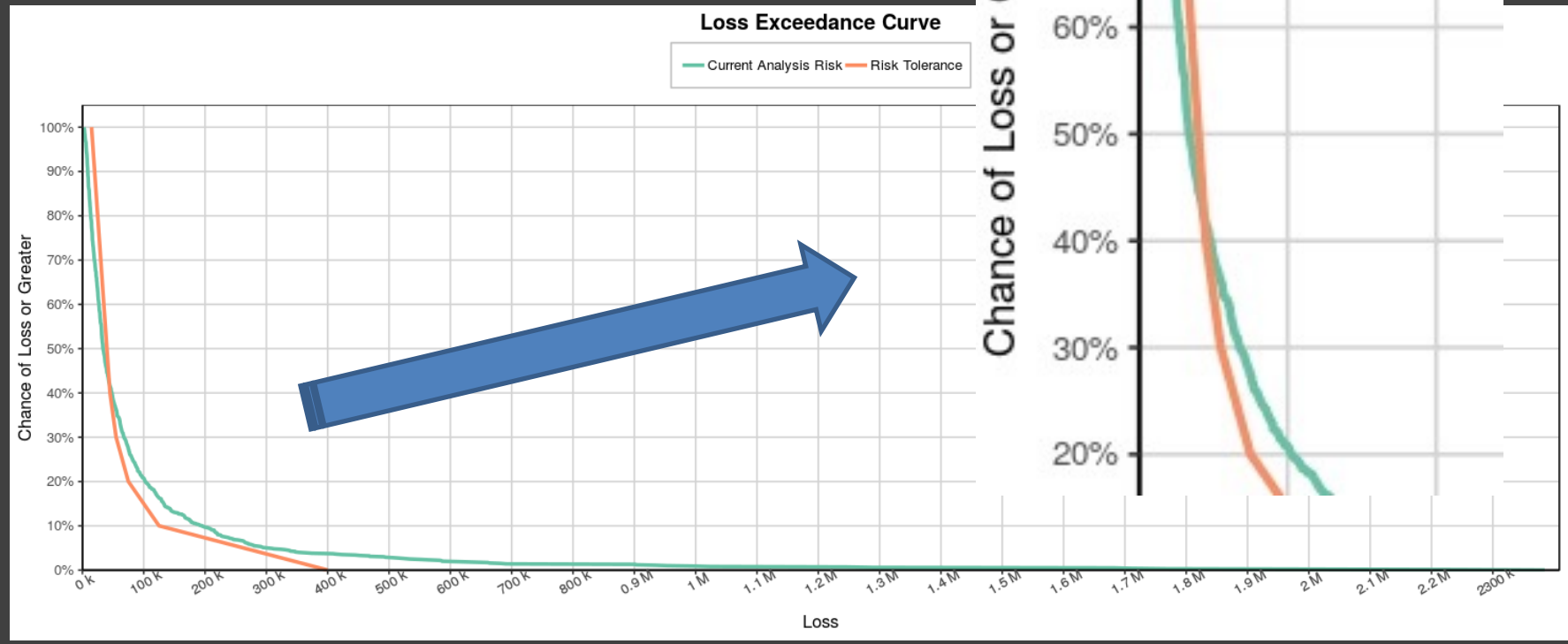
Loss	Chance of Loss or Greater
€15,000	100%
€20,000	90%
€25,000	80%
€30,000	70%
€35,000	60%
€40,000	50%
€45,000	40%
€55,000	30%
€75,000	20%
€125,000	10%
€400,000	0%

Table 3: Summary table for Loss

	Min	Avg	Max	Iterations
Current Analysis Risk	€1,892	€90,037	€2,384,545	1,000

Table 4: Loss percentiles

	10%	25%	50%	75%	90%	Iterations
Current Analysis Risk	€8,831	€16,328	€33,877	€81,922	€195,636	1,000



N3 Risultati simulazione

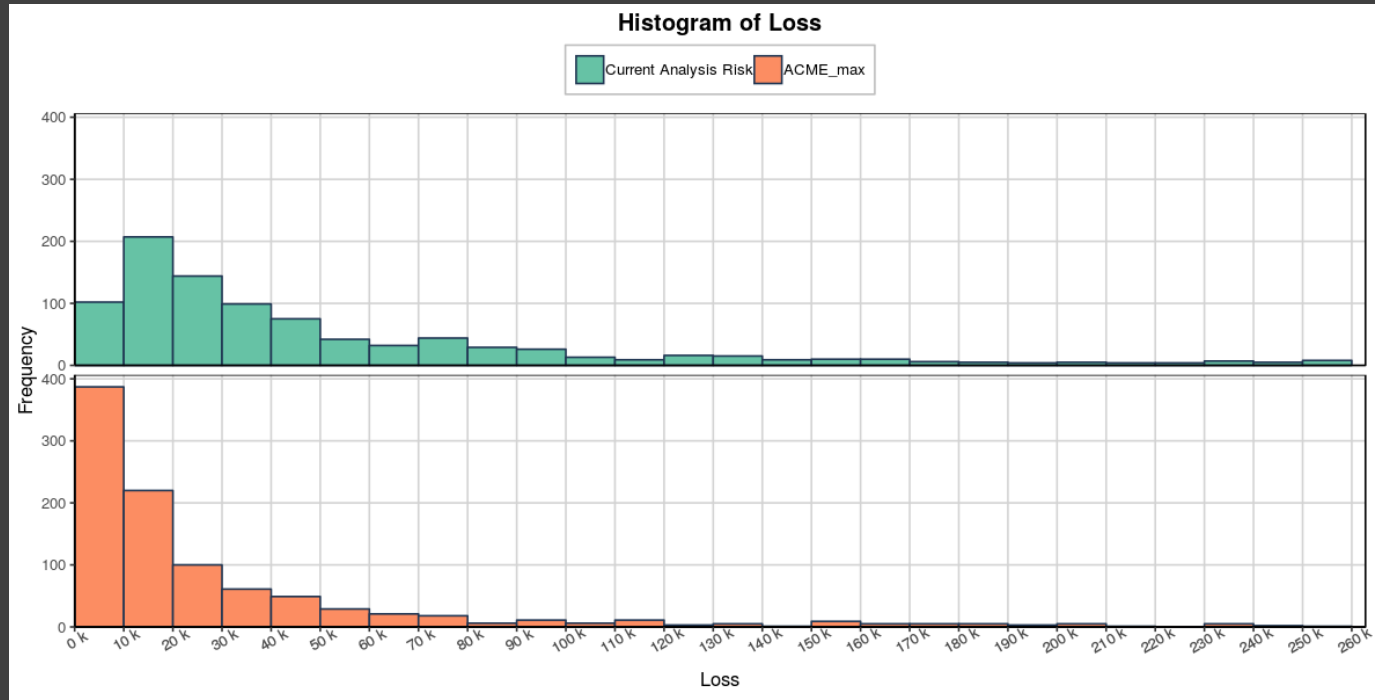
Table 3: Summary table for Loss

	Min	Avg	Max	Iterations
Current Analysis Risk	€1,739	€90,936	€2,642,385	1,000
ACME_max	€0	€43,566	€1,913,584	1,000

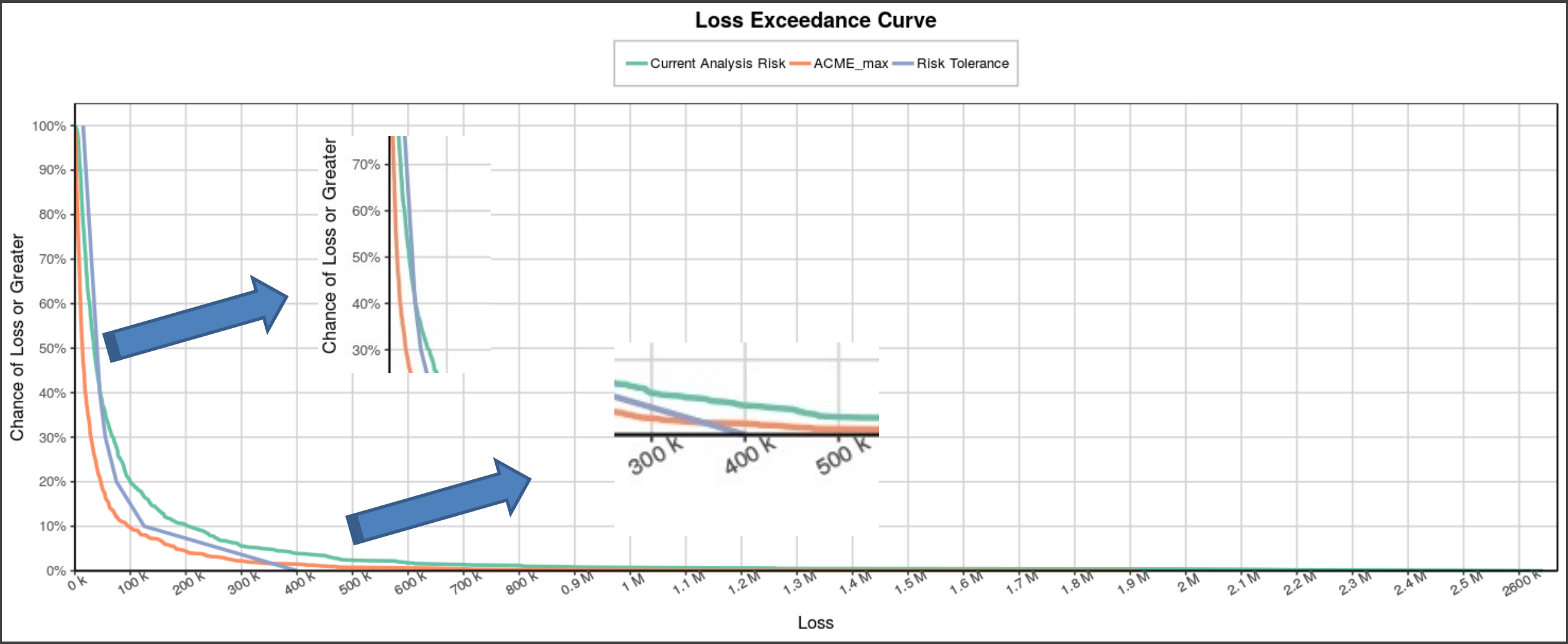
Table 4: Loss percentiles

	10%	25%	50%	75%	90%	Iterations
Current Analysis Risk	€9,852	€16,915	€34,582	€82,465	€204,532	1,000
ACME_max	€2,909	€6,267	€13,673	€37,053	€96,358	1,000

Comparazione tra corrente e massimizzato



N3 Risultati simulazione



N3 Utilizzo del metodo di assessment MAGIC

- Riepilogando, abbiamo applicato il metodo Magic ad un modello reale di azienda specifica ottenendo delle indicazioni interessanti riguardo il lavoro possibile sulla maturità aziendale;

A questo punto speriamo di lavorare insieme per poter affinare al meglio il metodo e applicarlo nel nostro lavoro quotidiano di supporto alle aziende.

Grazie .