RISK QUANTIFICATION IN PRATICA

Alberto Piamonte
alberto.piamonte@alice.it

The Biggest Cybersecurity Risk

Question: What is Your Single Biggest Risk in Cybersecurity?

Answer: How You Measure Cybersecurity Risk

Cosa dicono gli esperti (ed ISACA !)

- **It is possible to greatly improve on the existing methods.**

  Many aspects of existing methods have been measured and found wanting. This is not acceptable for the scale of the problems faced in cybersecurity.
- **Cybersecurity can use the same quantitative language of risk analysis used in other problems.**

  As we will see, there are plenty of fields with massive risk, minimal data, and profoundly chaotic actors that are regularly modelled using traditional mathematical methods. We do not need to reinvent terminology or methods from other fields that also have challenging risk analysis problems.
- **Methods exist that have already been measured to be an improvement over expert intuition**.

  This improvement exists even when methods are based, as are the current methods, on only the subjective judgment of cybersecurity experts.
- **These improved methods are entirely feasible.**

  We know this because it has already been done. One or both authors have had direct experience with using every method described in this book in real-world corporate environments. The methods are currently used by cybersecurity analysts with a variety of backgrounds.
- **You can improve further on these models with empirical data.**

  You have more data available than you think from a variety of existing and newly emerging sources. Even when data is scarce, mathematical methods with limited data can still be an improvement on subjective judgment alone. Even the risk analysis methods themselves can be measured and tracked to make continuous improvements.

Technical Guide

Requirements for Risk Assessment Methodologies

THE Open GROUP
Making standards work®

3 What Makes a Good Risk Assessment Methodology?

It is important that the information provided by the risk assessment is meaningful to both IT and non-IT management. There is one key component and several key traits that can help a risk assessment methodology provide meaning to an organization.

3.1 Key Component: ~~Taxonomy~~ Ontology

First and foremost, the risk management framework should provide a taxonomy for risk. Taxonomies are used to help those who study a certain body of knowledge to describe and define their problem space. A taxonomy provides a means for categorizing the information around us and helps organize the volumes of information in the field, increase the effectiveness of communication, and develop standardization.

A taxonomy for risk should seek to remove the ambiguity from terms like threat, vulnerability, and risk (itself having valid but similar definitions to threat and vulnerability).

3.2 Key Risk Assessment Traits

This section describes the traits that are indicative of a good risk assessment methodology. The set of traits provided is by no means complete or comprehensive, but establishes the fundamental concepts that risk assessment methodology development should strive for.

3.2.1 Probabilistic

A study and analysis of risk is a difficult task. Such an analysis involves a discussion of potential states, and it commonly involves using information that contains some level of uncertainty. And so, therefore, an analyst cannot exactly know the risk in past, current, or future state with absolute certainty.

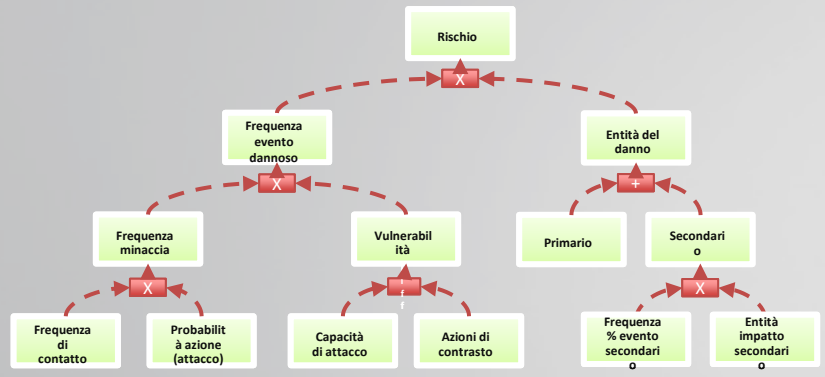
But ultimately a statement concerning risk is a belief statement – a belief statement that is simply the act of describing the issue currently at hand (sometimes referred to as a "state of nature") based on the evidence available at the time. The act of creating a belief statement based on evidence lends itself to using probabilistic methods. Treating risk as a probability problem can add needed rigor, scrutiny, and structure to the risk analysis process and outcome.

A good risk assessment methodology will be organized so as to assist the analyst in creating probabilities for risk and its component factors.

3.2.2 Accurate

A good risk assessment methodology should deliver accurate results. And while it seems self-evident that the results of the risk assessment should be accurate, many risk assessment methodologies focus more on the technical aspects of system weakness instead of the probability of exploitation and resultant impact.

Ontologia



Ontologia è il tentativo di formulare uno **schema concettuale esaustivo e rigoroso nell'ambito di un dato dominio**; si tratta generalmente di una struttura gerarchica di dati che contiene tutte le **entità rilevanti**, le **relazioni** esistenti fra di esse, le **regole**, gli assiomi, ed i vincoli specifici del dominio.

[Wikipedia: ontologia (informatica)]

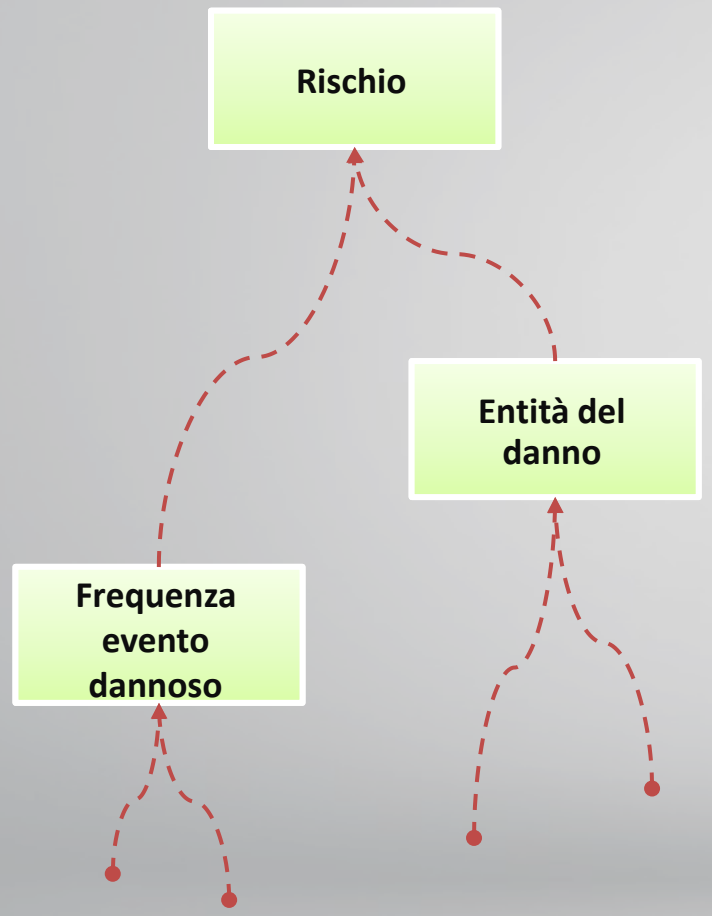
Probabilistico

- Uno studio e un'analisi del rischio è un compito difficile, infatti, spesso si deve partire da ipotesi fondate su informazioni incomplete, che contengono quindi un certo livello di incertezza.
- Tale “incertezza” non va mascherata, ma deve costituire anch’essa parte dell’informazione.
- Essa va quindi misurata e registrata perché divenga parte di una corretta analisi del rischio.
- L’incertezza può e deve essere un attributo dell’informazione, piuttosto che un limite della stessa.
- La sua comunicazione e il suo uso possono ottimizzare la gestione del rischio ed in particolare quella degli eventi dannosi e delle loro conseguenze.
- Solo trattando il rischio come un problema di previsione probabilistica può aggiungere il necessario rigore, controllo e struttura al processo di analisi.
- Una buona metodologia per la valutazione del rischio deve fornire all’analista gli strumenti per la stima delle sue probabilità e di quelle dei fattori costituenti.

Accuratezza e Precisione

- Accuratezza e precisione sono due termini spesso utilizzati in modo errato nel contesto della misurazione, perciò è importante conoscerne bene la differenza.
- *L'**accuratezza*** indica quanto una misura vicina è al valore reale, e quindi, **descrive una proprietà del *risultato***.
- La ***precisione***, d'altra parte, quantifica il grado di efficacia con cui sono state effettuate le misure, o quanto bene sono stati effettuati i calcoli.
- La precisione **dice qualcosa sul *processo di misurazione*** o sul calcolo, ma non dice nulla sul risultato della misurazione o sul valore calcolato.

Ontologia FAIR



Come considerare le grandezze coinvolte ?

Un concetto fondamentale:

Definition of Measurement

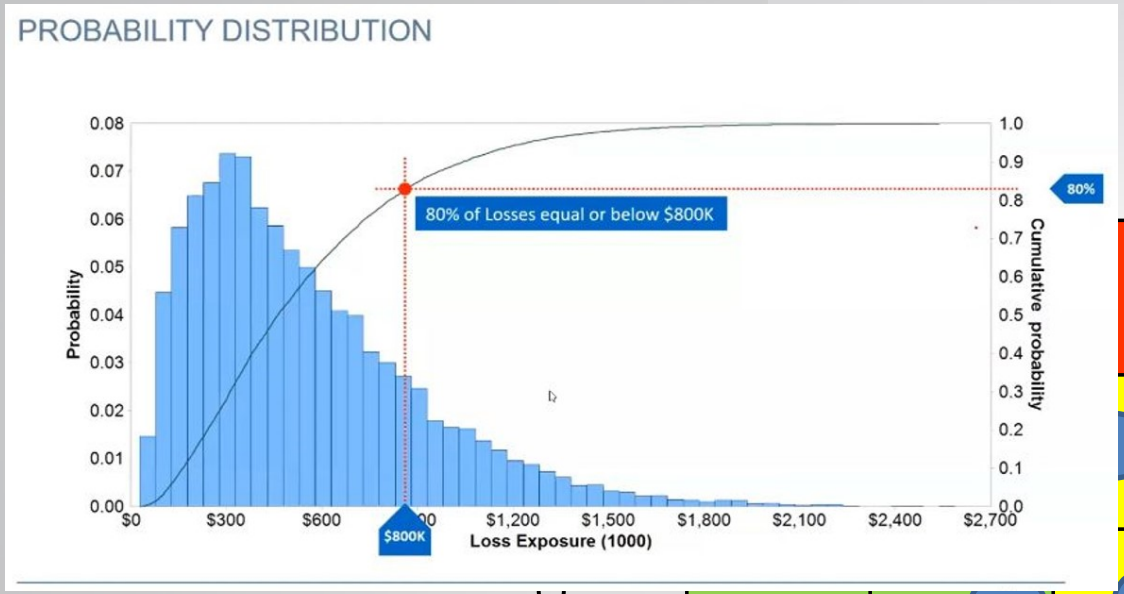
Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

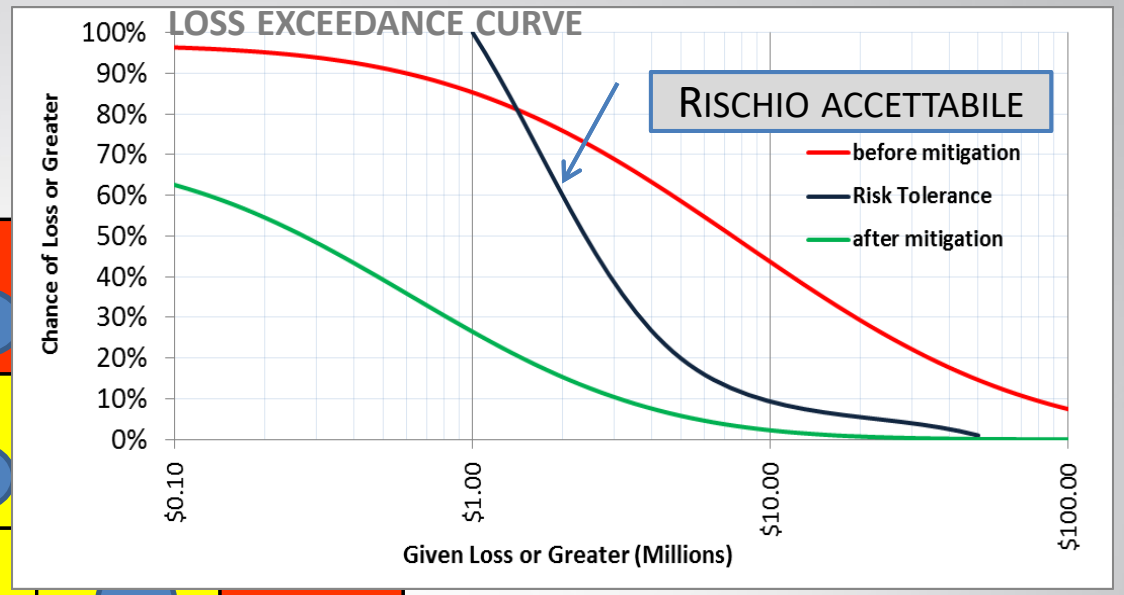
The practical differences between this definition and the most popular definitions of measurement are enormous.

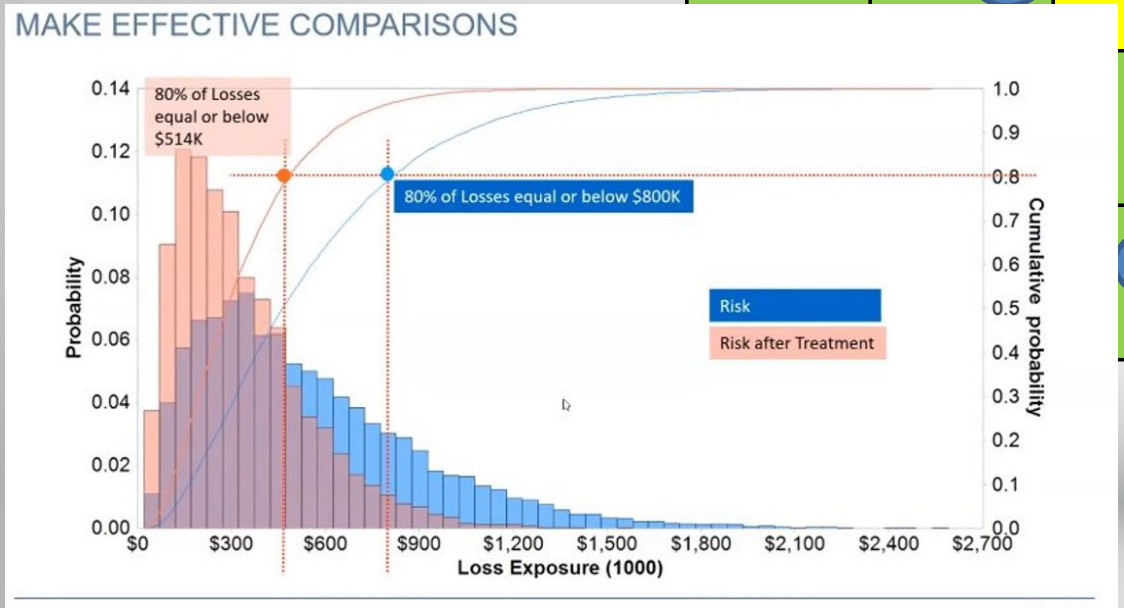
Not only does a true measurement not need to be infinitely precise to be considered a measurement, but the lack of reported error—implying the number is exact—can be an indication that empirical methods, such as sampling and experiments, were not used (i.e., it's not really a measurement at all).

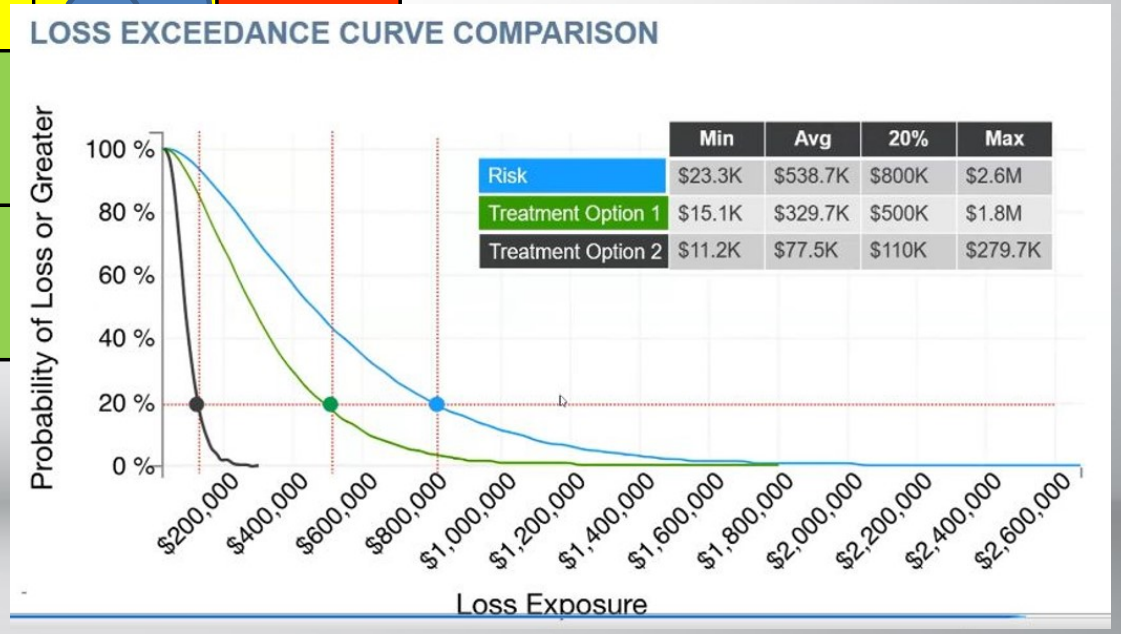
Measurements that would pass basic standards of scientific validity would report results with some specified degree of uncertainty, such as, "**There is a 90% chance that an attack on this system would cause it to be down somewhere between 1 and 8 hours**."

…. A measurement is, ultimately, **just information**, and there is a rigorous theoretical construct for information. field called "information theory", was developed in the 1940s by Claude Shannon, an American electrical engineer and mathematician.









Visione statistica

No Data? No Problem

by Jack Jones

- ……
- Start with an absurd estimate (e.g., less than an inch or greater than ten feet tall). It breaks the ice and gets people out of the “I have no idea” mindset.
- Use references and logical reasoning to begin narrowing the range.
- Challenge your reasoning along the way, and consciously look for reasons your range might be wrong.
- Remember that ***accuracy — not precision — is king***. Many people gravitate toward precision, but that’s a great way to end up with an inaccurate answer.
- …

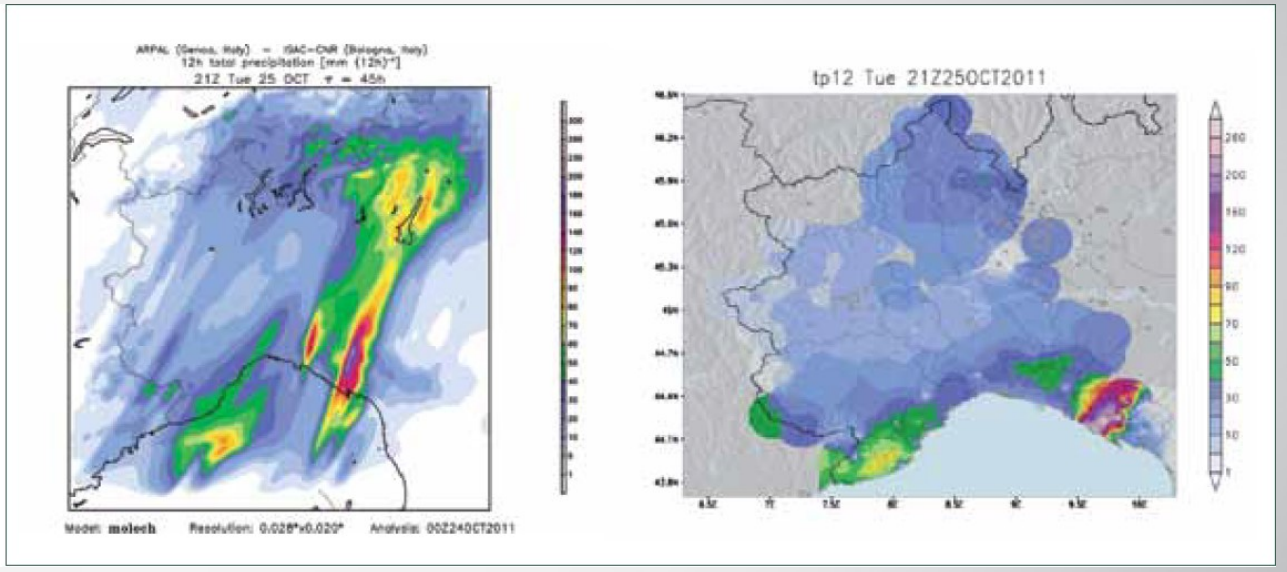
https://www.fairinstitute.org/blog/no-data-no-problem

Il valore della previsione, ovvero non solo qualità, ma anche utilità

Se la qualità si misura attraverso la “differenza” tra la previsione e l’osservazione, il valore indica la capacita di una previsione di incidere sui processi decisionali degli utenti che ne fanno uso: una previsione sarà di alto valore se permetterà a un *decision maker* di prendere la decisione più corretta in un dato contesto.

FIG. 2
PREVISIONI E ALLERTE

Alluvione del 25 ottobre 2012 sullo spezzino: a destra la pioggia osservata dalle 9 alle 21 UTC; a sinistra la stessa pioggia prevista dal modello MOLOCH del CNR-ISAC il giorno prima.



Previsione → Realtà

Da: **ecoscienza** N. 4/2012 Comunicare l’incertezza della previsione
Elisabetta Trovatore
Responsabile del Centro funzionale meteoidrologico della regione Liguria (Arpal)

Utilizzo FAIR con soluzioni DIY

- Lo standard è molto ben documentato anche nella parte relativa agli algoritmi di calcolo da utilizzare nei vari passaggi.
- EXCEL ha prestazioni eccellenti nei calcoli più complessi (Monte Carlo), possibili implementazioni del metodo sono ampiamente documentate
- Le funzioni statistiche necessarie (Beta-Pert) sono disponibili.
- Uno sviluppo autonomo non richiede competenze particolari e consente di rispondere anche ad esigenze specifiche.

. . . . a tra poco

OBIETTIVI DEL GRUPPO DI LAVORO SULL'ANALISI DEL RISCHIO.
A CHE PUNTO SIAMO

Glauco Bertocchi
g.bertocchi@isacaroma.it

I componenti del Gruppo di Lavoro sull'analisi del rischio

- Bari Silvano
- Bertocchi Glauco
- Cocozza Riccardo
- Della Mea Francesca
- Fei Luca
- Piamonte Alberto (*Coordinatore)*
- Pieralice Fabio
- Turano Fabio
- Valentini Alessia

Cosa abbiamo previsto come programma di attività all'inizio
(fine settembre 2020)

1. Posizionare i nuovi metodi quantitativi proposti rispetto allo schema di analisi del rischio ISO31000, in particolare individuando ruolo ed utilizzo dei controlli ISO 27001.
2. Gli scenari di minaccia (fonti ISACA (RiskIT), ENISA, ecc.) e i metodi quantitativi.
3. Utilizzo dei dati aziendali. Come utilizzare i dati aziendali relativi agli eventi ed agli incidenti di sicurezza per aggiornare in modo quantitativo l'analisi del rischio aziendale.
4. Analisi del rischio in campo privacy. Quale contributo si può avere utilizzando metodi quantitativi in ambito privacy.

Cosa abbiamo sinora affrontato (febbraio 2021)

1. Posizionare i nuovi metodi quantitativi proposti rispetto allo schema di analisi del rischio ISO31000, in particolare individuando ruolo ed utilizzo dei controlli ISO 27001.

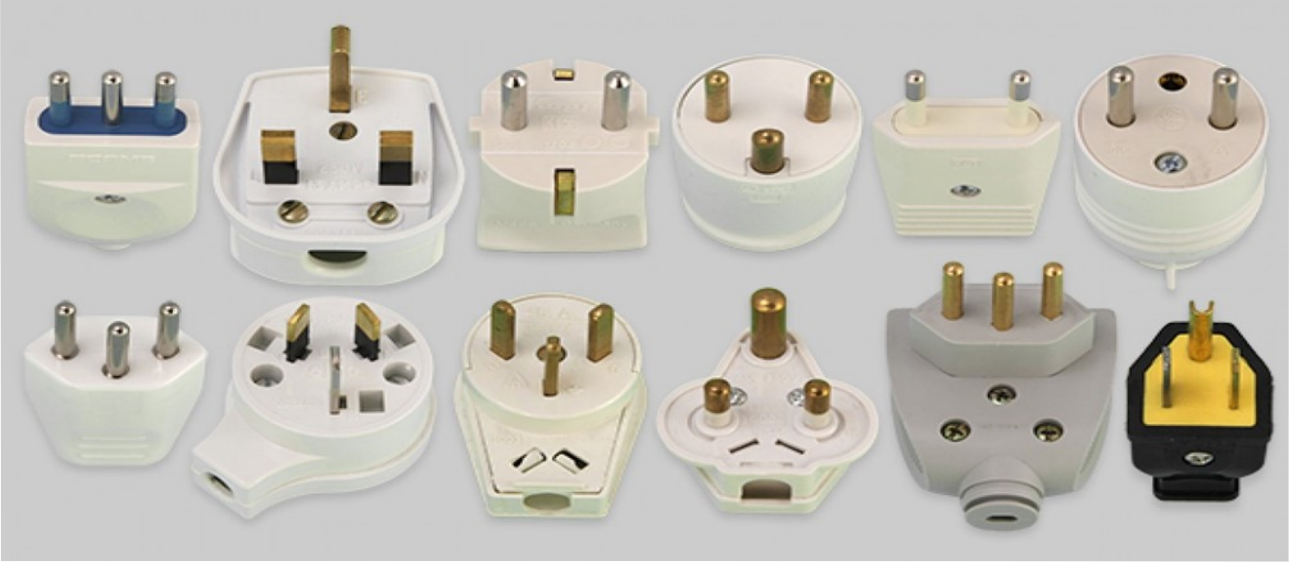
Sembra che sinora nessuno lo abbia affrontato

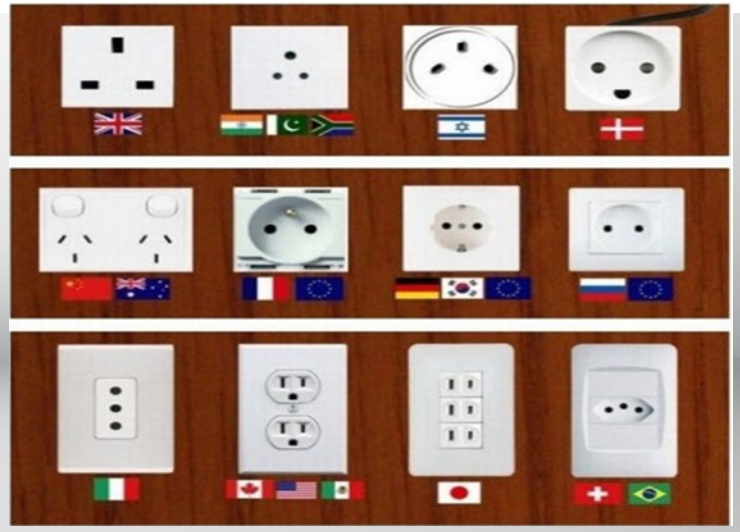
2. Utilizzo di scenari di minaccia con i metodi quantitativi.

Come abbiamo proceduto?

- *Cercando di definire termini e concetti (significati condivisi)*
- *Studiando, facendo esercizi «a casa», discutendo le differenze di opinione*
- *Sperimentando con un modello matematico per approfondire i concetti e consolidare le scelte*
- *Sinora abbiamo fatto 10 riunioni di tutto il Gruppo e diversi incontri ridotti – Tutto rigorosamente online*

Cosa pensavamo di dover affrontare? Un adattamento tra spine e prese?





La soluzione poteva essere un adattatore universale, un insieme di adattatori? O cosa?

A che punto siamo?

- E’ stato definito il **contesto** e le **finalità** con cui utilizzare i controlli ISO e l’ontologia FAIR per la valutazione quantitativa di uno **scenario** di minaccia
- E’ stato definito uno schema di **relazione** tra **i controlli** dell’ ISO 27001 e **l’ontologia** FAIR
- Esiste una **proposta di quantificazione** dei controlli ISO 27001 verso l’ontologia FAIR
- E’ stato realizzato un **modello di calcolo funzionante**

NELLA PROSSIMA ORA

PROVIAMO A RACCONTARVELO

DEFINIZIONE DEL PROBLEMA DI UN “BRIDGE” ISO 27001-FAIR.

Glauco Bertocchi

Porsi le domande giuste per definire gli obiettivi
La prima domanda

- E’ necessaria la definizione dell’ambito nel quale costruire un bridge (e quindi un modello) per “connettere” ISO 27k e FAIR
- La prima domanda cui rispondere è**: *quali parti dell’ISO 27k e del FAIR vogliamo porre in relazione?***
- Poiché il nostro ambito è **l’analisi dei rischi** dovremo scegliere la parte di **ISO 27k** che contiene tale ambito. Lo **Statement of Applicability (SOA)** elenca lo stato di applicazione dei controlli previsti dall’Annex A dello standard.
- Dal lato **FAIR** l’equivalente è rappresentato **dall’ontologia dei controlli** descritta nel cap. 11 del Il manuale di FAIR (2015).

La seconda domanda

- La seconda domanda è: ***quali sono le «dimensioni» del problema ?***
- La **prima ipotesi** è stata quella di considerare la modellazione **tutti i controlli ISO** elencati nell'Annex A **nell'ontologia FAIR corrispondente**.
- Ci sono almeno 114 controlli **lato ISO 27k**, ognuno dei quali composto **da N sub-controlli con N in funzione** delle varie modalità di attuazione di un singolo controllo (vedi ad esempio lo standard ISO 27002)
- **lato FAIR potremmo avere circa 30 controlli** per **ogni sub-controllo del lato ISO**. In caso di defence in depth la situazione si moltiplicherebbe per ogni livello di difesa.
- 114xNx30x livelli di difesa (con N probabilmente <100)
- **L'insieme risultante delle combinazioni** è probabilmente affrontabile dal punto di vista computazionale, anche se molto complesso.
- **MA… forse è meglio porsi qualche altra domanda**

La terza domanda

- La terza domanda è: ***quali sono i requisiti di utilità, gestibilità e validazione del «bridge»? (forse doveva essere la prima?)***
- **Deve essere utile e gestibile nell'applicazione a casi concreti, nonché deve produrre risultati significativi e possibilmente «validabili».**
- Per una modellazione completa si dovrebbero valutare migliaia di "stime" dei controlli ISO
- Come faremo a validare un modello così complesso e quale sarebbe l'affidabilità dei risultati?

Temo che potrebbe finire così

Questo è quello che volevamo ottene

ISO

FAIR

Cambiamo approccio:
per cosa è stato ideato FAIR e per quali obiettivi è utile ISO?

- La **metodologia FAIR** si presta ad un approccio **top-down** e ha la capacità di utilizzare **scenari e valutazioni su fattori aggregati**, anche senza disporre di dati dettagliati.
- ISO 27001 ha l'obiettivo di definire un **sistema di gestione della sicurezza delle informazioni (ISMS)** che sia certificabile e quindi sia sottoponibile ad audit.
- L'obiettivo ISO è quello **della compliance e della esaustività dei processi aziendali di sicurezza** (controlli) rispetto ad un'**analisi complessiva dei rischi** cui l'organizzazione è esposta. Può indicare la **postura aziendale** nei confronti della sicurezza in termini **di efficacia ed efficienza dei processi.**

Cambiato l'approccio si deve variare anche il tipo di domanda

- Se la **mia organizzazione** subisce un **attacco** (ad esempio ramsonware) quali sono i **probabili danni in termini economici** e quali sono **i fattori su** cui posso maggiormente **incidere** per **ridurre** i danni e come **comparo economicamente le alternative**?" .
- Per rispondere alla prima parte della domanda, devo contestualizzare la **minaccia rispetto alla difesa cyber già presente in azienda.** Quindi utilizzare i dati provenienti dallo ISMS ISO 27k, nel quale sono contenute le informazioni relative ai **controlli in atto , alla loro implementazione e all'efficacia**.
- Per rispondere alla seconda parte della domanda devo utilizzare uno **strumento** che consenta **l'analisi quantitativa** (importi e probabilità) dello scenario di minaccia con **tecniche statistiche evolute** come, ad esempio le distribuzioni di probabilità e le simulazioni di tipo Montecarlo.

Abbiamo compreso in quale ambito e come realizzare il Bridge ISO 27k -FAIR

- La modellazione ISO -FAIR è **utile**, e **limitata in termini di complessità,** per analizzare uno **scenario di minaccia,** ed effettuare una **valutazione quantitativa** dei rischi derivanti dallo stesso. A tal fine si **utilizzano anche i controlli** dello I**SMS** eventualmente presente.
- Abbiamo esemplificato lo ISMS con l'ISO 27001 ma riteniamo che la **metodologi**a si possa **applicare**, ovviamente con adattamenti di dettaglio, per un **sistema similare quale, ad esempio il NIST800-53r4, basato sulla definizione e l'applicazione di famiglie di controlli**.
- **Dai controlli (ambito ISO 27k**) in **atto** e dalla loro **efficacia** si derivano delle **stime di mitigazione** dei **fattori di rischio** dell'ontologia **FAIR**.

La metodologia

Per **utilizzare** i controlli (ISO 27k o altro similare) per **mitigare** i rischi di uno **scenario di minaccia analizzato con FAIR** si può utilizzare la seguente metodologia:

1. Si identificano i controlli ISO che sono interessati dallo scenario oggetto di analisi
2. Per ciascuno dei controlli ISO identificati si esegue la modellazione nei confronti dei controlli dell'ontologia FAIR; ossia si valorizzano, con i metodi descritti nel prosieguo della presentazione, i controlli ISO
3. Si utilizzano i controlli FAIR, modellati e valorizzati con quelli ISO, per l'analisi quantitativa dello scenario di minaccia.

Grazie per l’attenzione

Passo la parola al prossimo relatore

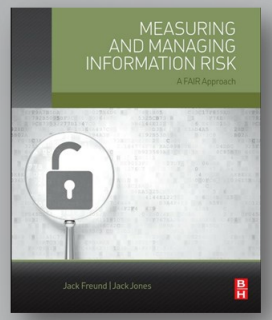
ONTOLOGIA FAIR E CONTROLLI ISO

Francesca Della Mea
f.dellamea@hotmail.com

Facciamo un passo indietro… di cosa parliamo quanto parliamo di FAIR?

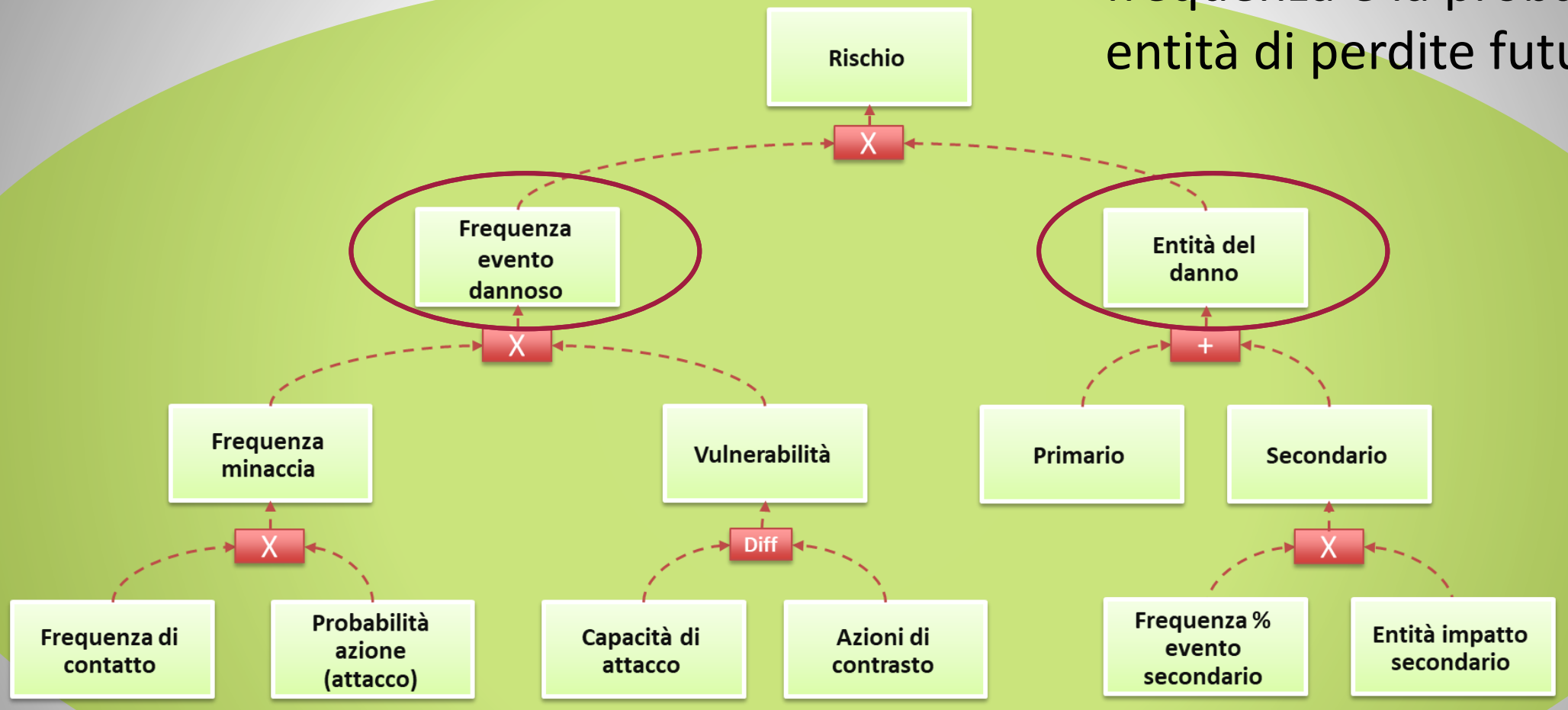
- **Framework** di risk assessment and management
- **Ontologia di fattori**, per arrivare ad una stima quantitativa accurate delle possibili perdite

- Non a caso «FAIR»: **Factor Analysis** of Information Risk



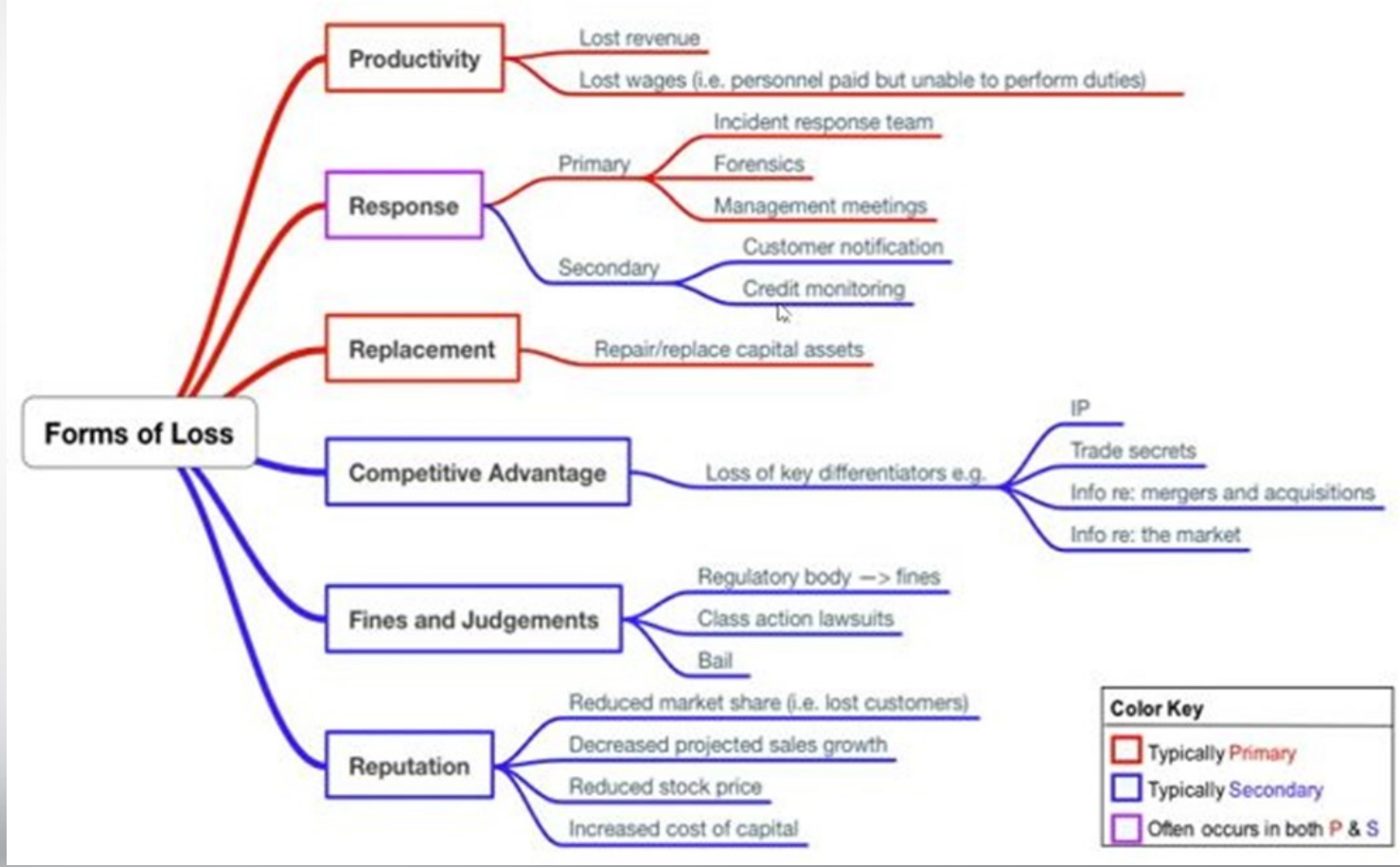
Ontologia dei fattori FAIR

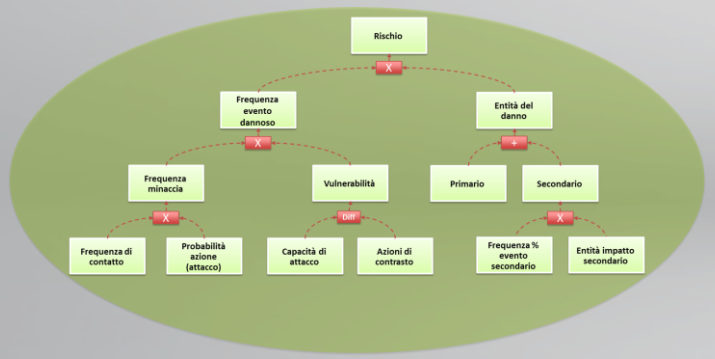
Rischio è “la probabile frequenza e la probabile entità di perdite future”



Ampiezza delle forme di danno

- Tipologie di danno legate non solo IT, ma legate a possibili impatti del “digital risk”

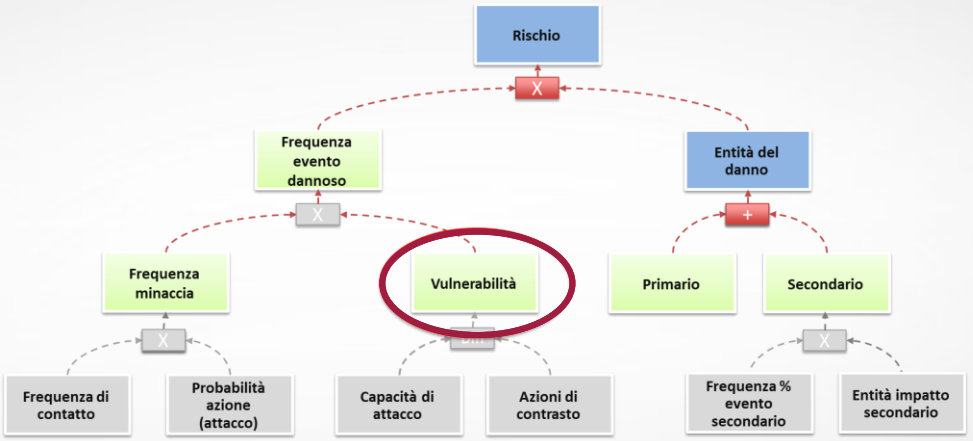




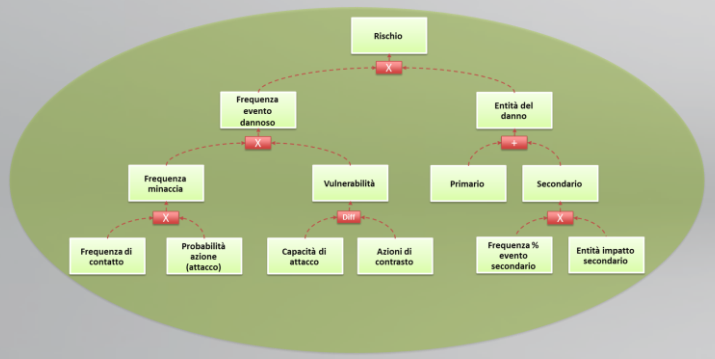
https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model

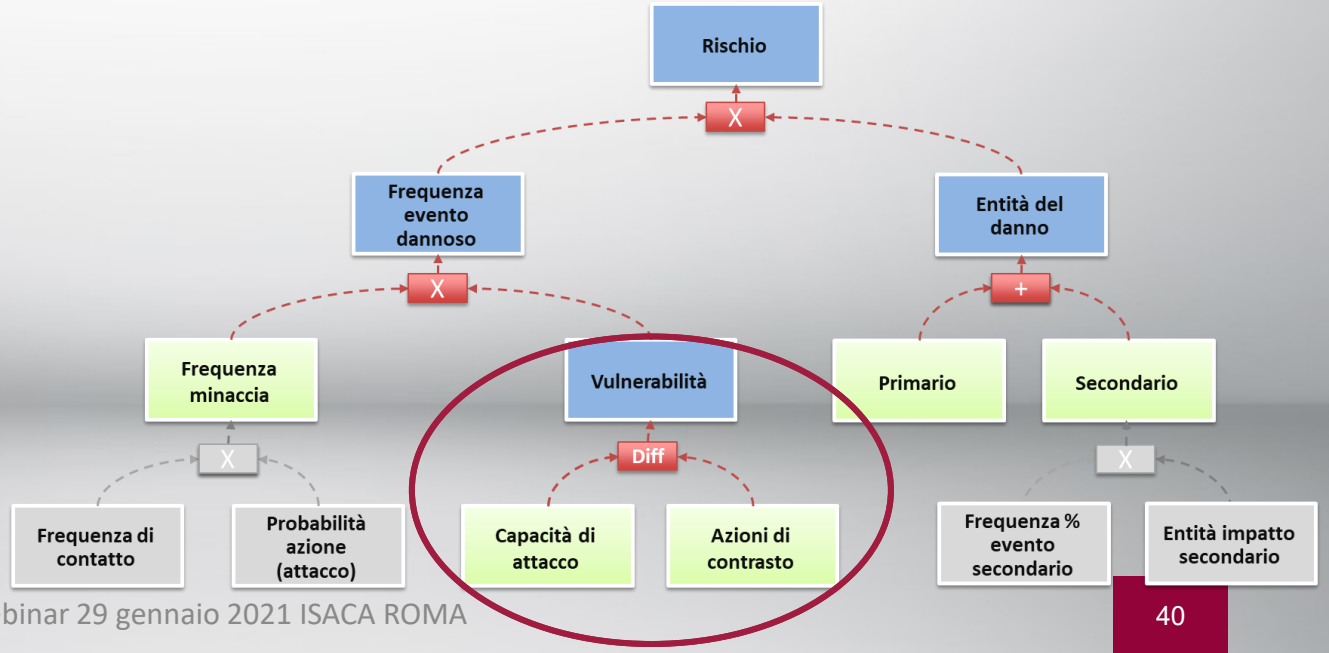
Livello di dettaglio delle stime

- L'accuratezza della stima in generale è maggiore quanto più dettagliato è l'input che si inserisce



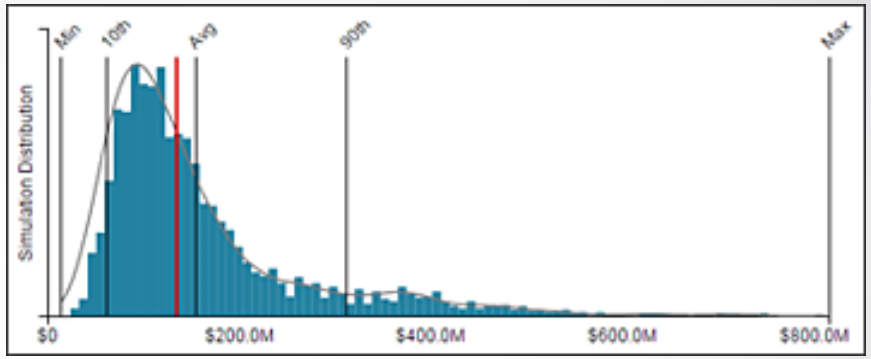
Non utilizzato	
Inserito	
Calcolato	





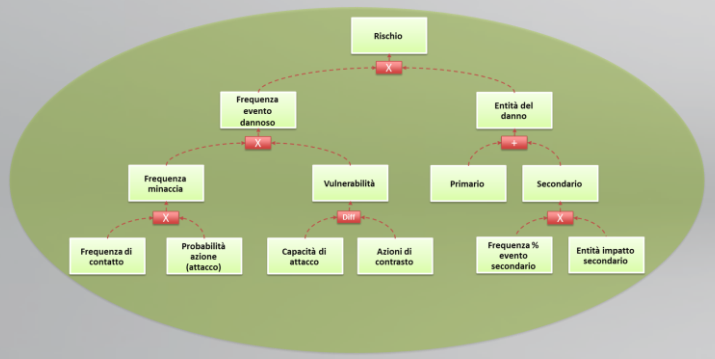
Ontologia FAIR e approccio probabilistico

- L'approccio probabilistico è applicato a tutti i fattori



Non utilizzato	
Inserito	
Calcolato	

Non utilizzato			
Inserito	**MIN**	**PIÙ PROB**	**MAX**
Calcolato	**MONTE CARLO**		



=> se ne parlerà in dettaglio nella sessione pratica

Come misurare le grandezze coinvolte?

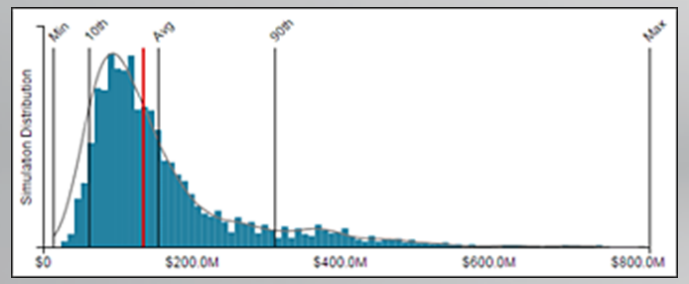
- **Un concetto fondamentale: misura come riduzione dell'incertezza**

Definition of Measurement

Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

Cioè: non è necessaria la precisione per considerare valida una misurazione, mentre la mancata indicazione di margine errore (cioè affermare che il valore è esatto), può essere un indicatore che non sono stati adottati metodi adeguati, e quindi che la misura non è valida.

Ad es. *"un attacco a questo sistema può causare un down tra 1 e 8 ore con una probabilità del 90% "*



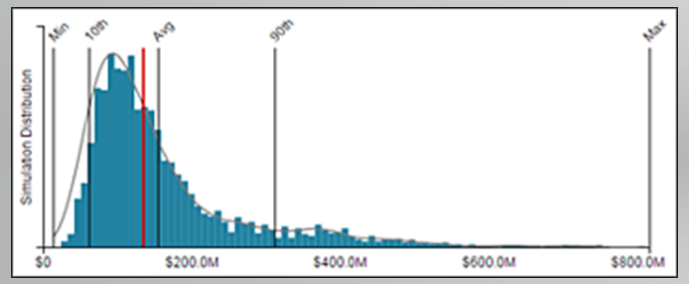
Cerchiamo misure accurate:

- L'**accuratezza** indica quanto una misura vicina è al valore reale, e quindi, descrive una proprietà del risultato
- La **precisione** quantifica il grado di efficacia con cui sono state effettuate le misure, o quanto bene sono stati effettuati i calcoli

Affrontare l’incertezza

- Uno studio e un'analisi del rischio è un compito **difficile**, infatti, spesso si deve partire da **ipotesi** fondate su **informazioni incomplete**, che contengono quindi un certo livello di incertezza.
    - Questa “incertezza” non va mascherata, ma deve costituire anch’essa parte dell’informazione
    - L’incertezza può e deve essere un attributo dell’informazione, piuttosto che un limite della stessa
    - Va quindi misurata e registrata perché divenga parte di una corretta analisi del rischio
    - La sua comunicazione e il suo uso possono ottimizzare la gestione del rischio ed in particolare quella degli eventi dannosi e delle loro conseguenze

- Le ricerche ci dicono che:
    - Non tutti siamo in grado di stimare correttamente le probabilità di accadimento di un evento o l’entità del danno potenziale
    - **Tutti possono imparare a farlo**, anche in modo più che soddisfacente
    - Conosciamo molto più di quanto si creda!

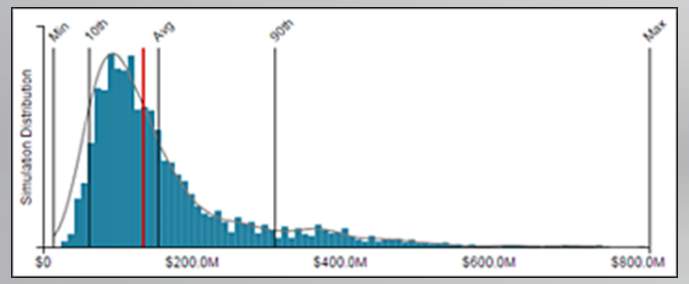


Stimando s'impara: la calibrazione

- La **calibrazione** della stima è un processo che permette di ridurre i pregiudizi cognitive e fornire stime **accurate** anche quando I dati disponibili sono pochi

    1. Comincia con una stima assurda – aiuta a far capire che raramente è vera l'impressione di «non averne idea»
    2. Elimina i valori molto improbabili
    3. Fai riferimento ad elementi che conosci e ragionamenti logici per restringere il campo
    4. Valuta ripetutamente il livello di confidenza che hai della stima, e analizza possibili ragioni per chi l'intervallo potrebbe essere sbagliato

Remember that ***accuracy — not precision — is king***. Many people gravitate toward precision, but that's a great way to end up with an inaccurate answer *



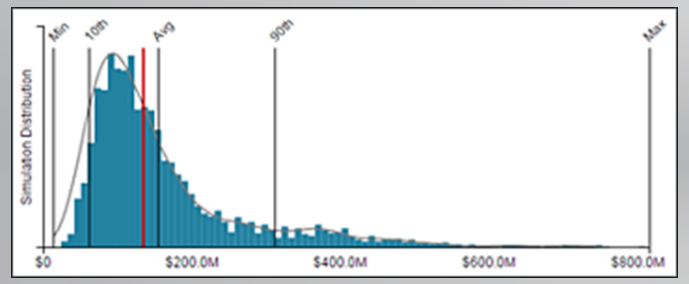
**https://www.fairinstitute.org/blog/no-data-no-problem*

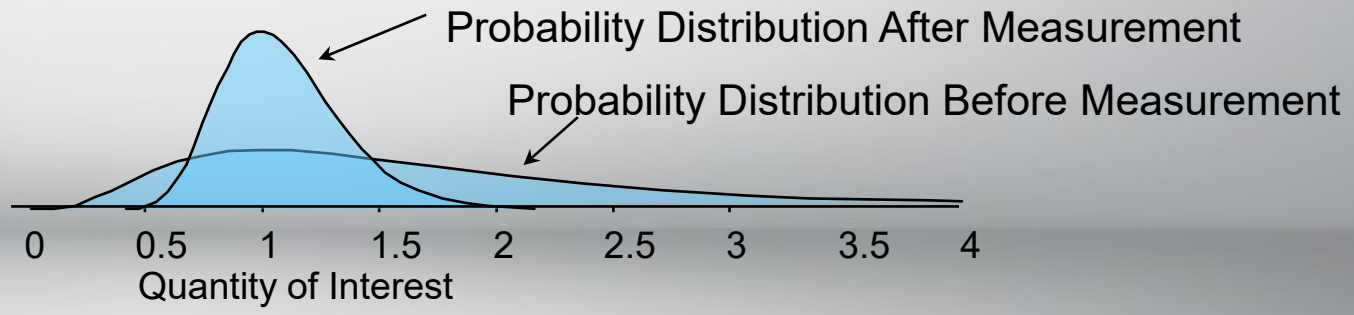
Misurare per ridurre l'incertezza

Definition of Measurement

Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

- Riduzioni anche marginali dell'incertezza della misurazione possono essere di gran valore
- Quindi: ripetere le osservazioni, applicare i metodi di calibrazione, migliorare la capacità di stima

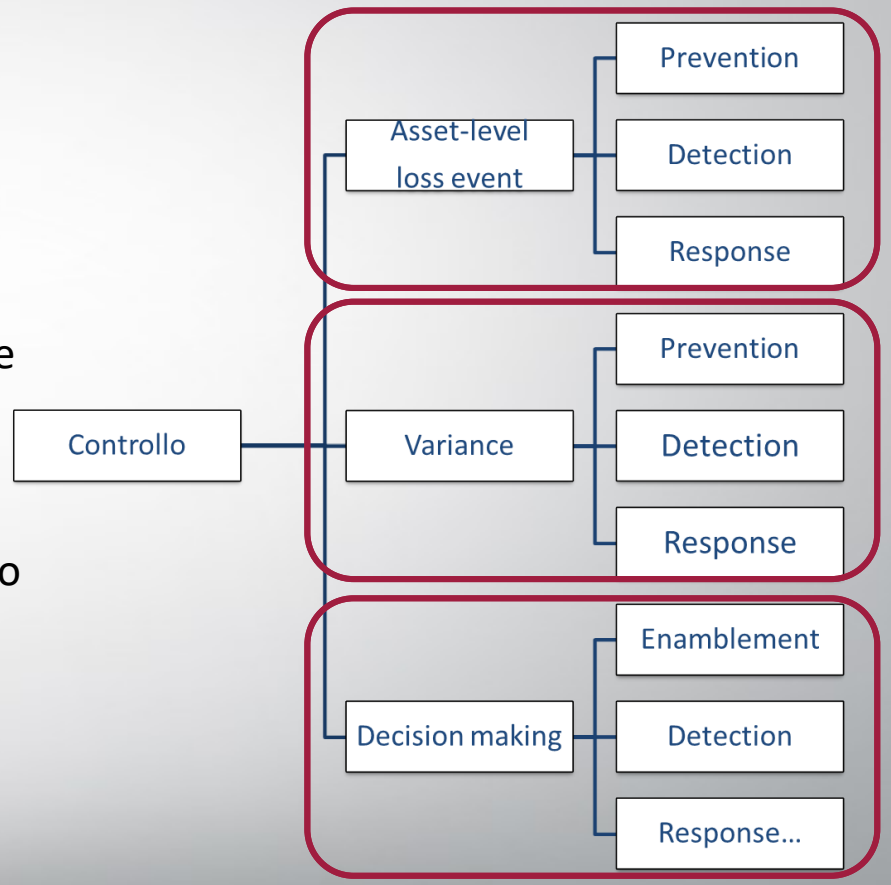


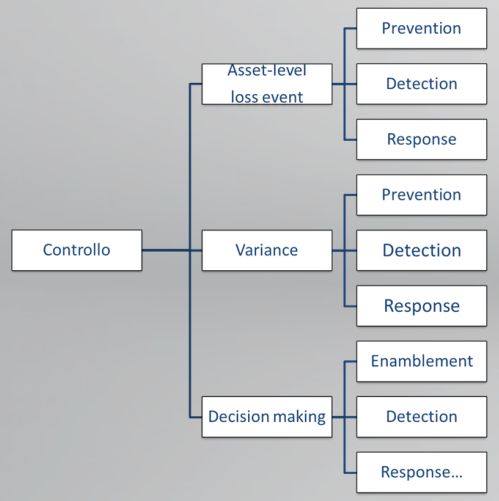


Ontologia dei controlli

Anche per i controlli FAIR è disponibile una dettagliata ontologia

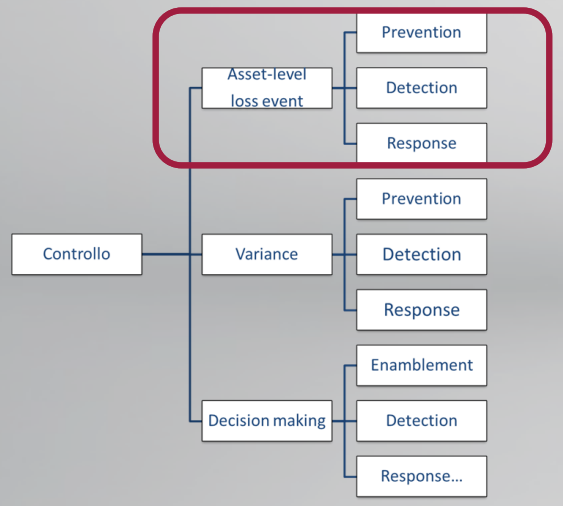
- L'ontologia, ad alto livello, identifica tre categorie di controlli:
  - *Asset-level*
  - *Variance*
  - *Decision Making*
- Correla i controlli con il ruolo che assolvono nella gestione del rischio
- I ruoli chiamati in causa non sono sovrapponibile alle "linee di difesa" – sono piuttosto livelli di responsabilità nelle decisioni





=> Questa ontologia finora è stata meno utilizzata sul campo rispetto a quella dei fattori di rischio

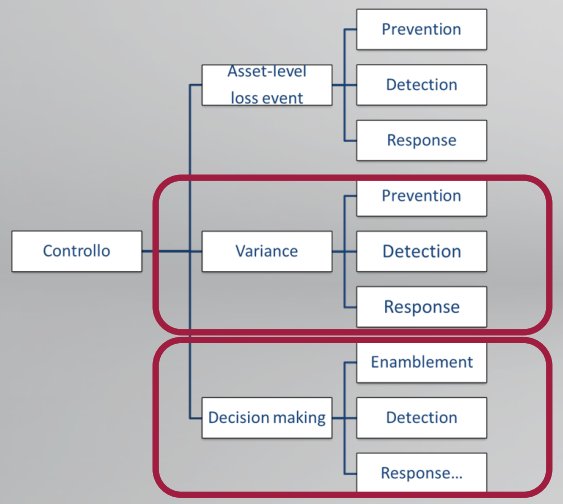
Asset Level control



Asset-level control

- Controlli con effetto diretto su frequenza o entità della perdita derivante da **eventi** che possono accadere **agli asset**
  - Patching sistemi, controllo accessi, privilegi, backup e recovery…
- Questi controlli sono collegati alla gestione dell'esposizione al rischio

Variance Control e Decision Making Control



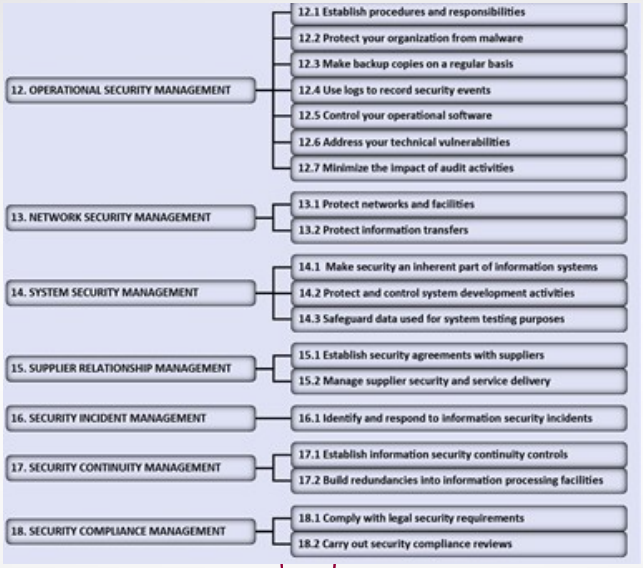
Variance control

- Controlli che hanno l'obiettivo di ridurre la variazione dell'efficacia dei controlli asset-level nel tempo.
- Esempi:
  - Politiche, standard, training, awareness, definizione di processi, automazione
  - Auditing, testing, verifiche a posteriori
- La gestione della varianza è elemento chiave perché i controlli asset-level siano efficaci nel tempo
- Spesso lo stato delle controlli di varianza è il migliore indicatore della «posture» di rischio di una organizzazione

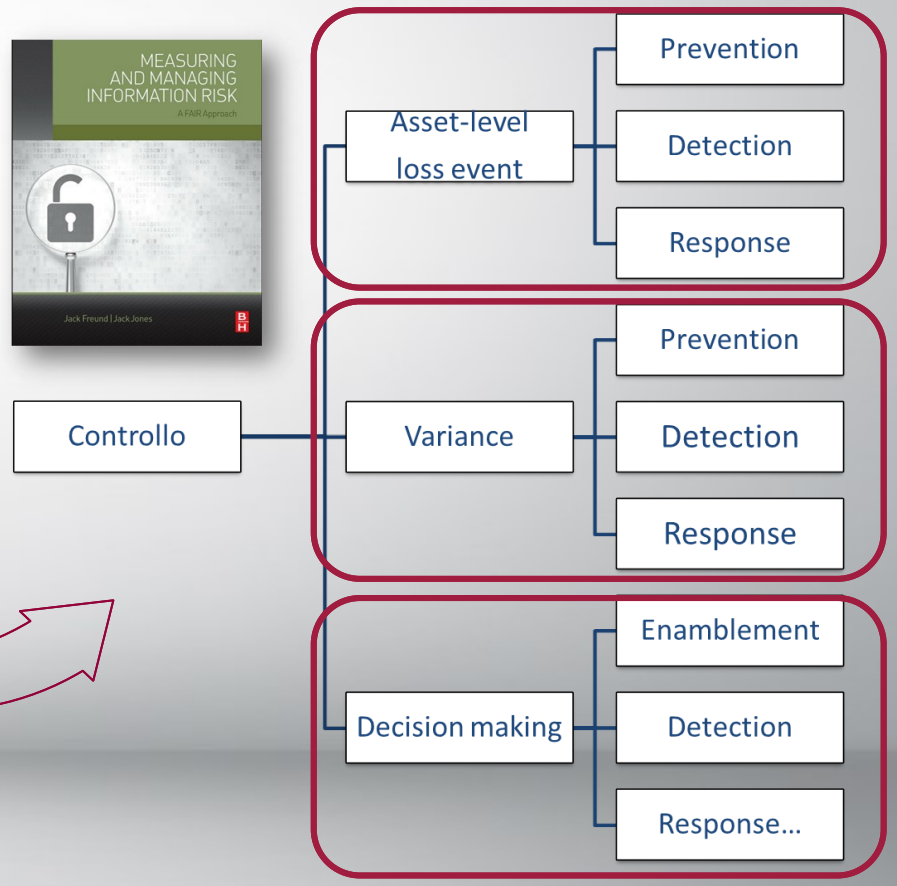
Decision-making control

- Elementi che aiutano a definire le aspettative a livello di rischio, e ad allocare le risorse per raggiungere gli obiettivi di gestione del rischio
- Controlli che hanno l'obiettivo di prevenire, rilevare e rispondere a decisioni errate di gestione del rischio

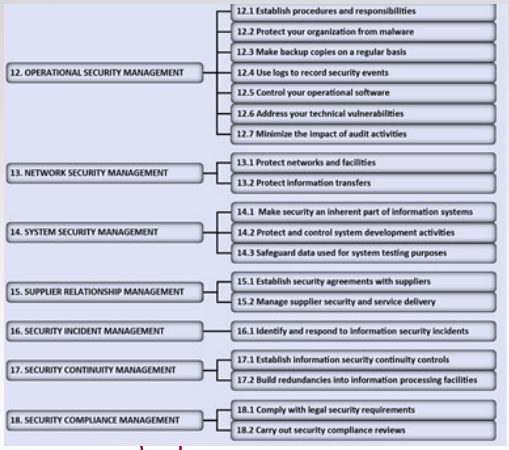
Controlli ISO e controlli FAIR

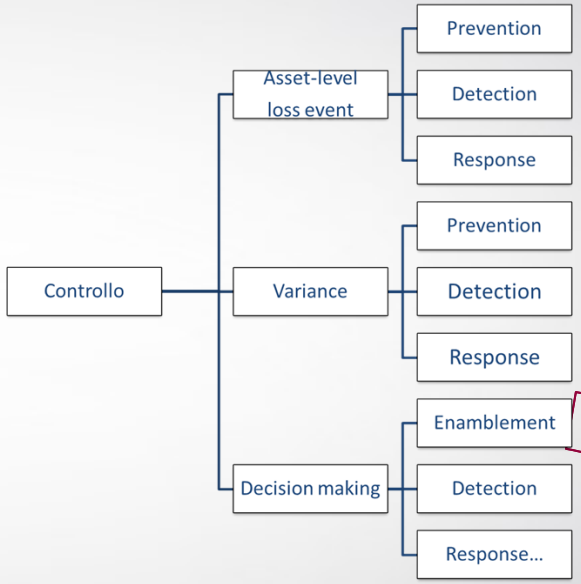


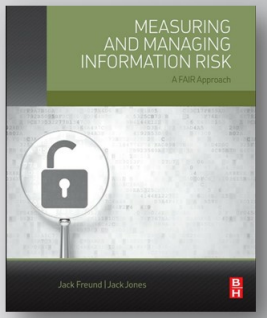
- I controlli FAIR sono di tre tipologie!

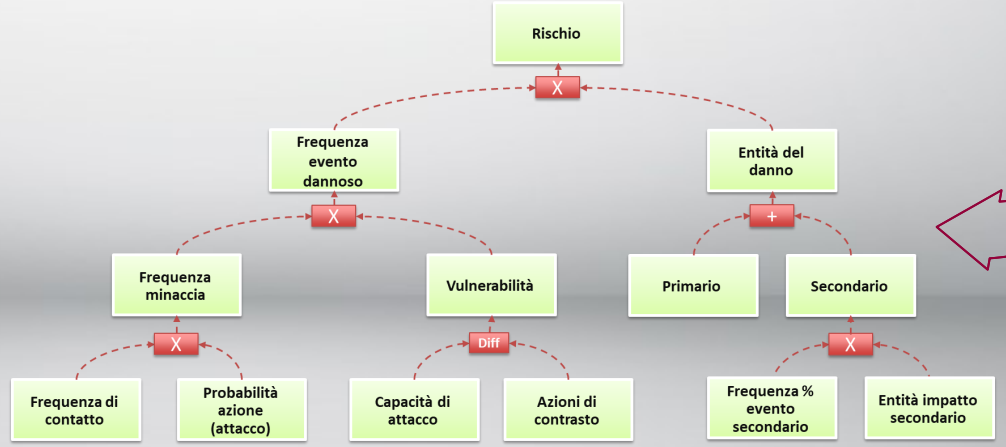


Controlli ISO e fattori FAIR









Come confrontare ISO e FAIR?

ISO List	Compilato da:								
Controllo ISO			Misura di gestione del rischio	Categoria					
				Asset				Variance	Decision
				Prevention					
				Threat	Vulnerabili	Detection	Response		
	A.12.1 Procedure operative e responsabilità	A.12.1.1 - Procedure operative documentate						x	
		A.12.1.2 - Gestione dei cambiamenti							
		A.12.1.3 - Gestione della capacità							
		A.12.1.4 - Separazione degli ambienti di sviluppo, di test e produzione							
	A.12.2 Protezione dal malware	A.12.2.1 - Controlli contro il malware		x					
			Implement strong spam filter						
	A.12.3 Backup	A.12.3.1 - Backup delle informazioni			x			x	
A.12 Sicurezza delle attività operative		A.12.4.1 - Raccolta di log degli eventi							

ISO/IEC 27002:2013

Information technology — Security techniques — Code of practice for information security controls

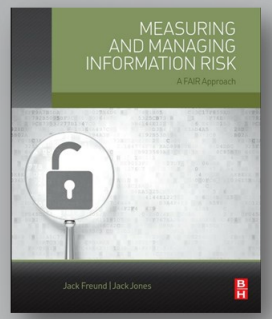
ISO IEC

=> *se ne parlerà in dettaglio nella sessione successiva*

Fair ed i framework di controlli

Jack Jones (Decembre 2020):

- The **controls frameworks we have today** are not analytic models; they are lists of control good practices.
- And although these frameworks are very useful as checklists, they inherently aren't able to support defensible measurement of control efficacy.
- For example, none of them capture **dependencies** between controls, many of the **control descriptions are too ambiguous** for reliable measurement, and they all **rely on ordinal measurements**, which can't reliably be translated into risk reduction.

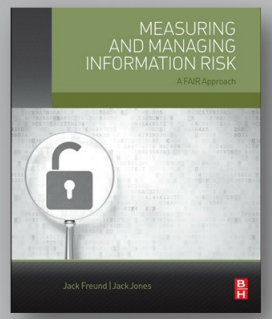


https://www.fairinstitute.org/blog/interview-jack-jones-talks-lessons-of-2020-and-new-research-on-controls-to-risk-mapping-coming-in-2021?utm_campaign=Blog&utm_medium=email&_hsmi=105667753&_hsenc=p2ANqtz-9TxF5Bplmu7YHpRDmF2VDVF03B46YdXqmJgTTzdp1n8irDMpptKNxmWWOoOLM6xdbLwm-CtHUvgdiZ5Sjw2PgRuOlyP3na5oPawMZth_CwPpswcqQ&utm_content=105667753&utm_source=hs_email

In sintesi

- La metodologia FAIR si contrappone agli approcci “Black Box”, che:
  - Sono approcci tradizionali di quantificazione del rischio, con input «misteriosi» e algoritmi non aperti
  - Non supportano efficacemente le decisioni di gestione del rischio

- FAIR non è solo una metodologia in ausilio alla quantificazione del rischio, ma anche una disciplina che richiede pensiero critico, analisi e comprensione del rischio
  - Gli input non sono mai automatici, ma devono essere definiti chiaramente; è la fase di definizione degli obiettivi che guida l’analisi
  - Il punto centrale delle quantificazione del rischio FAIR non è la fase di calcolo, ma la chiara definizione degli domande a cui si vuole risponde

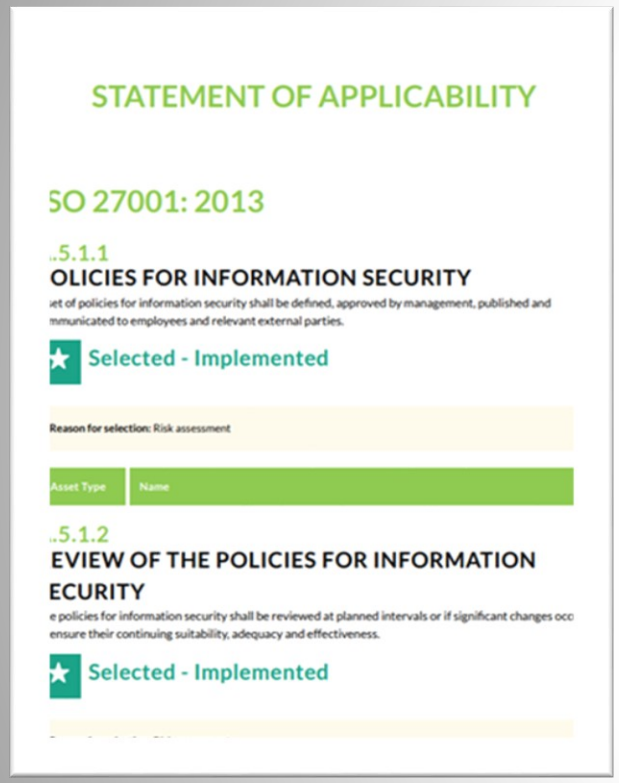


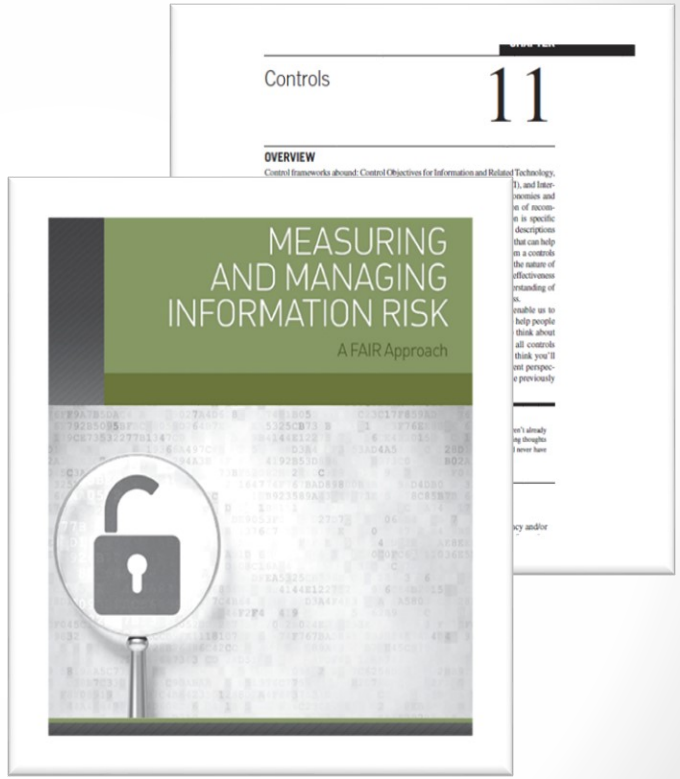
Lascio la parola al prossimo relatore

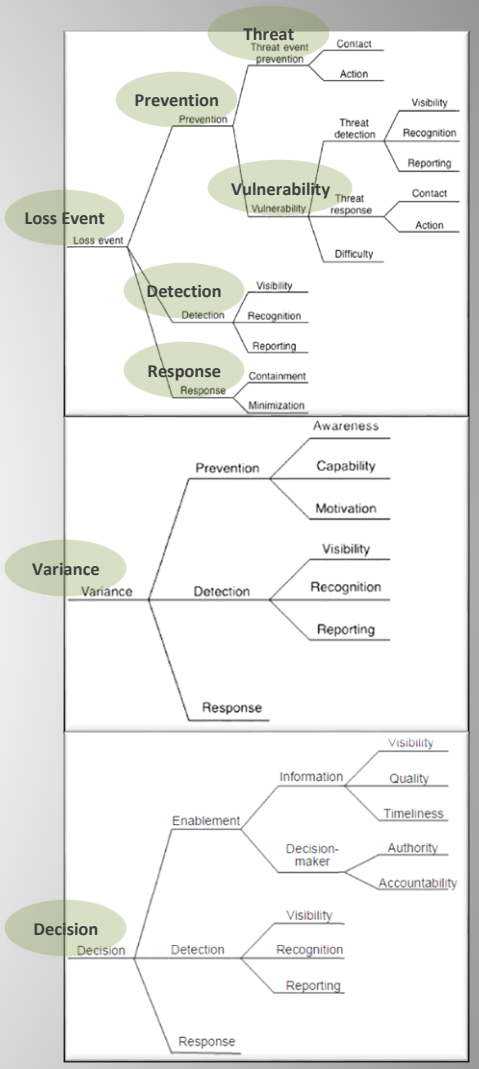
UNA PROPOSTA DI APPLICAZIONE DEI CONTROLLI ISO PER LA VALORIZZAZIONE DEI FATTORI FAIR

Luca Fei
luca.fei@inwind.it

Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR







Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR

ISO 27002			Categoria					
			Asset					
			Prevention		Detection	Response	Variance	Decision
			Threat	Vulnerability				
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					x	x
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni					x	x
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni	x	x				
		A.6.1.2 - Separazione dei compiti	x					
		A.6.1.3 - Contatti con le autorità	x					
		A.6.1.4 - Contatti con gruppi specialistici	x					
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti	x					
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili					x	
		A.6.2.2 - Telelavoro					x	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell`impiego	A.7.1.1 - Screening			x			
		A.7.1.2 - Termini e condizioni di impiego						x
	A.7.2 Durante l`impiego	A.7.2.1 - Responsabilità della direzione			x			
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			x			
		A.7.2.3 - Processo disciplinare				x		

Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR

ISO 27002			Categoria					
			Asset				Variance	Decision
			Prevention		Detection	Response		
			Threat	Vulnerability				
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					5	3
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni					5	3
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni	3	2				
		A.6.1.2 - Separazione dei compiti	4					
		A.6.1.3 - Contatti con le autorità	4					
		A.6.1.4 - Contatti con gruppi specialistici	4					
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti	4					
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili					5	
		A.6.2.2 - Telelavoro					3	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell`impiego	A.7.1.1 - Screening			4			
		A.7.1.2 - Termini e condizioni di impiego						3
	A.7.2 Durante l`impiego	A.7.2.1 - Responsabilità della direzione			3			
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			3			
		A.7.2.3 - Processo disciplinare				5		

Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR

ISO 27002			Categoria						Efficacia	Implementazione (stato attuale)	Implementazione (stato futuro)
			Asset								
			Prevention		Detection	Response	Variance	Decision			
			Threat	Vulnerability							
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					5	3		5	
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni					5	3		5	
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni	3	2						1	
		A.6.1.2 - Separazione dei compiti	4							0	
		A.6.1.3 - Contatti con le autorità	4							3	
		A.6.1.4 - Contatti con gruppi specialistici	4							0	
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti	4							1	
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili					5			4	
		A.6.2.2 - Telelavoro					3			4	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell`impiego	A.7.1.1 - Screening			4					4	
		A.7.1.2 - Termini e condizioni di impiego						3		3	
	A.7.2 Durante l`impiego	A.7.2.1 - Responsabilità della direzione			3					5	
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			3					2	
		A.7.2.3 - Processo disciplinare				5				1	

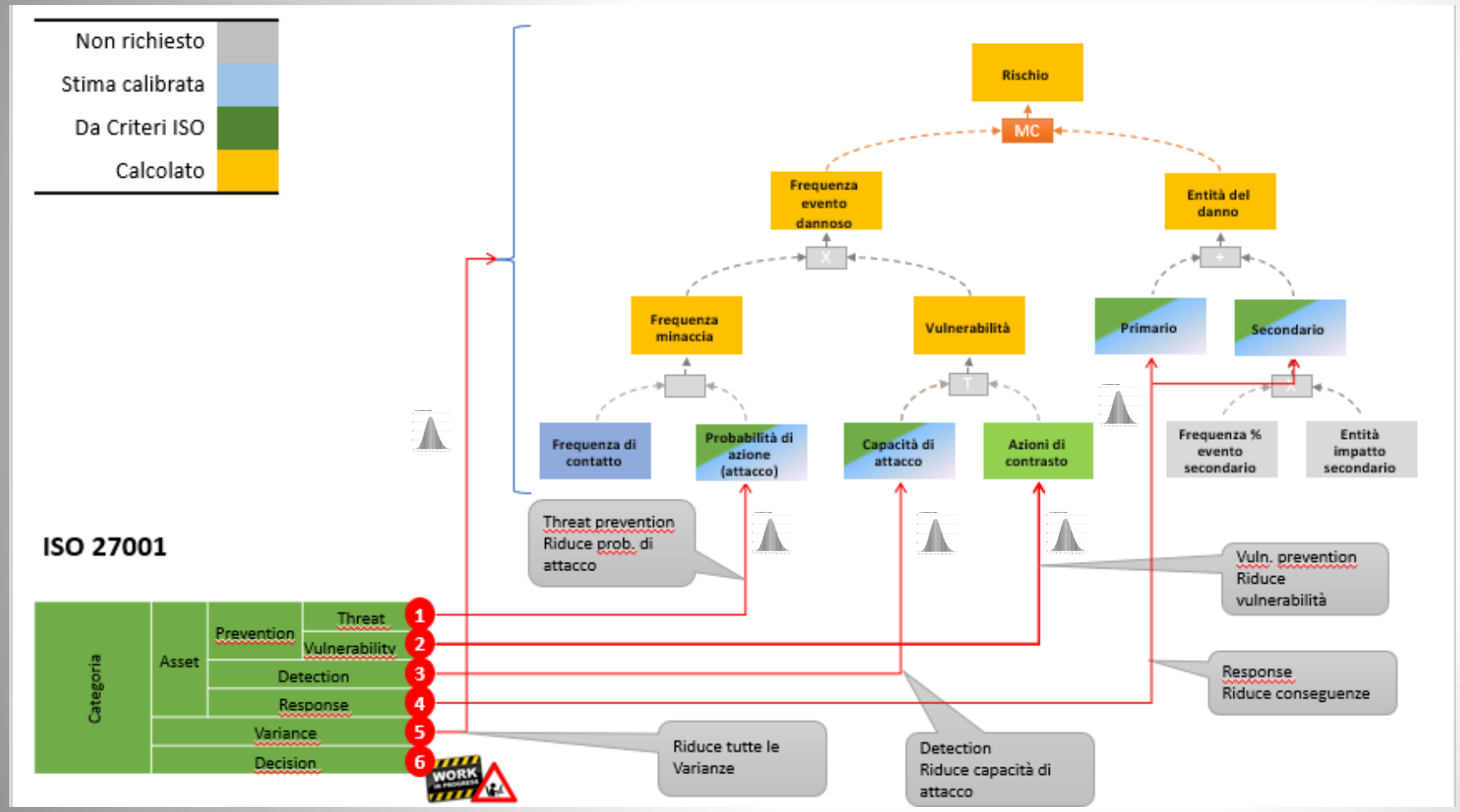
Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR

Controllo ISO 27002			Categoria						Efficacia	Implementazione (stato attuale)	Implementazione (stato futuro)
			Asset								
			Prevention		Detection	Response	Variance	Decision			
			Threat	Vulnerability							
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					x	x		5	
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni				x				5	
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni				x				1	
		A.6.1.2 - Separazione dei compiti								0	
		A.6.1.3 - Contatti con le autorità			x					3	
		A.6.1.4 - Contatti con gruppi specialistici			x					0	
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti			x					1	
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili				x				4	
		A.6.2.2 - Telelavoro			x	x				4	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell'impiego	A.7.1.1 - Screening			x					4	
		A.7.1.2 - Termini e condizioni di impiego		x						3	
	A.7.2 Durante l'impiego	A.7.2.1 - Responsabilità della direzione		x						5	
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			x					2	
		A.7.2.3 - Processo disciplinare				x				1	
	A.7.3 Interruzione o variazione del rapporto di lavoro	A.7.3.1 - Cessazione o variazione delle responsabilità durante il rapporto di lavoro	x							1	

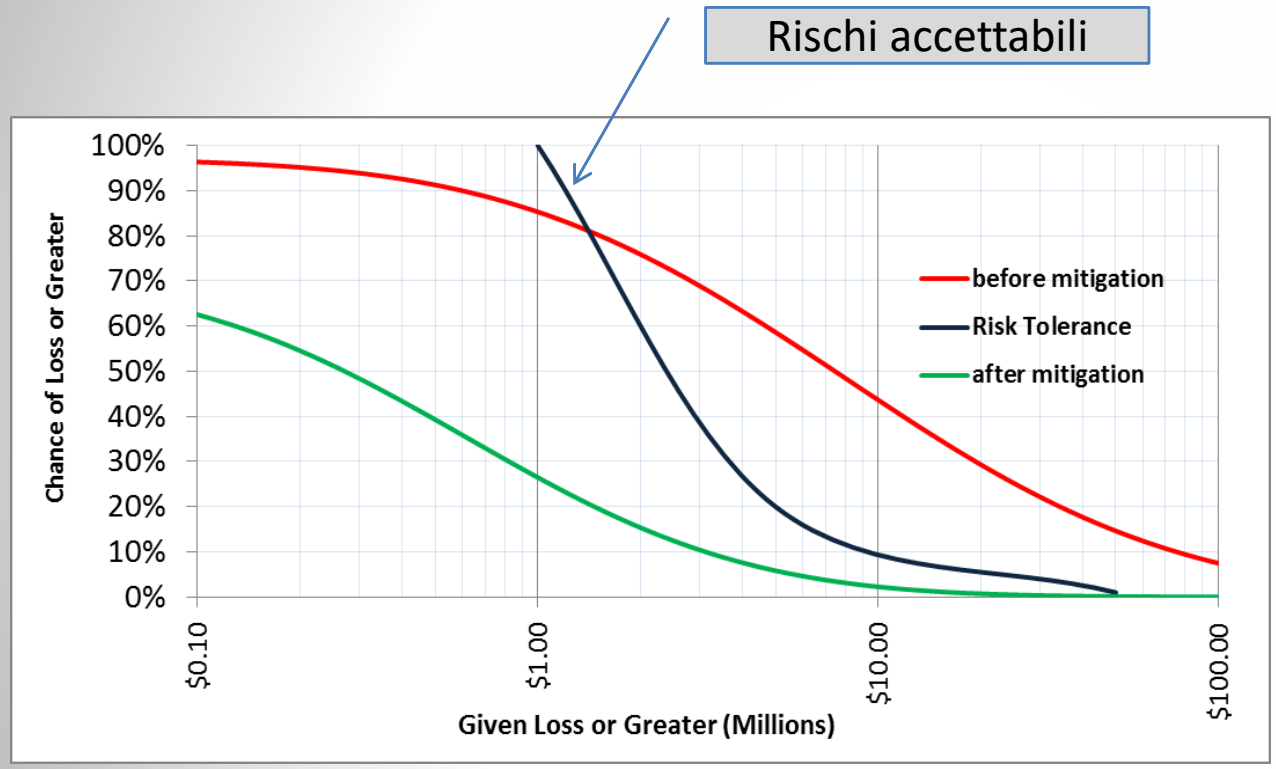
	Thr	Vul	Det	Res	Var	Dec
Count	12	16	18	7	7	8
Min	0%	0%	5%	8%	0	10%
Awg	52%	34%	27%	89%	45%	64%
Max	100%	100%	90%	100%	80%	100%

esempio

Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR



Una proposta di applicazione dei controlli ISO per la valorizzazione dei fattori FAIR



RISK QUANTIFICATION
UN MODELLO

Alberto Piamonte
alberto.piamonte@alice.it

Strumenti disponibili «Free»

- http://app.fairu.net (RiskLens)
- OpenFair™
- Python
- . . .

http://app.fairu.net/

FAIR-U - Analysis

app.fairu.net/analysis/15750

FAIR POWERED BY RISKLENS

SdS - ISACA : 11 settembre 2020
Created June 27, 2020

Alberto Piamonte

My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?

My Analyses
- Example - Phishing Database Breach
  Created June 27, 2020
- SdS - ISACA : 11 settembre 2020
  Created June 27, 2020
- prova 2
  Created August 3, 2020
- My new FAIR Analysis
  Created August 3, 2020
- Example - Phishing Database Breach - Copy
  Created August 3, 2020

New Analysis

Run Analysis

ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€102,7k €315,9k €2,1M
Min — Avg — Max

LOSS EVENT FREQUENCY
Minimum: 2
Most Likely: 3
Maximum: 5
Confidence: Medium

LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels

THREAT EVENT FREQUENCY
You are estimating at the Loss Event Frequency level; no estimate is needed here.

VULNERABILITY
You are estimating at the Loss Event Frequency level; no estimate is needed here.

PRIMARY LOSS
Minimum: €46.410
Most Likely: €79.850
Maximum: €133.450

SECONDARY RISK
Enter Secondary Risk at the Secondary LEF and Secondary LM levels

CONTACT FREQUENCY
You are estimating at the Loss Event Frequency level; no estimate is needed here.

PROBABILITY OF ACTION
You are estimating at the Loss Event Frequency level; no estimate is needed here.

THREAT CAPABILITY
You are estimating at the Loss Event Frequency level; no estimate is needed here.

RESISTANCE STRENGTH
You are estimating at the Loss Event Frequency level; no estimate is needed here.

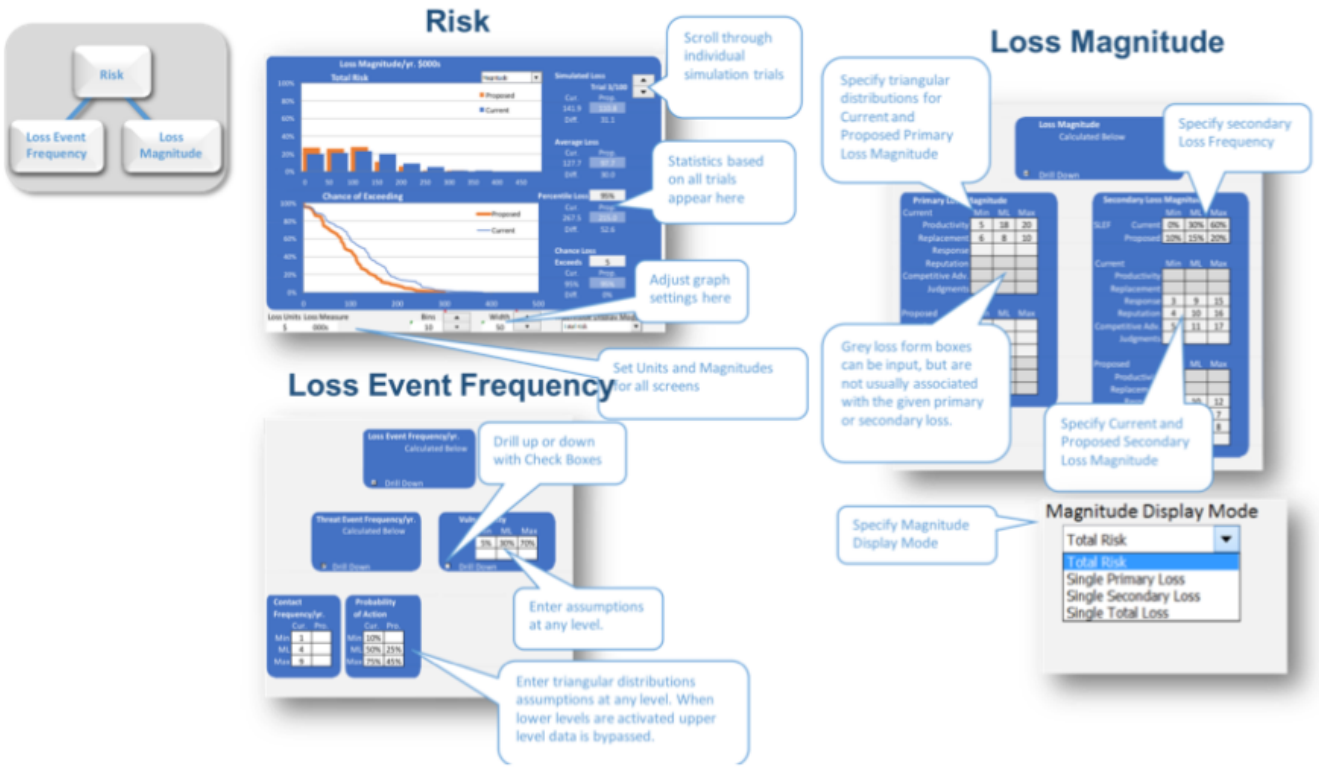
SECONDARY LEF
Minimum: 2%
Most Likely: 3%
Maximum: 5%
Confidence: Medium

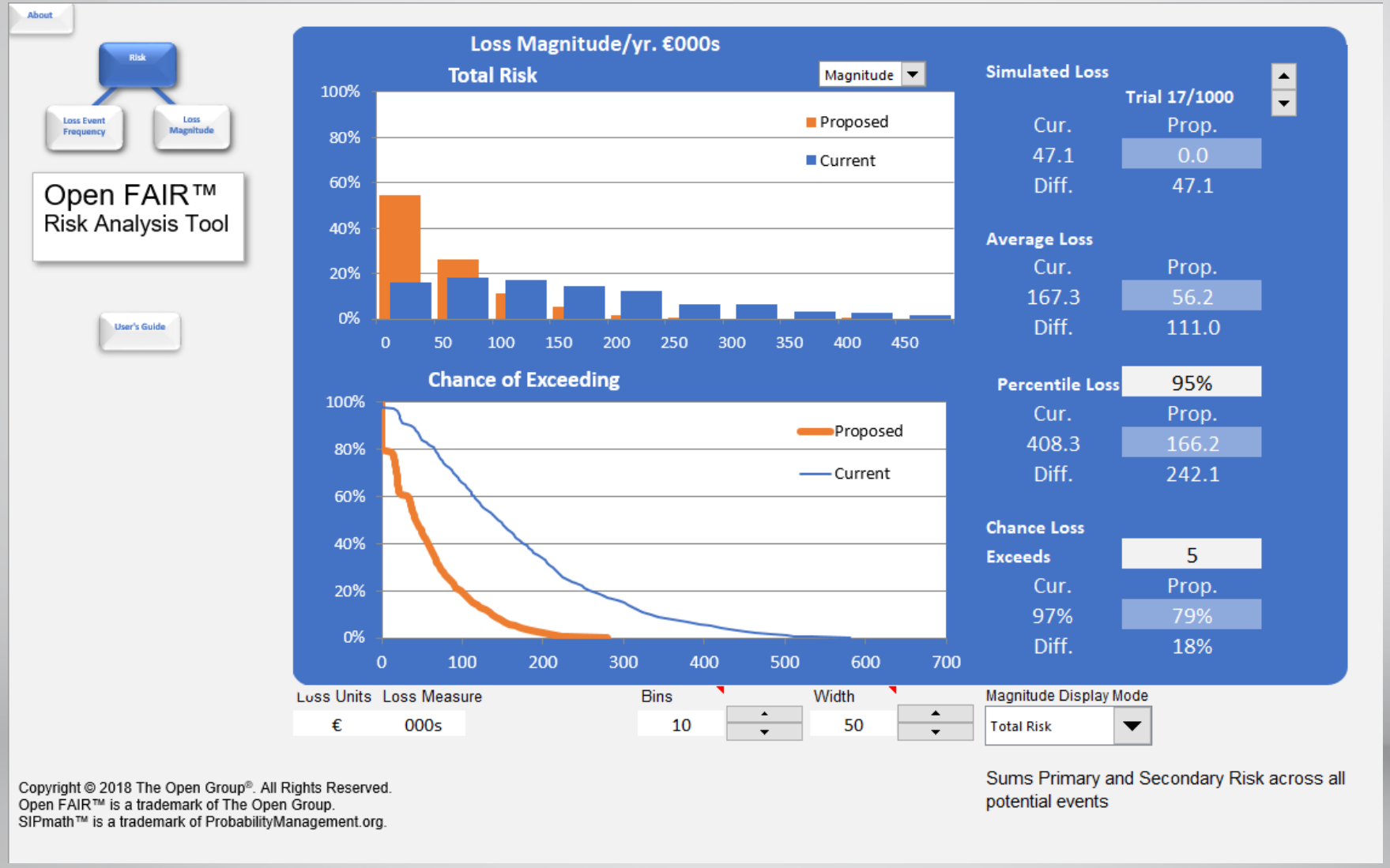
SECONDARY LM
Minimum: €300.000
Most Likely: €450.000
Maximum: €900.000

Metodologie di Cybersecurity che utilizzano Monte Carlo:

Open FAIR

With a view to creating a tool that helps accelerate the adoption of the Open FAIR standard, the tool provides both experienced and novice risk practitioners with a practical and pragmatic tool to help analyze perceived risk in a consistent and simple to use way, whatever industry they work in. It is now available for our members and others to download and evaluate.




About
Risk
Loss Event Frequency
Loss Magnitude
Open FAIR™
Risk Analysis Tool
User's Guide
Loss Magnitude/yr. €000s
Total Risk
Magnitude
Proposed
Current
100%
80%
60%
40%
20%
0%
0
50
100
150
200
250
300
350
400
450
Chance of Exceeding
Proposed
Current
100%
80%
60%
40%
20%
0%
0
100
200
300
400
500
600
700
Simulated Loss
Trial 17/1000
Cur.
Prop.
47.1
0.0
Diff.
47.1
Average Loss
Cur.
Prop.
167.3
56.2
Diff.
111.0
Percentile Loss
95%
Cur.
Prop.
408.3
166.2
Diff.
242.1
Chance Loss Exceeds
5
Cur.
Prop.
97%
79%
Diff.
18%
Loss Units
Loss Measure
€
000s
Bins
10
Width
50
Magnitude Display Mode
Total Risk
Sums Primary and Secondary Risk across all potential events
Copyright © 2018 The Open Group®. All Rights Reserved.
Open FAIR™ is a trademark of The Open Group.
SIPmath™ is a trademark of ProbabilityManagement.org.

DIY Python

Report Output
Overview
Risk Distribution
Regular Model 1
My Meta Model
Exceedence Probability Curve
Loss Exceedence Curve
Regular Model 1
Calculation Dependency Tree
R
LEF
LM
TEF
V
PL
SL
C
A
TC
CS
SLEF
SLEM
Not Required
Supplied
Calculated
Loss Event Frequency
Primary Loss
Secondary Loss

Sviluppo di soluzioni DIY con Excel

- Lo standard è molto ben documentato anche nella parte relativa agli algoritmi di calcolo da utilizzare nei vari passaggi.
- EXCEL ha prestazioni eccellenti nei calcoli più complessi (MonteCarlo), possibili implementazioni del metodo sono ampiamente documentate
- Le funzioni statistiche necessarie (Beta-Pert, Poisson, Binomiale, ecc.) sono disponibili.
- È possibile uno sviluppo autonomo (DIY) ?

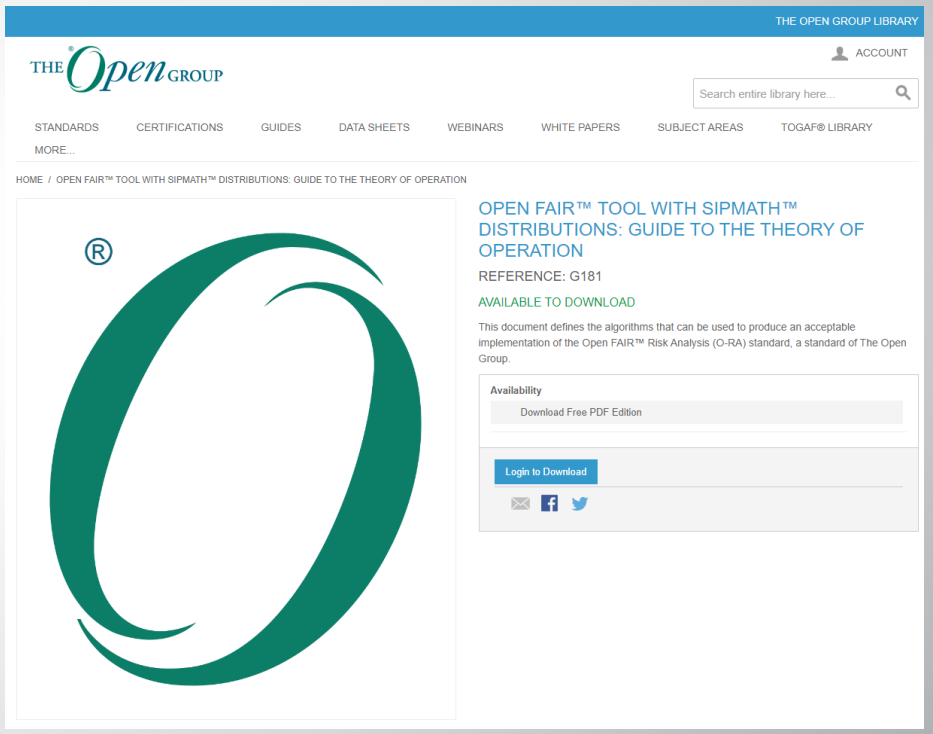
Dalla teoria alla pratica *(es: Excel®)*

Open Group Guide

Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation

THE Open GROUP

Scaricabile dal sito OpenGroup previa registrazione:



2.1 Open FAIR Tool Overview

2.3 Loss Event Frequency (LEF)

Frequenza evento dannoso

Loss Event Frequency (LEF) is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset. In order for a loss event to occur, a threat agent has to act upon an asset, such that loss results. Probability is always based on a timeframe (event X is 10% likely to occur over the next Y).

Objective Loss Event Frequency is the count of events for the trial period.

4 Open Group Guide (2018)

Each of the following sections describes one factor, using the following naming convention:

- Estimate – produce output based on direct user input
- Derive – produce output based only on data in the model

Each section begins with a description in *italics* derived from the risk taxonomy.

Open FAIR™ Tool with SIPmath Distributions: Guide to the Theory of Operation 3

2.3.1 Estimate LEF

Develop a calibrated estimated range of LEF values with a 90% confidence interval, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the LEF SIP containing real numbers. The LEF SIP is input to a Poisson distribution to produce the loss events SIP containing integers.

Inputs

Min	ML	Max
2	5	7

Triangular →

LEF SIP

Row	Value
1	5.39
2	4.83
3	5.28
4	5.30
5	3.48
6	2.14
7	3.24
8	4.01
9	4.45
10	2.96

⋮

Poisson →

Events SIP

Row	Value
1	5
2	1
3	5
4	3
5	3
6	3
7	1
8	0
9	4
10	4

⋮

2.3.2 Derive LEF

The LEF SIP is produced by multiplying the TEF SIP by the value of Vuln – if estimated – or by the value of Vuln from the simulator. The LEF SIP is input to a Poisson distribution to produce the Loss Events SIP containing integers.

TEF SIP

Row	Value
1	37.41
2	33.80
3	6.69
4	13.86
5	29.65
6	40.61
7	25.54
8	19.50
9	54.81
10	12.74

⋮

*

Vuln SIP

Row	Value
1	59%
2	53%
3	53%
4	48%
5	47%
6	56%
7	47%
8	48%
9	49%
10	48%

⋮

=

LEF SIP

Row	Value
1	21.95
2	17.81
3	3.51
4	6.66
5	13.87
6	22.67
7	11.95
8	9.43
9	27.06
10	6.16

⋮

Poisson →

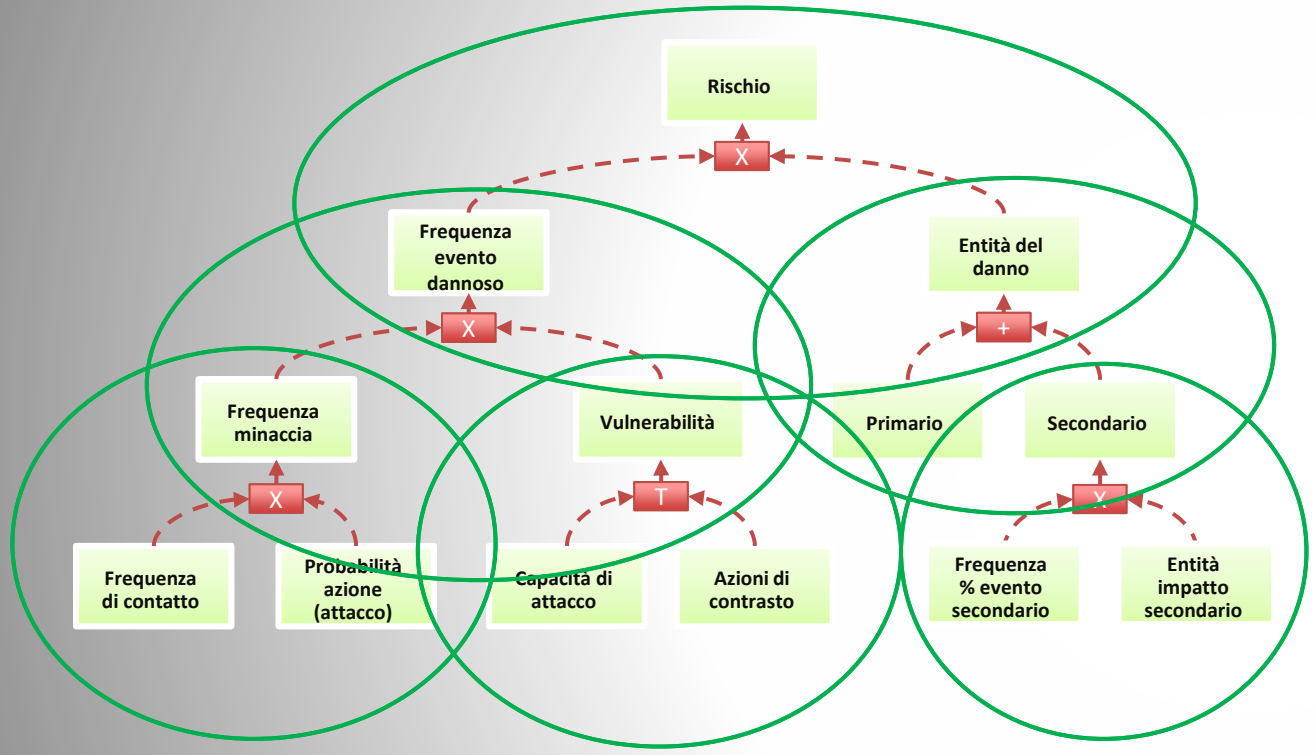
Events SIP

Row	Value
1	22
2	10
3	3
4	4
5	13
6	24
7	8
8	1
9	25
10	8

⋮

Or:

Proviamo ad usare Excel



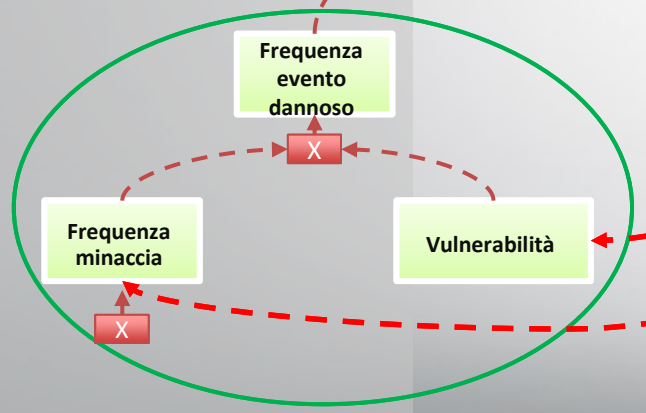
?

Foglio excel: LEF (Frequenza evento dannoso)

Calcolo LEF da Frequenza annuale ridotta e Vulnerabilità

MonteCarlo

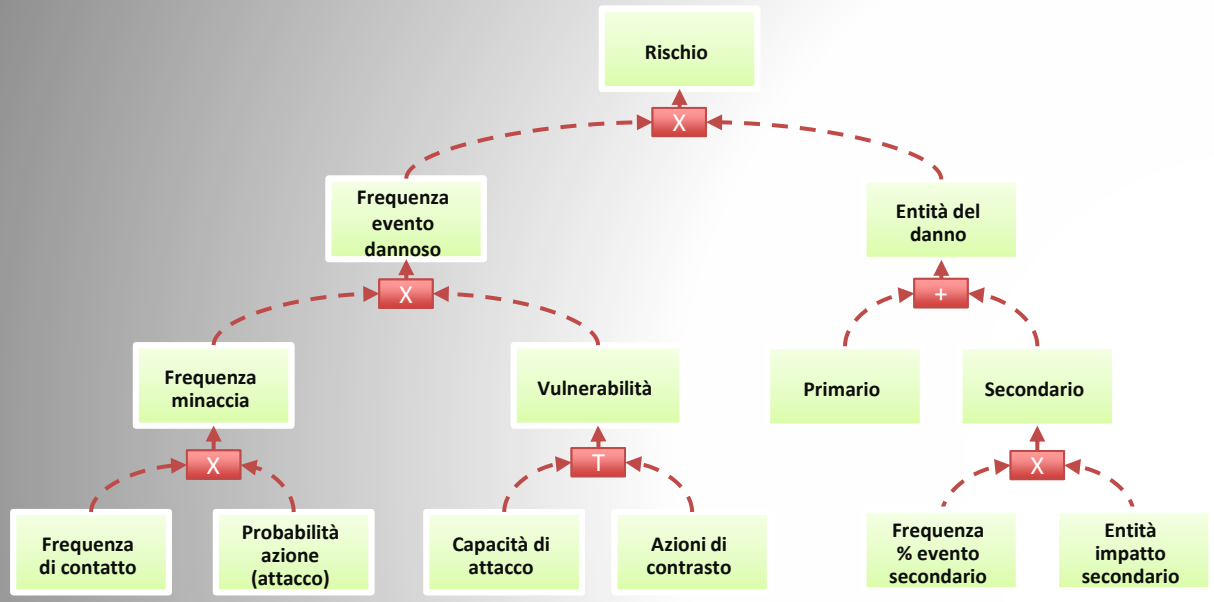
	Dim.	*min*	*pp*	*max*	*Conf*	*Nome*	*Descrizione*		VUL	TEFR	LEF
In 1	***%***	10%	30%	50%	M	VUL	Vulnerabilità		0.279357		0.738807902
In 2	***ev/anno***					TEFR	Frequenza annuale eventi ridotta		0.322571		1.212841938
									0.242841		0.891099731
Operazione	*								0.327357		1.366728854
									0.225047		0.811502982
Out	***ev/anno***					LEF	Frequenza annuale eventi perdita		0.281838		0.751330377
									0.227388		0.760610611



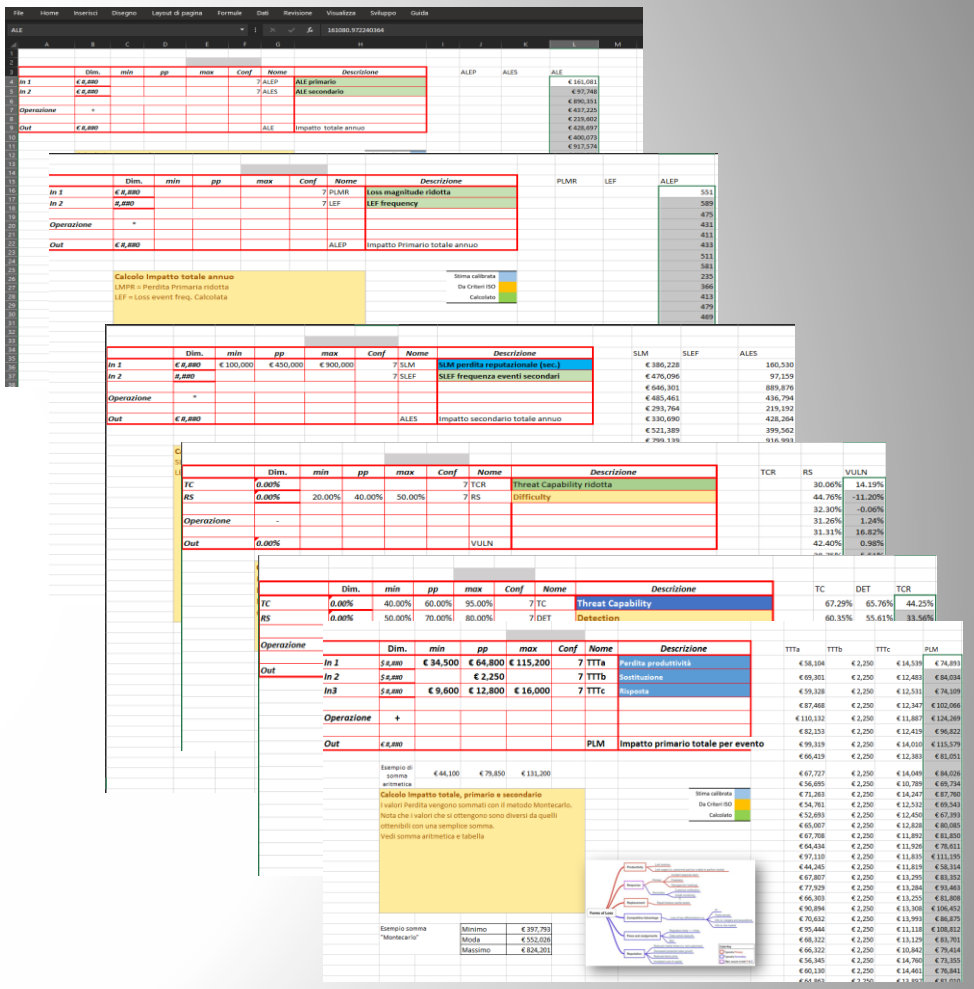
INPUT
Se **min, pp** e **max** non sono definiti, viene usato con il nome indicato (che deve essere definito altrove).
Se è definito solo **«pp»** viene generato un valore costante.
Se **min**, **pp** e **max** sono definiti, viene generata una distribuzione ***Pert + Conf***

OUPUT
I dati in input vengono combinati con l'operazione indicata (*, +, %, -, ….)

DISTRIBUZIONI
Utilizzabili nel modello o per generare istogrammi e percentuali.

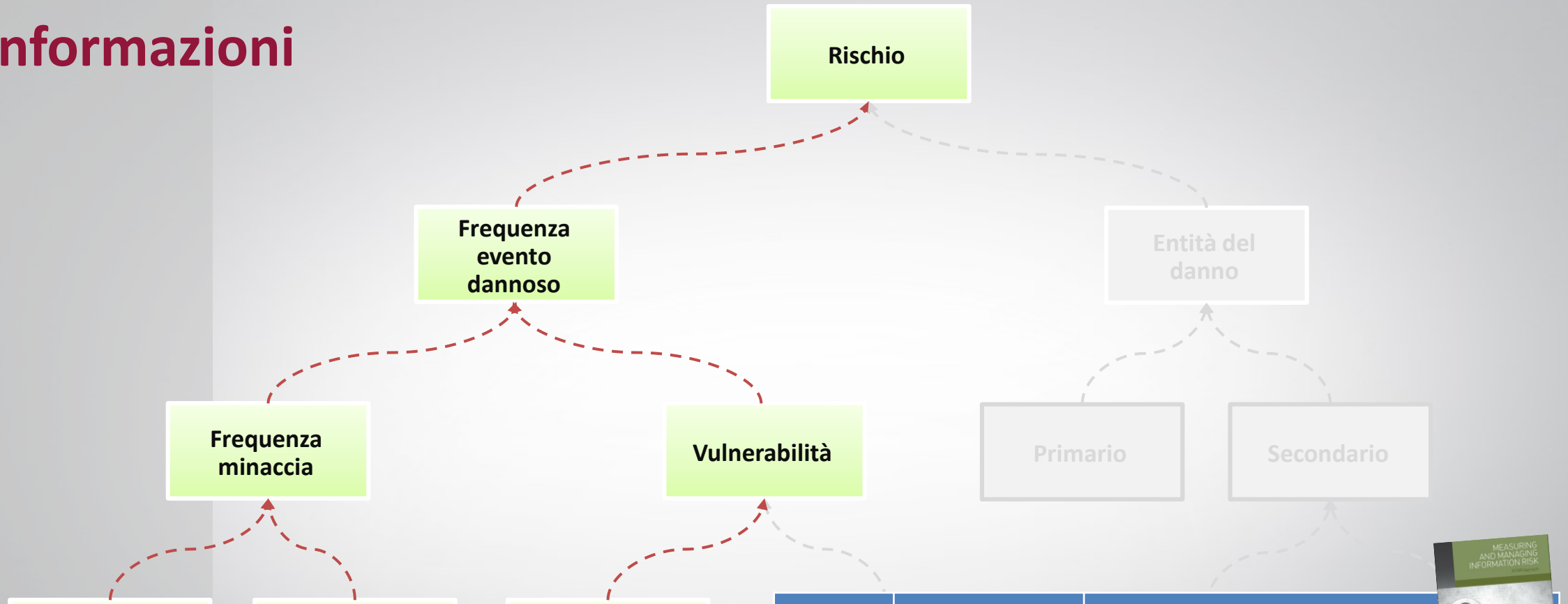


Un foglio Excel per ogni fattore FAIR

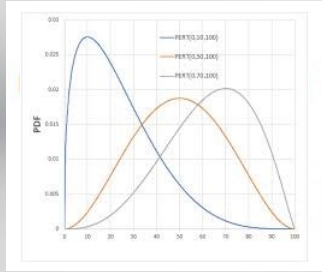


- Aperto
- Facilmente interfacciabile (in e out)
- Modificabile
- Prestazioni
- Programmabile

Le informazioni

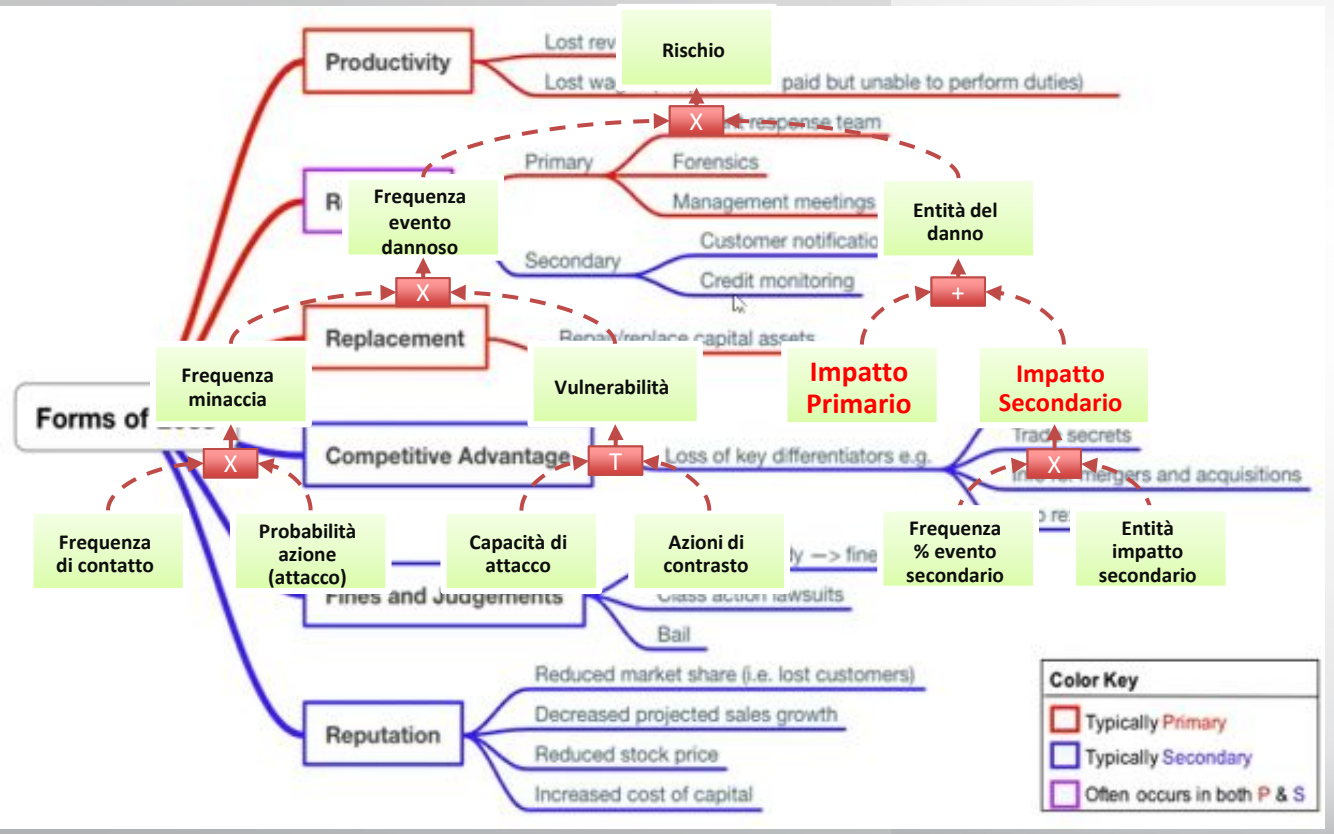


Distribuzione di valori (Pert) + incertezza !



TCAP	Scala qualitativa	esempio
2 %	Molto bassa	Principianti totali
16 %	Bassa	Uso di semplici strumenti, seguendo istruzioni
50 %	Media	In grado di utilizzare normali strumenti e tecniche
84 %	Sopra la media	In grado di utilizzare strumenti e tecniche avanzate
98 %	«Veri» esperti	In grado di creare nuove tecniche di attacco

Valutazione degli impatti :



Primari

Tipo

Column1	Column2	Column3	Column4	Column5
		Min	Più probabile	Max
Produttività (perdita)	Costo annuo	€ 50,000	€ 70,000	€ 100,000
	Giornate lavorative	260	260	260
	Costo/giorno	€ 192	€ 269	€ 385
	Perdita produttività %	60%	60%	60%
	# impiegati	50	50	50
	Costo giorno non produttività	€ 5,769	€ 8,077	€ 11,538
	Giorni non produttivi	6	8	10
	Totale perdite	€ 34,615	€ 64,615	€ 115,385

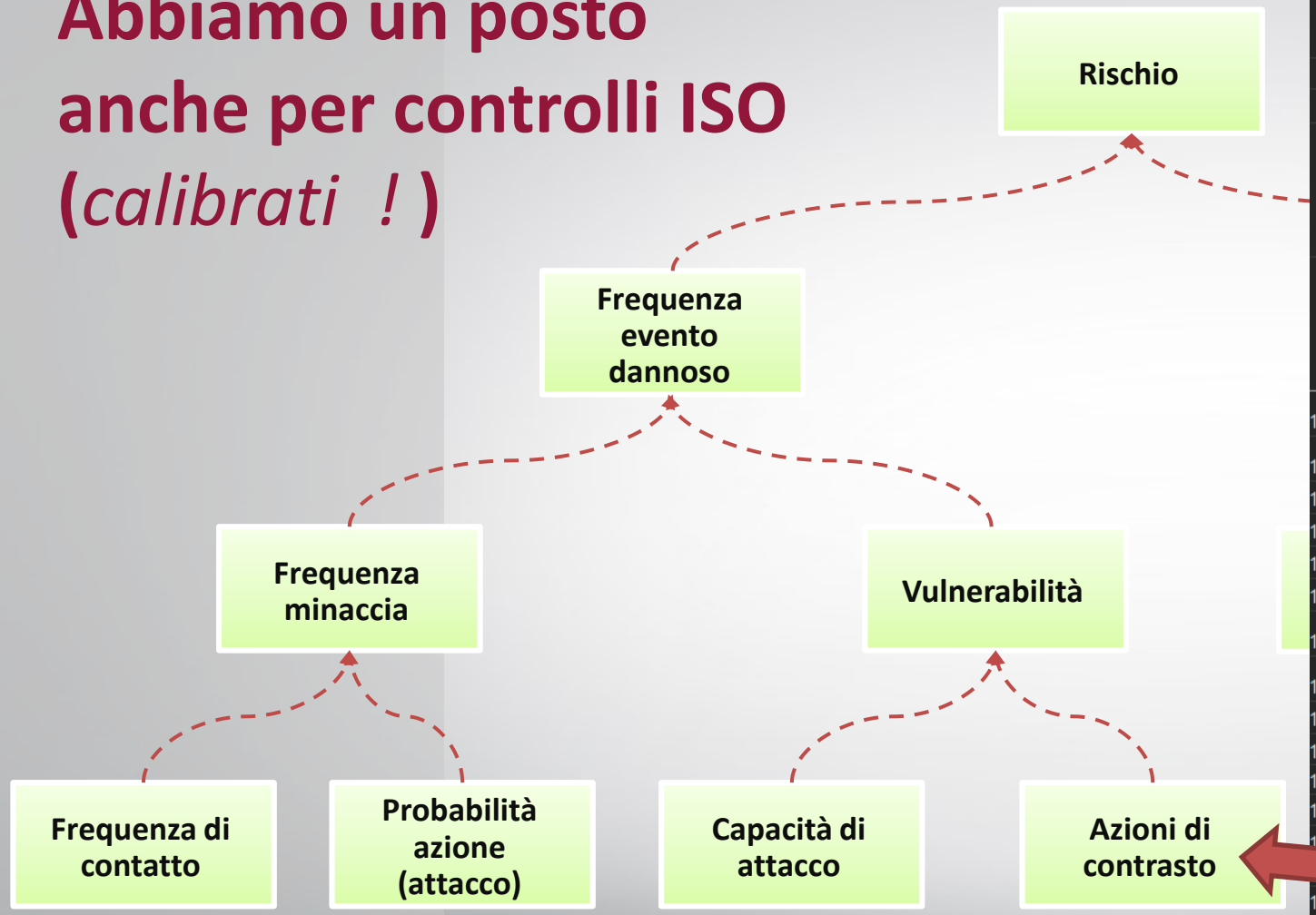
Secondari

Column1	Column2	Column3	Column4	Column5
Sostituzione		€ 2,250.00	€ 2,250.00	€ 2,250.00

Column1	Column2	Column3	Column4	Column5
Risposta		€ 9,600	€ 9,600	€ 12,800

Column1	Column2	Column3	Column4	Column5
Reputazione		€ 300,000	€ 450,000	€ 900,000

Abbiamo un posto anche per controlli ISO (*calibrati !*)



	C	D	E	F	G	H	I	J	K	L	M
1											
2		Categoria						Efficacia	Implementazione		
3		Asset									
4		Prevention				Variance	Decision				
5		Threat	Vulnerability	Detection	Response				Intrinseco	Attuale	Pianificata
111	A.17.2.1 - Disponibilità delle strutture per l'elaborazione delle informazione	x									
112	A.18.1.1 - Identificazione della legislazione applicabile e dei requisiti contrattuali					x					
113	A.18.1.2 - Diritti di proprietà intellettuale					x					
114	A.18.1.3 - Protezione delle registrazioni					x					
115	A.18.1.4 - Privacy e protezione dei dati personali					x					
116	A.18.1.5 - Regolamentazione sui controlli crittografici					x					
117	A.18.2.1 - Riesame indipendente della Sicurezza delle Informazioni					x					
118	A.18.2.2 - Conformità alle politiche e alle norme per la sicurezza					x					
119	A.18.2.3 - Verifica tecnica della conformità					x					
120											
121											
122											
123	Sommario										
		17	18	7	4	12	5				
125	Min	70%	0%	0%	40%	0%	40%				
126	Awg	80%	47%	40%	80%	48%	56%				
127	Max	90%	100%	100%	100%	100%	80%				
128		PoA	RS	Det	Res	Var					
129											
130											

GDL ISACA Roma

Modello	SPERT 01
data	2021 01 29
Confidence	7
N. Iterazioni	10,000

Elabora

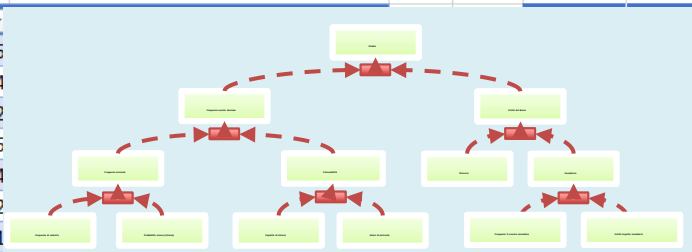
Genera Descrizione Distribuzioni

CLEAR DESCR

Aggiorna Elenco Distribuzioni

CLEAR DISTRIBUZIONI

	Wksheet	Tempo
1	TEF	00:00:05
2	TC	00:00:04
3	VUL	00:00:02
4	PLM	00:00:05
5	PLMR	00:00:04
6	LEF	00:00:02
7	ALEP	00:00:01
8	SLF	00:00:03
9	ALES	00:00:02
10	ALE	00:00:02
11		
12		
13		
14		
15		
16		
	Tempo Tot.	00:00:30



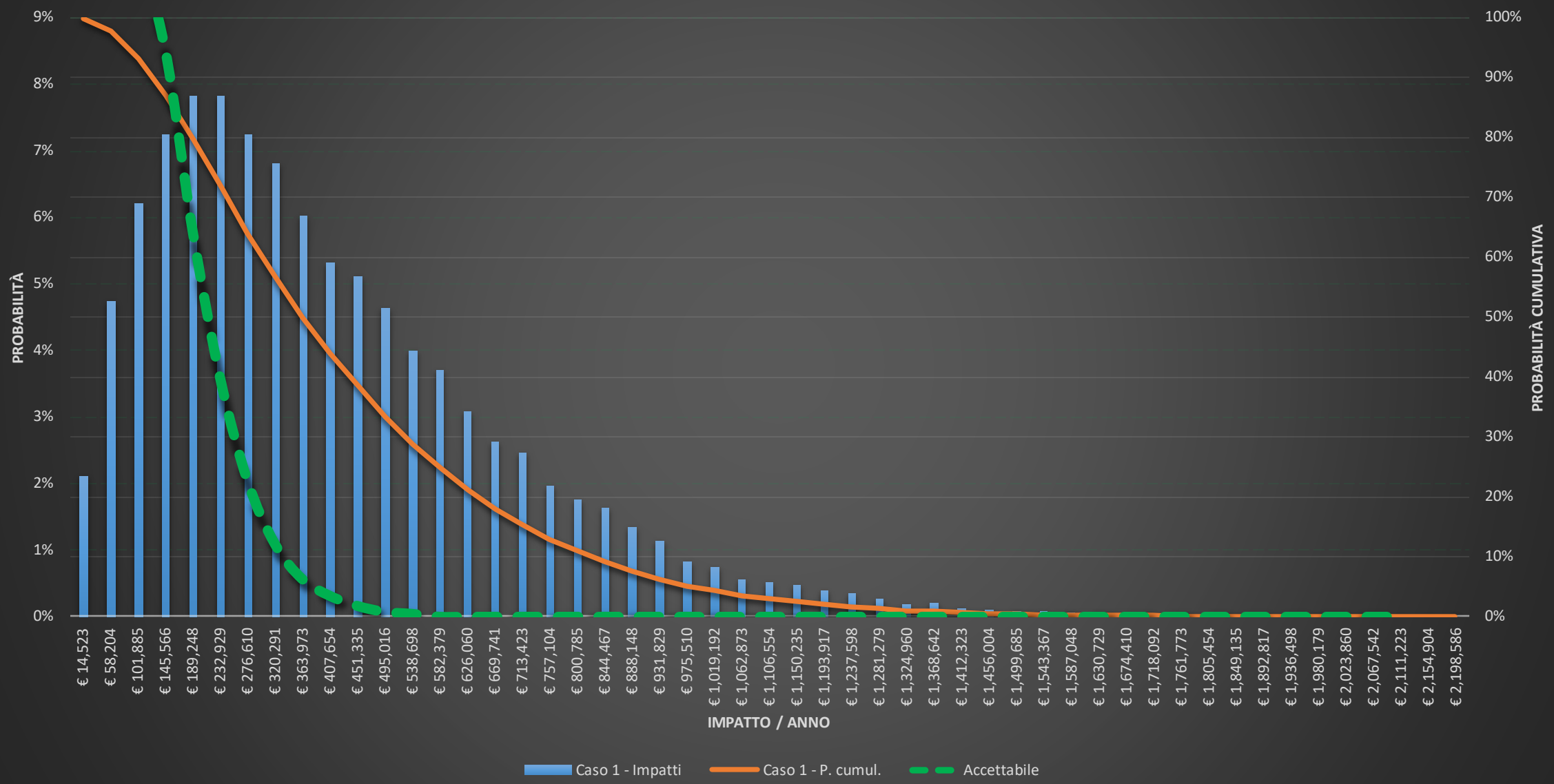
Confronto tra distribuzioni

	Nome	*Note*
COPY 1	ALE	AAA
COPY 2	ALE	BBB SLF

Nome	Definizione	Definito in:	Form
ALE	Impatto totale annuo	=ALE!$L$4:$L$10004	€ #,#
ALEP	Impatto Primario totale annuo	=ALEP!$L$4:$L$10004	#,##
ALES	Impatto secondario totale annuo	=ALES!$L$4:$L$10004	#,##
CONF	Confidence	=Cover!$B$5	
DET	Detection	=TC!$K$4:$K$10004	0.00
LEF	Loss event frequency	=LEF!$L$4:$L$10004	#,##
PLM	Impatto primario totale per evento	=PLM!$M$4:$M$10004	$ #,#
PLMmin	Perdita Minima	=PLMR!$K$4:$K$10004	€ #,#
PLMR	Perdita ridotta primaria	=PLMR!$M$4:$M$10004	0
POA	Prob. of Action	=TEF!$L$4:$L$10004	#,##
R_PLM	Response	=PLMR!$L$4:$L$10004	0
RS	Difficulty	=VUL!$K$4:$K$10004	0.00
SLEF	Secondary loss event frequency	=SLF!$L$4:$L$10004	#,##
SLF	Percentuale eventi secondari	=SLF!$K$4:$K$10004	#,##
SLM	SLM perdita reputazionale (sec.)	=ALES!$J$4:$J$10004	€ #,#
TC	Threat Capability	=TC!$J$4:$J$10004	0.00
TCR	Capacità di attacco ridotta	=TC!$L$4:$L$10004	0.00
TEF	Threat Event Freq	=TEF!$M$4:$M$10004	#,##
TEFMax	Contact Frequency max PoA	=TEF!$J$4:$J$10004	#,##
TEFMin	Contact Frequency min PoA	=TEF!$K$4:$K$10004	#,##
TTTa	Perdita produttività	=PLM!$J$4:$J$10004	$ #,#
TTTb	Sostituzione	=PLM!$K$4:$K$10004	$ #,#
TTTc	Risposta	=PLM!$L$4:$L$10004	$ #,#
VUL	Vulnerability	=LEF!$K$4:$K$10004	#,##
VULN		=VUL!$L$4:$L$10004	0.00

RISO_List | Process | Cover | ALE | ALEP | ALES | VUL | TC | TEF | LEF | SLF | PLM | PLMR | COMP_Graph | COMP_Data | TEF Descrip ...

Caso 1 : Eventi, impatti, ma no controlli ISO

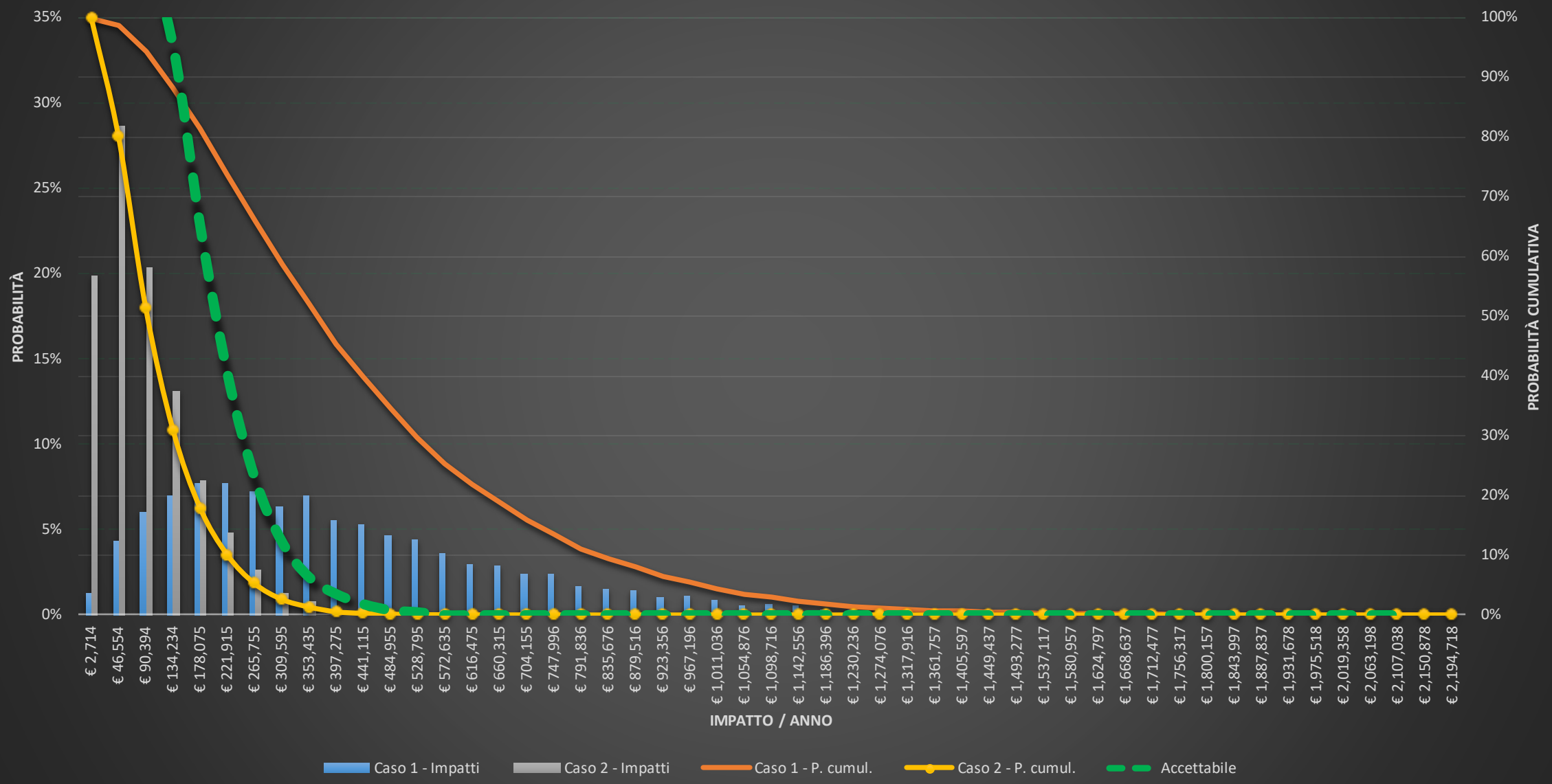


Mapping ISO

Controllo ISO 27002			Categoria						Efficacia	Implementazione (stato attuale)	Implementazione (stato futuro)
			Asset								
			Prevention		Detection	Response	Variance	Decision			
			Threat	Vulnerability							
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					x	x		5	
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni				x				5	
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni				x				1	
		A.6.1.2 - Separazione dei compiti								0	
		A.6.1.3 - Contatti con le autorità			x					3	
		A.6.1.4 - Contatti con gruppi specialistici			x					0	
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti			x					1	
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili				x				4	
		A.6.2.2 - Telelavoro			x	x				4	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell`impiego	A.7.1.1 - Screening			x					4	
		A.7.1.2 - Termini e condizioni di impiego		x						3	
	A.7.2 Durante l`impiego	A.7.2.1 - Responsabilità della direzione		x						5	
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			x					2	
		A.7.2.3 - Processo disciplinare				x				1	
	A.7.3 Interruzione o variazione del rapporto di lavoro	A.7.3.1 - Cessazione o variazione delle responsabilità durante il rapporto di lavoro	x							1	

	PoA	RS	Det	Res	Var	Dec
Count	12	16	18	7	7	8
Min	0%	0%	5%	8%	0	10%
Awg	52%	34%	27%	89%	45%	64%
Max	100%	100%	90%	100%	80%	100%

Caso 2 : Controlli ISO attuali



Mapping ISO

Controllo ISO 27002			Categoria						Efficacia	Implementazione (stato attuale)	Implementazione (stato futuro)
			Asset								
			Prevention		Detection	Response	Variance	Decision			
			Threat	Vulnerability							
A.5 Politiche per la sicurezza delle informazioni	A.5.1 Indirizzi della direzione per la sicurezza delle informazioni	A.5.1.1 - Politiche per la sicurezza delle informazioni					x	x		5	
		A.5.1.2 - Riesame delle politiche per la sicurezza delle informazioni				x				5	
A.6 Organizzazione della sicurezza delle informazioni	A.6.1 Organizzazione interna	A.6.1.1 - Ruoli e responsabilità per la sicurezza delle informazioni				x				1	
		A.6.1.2 - Separazione dei compiti								0	
		A.6.1.3 - Contatti con le autorità			x					3	
		A.6.1.4 - Contatti con gruppi specialistici			x					0	
		A.6.1.5 - Sicurezza delle informazioni nella gestione dei progetti			x					1	
	A.6.2 Dispositivi portatili e telelavoro	A.6.2.1 - Policy relativa ai dispositivi portatili				x				4	
		A.6.2.2 - Telelavoro			x	x				4	
A.7 Sicurezza delle risorse umane	A.7.1 Prima dell`impiego	A.7.1.1 - Screening			x					4	
		A.7.1.2 - Termini e condizioni di impiego		x						3	
	A.7.2 Durante l`impiego	A.7.2.1 - Responsabilità della direzione		x						5	
		A.7.2.2 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni			x					2	
		A.7.2.3 - Processo disciplinare				x				1	
	A.7.3 Interruzione o variazione del rapporto di lavoro	A.7.3.1 - Cessazione o variazione delle responsabilità durante il rapporto di lavoro	x							1	

	PoA	RS	Det	Res	Var	Dec
Count	12	16	18	7	7	8
Min	0%	0%	5%	8%	0	10%
Awg	52%	34%	27%	89%	45%	64%
Max	100%	100%	90%	100%	80%	100%

Sviluppo di soluzioni DIY con Excel

- ✓ Lo standard è molto ben documentato anche nella parte relativa agli algoritmi di calcolo da utilizzare nei vari passaggi.
- ✓ EXCEL ha prestazioni eccellenti nei calcoli più complessi (MonteCarlo), possibili implementazioni del metodo sono ampiamente documentate
- ✓ Le funzioni statistiche necessarie (Beta-Pert, Poisson, Binomiale, ecc.) sono disponibili.
- ✓ Uno sviluppo autonomo non richiede competenze particolari e consente di estendere l'ontologia per rispondere ad esigenze specifiche *(Mapping ISO !!!).*

Grazie per l'attenzione !

Domande ?

alberto.piamonte@alice.it

QUALCHE CONSIDERAZIONE FINALE

COME PROSEGUIAMO

IL Gruppo di lavoro

Lezioni apprese dal lavoro sinora svolto

- L’uso combinato di ISO e FAIR evidenzia l’utilità dei sistemi ISMS come strumenti di gestione della sicurezza che consentono di valutare i risultati della loro efficace applicazione
- Siamo in presenza di uno strumento con grandi potenzialità per il reporting ai massimi livelli aziendali
- L’uso combinato di ISO e FAIR apre nuovi scenari, non solo nell’analisi del rischio ma anche di governance dell’azienda

Lezioni apprese dal lavoro sinora svolto

- Ci sono alcuni aspetti «teorici» da approfondire
  - L'ontologia FAIR è in evoluzione e molti concetti devono essere rivisitati e precisati (controlli, relazioni tra alcuni elementi dell'ontologia)
  - Anche dal punto di vista dell'uso degli strumenti matematici ci sono ambiti di studio e implementazione
- L'analista non deve applicare check-list ma deve «calibrare» i valori che usa e come li usa

In sintesi

Se vogliamo che i sistemi di gestione e le metodologie di analisi del rischio siano veramente utili :

- Far evolvere l'utilizzo dei sistemi di gestione da compliance a strumento di misura delle componenti aziendali della sicurezza
- Far evolvere la consulenza verso complessità e strumenti adeguati a rispondere alle vere sfide cui le organizzazioni sono sottoposte

Si deve fare un salto di qualità

Come proseguiamo

- Ci sono diversi aspetti di dettaglio della metodologia e del modello da approfondire
- Vogliamo provare ad utilizzare il feed back dei dati aziendali (SIEM e strumenti simili)
- Vogliamo vedere come utilizzare i metodi quantitativi in ambito Privacy (GDPR)

Infine

- *Che ne pensate?*
- *Volete dare il vostro apporto di pensiero e tempo? Contattateci*

Grazie per l’attenzione
a nome di tutti i componenti del Gruppo