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

Glauco Bertocchi
g.bertocchi@isacaroma.it

PREMESSA

- L’ultima volta ci siamo visti al webinar di 10 mesi fa (29 gennaio 2021)
- Se per caso, spero di no, foste curiosi potete rivedere la presentazione presente sul sito ISACA ROMA
- Molte delle cose allora dette sono state fatte, altre si sono rivelate troppo complesse o praticamente non utilizzabili
- Insomma si impara dagli errori…..o sbagliando si impara, come preferite..

Quale è stata la motivazione che ha avviato il GDL?

Provare a rispondere alla domanda :

E’ possibile calcolare in modo quantitativo (valori e probabilità) il valore di un sistema ISMS tipo ISO 27k per la riduzione del rischio in azienda?

Oppure

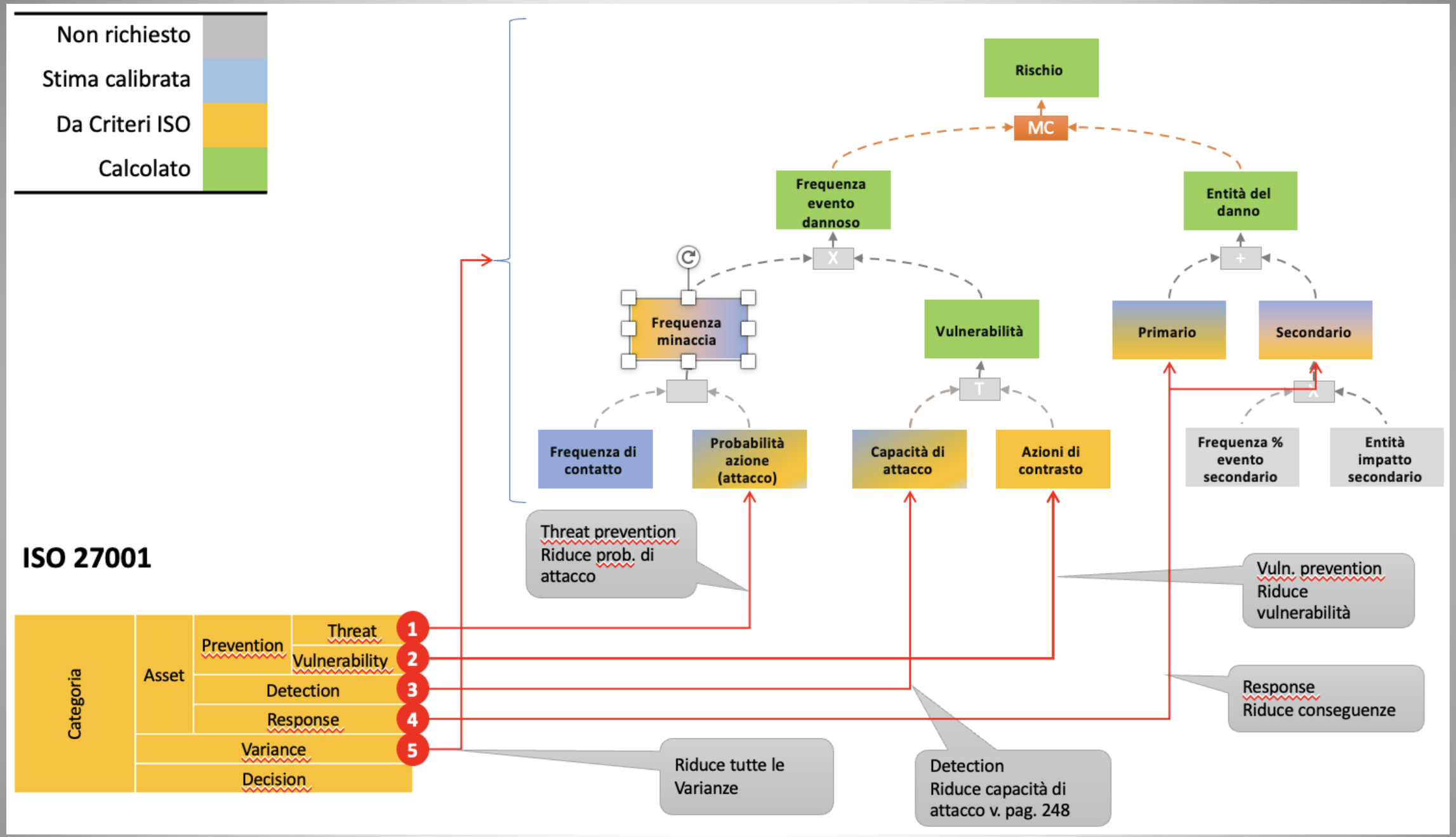
Se la mia azienda è ISO27k compliant quanto riduco la probabilità e l’impatto di un attacco tipo ramsonware ? O di altri scenari di minaccia?

Sintesi di più di un anno di lavoro (1)

- Abbiamo avviato il Gruppo di Lavoro (GDL) più di un anno fa
- Nel frattempo abbiamo fatto molta strada
  - Abbiamo scelto FAIR come metodo quantitativo anche perché indicato da ISACA
  - Abbiamo ipotizzato di fare un «ponte» o un «mapping» tra ISO 27k e FAIR
  - Abbiamo verificato che in realtà il problema era simile per tutti i framework analoghi all'ISO 27k , ossia che prevedevano un approccio di conformità ad una serie di controlli (CIS,NIST 800-53 rev x, ..)
  - Abbiamo verificato che anche il GDPR poteva essere interessante da valutare per il profilo dei possibili danni al titolare a seguito di violazioni. IL GDPR è simile all'ISO 27701 che è l'estensione dell'ISO 27001 ai dati personali.

Sintesi di più di un anno di lavoro (2)

- Il gruppo è cresciuto numericamente : siamo arrivati ad un massimo di 15 partecipanti
- Ci siamo suddivisi in 2 sottogruppi : uno per l'ISO 27k e l'altro per il GDPR
- Abbiamo studiato e sperimentato diversi metodi di calcolo (oggi vi diamo un'idea di quelli che sono più utili)
- Abbiamo discusso anche animatamente per come realizzare al meglio quanto segue


Non richiesto
Stima calibrata
Da Criteri ISO
Calcolato
Rischio
MC
Frequenza evento dannoso
Entità del danno
X
+
Frequenza minaccia
Vulnerabilità
Primario
Secondario
T
X
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
Threat prevention
Riduce prob. di attacco
Vuln. prevention
Riduce vulnerabilità
ISO 27001
Categoria
Asset
Prevention
Threat
Vulnerability
Detection
Response
Variance
Decision
1
2
3
4
5
Response
Riduce conseguenze
Riduce tutte le Varianze
Detection
Riduce capacità di attacco v. pag. 248

Alcune volte la complessità era tale che siamo finiti così

NON CI SIAMO ARRESI

- Abbiamo constatato che la definizione dei controlli FAIR (2014) era incompleta (non è stato semplice e nemmeno breve)
- Giugno 2021, abbiamo contattato Jack Jones (il coautore di FAIR), gli abbiamo detto cosa volevamo fare, cosa stavamo facendo e quali erano secondo noi i problemi con FAIR
- Ci ha risposto che stava lavorando a una nuova versione e ci ha proposto di condividerla in anticipo ed era interessato al nostro mapping di ISO27k

Da giugno in poi..

- Abbiamo sospeso il sottogruppo GDPR, infatti se non si risolveva il mapping ISO 27001 non si poteva affrontare GDPR e ISO27701
- Abbiamo continuato il lavoro di mapping ISO 27001 con la nuova versione dei controlli FAIR (ve ne parleremo a breve)
- Il 20 ottobre abbiamo presentato il lavoro sinora svolto alla FAIRCON21 (conferenza annuale del FAIR INSTITUTE a livello world wide) con un breve video
- Dobbiamo completare il lavoro
- Riprenderemo anche il lavoro GDPR

Agenda

- Un riepilogo dei concetti base e dei metodi delle valutazioni quantitative a partire dalla nostra esperienza , con esempio di calcolo dal vivo
- Una illustrazione della nuova ontologia dei controlli FAIR (useremo la presentazione di Jack Jones). Ci sono concetti molto interessanti da approfondire
- Un esempio del nostro mapping ISO 27k FAIR
- ……

I partecipanti alla FAIRCON21

- Glauco Bertocchi
- Alessia Valentii
- Mario Taddonio
- Alberto Piamonte
- Maurizio Pagano
- Giuseppe Cagnetta
- Francesca Della Mea
- Luca Fei

Gli altri partecipanti

- Ringraziamo chi ci ha dato il suo contributo e poi ha dovuto lasciare : Luciano Capone, Cristina Nunu, Silvano Bari, Raffaella D’alessandro,.

- Sono rimasti in «panchina» (gruppo GDPR)
  - Fabio Pieralice
  - Riccardo Cocozza
  - Fabio Turano

Grazie per l’attenzione

Passo la parola al prossimo relatore

AGGIORNAMENTO FAIR

GDL ISACA ROMA

Alberto Piamonte
alberto.piamonte@alice.it

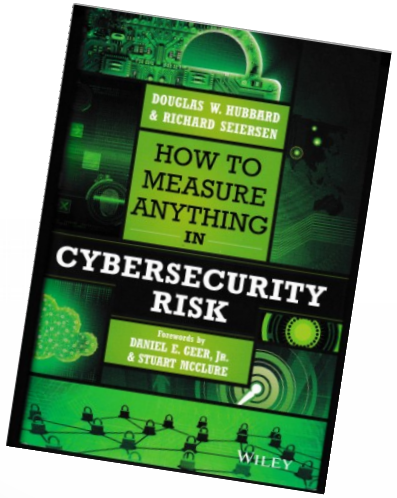
29 ottobre 2021

SECURE360

The Biggest Cybersecurity Risk

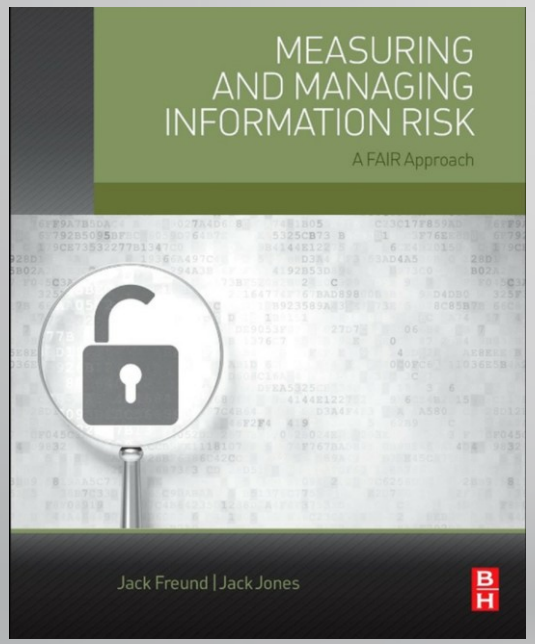
Question: What is Your Single Biggest Risk in Cybersecurity?

Answer: How You Measure Cybersecurity Risk

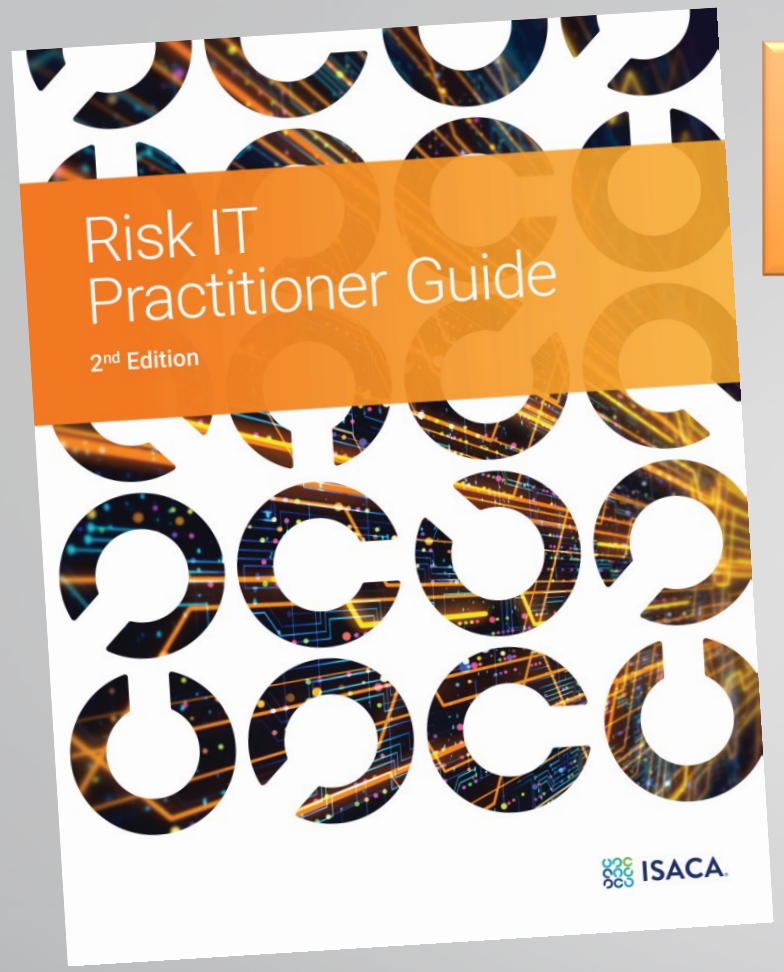


Hubbard Decision Research

Il metodo FAIR



- Un'associazione ed uno standard documentato e riconosciuto
- Un testo completo, pratico ed efficace che:
  - Identifica i fattori che determinano il rischio
  - Individua le aree possibili di intervento
  - Spiega come procedere per livelli di dettaglio progressivi
  - Considera il «*come*» comunicare i vari fattori del rischio
  - Istruzioni pratiche (*da «cosa» a «come»*)!
  - ….



Dal nuovo Risk IT…..

- **4.1.3 Risk Assessment and Analysis**
- ….
- If a risk is identified, enter it into a list, sometimes called a risk register, and determine the next step in analysis or response. This step in the risk management process often needs further analysis of the **risk factors** to determine an effective course of action or cost-justification for a plan of remediation.
  - **A recommended decision analysis process is to use Monte Carlo modeling** and simulation analysis to rank-stack, or prioritize, the list of risk concerns in a risk register for appropriate responses.
  - Monte Carlo simulations, such as those used in the **F**actor **A**nalysis of **I**nformation **R**isk (FAIR®) method, view risk as a function of likelihood (frequency of something happening) and impact.
- **The full analytic model of FAIR enables Monte Carlo analyses; however, it can be used to statically assess best- and worst-case outcomes of scenarios to enable quick triaging.**
- ….

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.

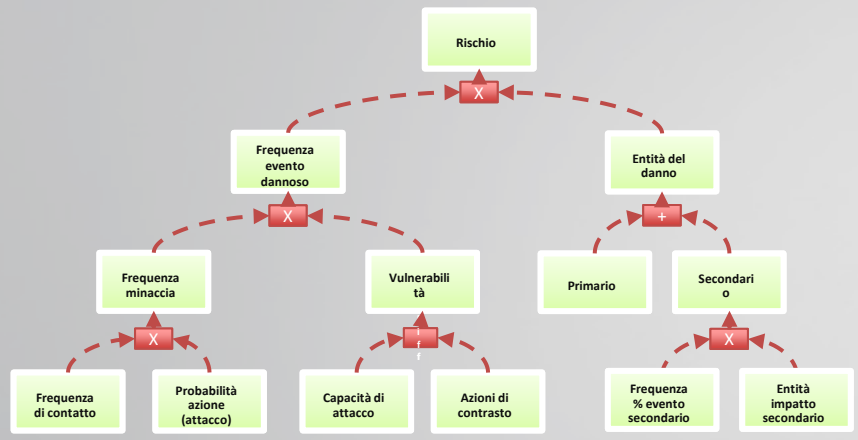
But ultimately a statement concerning risk is a belief statement – a belief statement that is simply the act of describing the issue currently at hand (sometimes referred to as a "state of nature") based on the evidence available at the time. The act of creating a belief statement based on evidence lends 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.

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.

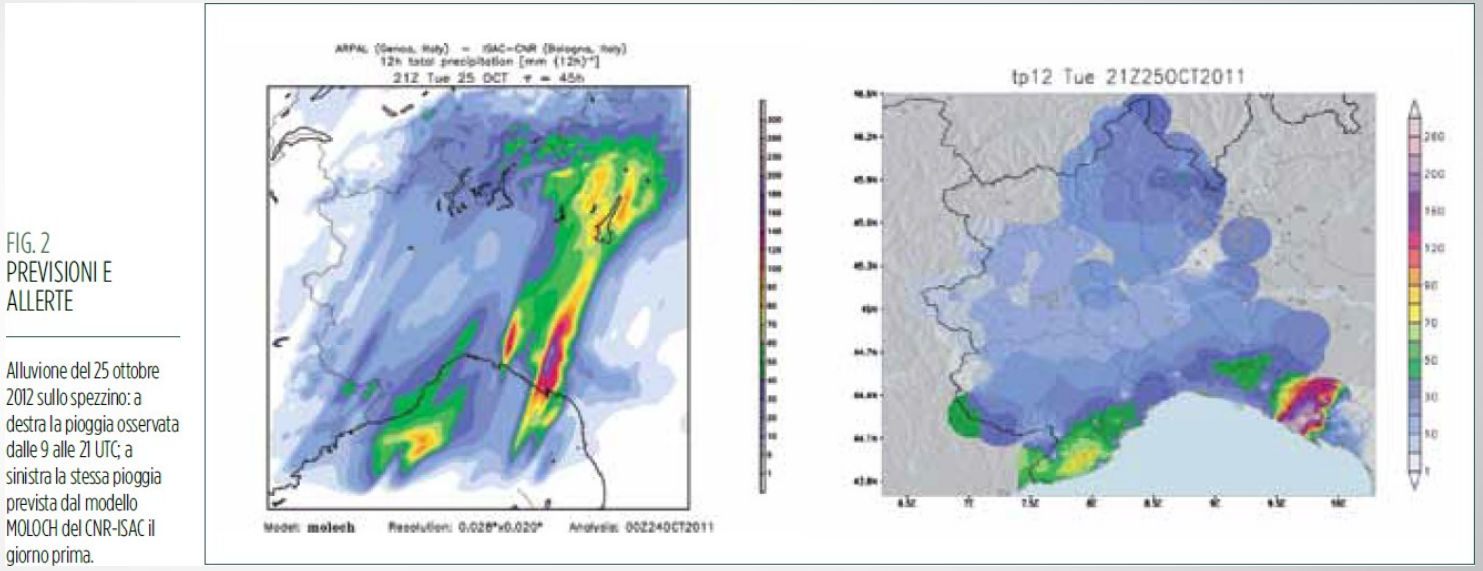


FIG. 2
PREVISIONI E ALLERTE

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)

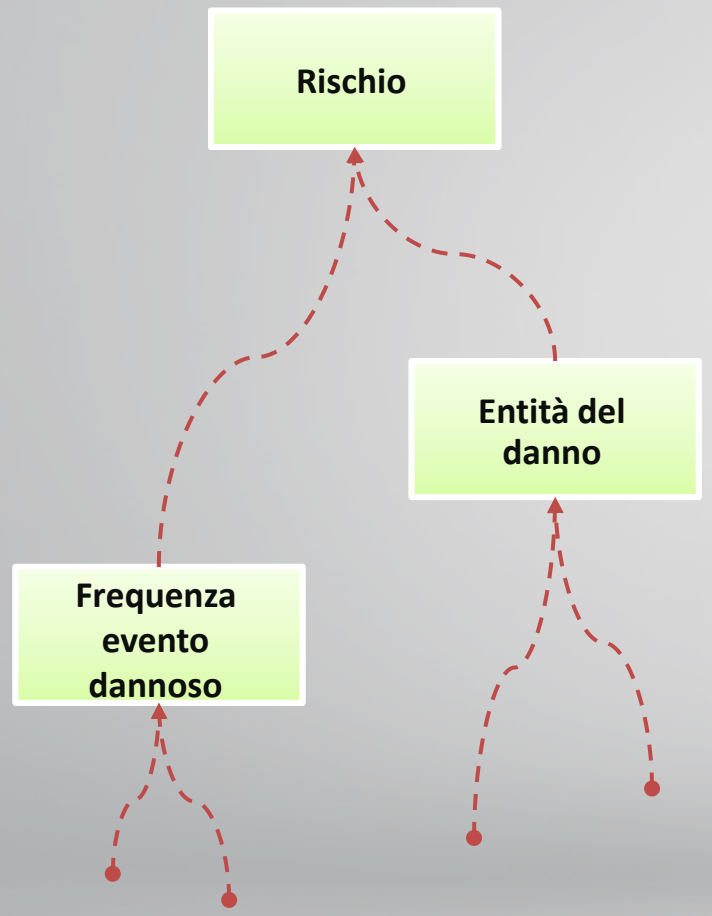
From a Compliance-based to a Risk-based Approach to Cyber Risk Quantification and Operational Risk

Organizations are increasingly transitioning to risk-based approaches to information security and operational risk, as compliance to regulations alone provide only a minimum layer of security and fail to adequately protect them.

- Information risk has become a business issue, not just a technology issue, as most business processes have digitalized.
- Boards of directors and business executives want to understand an organization's loss exposure in financial terms to enable effective decision-making.
- Risk and security professionals must become facilitators of the balance between protecting the organization and running the business.

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

Ontologia FAIR



Come misurare 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**."

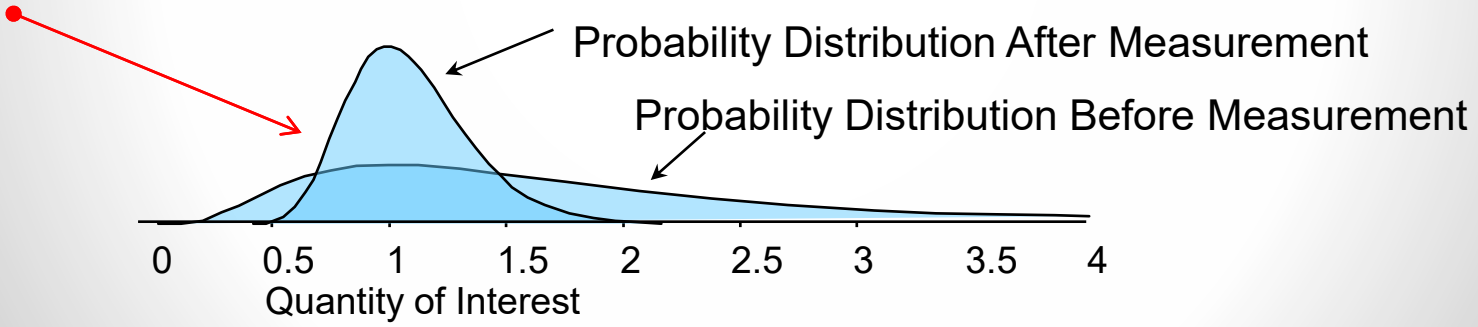
…. A measurement is, ultimately, **just information**, and there is a rigorous theoretical construct for information. field called "information theory", was developed in the 1940s by Claude Shannon, an American electrical engineer and mathematician.

The Concept of Measurement

It's not a point value.

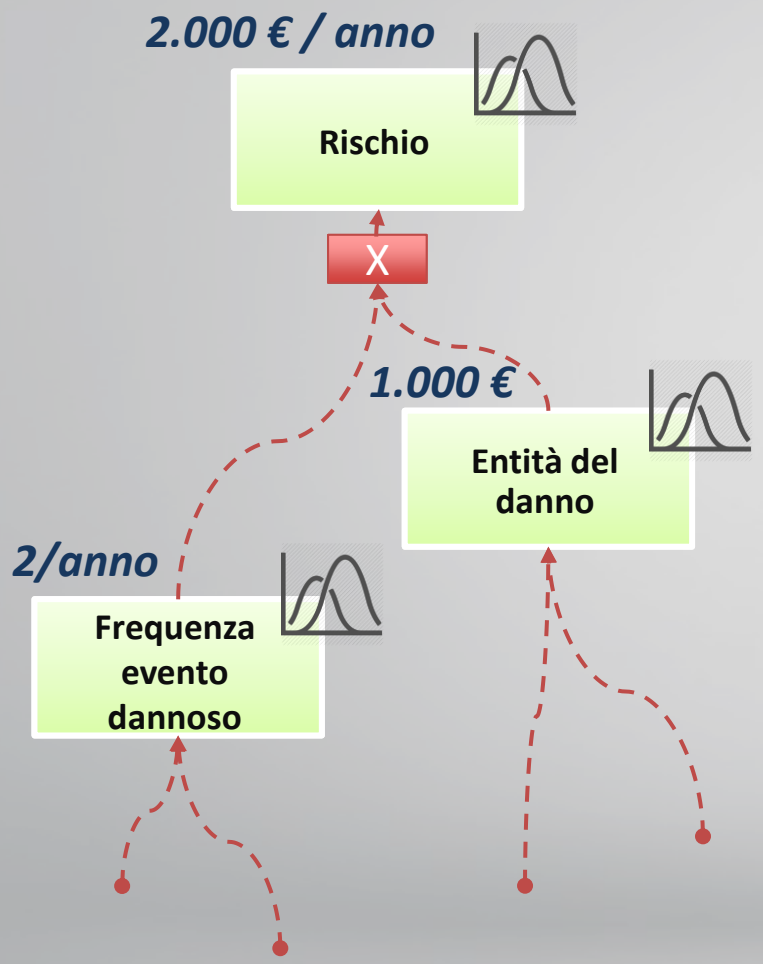
- Measurement: a quantitatively expressed reduction in uncertainty based on observation.
- You can quantify your current uncertainty – additional observations reduce it.
- Even marginal reductions in uncertainty can be extremely valuable.

Distribuzione dei possibili valori, complessivamente copre il 100% delle possibilità



25

La matematica «dell'incertezza»



Doing "Uncertainty Math"

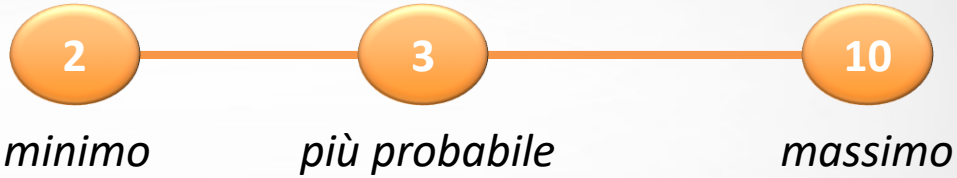
Using ranges to represent your uncertainty instead of unrealistically precise point values clearly has advantages. When you allow yourself to use ranges and probabilities, **you don't really have to assume anything you don't know for a fact**. But precise values have the advantage of being simple to add, subtract, multiply, and divide in a spreadsheet. If you knew each type of loss exactly it would be easy to compute the total loss. Since we only have ranges for each of these, we have to use probabilistic modeling methods to "do the math."

So how do we add, subtract, multiply, and divide in a spreadsheet when we have no exact values, only ranges?

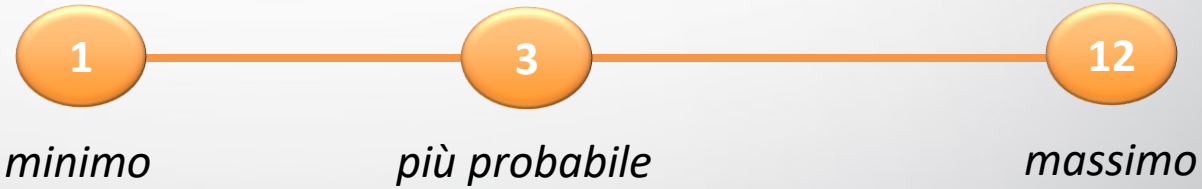
Fortunately, there is a practical, proven solution, and it can be performed on any modern personal computer—the "**Monte Carlo**" simulation method. A Monte Carlo simulation uses a computer to generate a large number of scenarios based on probabilities for inputs. For each scenario, a specific value would be randomly generated for each of the unknown variables. Then these specific values would go into a formula to compute an output for that single scenario.
This process usually goes on for thousands of scenarios.

Come esprimere l'incertezza ?

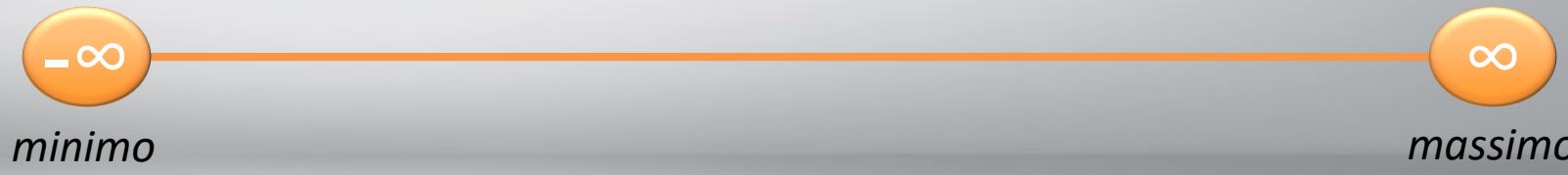
La gamma (estensione dei possibili valori) ci consente di esprimere numericamente il nostro livello di incertezza:



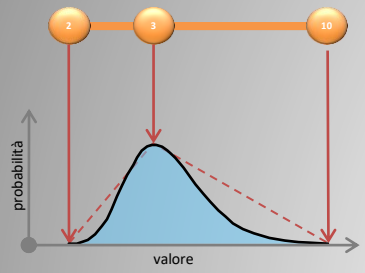
Oppure :



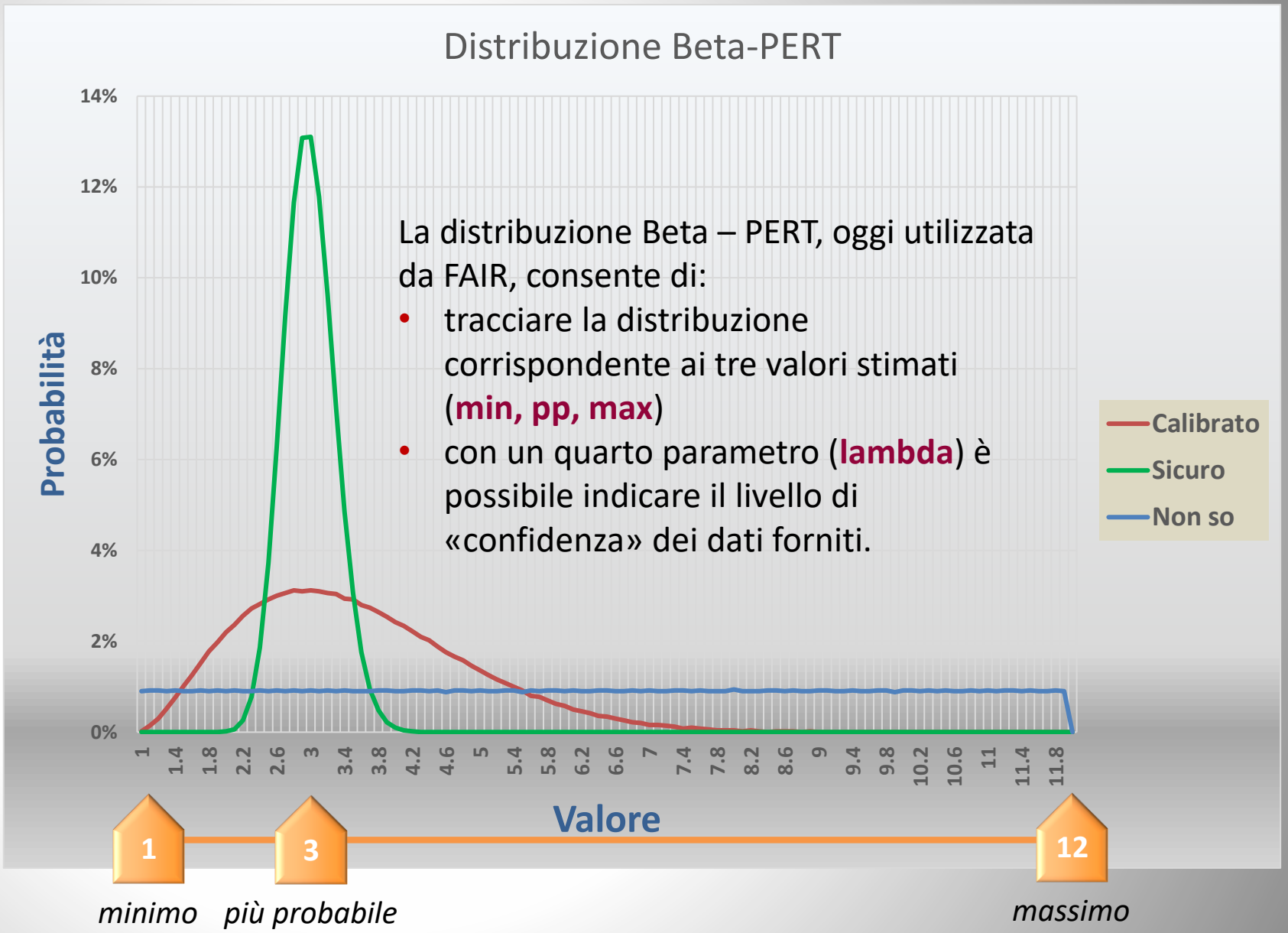
ma non :



Da gamma a distribuzione



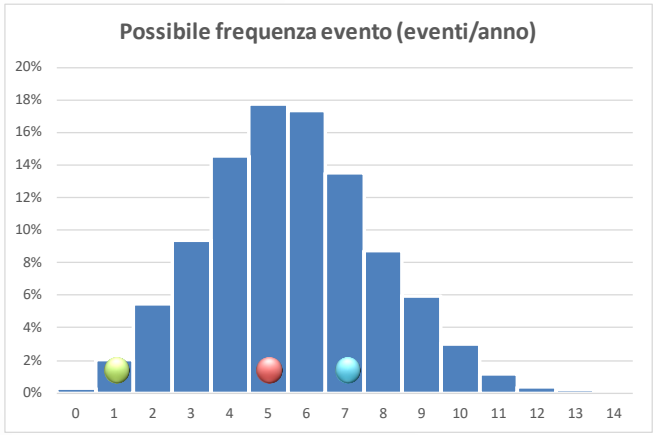
La distribuzione triangolare e la beta-Pert

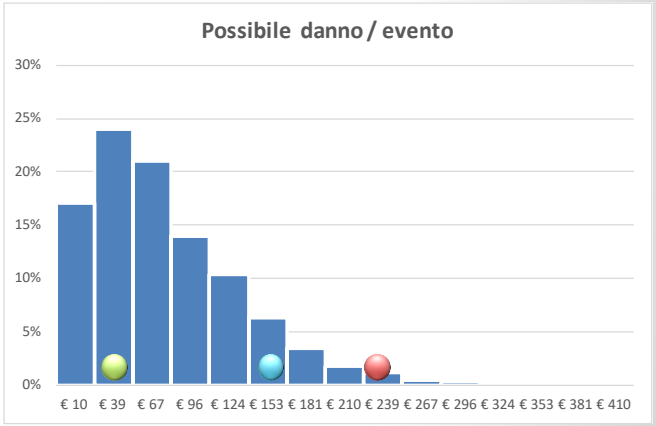


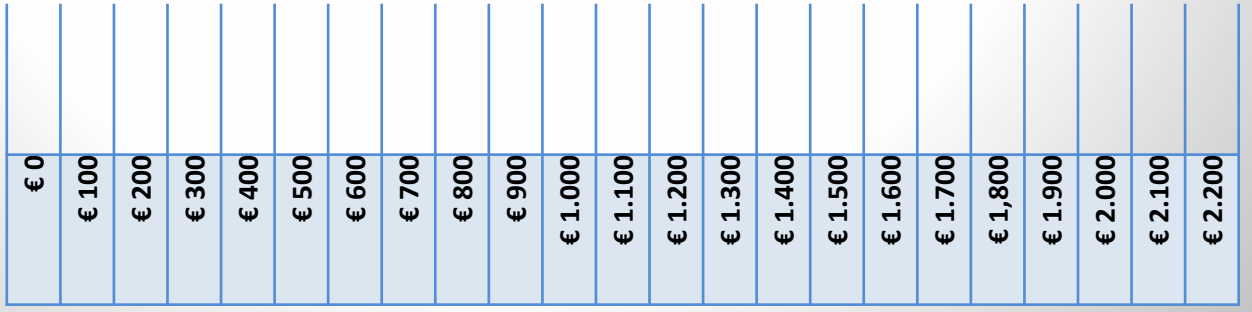
La distribuzione Beta – PERT, oggi utilizzata da FAIR, consente di:

- tracciare la distribuzione corrispondente ai tre valori stimati (**min, pp, max**)
- con un quarto parametro (**lambda**) è possibile indicare il livello di «confidenza» dei dati forniti.

Il metodo Monte Carlo







Fattore di confidenza : medio

€ 0	€ 100	€ 200	€ 300	€ 400	€ 500	€ 600	€ 700	€ 800	€ 900	€ 1.000	€ 1.100	€ 1.200	€ 1.300	€ 1.400	€ 1.500	€ 1.600	€ 1.700	€ 1,800	€ 1.900	€ 2.000	€ 2.100	€ 2.200

Alla fine

Percentili	
10%	€ 138.00
25%	€ 221.00
50%	€ 392.00
75%	€ 643.00
90%	€ 916.00
95%	€ 1,125.00
99%	€ 1,627.00

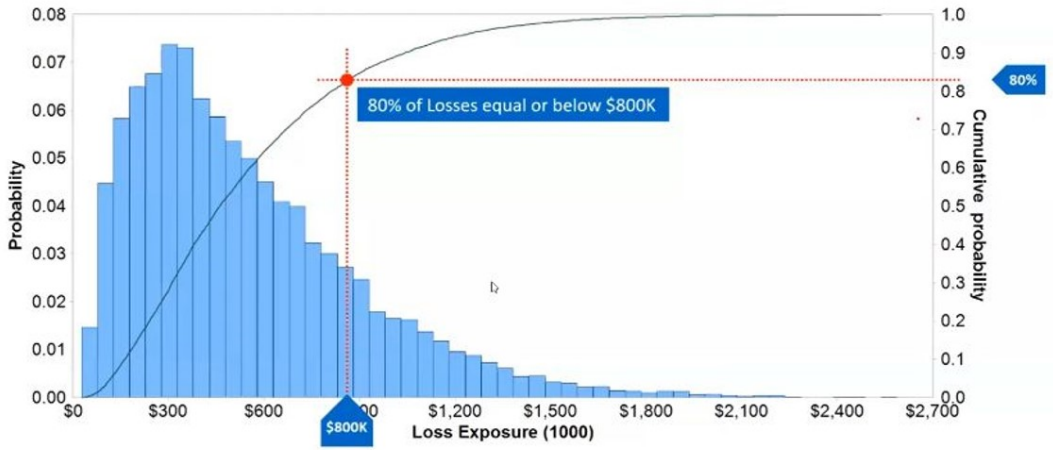
Fattore di confidenza : medio

Analisi del rischio «quantitativa - statistica» !

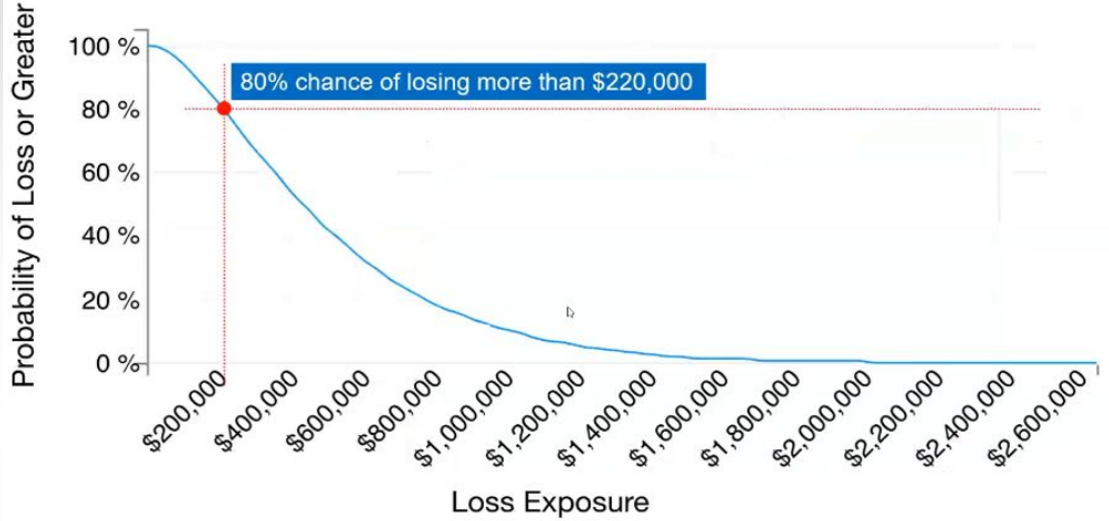
MonteCarlo Quando si può usare e per quali operazioni ?

- Distr. Rischio = Distr. Probabilità **X** Distr. Impatto
- Distr. Somma Impatti = **Σ Distr. Impatti**
- Distr. vulnerabilità = Distr. Forza attaccante – Distr. Resistenza Difese
- Ecc.

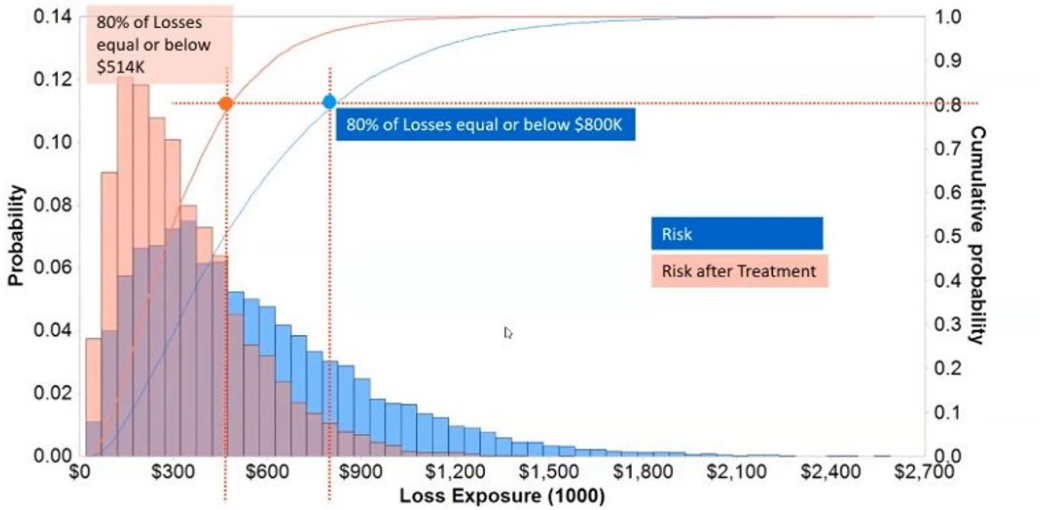
PROBABILITY DISTRIBUTION



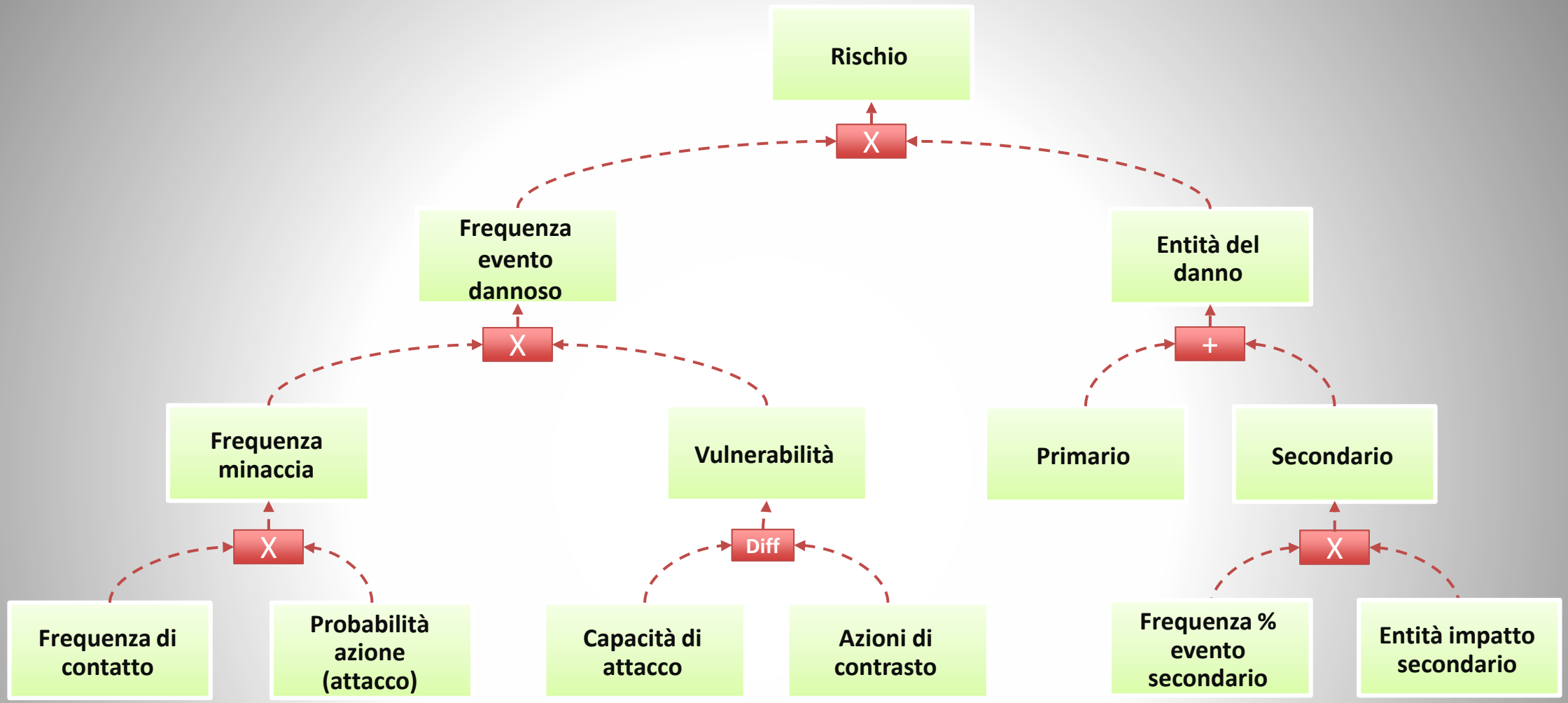
LOSS EXCEEDANCE CURVE



MAKE EFFECTIVE COMPARISONS



LOSS EXCEEDANCE CURVE COMPARISON


Rischio
X
Frequenza evento dannoso
Entità del danno
X
+
Frequenza minaccia
Vulnerabilità
Primario
Secondario
X
Diff
X
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario

Rischio

Frequenza evento dannoso

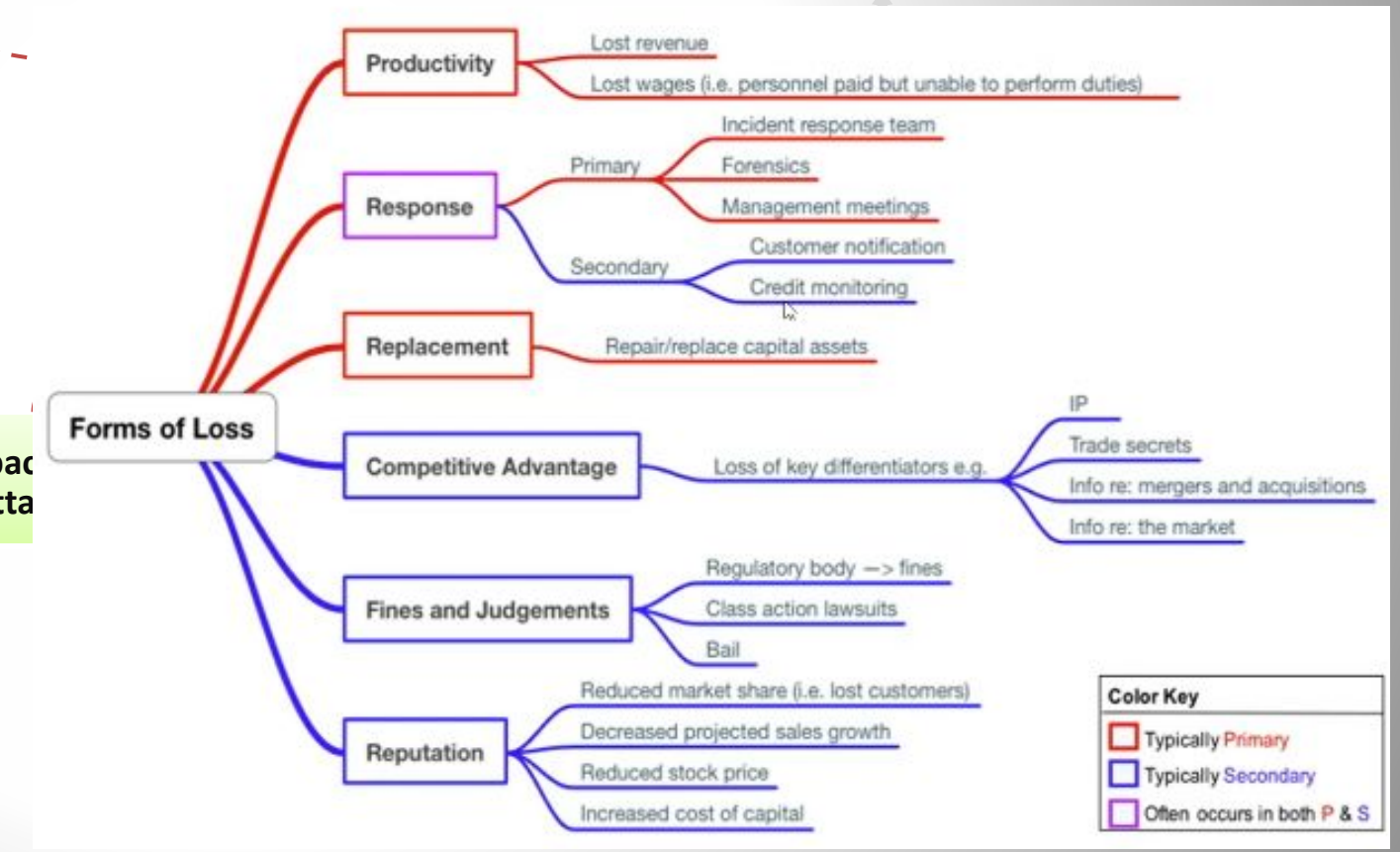
Entità del danno

Frequenza minaccia

Frequenza di contatto

Probabilità azione (attacco)

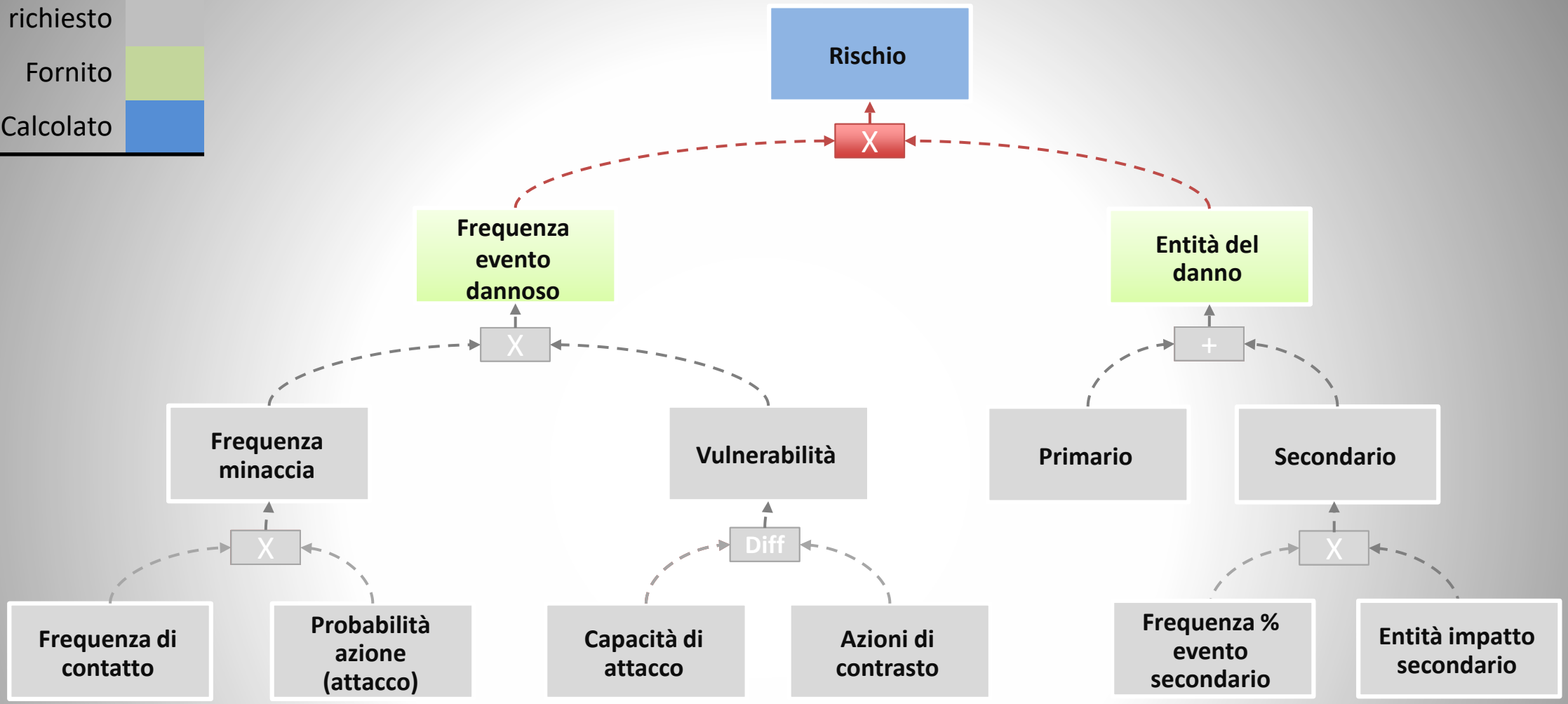
Capac atta



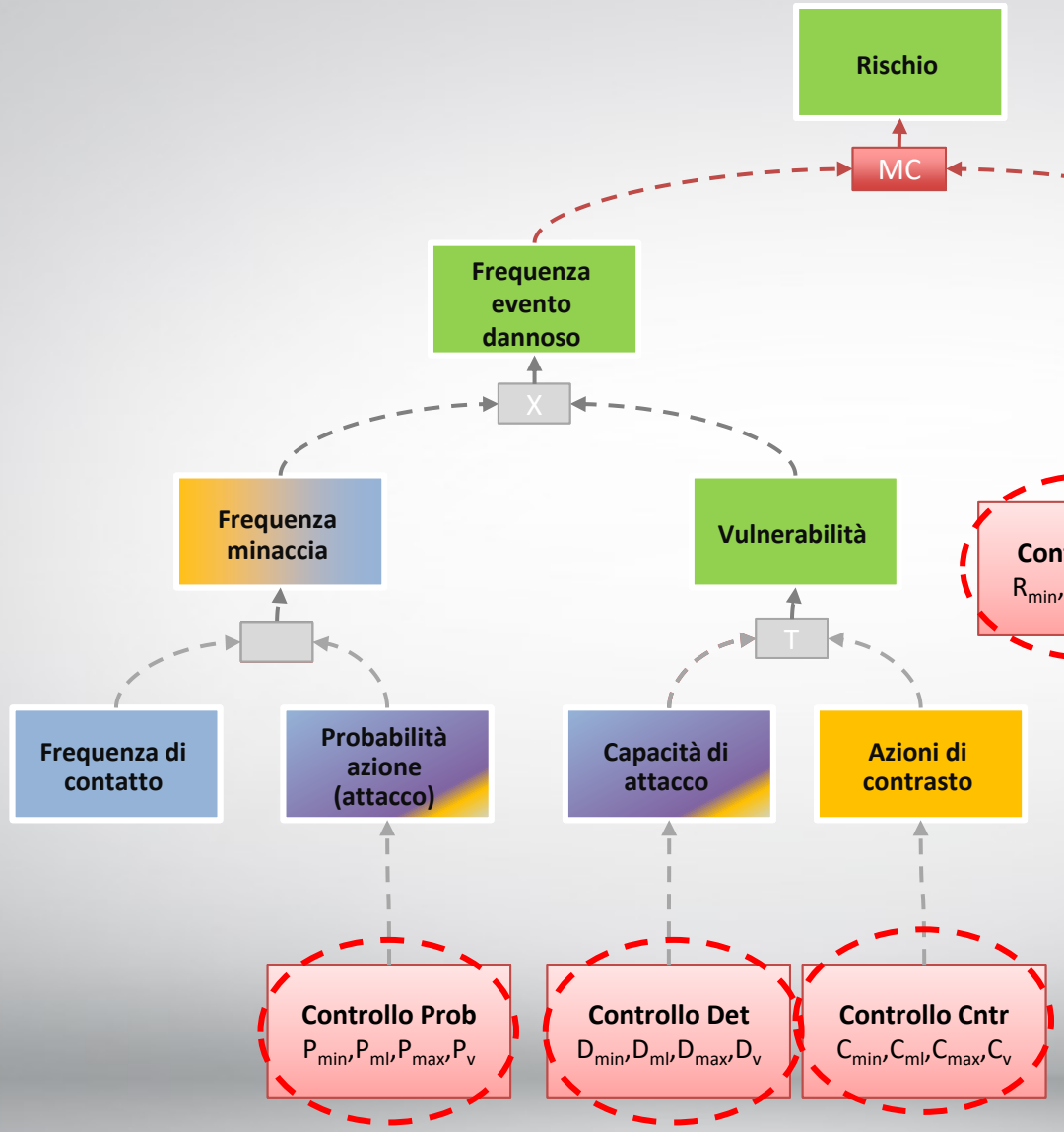
Non richiesto

Fornito

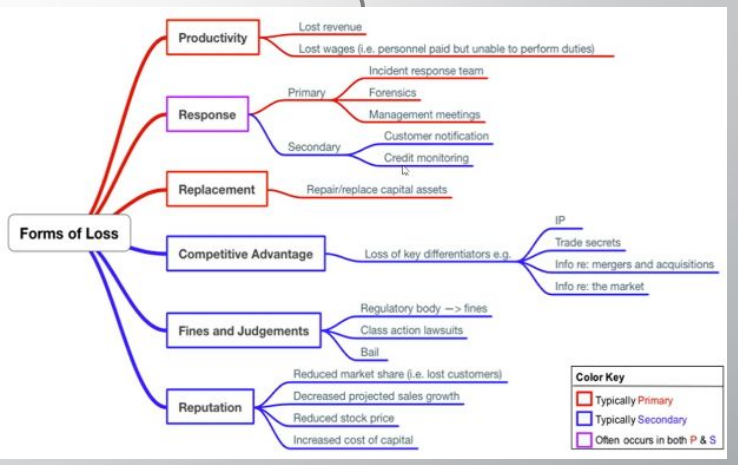
Calcolato



L'evoluzione FAIR-CAM : Ontologia dei Controlli



Da dedurre dalla «maturità» dei controlli applicati (o pianificati)



FAIR Controls Analytics Model™ (FAIR-CAM™)

Measure The Value of Controls

T

IN PRATICA

37

STIMARE

Stimando s'impara

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 (***Calibration***)
- Conosciamo molto più di quanto si creda . . .

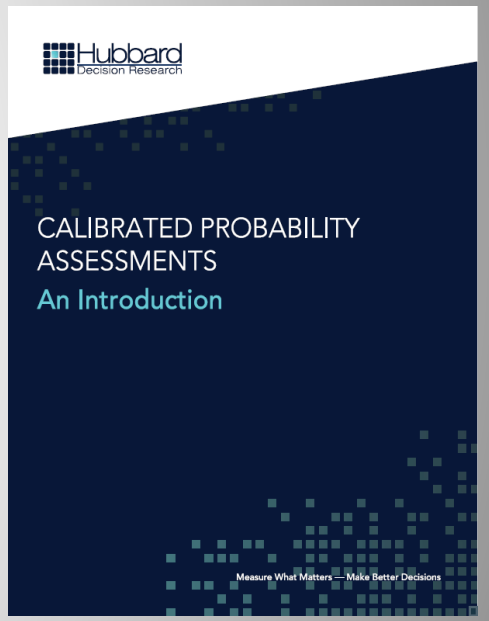
Quante commedie ha scritto Shakespeare ?

Calibration questions

#	Question	Lower Bound (95% chance value is higher)	Upper Bound (95% chance value is lower)
1	What percentage of bronze is typically made of copper?		
2	How many countries have at least one McDonald's?		
3	How many employees did ebay have in the first quarter of 2006?		
4	What was the population of Miami (within the city limits, not the entire metropolitan area) in 1990?		
5	How many casualties did the French suffer in the Battle of Waterloo?		
6	What is the range in miles of a Minuteman Missile?		
7	What is the percentage of IT jobs in the US were unfilled in 1997?		
8	The Supremes' (with Diana Ross) song "Stop! In the Name of Love" was how long? (minutes, seconds)		
9	How many undergraduates attended Cambridge in 1990?		
10	If you could jump 50 feet straight up into the air, how many seconds would you be airborne before you landed?		
11	How many gallons are in a bushel (they are both measures of volume)?		
12	How many sovereign rulers has England had in the last thousand years?		
13	If the air temperature was 5 degrees below zero (Fahrenheit) and the wind speed was 15 mph, what would the temperature adjusted for wind-chill be?		
14	Average cost of testing in software development is what percentage of total project costs?		
15	On average, if a software development project was projected to take 17 months, it actually takes how many months?		
16	How many meters tall is the Sears Tower?		
17	How many gold medals did Jesse Owens win at the 1936 Berlin Olympics?		
18	In 2005, the average combined MPG for all US cars and light trucks on the road was how much?		
19	The average house in the United States uses how many gallons of water per day?		
20	What was the average price in the United States of a house sold in 2001?		

	Statement	Answer (T/F)	Confidence that you are correct (Circle one)
1	The melting point of tin is higher than the melting point of aluminum.		50% 60% 70% 80% 90% 100%
2	In English, the word "quality" is more frequently used that the word "speed".		50% 60% 70% 80% 90% 100%
3	Any male pig is referred to as a hog.		50% 60% 70% 80% 90% 100%
4	California's giant sequoia trees are named for an early 19th century leader of the Cherokee Indians.		50% 60% 70% 80% 90% 100%
5	The Model T was the first car produced by Henry Ford.		50% 60% 70% 80% 90% 100%
6	When rolling 2 dice, a roll of 7 is more likely than a 3.		50% 60% 70% 80% 90% 100%
7	No one has ever been reported to have been hit by any object that fell from space.		50% 60% 70% 80% 90% 100%
8	Sir Christopher Wren was a British anthropologist.		50% 60% 70% 80% 90% 100%
9	Pakistan does not border Russia.		50% 60% 70% 80% 90% 100%
10	The Navy won the first Army-Navy football game.		50% 60% 70% 80% 90% 100%
11	The paperback version of the book "The Da Vinci Code", as of July 2007, still ranks in the top 500 bestselling books on Amazon.		50% 60% 70% 80% 90% 100%
12	Italian has more words than any other language.		50% 60% 70% 80% 90% 100%
13	The month of August is named after a Greek god.		50% 60% 70% 80% 90% 100%
14	The deepest ocean trench is deeper than the Grand Canyon.		50% 60% 70% 80% 90% 100%
15	Abraham Lincoln was the first president born in a log cabin.		50% 60% 70% 80% 90% 100%
16	As of July of 2007, more people search Google for "Harry Potter" than "Hillary Clinton" (according to GoogleTrends).		50% 60% 70% 80% 90% 100%
17	The population of Alabama is higher than the population of Arizona.		50% 60% 70% 80% 90% 100%
18	No category 5 hurricane hit the US in 2004.		50% 60% 70% 80% 90% 100%
19	The UK is among the top 10 largest economies in the world (by GDP).		50% 60% 70% 80% 90% 100%
20	The movie Forest Gump has grossed more to date than E.T. The Extra Terrestrial.		50% 60% 70% 80% 90% 100%

Come interpretare i risultati



http://www.hubbardresearch.com/wp-content/uploads/2019/06/Introduction-to-Calibrating-Probability-Assessments-Hubbard-Decision-Research.pdf

No Data? No Problem

by Jack Jones

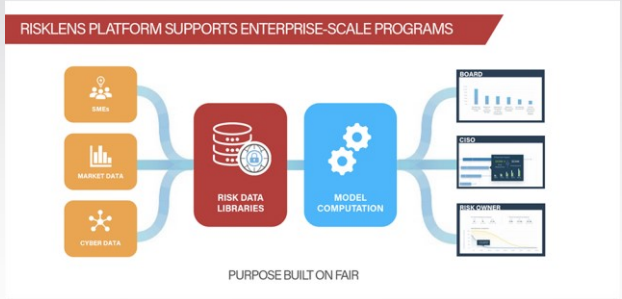
- ……
- Start with an absurd estimate (e.g., less than an inch or greater than ten feet tall). It breaks the ice and gets people out of the "I have no idea" mindset.
- Use references and logical reasoning to begin narrowing the range.
- Challenge your reasoning along the way, and consciously look for 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.
- …

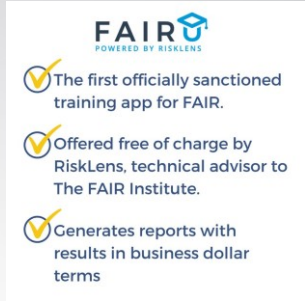
https://www.fairinstitute.org/blog/no-data-no-problem

TOOLS FAIR

- RiskLens

SaaS

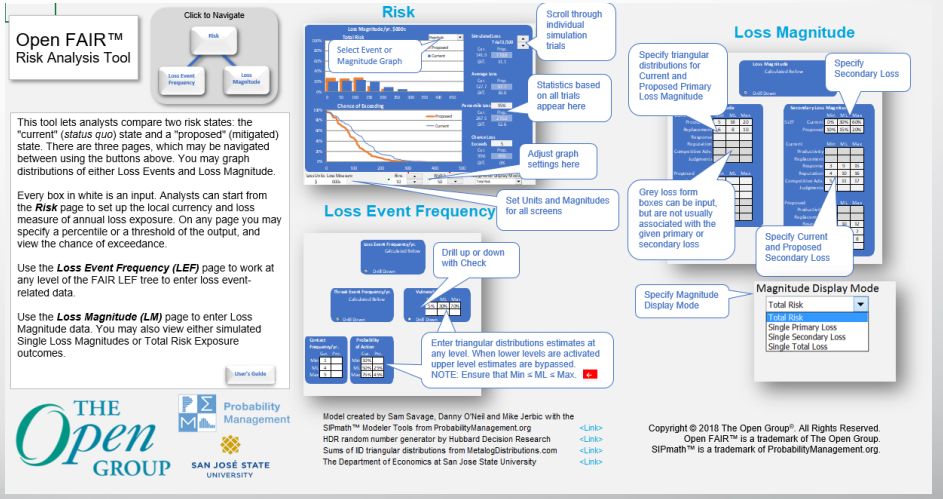




Free training

- Open Group

EXCEL (scaricabile, free 90 gg poi . . .)



- Fogli EXCEL + tools (OPENPERT, ecc.) + ……..
- Python da GitHub
- …

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) ?

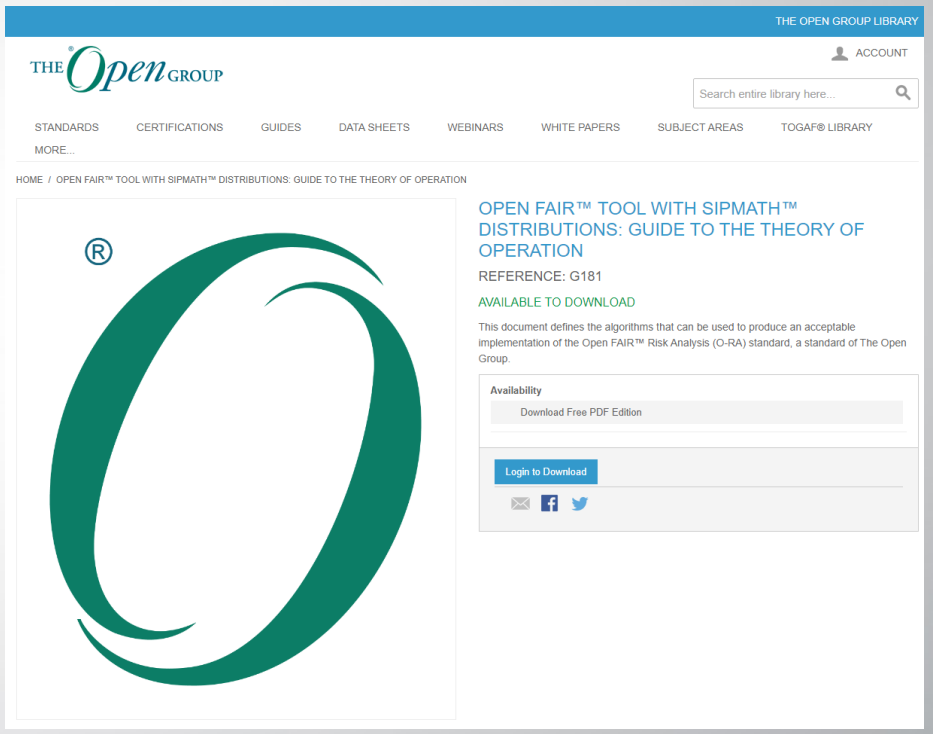
Dalla teoria alla pratica *(es: Excel®)*

Open Group Guide

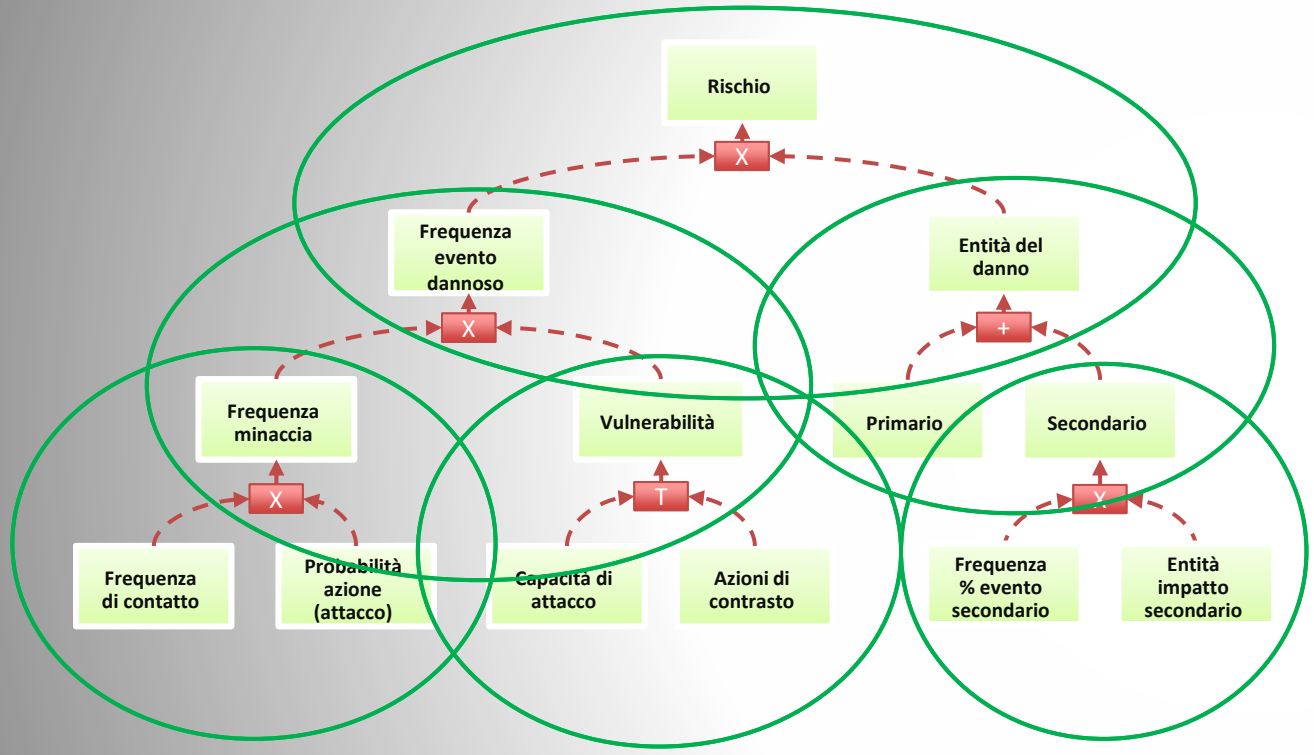
Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation

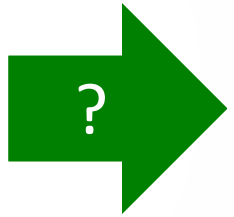
THE Open GROUP

Scaricabile dal sito OpenGroup previa registrazione:



Proviamo ad usare Excel





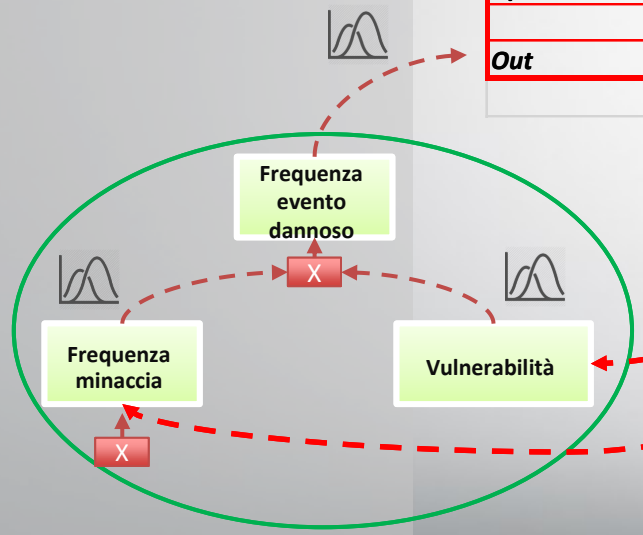
Foglio excel: LEF (Frequenza evento dannoso)

Calcolo LEF da Frequenza annuale ridotta e Vulnerabilità

	Dim.	*min*	*pp*	*max*	*Conf*	*Nome*	*Descrizione*
In 1	***%***	10%	30%	50%	M	VUL	Vulnerabilità
In 2	***ev/anno***					TEFR	Frequenza annuale eventi ridotta
Operazione	*						
Out	***ev/anno***					LEF	Frequenza annuale eventi perdita

MonteCarlo

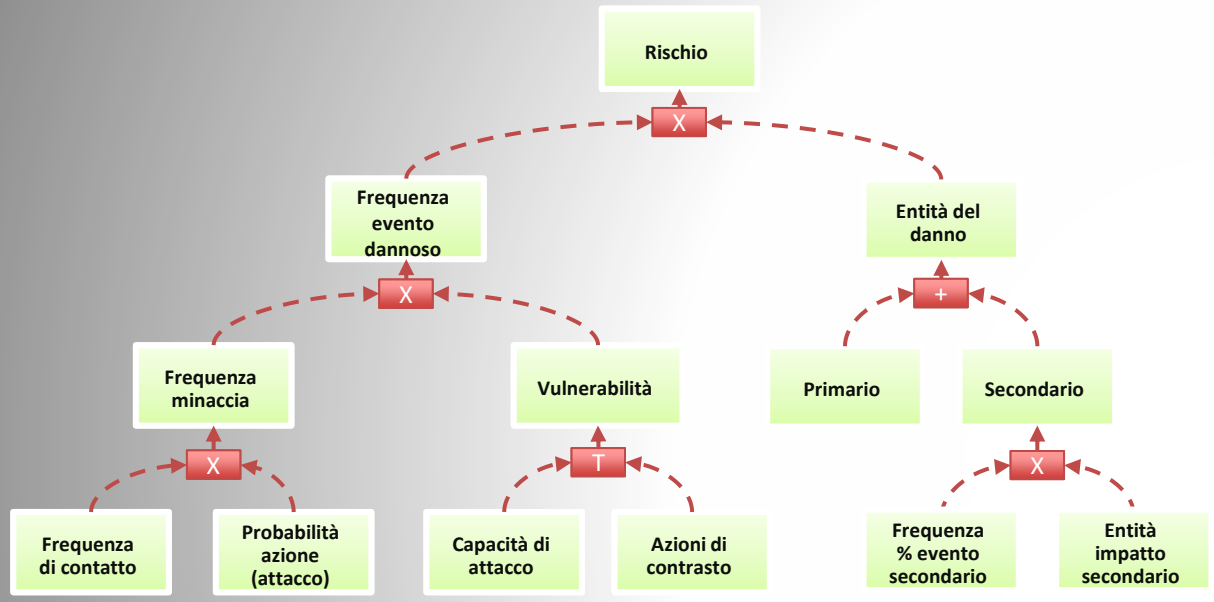
VUL	TEFR	LEF
0.279357		0.738807902
0.322571		1.212841938
0.242841		0.891099731
0.327357		1.366728854
0.225047		0.811502982
0.281838		0.751330377
0.227388		0.760610611



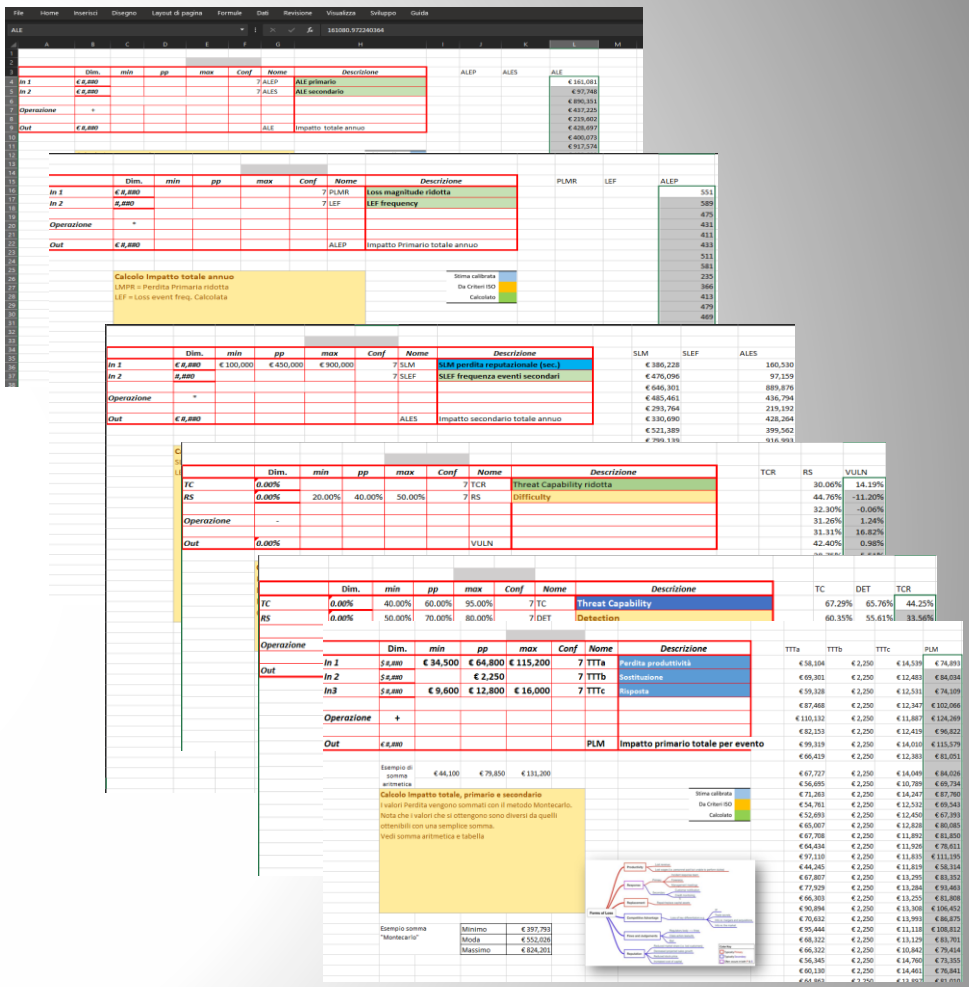
INPUT
Se **min, pp** e **max** non sono definiti, viene usato con il nome indicato (che deve essere definito altrove).
Se è definito solo **«pp»** viene generato un valore costante.
Se **min**, **pp** e **max** sono definiti, viene generata una distribuzione ***Pert + Conf***

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

DISTRIBUZIONI
Utilizzabili nel modello o per generare istogrammi e percentuali.

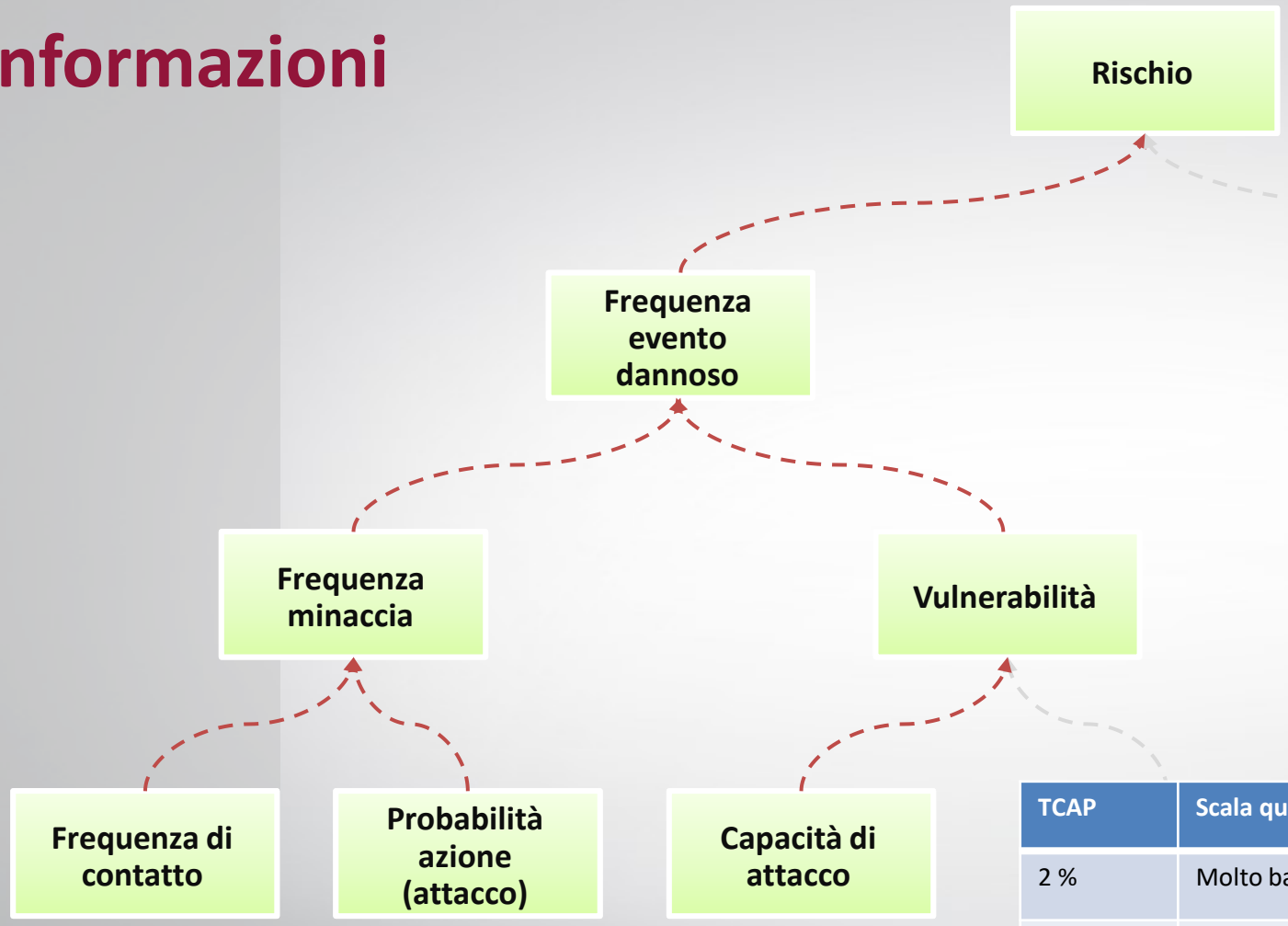


Un foglio Excel per ogni fattore FAIR

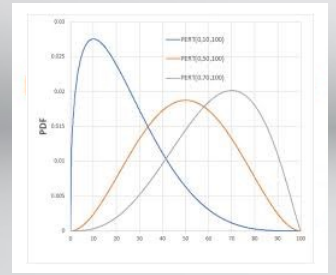


- Aperto
- Facilmente interfacciabile (in e out)
- Modificabile
- Prestazioni
- Programmabile

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

GDL ISACA Roma

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

Elabora

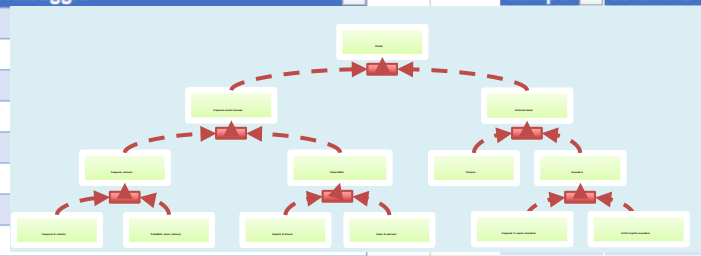
Genera Descrizione Distribuzioni

CLEAR DESCR

Aggiorna Elenco Distribuzioni

CLEAR DISTRIBUZIONI

	Wksheet	Tempo	Messaggio
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	



Campo	Column1

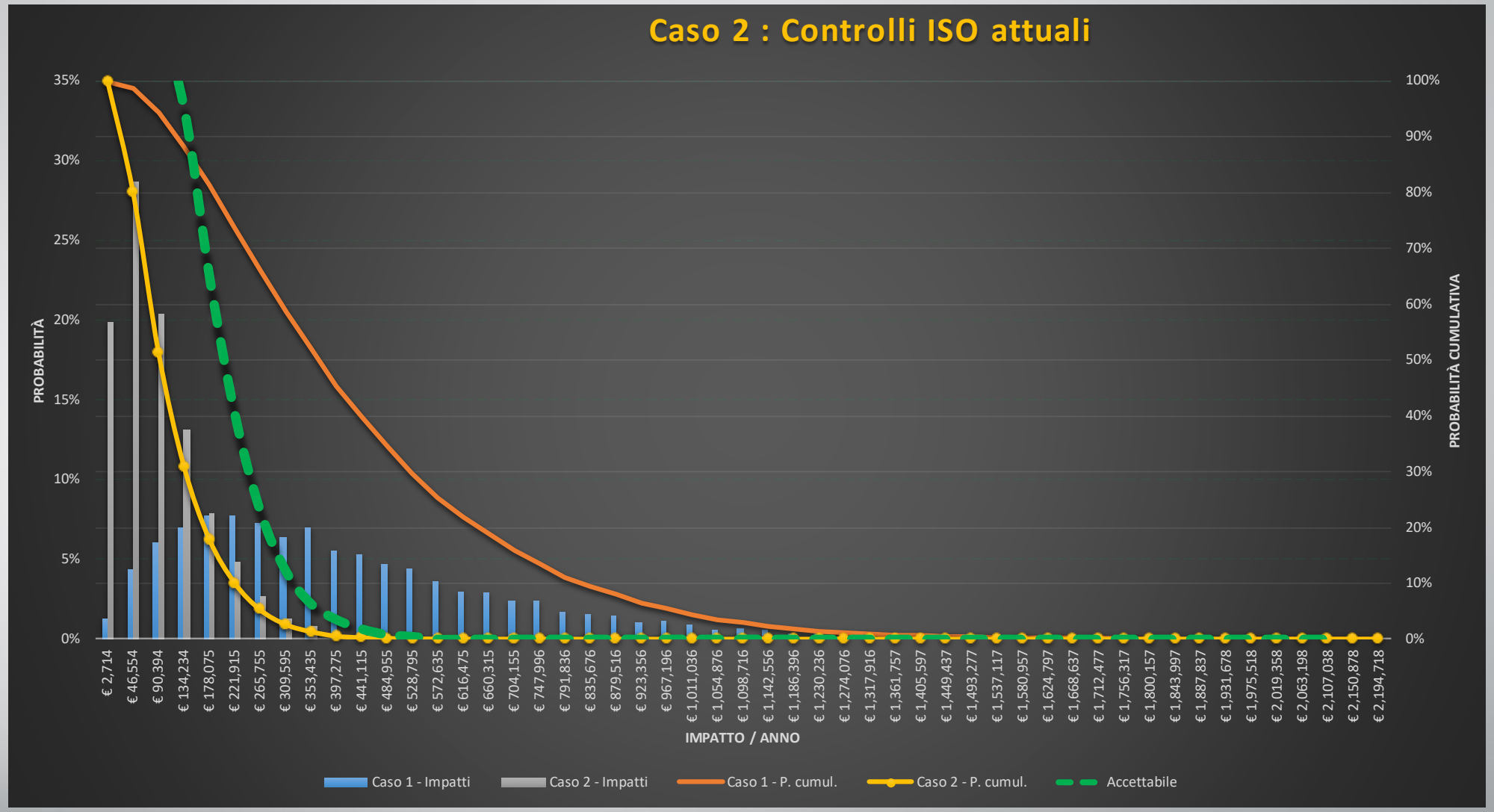
Confronto tra distribuzioni

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

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

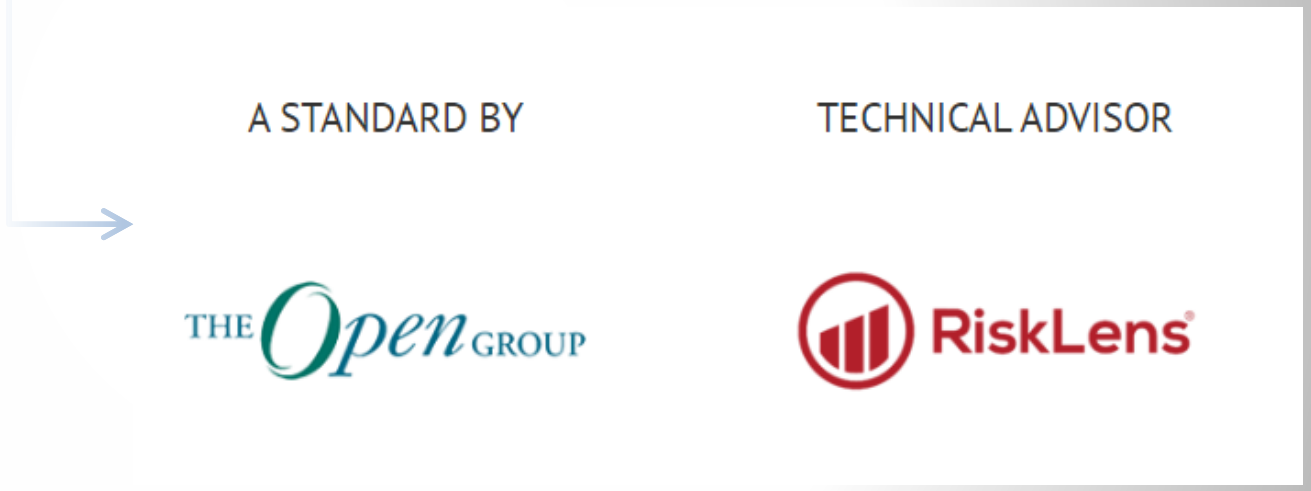
RISO_List | Process | Cover | ALE | ALEP | ALES | VUL | TC | TEF | LEF | SLF | PLM | PLMR | COMP_Graph | COMP_Data | TEF Descrip ...

Un esempio: confronto tra Rischio Intrinseco e Rischio attuale: proviamo ad usare l'excel



Riferimenti

https://www.fairinstitute.org



https:// www.opengroup.org

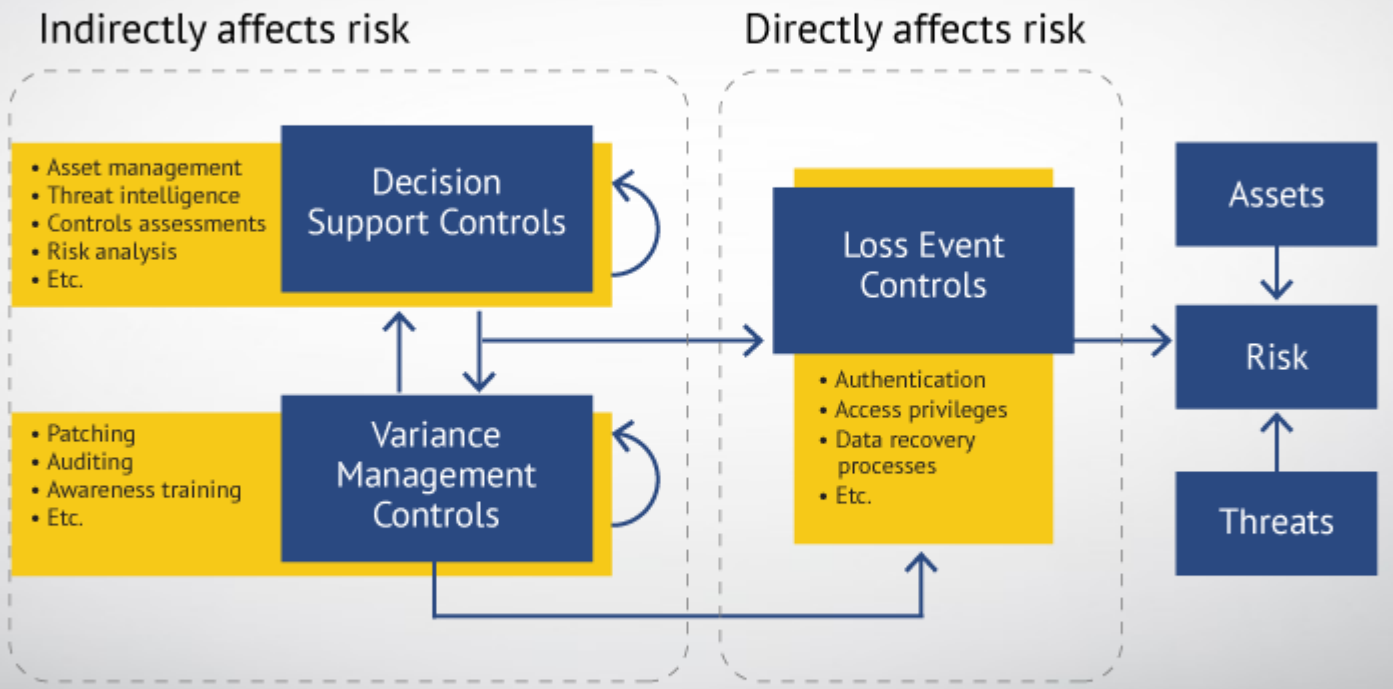
https:// www.risklens.com

Grazie per l'attenzione !

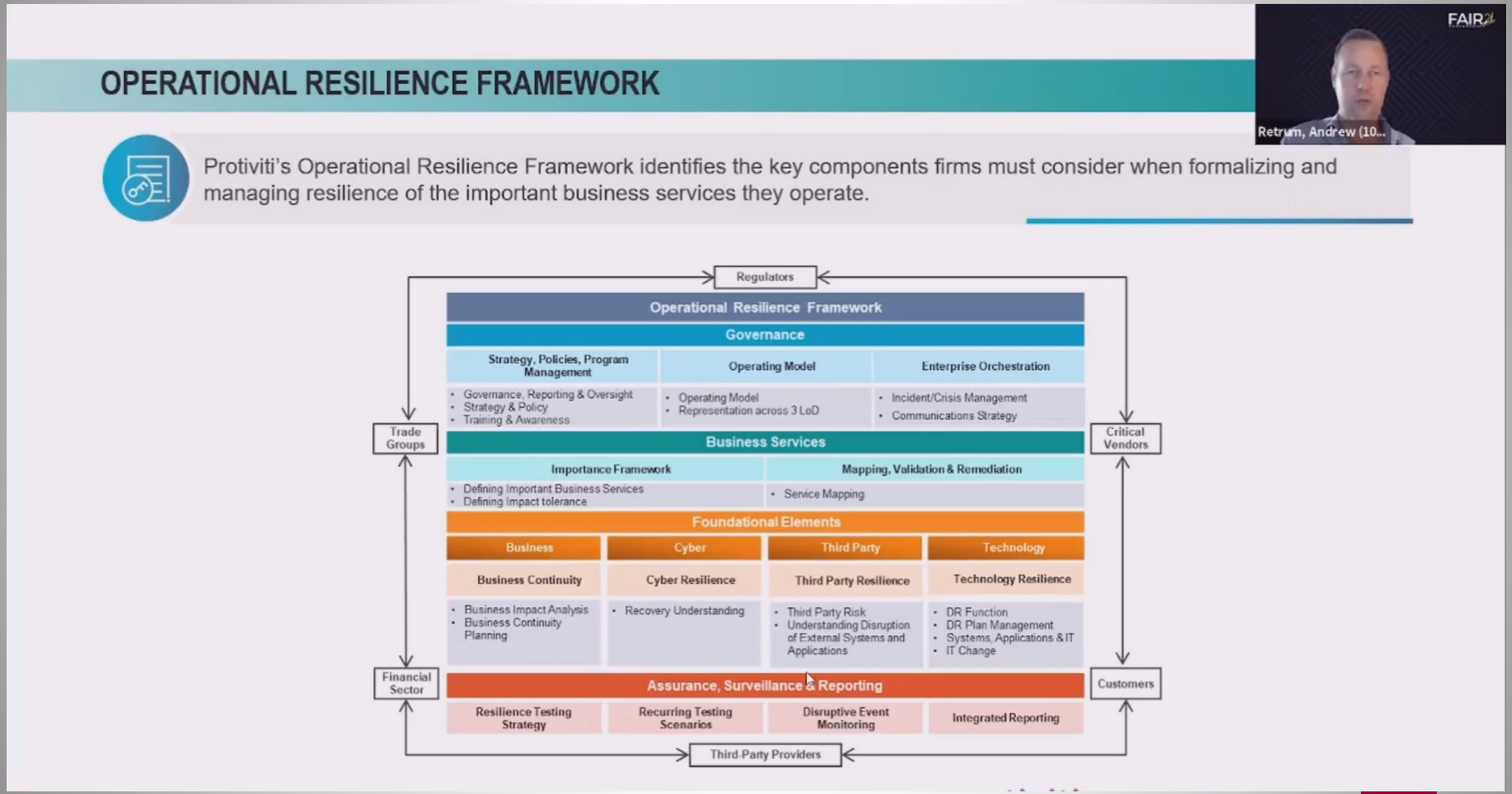
Domande ?

alberto.piamonte@alice.it

FAIR-CAM™ MODEL: Control Functional Domain Relationships



Un approccio sistematico . . . . .



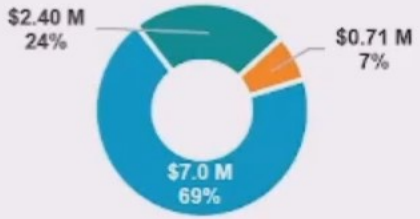
CASE STUDY – MAMMOTH BANK

EXECUTIVE SUMMARY – MAMMOTH BANK SCENARIO RESULTS

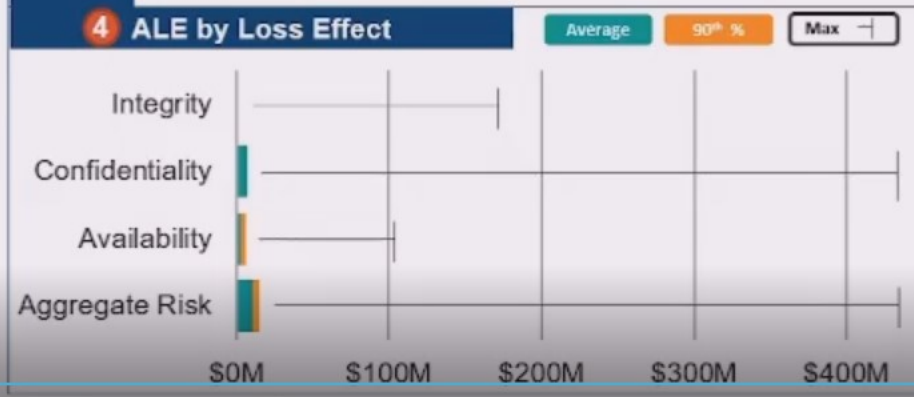
1 Annualized Loss Exposure (ALE)

2 Per Event Loss

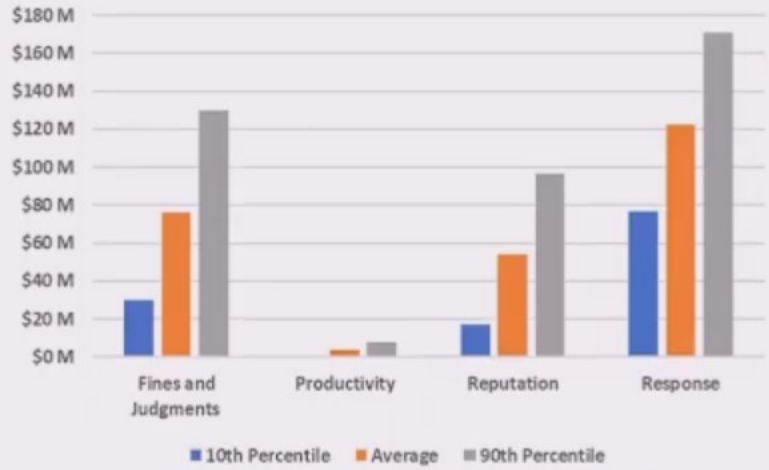
3 Avg. ALE by Loss Effect



4 ALE by Loss Effect



5 ALE by Form of Loss



6 Loss Exceedance Curve – Availability Risk

Introduction to the FAIR Controls Analytics Model (FAIR-CAM)

Jack Jones

Chairman FAIR Institute

Ask yourself these questions…

- What's the most valuable control in your cybersecurity program?
- What's the least valuable control?

Would your answers be the same as someone else's in your organization?

Is it important to be able to answer these questions?

What do we mean by “value”?

The value proposition of any risk management control boils down to this:

Its ability to affect the frequency or magnitude of loss

Ask yourself these questions…

- How does patching reduce risk? How do you measure its effect?
- What about policies, awareness training, or logging?
- How does risk analysis reduce risk?

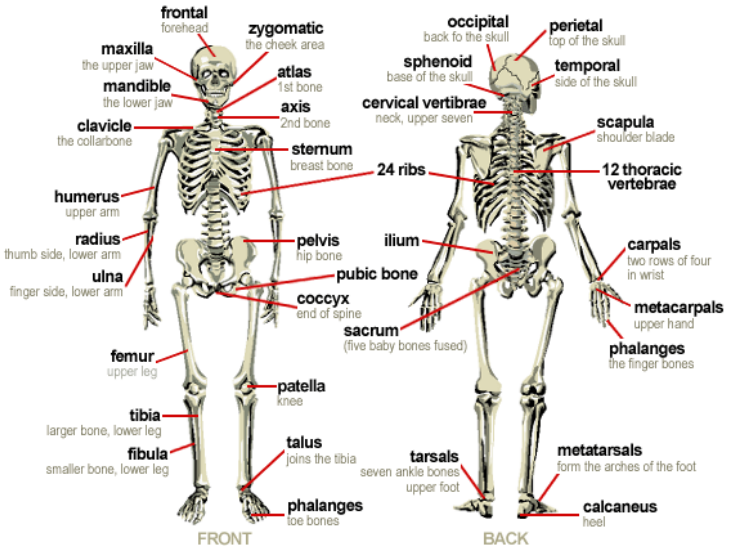
What’s been missing…

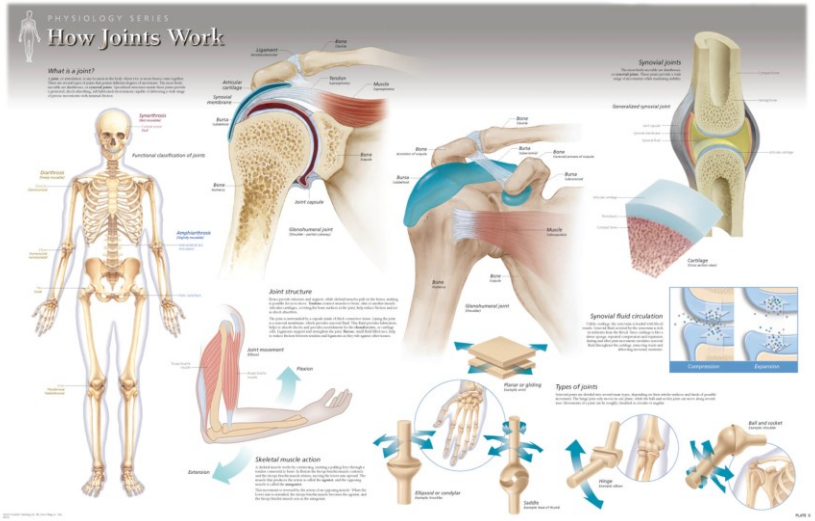
In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)

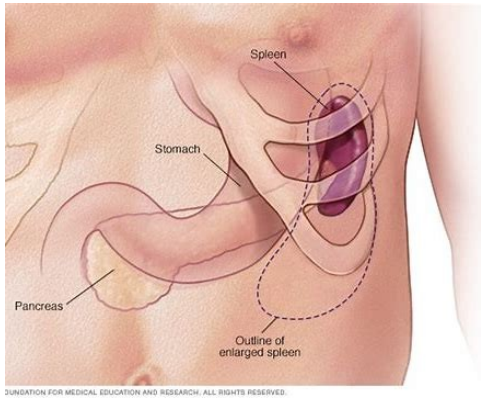




Neither. You need to know both.

Human Anatomy vs. Physiology

- **Anatomical component**: Spleen
  - Size: Approximately 1 x 3 x 5 inches
  - Weight: Approximately 7 oz
  - Location: Upper-left abdomen



- **Purpose**: Supports the immune system

- **Physiology**
  - Function: Blood filtering via white pulp and red pulp
  - Depends upon: Arteries, veins, nerves, lungs, etc…
  - Is depended upon by: Liver, brain, etc…
  - When missing or damaged is partially compensated for by: Lymph nodes, etc…

In other words, it's part of a system.

Cybersecurity Anatomy vs. Physiology

- **Anatomical component**: Awareness training
  - Content: Passwords, phishing, clean desk, etc.
  - Periodicity: Annual

- **Purpose**: Informs personnel of expectations

- **Physiology**
  - Function: Reduces the frequency of variant (i.e., deficient) control conditions
  - Depends upon: Policies, risk appetite, risk measurement, etc…
  - Is depended upon by: Authentication, system security, access privileges, physical security, data protection, etc…
  - When deficient, may be partially compensated for by: DLP, password enforcement, Anti-malware, etc.

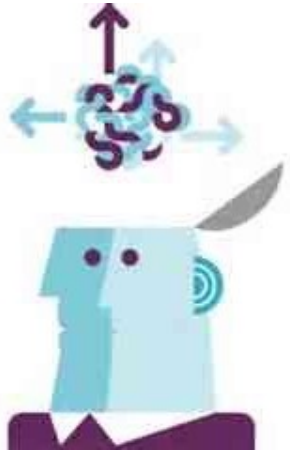
Example of cybersecurity “anatomy” (ISO27001)

A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users’ access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

But, how controls function, and function together, to reduce risk has been mostly undefined, leaving us to rely on…



Mental models

FAIR Controls Analytics Model (FAIR-CAM)

FAIR-CAM Objectives

- Describe controls physiology so that we can:
  - Bridge the gap between controls “anatomy” and risk
  - Properly account for individual control functionality as well as systemic functionality
  - Reliably forecast, measure, and validate control efficacy and value
  - Enable better use of security telemetry
  - Evaluate program maturity more effectively
- Become an industry standard
  - Anticipate that this will be covered under a creative commons Attribution-Non Commercial-No Derivative license, similar to how the Open Group and CIS protect their work
    - Licensing and exemption processes will be available

Setting expectations…

Modern medicine is complex because human physiology and pathology are complex.

If we want to effectively manage a problem space like cybersecurity, we have to account for its complex nature.

There is no easy button for cybersecurity.

Clarifying terms

Controls:

"Anything used to directly or indirectly affect the frequency or magnitude of loss."

Examples:

Policies
Passwords
Patching
Data backups
Auditing
etc…

Control Functions:

"How a control directly or indirectly affects the frequency or magnitude of loss."

Examples:

Loss Event Prevention
Loss Event Detection
Variance Prevention
Variance Correction
etc…

Current controls functions in the industry?

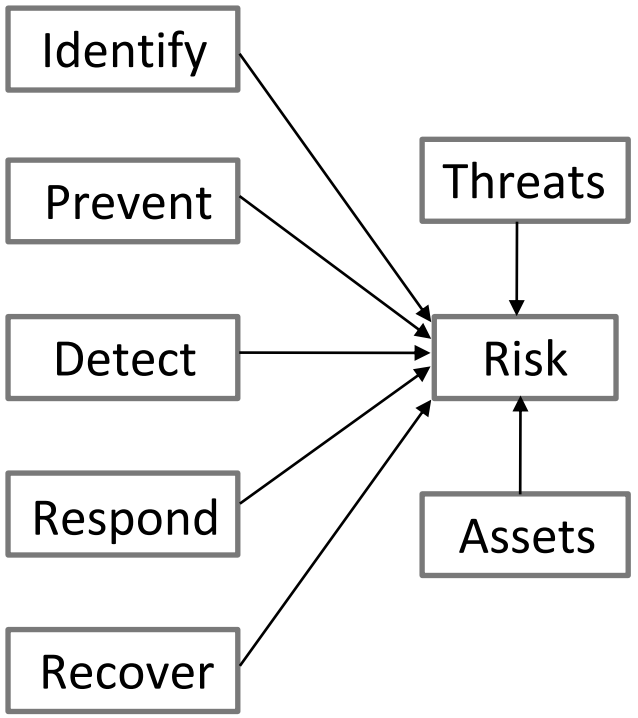
Problems include, but aren't limited to:

- Doesn't differentiate between functions that directly vs. indirectly affect risk (commonly inferred that all controls affect risk directly)
- Doesn't account for dependencies between controls
- Not granular enough to enable accurate or verifiable measurement of control efficacy or value

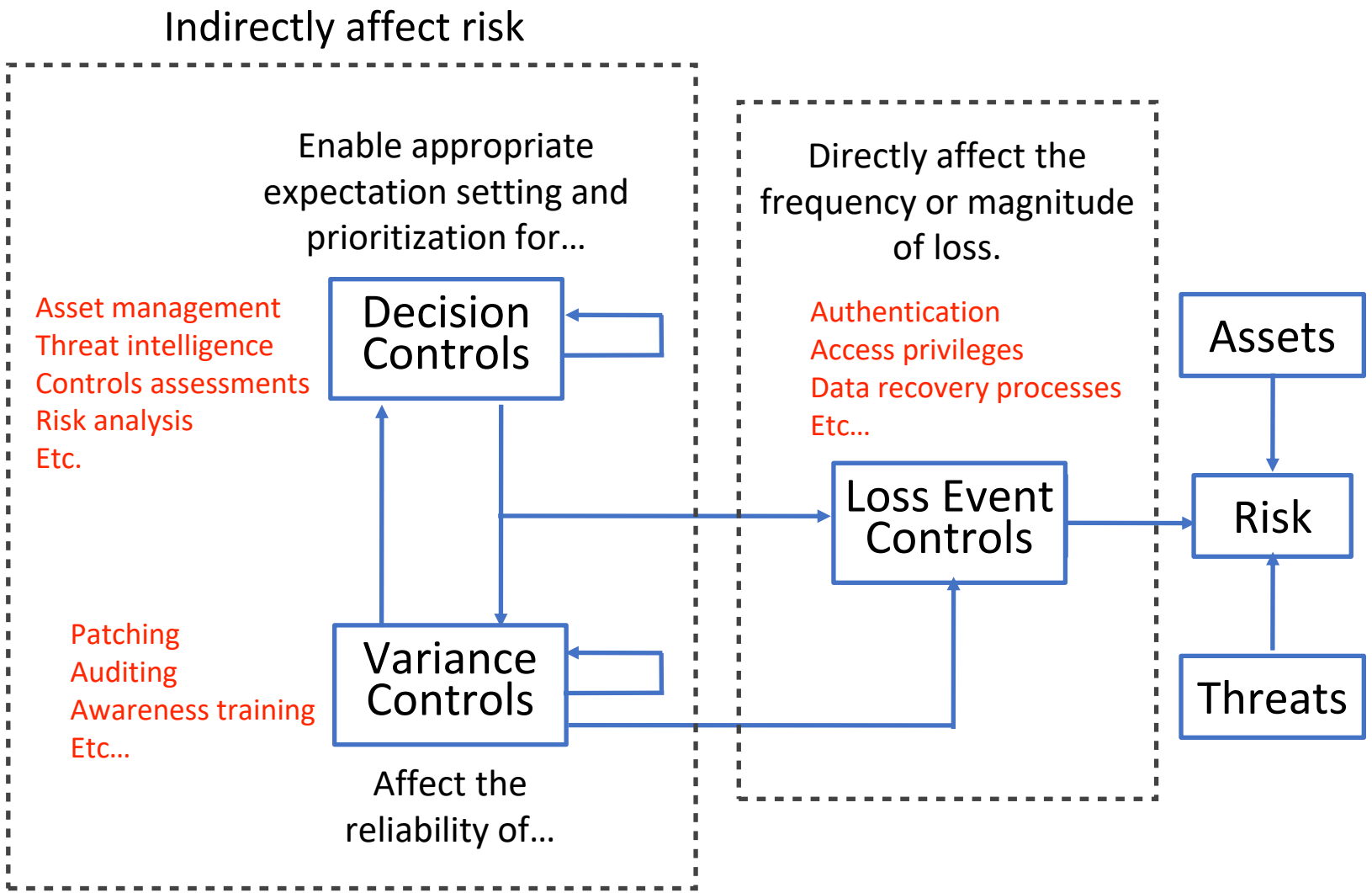
NOTES:

- NIST 800-53 mentions that controls are "related", but does not define the nature of the relationships.
- "Threat Kill Chain" analysis is somewhat similar in principle, but has a very narrow scope, focuses only on a subset of controls, and doesn't account for control relationships.

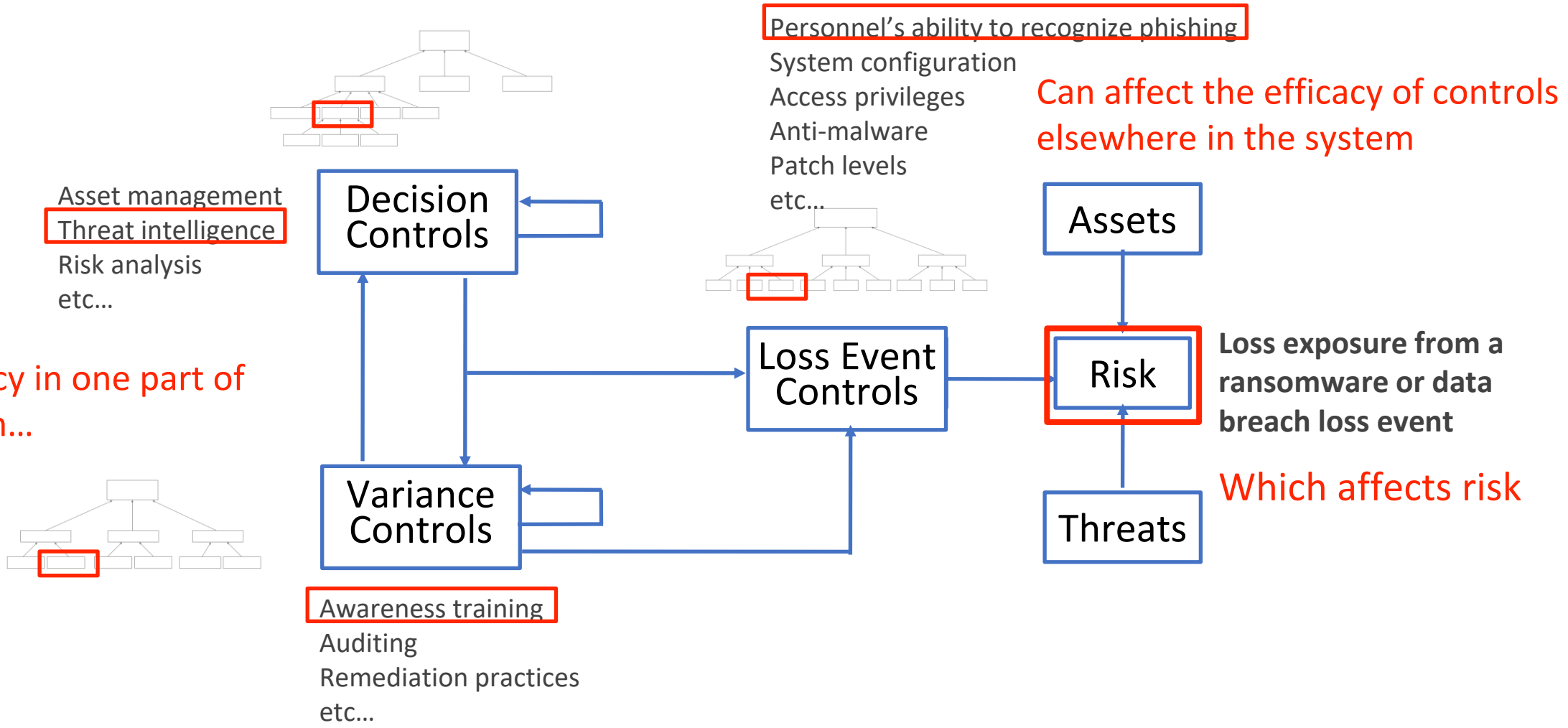
Control Functions
(NIST CSF)



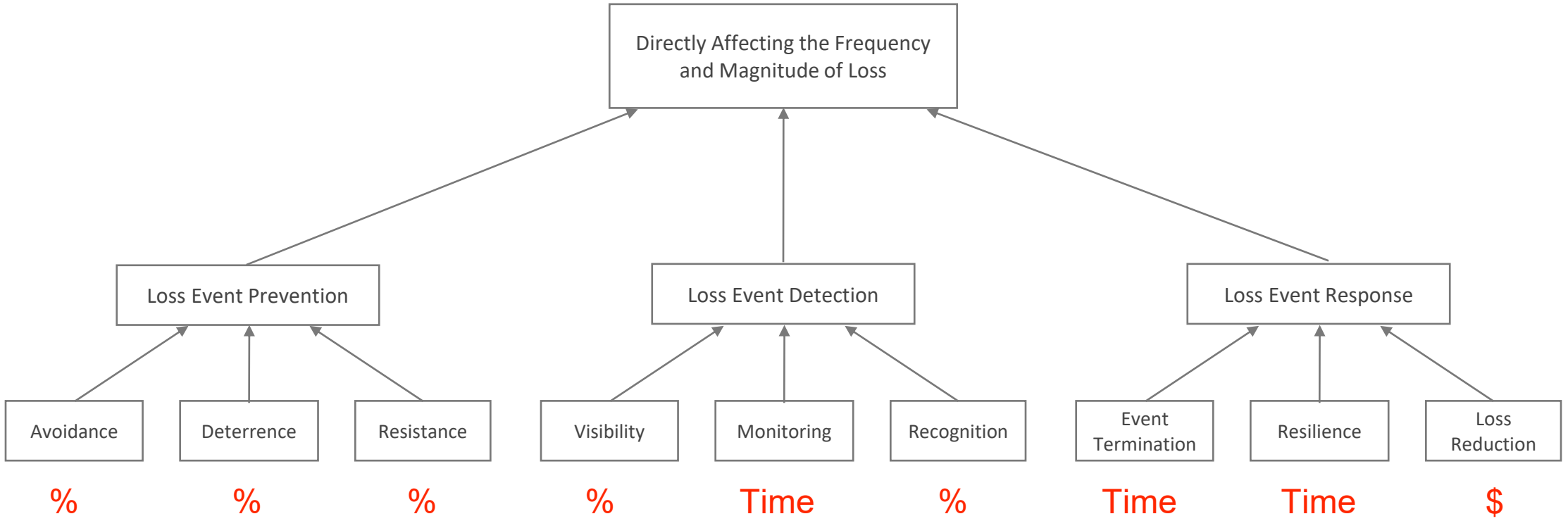
Control Functional Domain Relationships



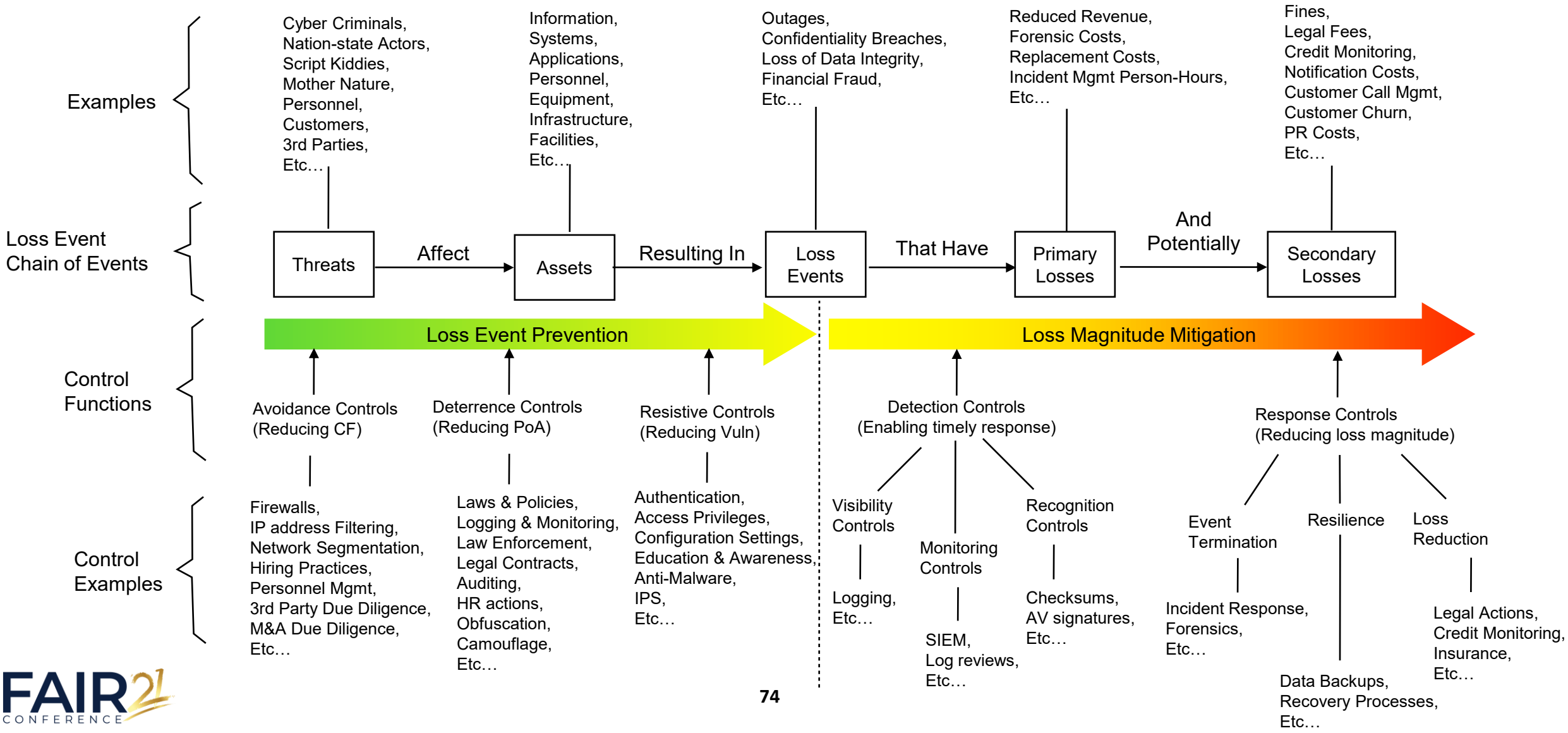
Control Functional Domain Relationships



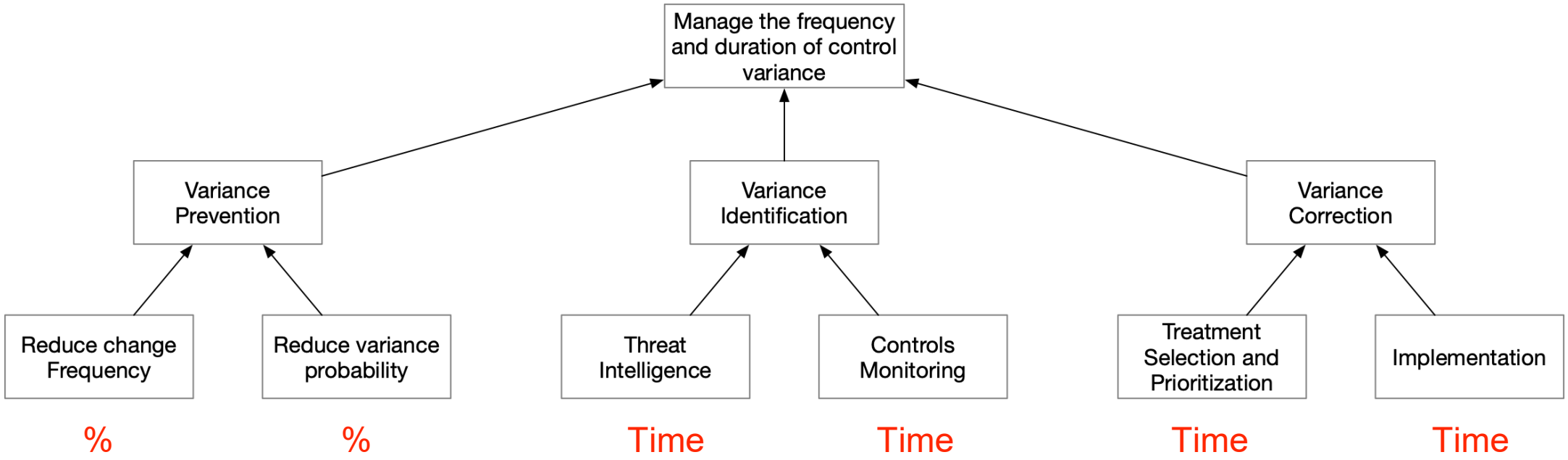
Loss Event Control Functions



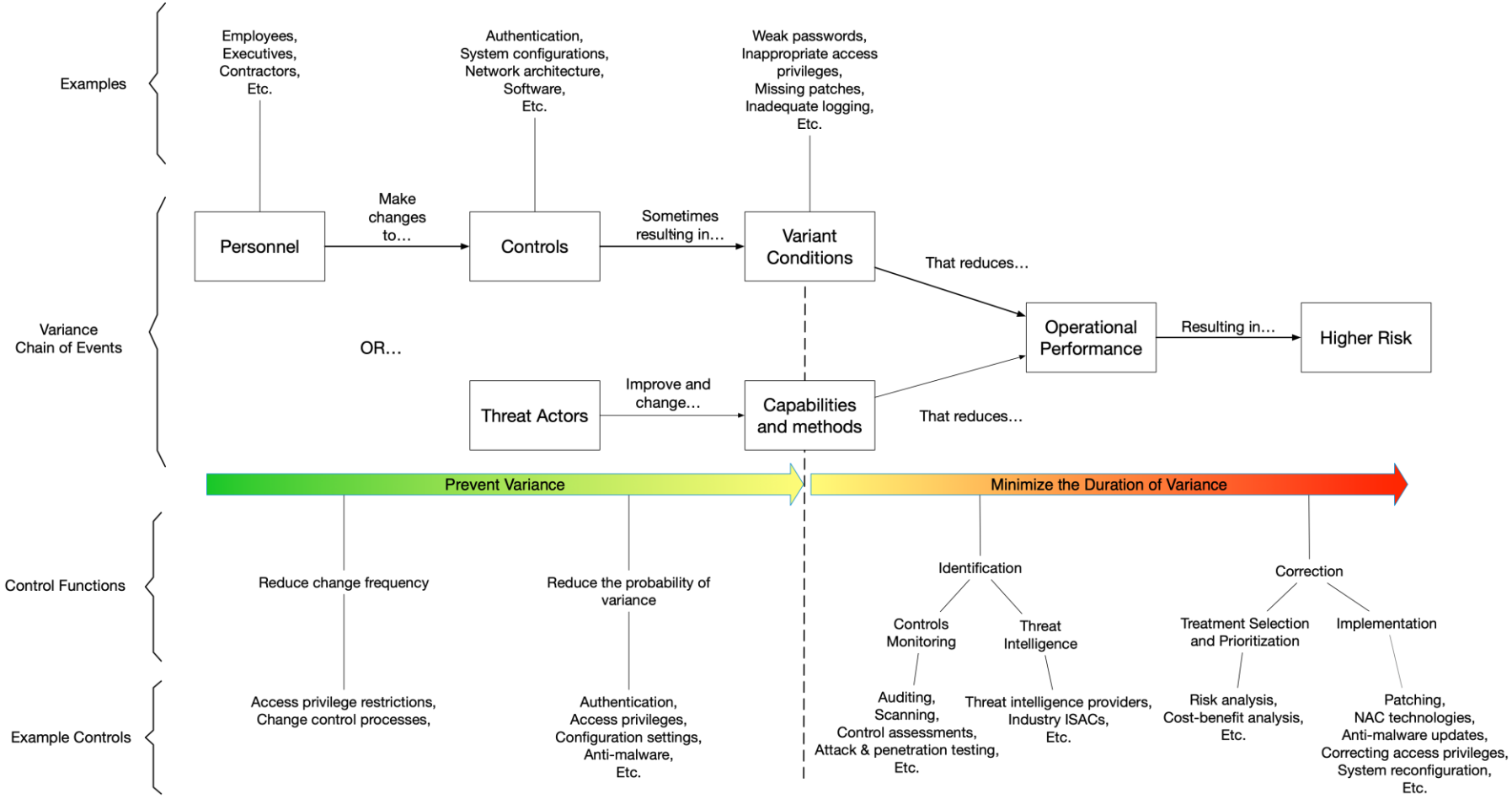
Loss Event Controls applied to risk



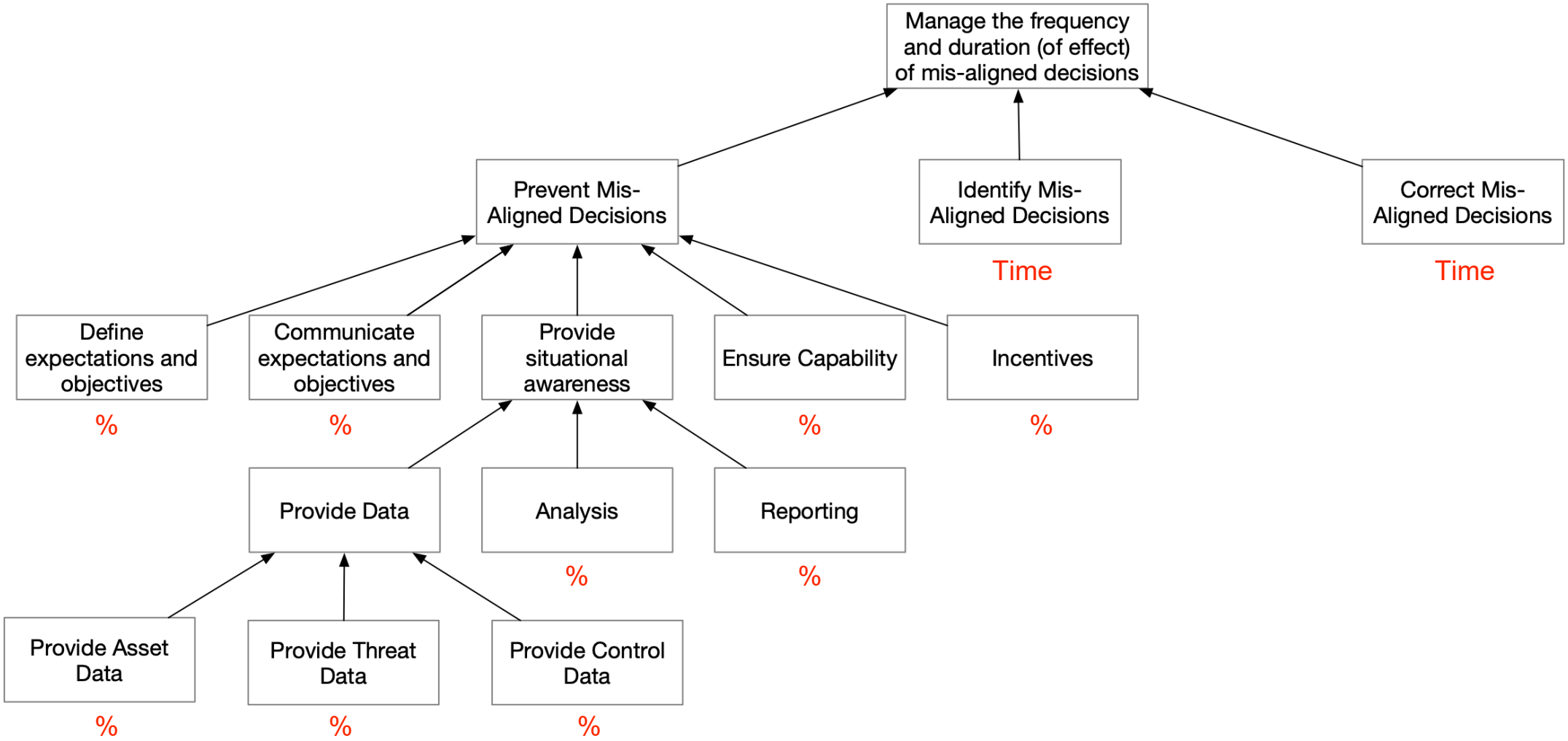
Variance Management Control (VMC) Functions



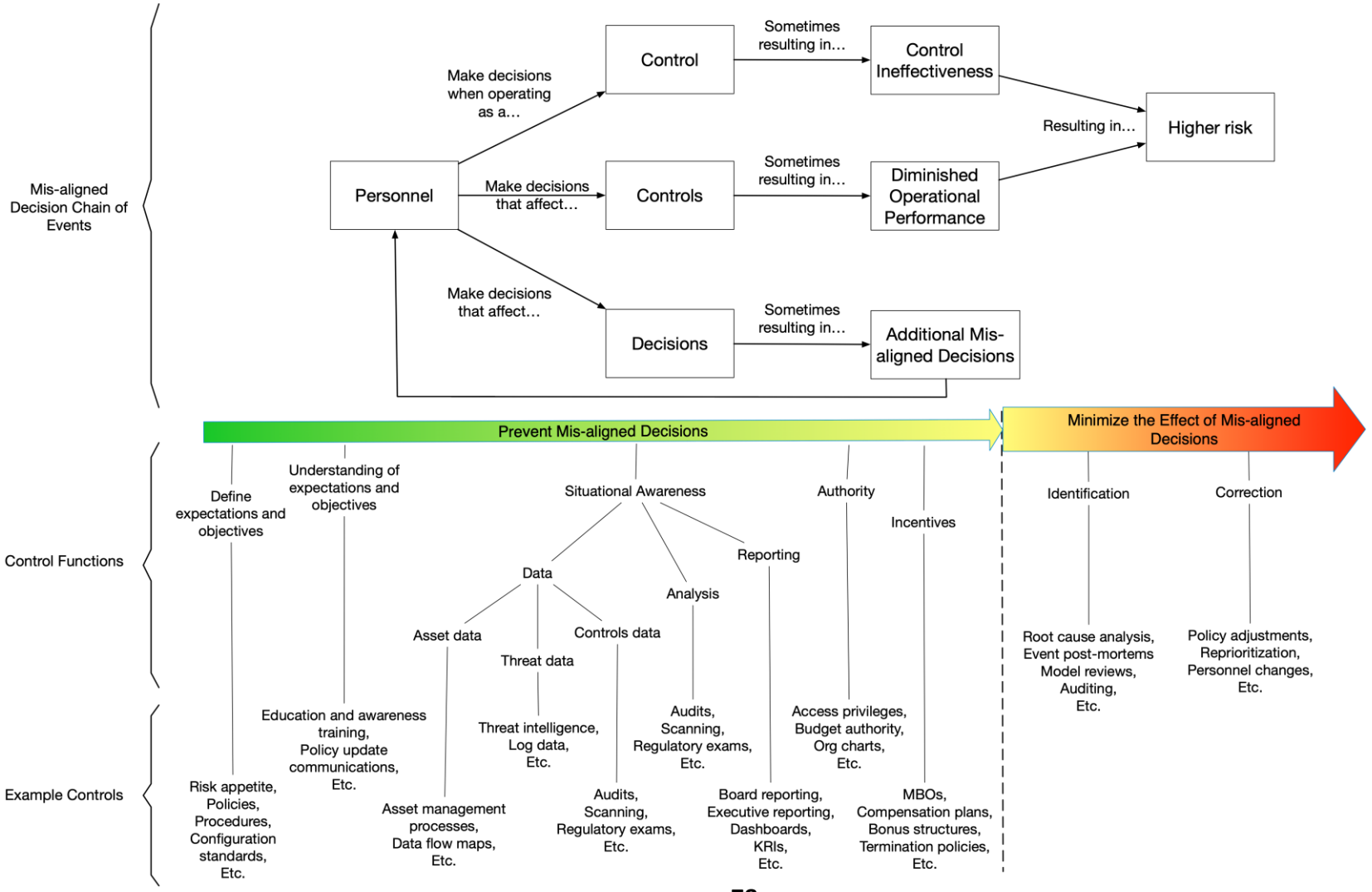
Variance Management Controls affect on risk



Decision Support Control (DSC) Functions



Decision Support Controls affect on risk



Combining controls “anatomy” with “physiology”

The objectives...

- Clarify how framework elements affect risk
- Make it easier to apply control frameworks within risk analysis
- Enable more reliable prioritization of control gaps
- Enable the refinement of control frameworks

Current mapping efforts…

- ISO27k
- CIS v8.0
- NIST 800-53
- HITRUST

Future mapping efforts…

- Mitre Att&ck
- COBIT
- PCI-DSS
- Others as requested

Wrapping up...

Summary

- Current control frameworks provide a view of control “anatomy” but rely on practitioner mental models to deal with “physiology”.
- As a result, we are unable to reliably measure or prioritize our control efforts.
- FAIR-CAM provides a “controls physiology” view, which complements existing frameworks and fills a critical gap in our ability to manage risk effectively.
- When FAIR-CAM is combined with FAIR, we can measure control value in real terms and reliably prioritize where and how we apply our resources.

"In the 19th century we had a relatively advanced understanding of anatomy, but we had a terrible understanding of physiology.

We knew what was happening, but we didn't know why it was happening."

A retired surgeon

Resources

- Documents
  - Introduction to the FAIR Controls Analytics Model
  - Description of the FAIR Controls Analytics Model Standard [DRAFT]
  - Applying the FAIR Controls Analytics Model Coming soon…
  - CIS 8.0 to FAIR-CAM Mapping
  - Various other mapping documents… Coming soon…
- Training & Certification
  - Basic FAIR-CAM Under development…
  - Advanced FAIR-CAM Under development…
- Software
  - FAIR-CAM enabled prototype in development

Questions?

MAPPING ISO/IEC 27001 TO FAIR CAM

Recipe

Ingredients:

- FAIR CAM
- ISO/IEC 27001:2013 controls
- Context / Scenario

Directives:

- Build a big spreadsheet
- Interpret controls and FAIR CAM definitions
- Bring your own expertise
- Review, review, review

????

THE FAIR CONTROLS ANALYTICS MODEL (FAIR-CAM) STANDARD

"How much risk a control reduces."

- FAIR definition for risk — "The probable frequency and probable magnitude of future loss"
- Controls provide value by reducing either the frequency or magnitude of loss events.

- The FAIR Controls Analytics Model (FAIR-CAM) provides a rigorous description of how the risk management controls landscape works. It achieves this by describing the controls landscape as a **complex set of interdependent functions** that act as a **system** in the management of risk.

"How much risk a ISO/IEC 27001 control reduces."

Credits:
"Control model introduction v1.1" by FAIR Institute
"Description of FAIR CAM standard v1" by FAIR Institute
"ISO/IEC 27001:2013" by International Standard Organization
"ISO/IEC 27002:2013" by International Standard Organization

THE FAIR CONTROLS ANALYTICS MODEL (FAIR-CAM) STANDARD

Some definitions

Control
"Anything that can be used to reduce the frequency or magnitude of loss."

Laws, regulations, policies, standards, processes, technologies, people, software, physical structures, etc.

Control functions
"How a control directly or indirectly affects the frequency or magnitude of loss."

Limiting, making, providing, restoring , reducing, detecting, etc.

Functional domains
"High-level categories of control functions"

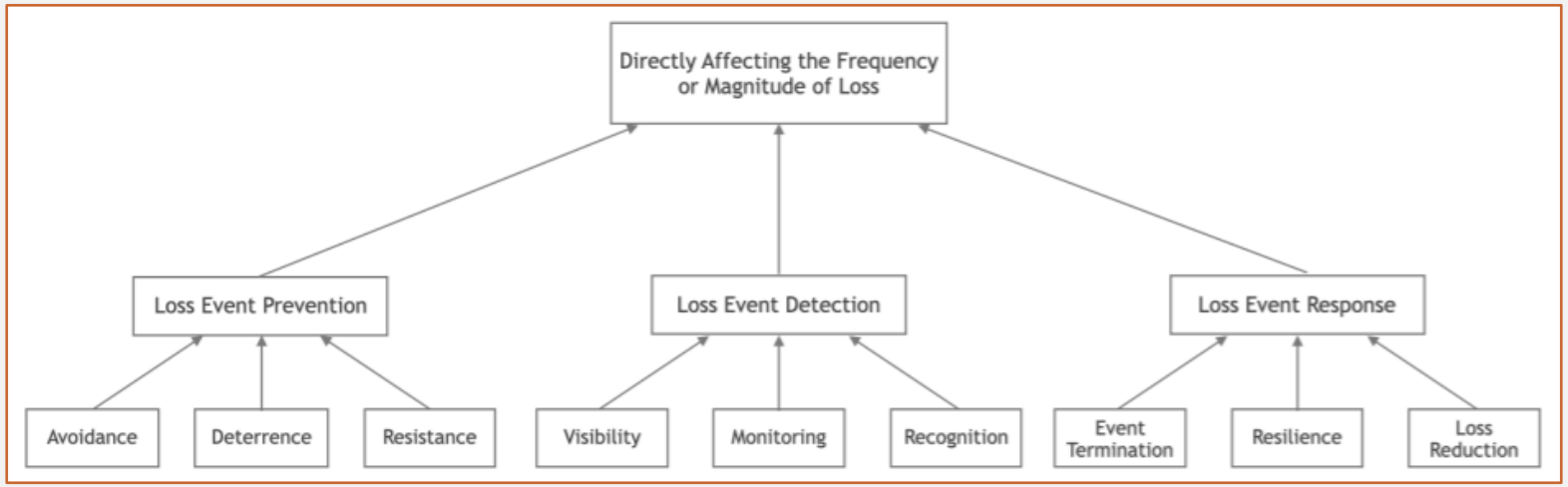
Categories to distinguish between control functions that affect risk directly (Loss Event Controls), versus those that affect the operational performance of controls (Variance Management Controls), versus those that affect decision-making (Decision Support Controls).

Function relationships
"How control functions relate to each others"

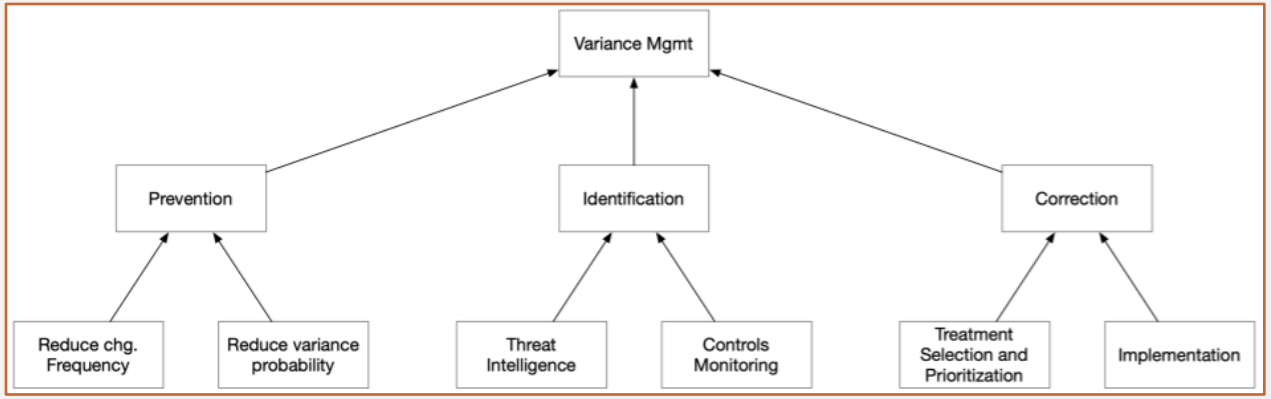
Boolean operators: AND, OR.

A simple example for OR relationships is the loss event prevention. If you can a) prevent contact with a threat agent, or b) deter action on the part of the threat agent, or c) successfully resist the actions of a threat agent, then a loss event will not occur.

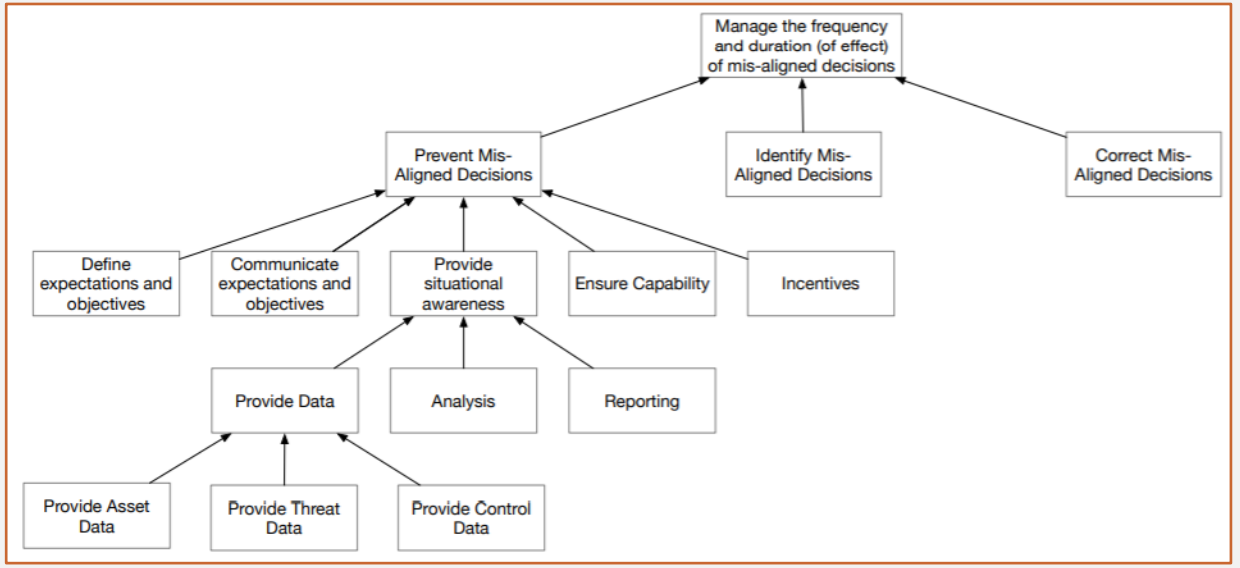
Loss Event Controls



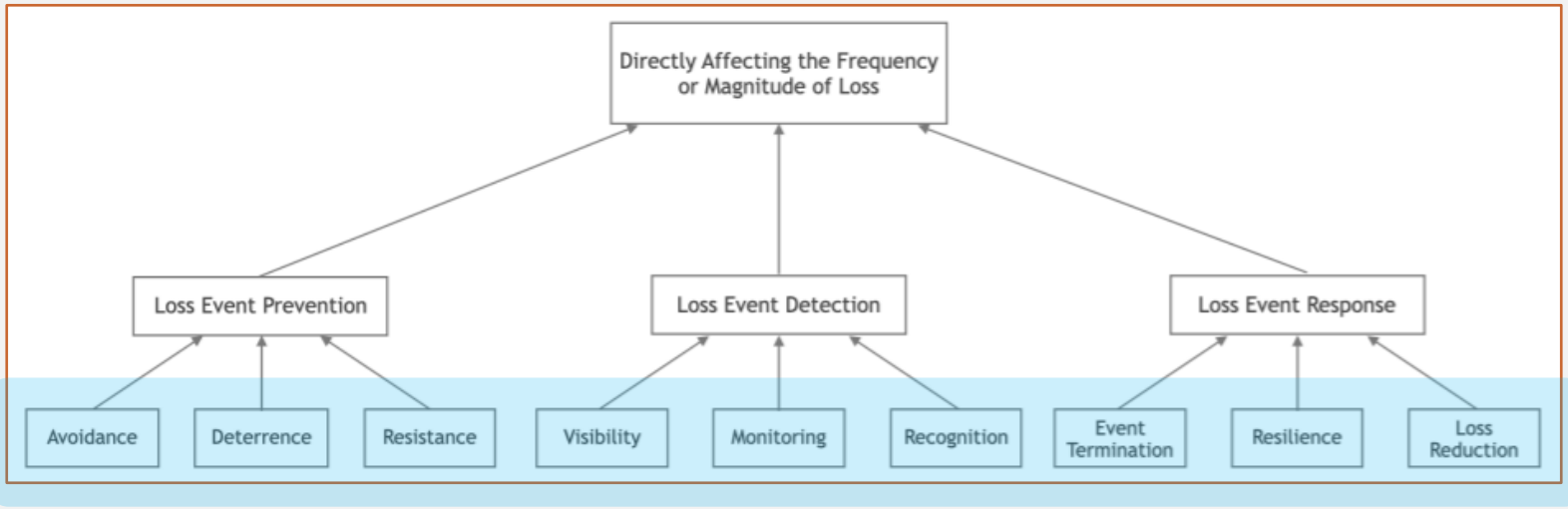
Variance Management Controls



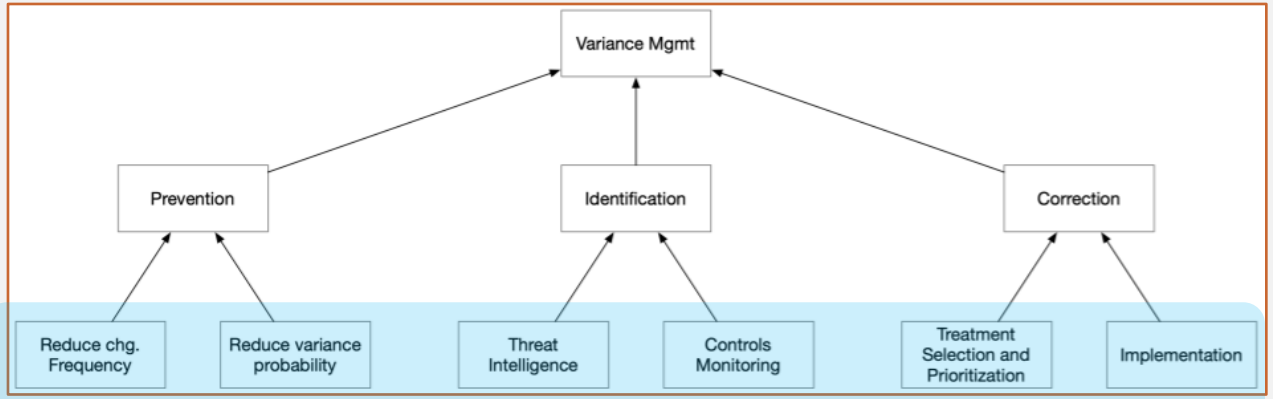
Decision Support Controls



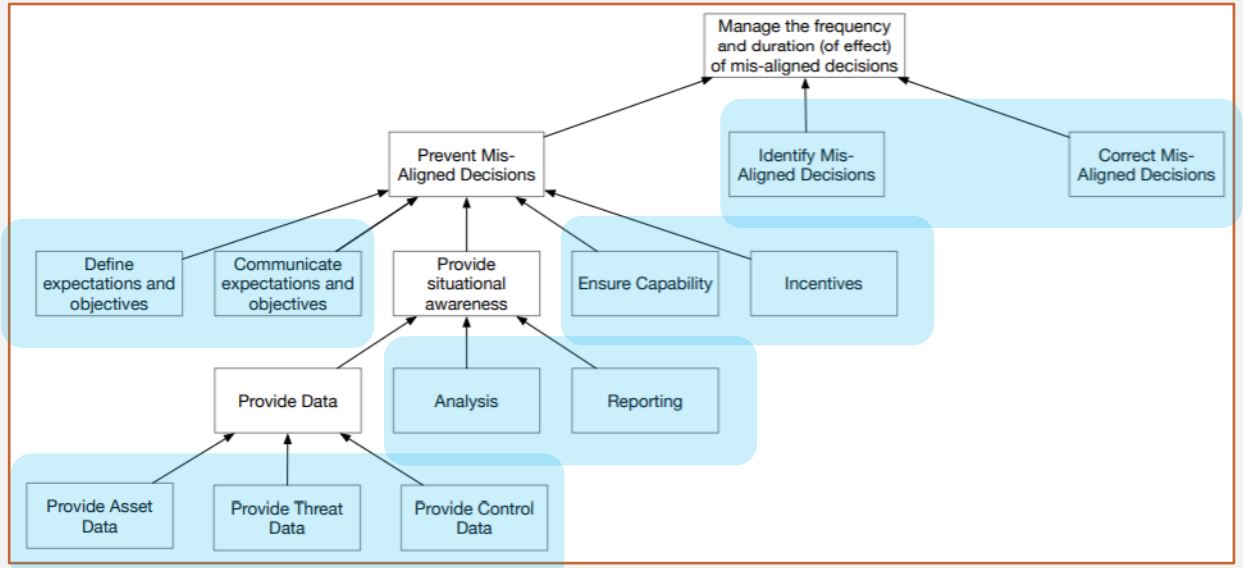
Loss Event Controls

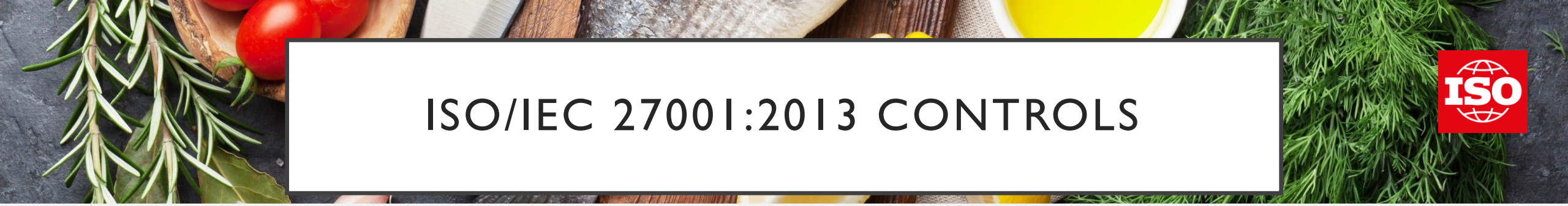


Variance Management Controls



Decision Support Controls





ISO/IEC 27001:2013 CONTROLS

- ISO/IEC 27001 controls listed in Annex A (Reference control objectives) and detailed in ISO/IEC 27002 (Code of practice for information security controls)

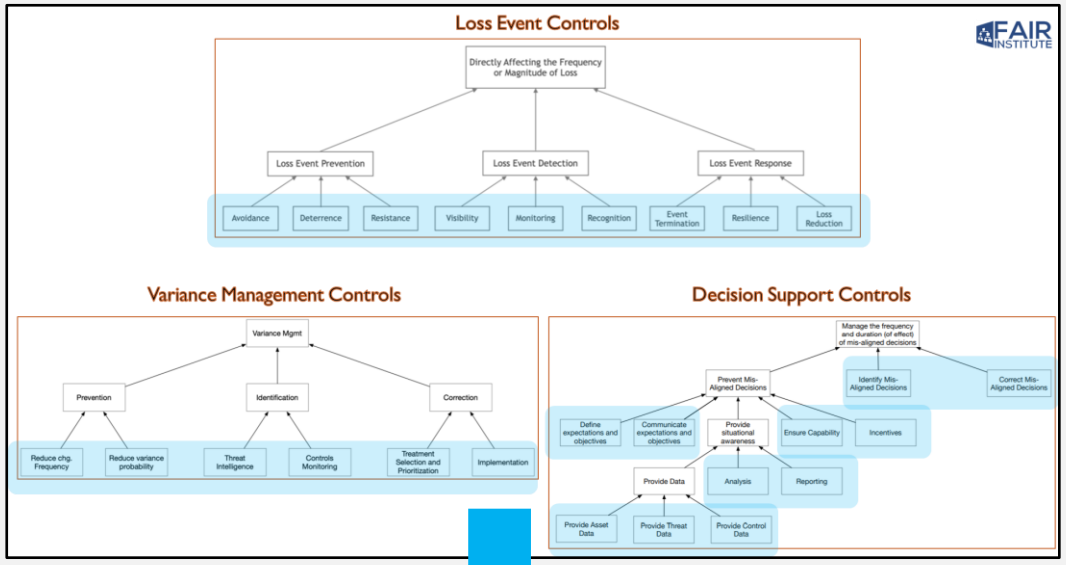
- Total of 114 controls in the following domains:
  - Information security policies
  - Organization of information security
  - Human resources security
  - Asset management
  - Access control
  - Cryptography
  - Physical and environmental security
  - Operations security
  - Communications security
  - System acquisition, development and maintenance
  - Supplier relationships
  - Information security incident management
  - Information security aspects of business continuity management
  - Compliance

ISO/IEC 27001:2013 CONTROLS

- ISO/IEC 27001 controls listed in Annex A (Reference control objectives) and detailed in ISO/IEC 27002 (Code of practice for information security controls)

- Total of 114 controls in the following domains:
  - Information security policies
  - Organization of information security
  - Human resources security
  - Asset management
  - Access control
  - Cryptography
  - Physical and environmental security
  - Operations security
  - Communications security
  - System acquisition, development and maintenance
  - Supplier relationships
  - Information security incident management
  - Information security aspects of business continuity management
  - Compliance

9.0	**Access Control**
9.1	**Business requirements of access control**
9.1.1	Access control policy
9.1.2	Access to networks and network services
9.2	**User access management**
9.2.1	User registration and de-registration
9.2.2	User access provisioning
9.2.3	Management of privileged access rights
9.2.4	Management of secret authentication information of
9.2.5	Review of user access rights
9.2.6	Removal or adjustment of access rights
9.3	**User responsibilities**
9.3.1	Use of secret authentication information
9.4	**System and application access control**
9.4.1	Information access restriction
9.4.2	Secure log-on procedures
9.4.3	Password management system
9.4.4	Use of privileged utility programs
9.4.5	Access control to program source code
10	**Cryptography**
10.1	**Cryptographic controls**
10.1.1	Policy on the use of cryptographic controls

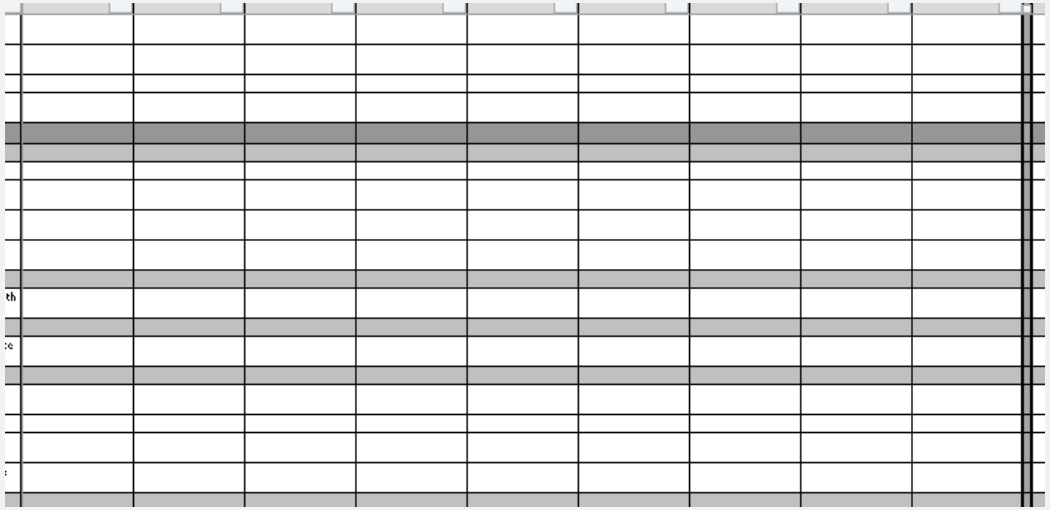


FAIR CAM CONTROL FUNCTIONS

ISO/IEC 27001:2013 CONTROLS

- ISO/IEC 27001 controls listed in Annex A (Reference control objectives) and detailed in ISO/IEC 27002 (Code of practice for information security controls)
- Total of 114 controls in the following domains:
  1. Information security policies
  2. Organization of information security
  3. Human resources security
  4. Asset management
  5. Access control
  6. Cryptography
  7. Physical and environmental security
  8. Operations security
  9. Communications security
  10. System acquisition, development and maintenance
  11. Supplier relationships
  12. Information security incident management
  13. Information security aspects of business continuity management
  14. Compliance

ISO 27001 CONTROLS

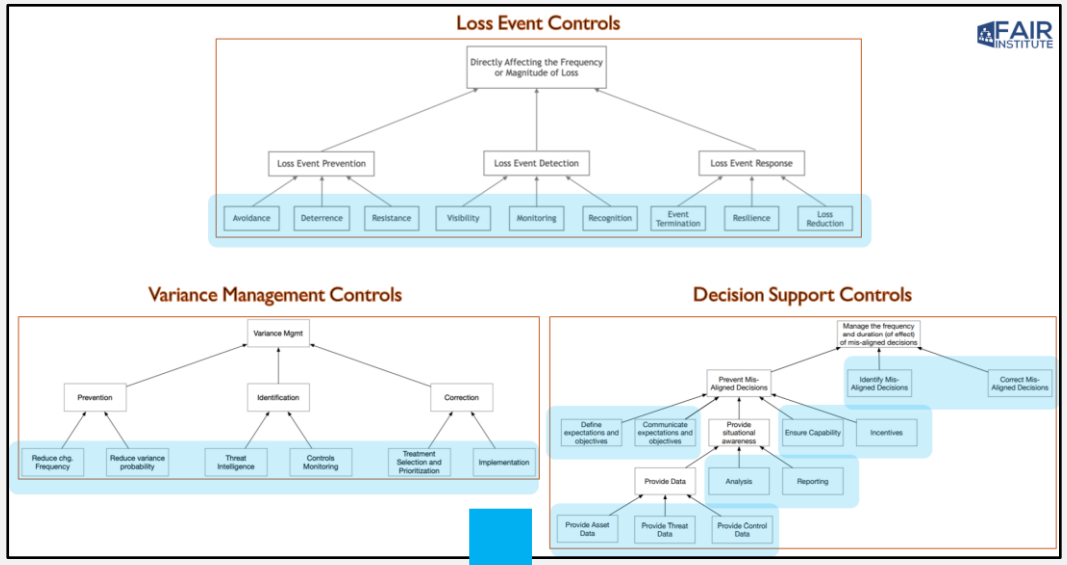


How?

- Direct mapping
- Indirect mapping

Why?

- Cross-check experiences, common understanding, cross-validation



FAIR CAM CONTROL FUNCTIONS

ISO/IEC 27001:2013 CONTROLS

- ISO/IEC 27001 controls listed in Annex A (Reference control objectives) and detailed in ISO/IEC 27002 (Code of practice for information security controls)
- Total of 114 controls in the following domains:
  1. Information security policies
  2. Organization of information security
  3. Human resources security
  4. Asset management
  5. Access control
  6. Cryptography
  7. Physical and environmental security
  8. Operations security
  9. Communications security
  10. System acquisition, development and maintenance
  11. Supplier relationships
  12. Information security incident management
  13. Information security aspects of business continuity management
  14. Compliance

ISO 27001 CONTROLS

X								
X						X		
X	X					X		
X	X					X		
		X					X	
	X	X						
	X	X	X	X	X	X	X	
							X	X
			X	X	X			
		X						
		X	X	X				
X								

MAPPING EXAMPLE #1

Control 5.1.1 - Policies for information security

- A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

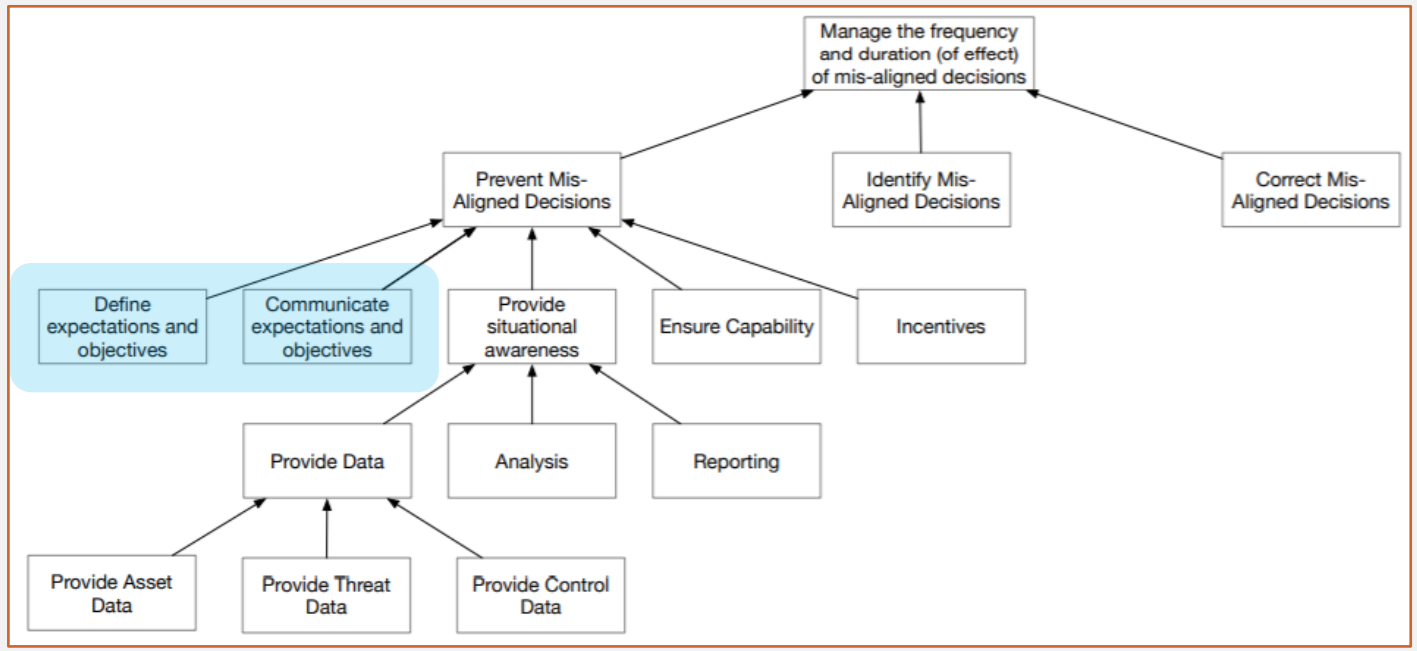
c) processes for handling deviations and exceptions.

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme.

MAPPING EXAMPLE #1

Control 5.1.1 - Policies for information security

Decision Support Controls



Define Expectations and Objectives

Clearly define expectations and/or objectives

Communicate expectations and objectives

Ensure that responsible persons are aware of and understand the organization's risk management objectives and priorities.

MAPPING EXAMPLE #1

Control 5.1.1 - Policies for information security

PROGR.	Ref #	Control Framework Elements	Decision Support Contro					
			Prevention					
			Define Exp's & Obj's	Communicate Exp's & Obj's	Ensure Situational Awareness			
					Data			Analysis
					Asset	Threat	Controls	
	5	Information security policies						
	5.1	Management direction for information security						
1	5.1.1	Policies for information security	X	X				

MAPPING EXAMPLE #2

Control 7.2.2 - Information security awareness, education and training

- All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information.

The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

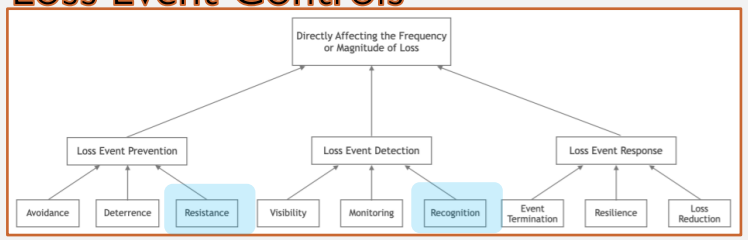
The awareness programme should be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly so it stays in line with organizational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others. ***[etc.]***

MAPPING EXAMPLE #2

Control 7.2.2 - Information security awareness, education and training

Loss Event Controls



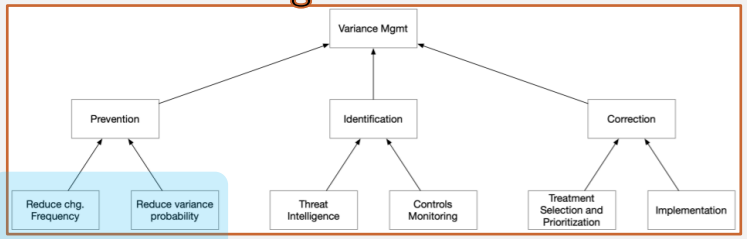
Resistance

Reduce the likelihood that a threat agent's act will result in a loss event.

Recognition

Enable differentiation of normal activity from abnormal activity.

Variance Management Controls



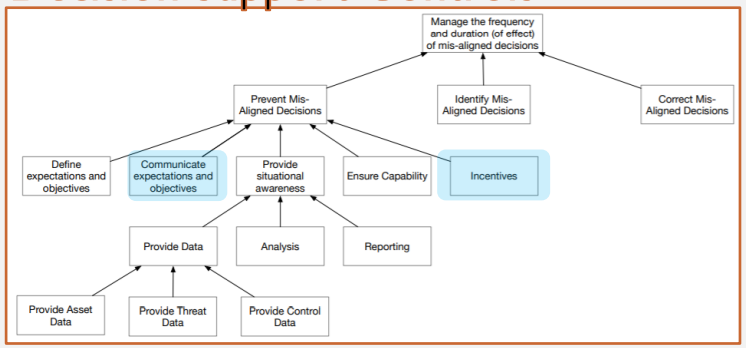
Reduce change frequency

Reduce the frequency of changes that might introduce variant control conditions.

Reduce variance probability

Enable the recognition of changes in the threat landscape that have resulted in loss event controls no longer being as effective as intended.

Decision Support Controls



Communicate expectations and objectives

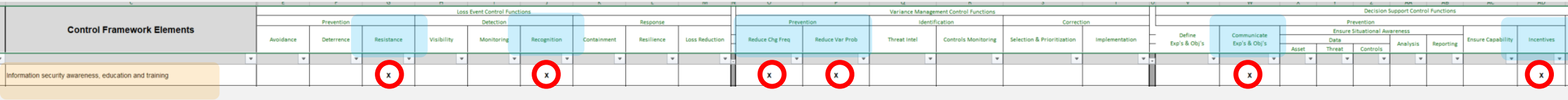
Ensure that responsible persons are aware of and understand the organization's risk management objectives and priorities.

Incentives

Ensure that personnel are motivated on a personal level to make decisions that are aligned with the organization's expectations and objectives.

MAPPING EXAMPLE #2

Control 7.2.2 - Information security awareness, education and training



Control Framework Elements	Loss Event Control Functions									Variance Management Control Functions							Decision Support Control Functions										
	Prevention			Detection			Response			Prevention		Identification		Correction			Prevention										
	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Containment	Resilience	Loss Reduction	Reduce Chg Freq	Reduce Var Prob	Threat Intel	Controls Monitoring	Selection & Prioritization	Implementation		Define Exp's & Obj's	Communicate Exp's & Obj's	Ensure Situational Awareness								
																			Data								
																			Asset	Threat	Controls	Analysis	Reporting	Ensure Capability	Incentives		
Information security awareness, education and training			x			x				x	x							x							x		

MAPPING EXAMPLE #2

Control 7.2.2 - Information security awareness, education and training

Control Framework Elements	Loss Event Control Functions									Variance Management Control Functions							Decision Support Control Functions									
	Prevention			Detection			Response			Prevention		Identification		Correction					Prevention							
	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Containment	Resilience	Loss Reduction	Reduce Chg Freq	Reduce Var Prob	Threat Intel	Controls Monitoring	Selection & Prioritization	Implementation	Define Exp's & Obj's	Communicate Exp's & Obj's	Ensure Situational Awareness			Analysis	Reporting	Ensure Capability	Incentives		
																		Data								
																		Asset	Threat	Controls						
Information security awareness, education and training			x			x				x	x						x							x		

Some observations

- The mapping is one-to-many
- The mapping is subject to the interpretation of the ISO/IEC 27001 control (it tells what but not how!)
- The mapping is subject to the interpretation of the FAIR CAM control functions' definitions
- Personal experience and expertise may influence the mapping

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking

- A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;

d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;

e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

f) the use of home networks and requirements or restrictions on the configuration of wireless network services;

g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

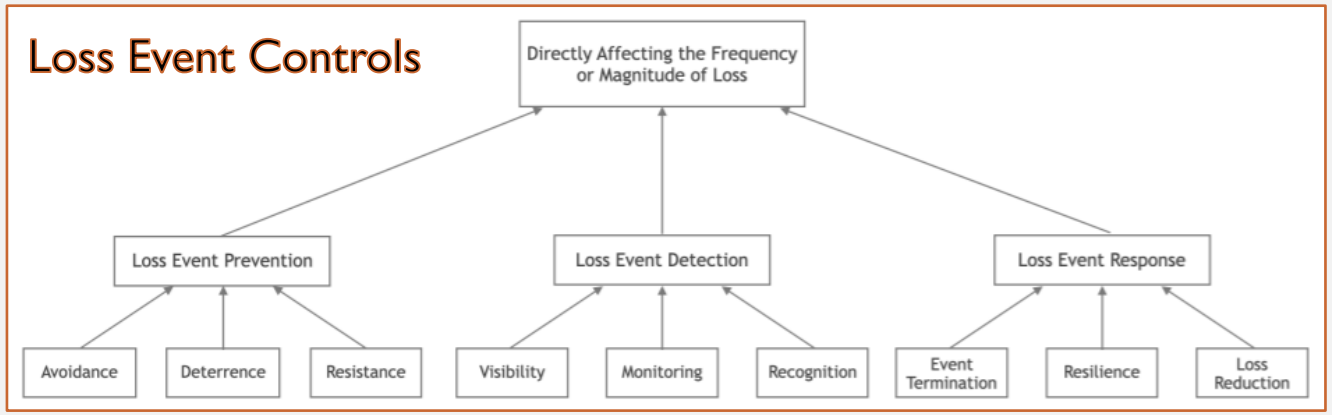
h) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;

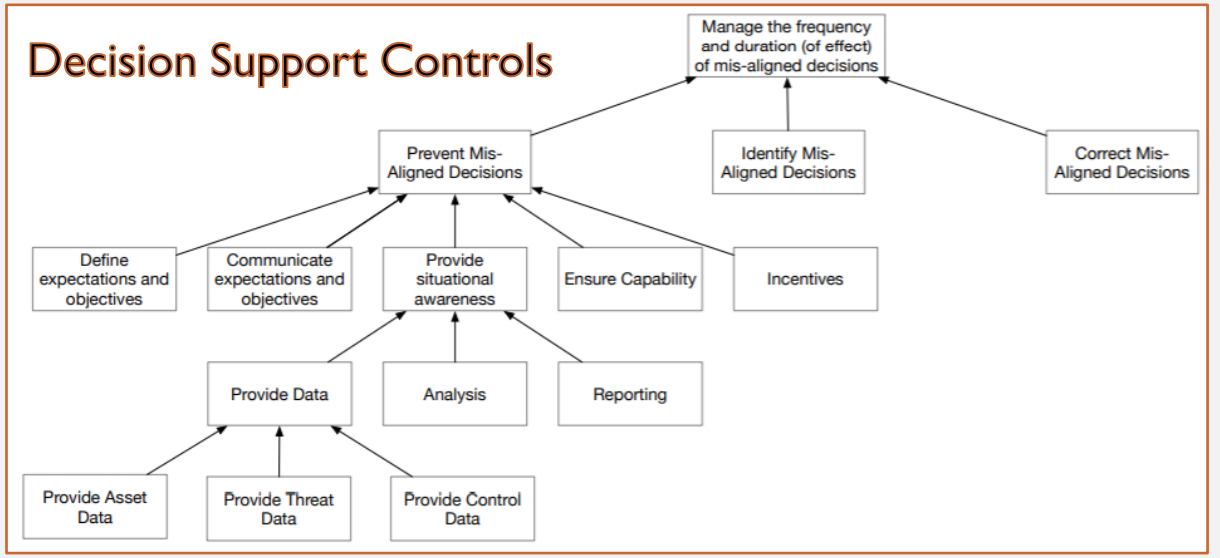
i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;

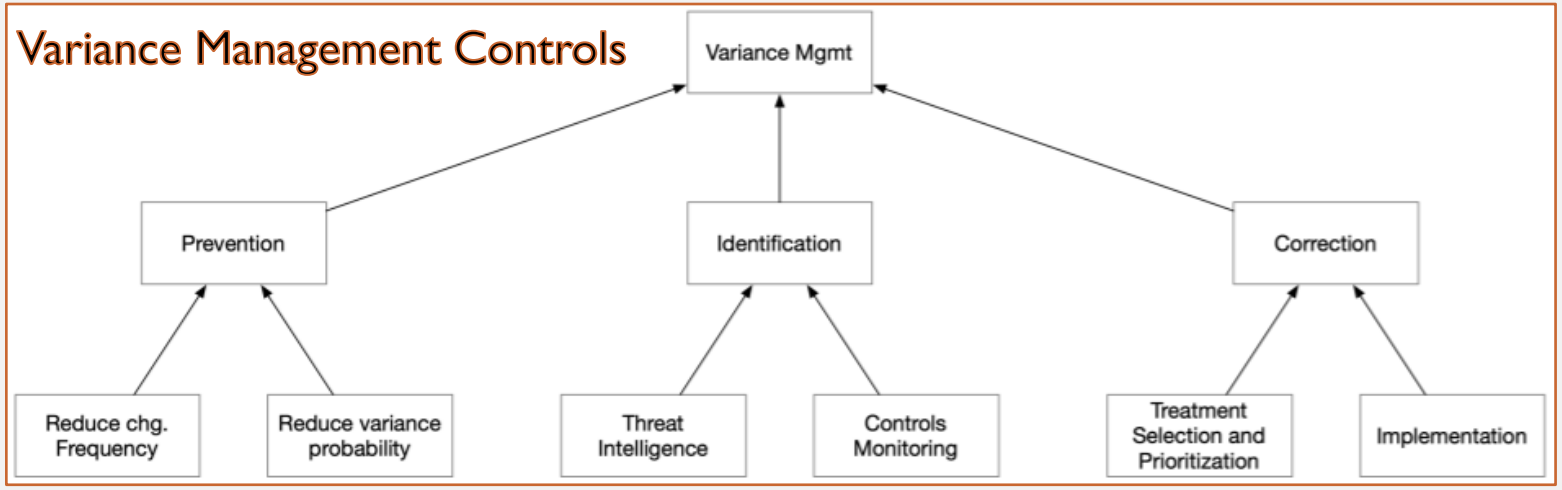
j) malware protection and firewall requirements. ***[etc.]***

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking



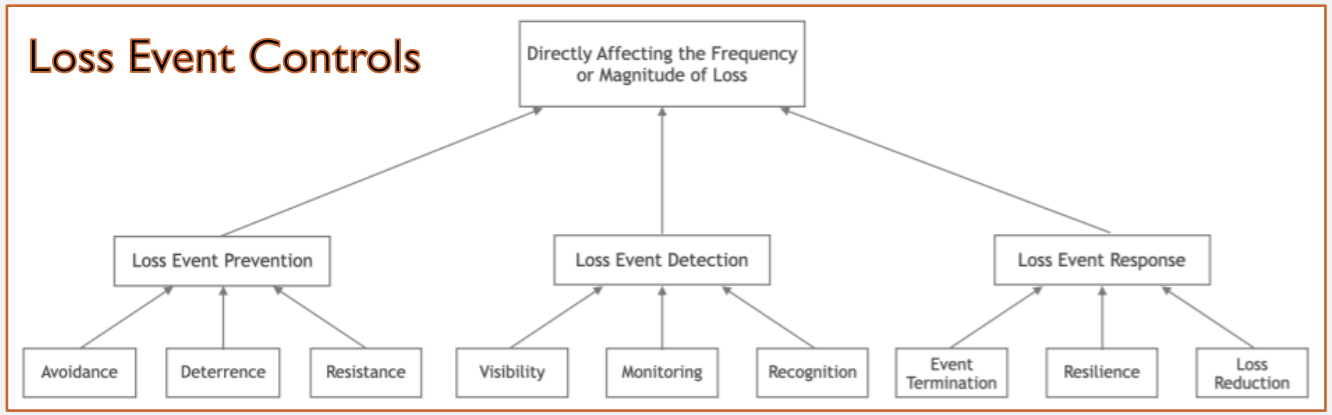


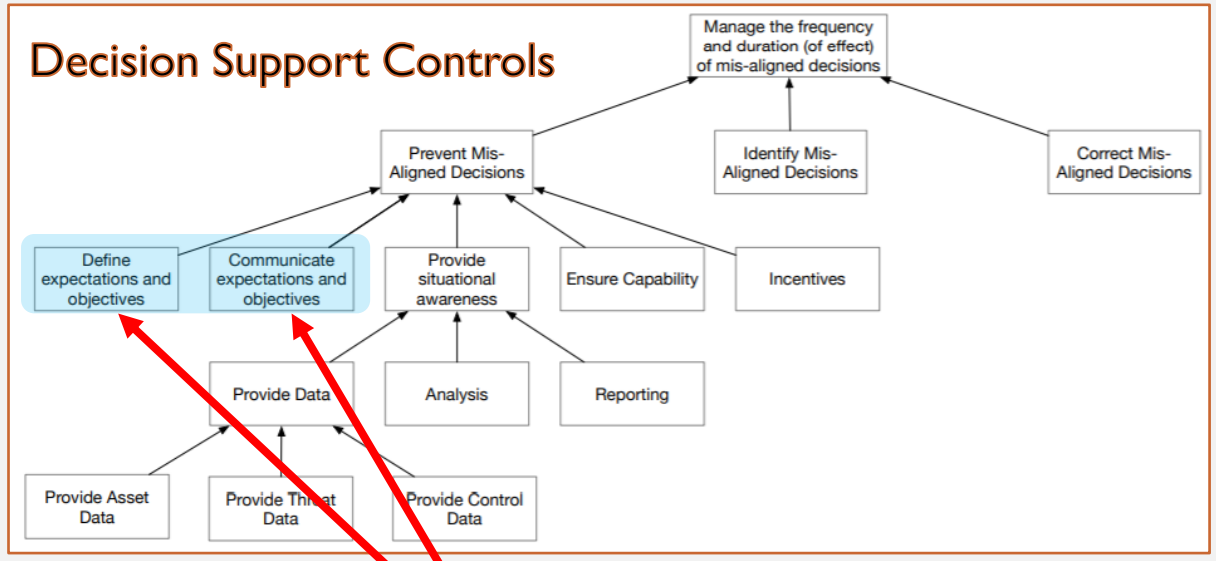


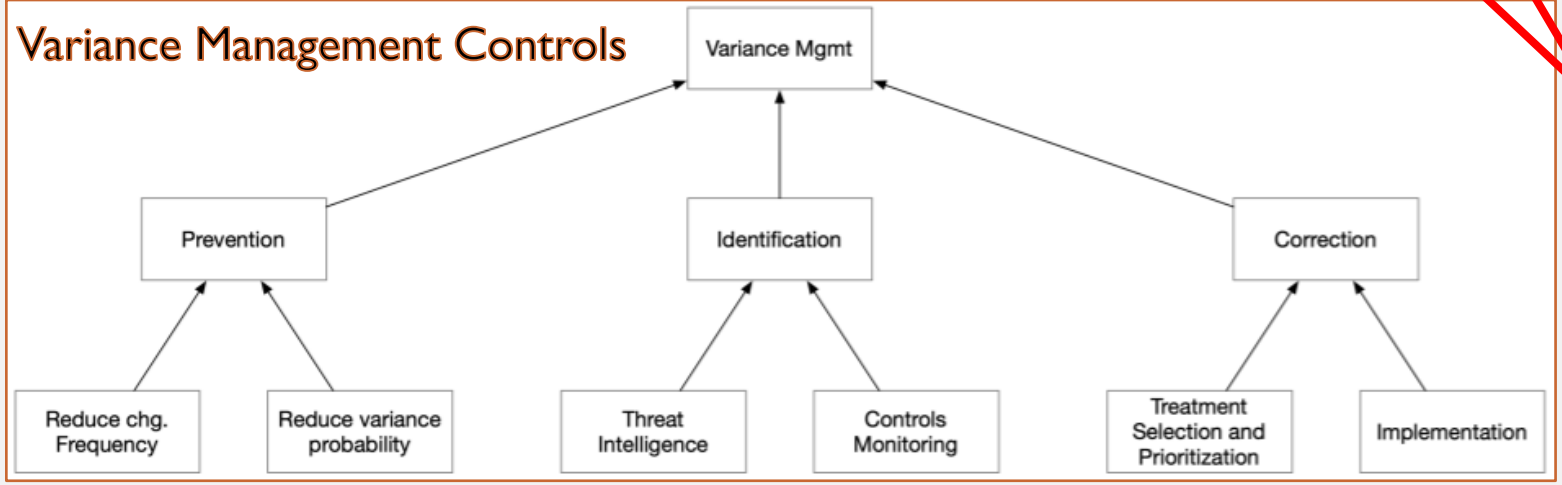
What to map?

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking



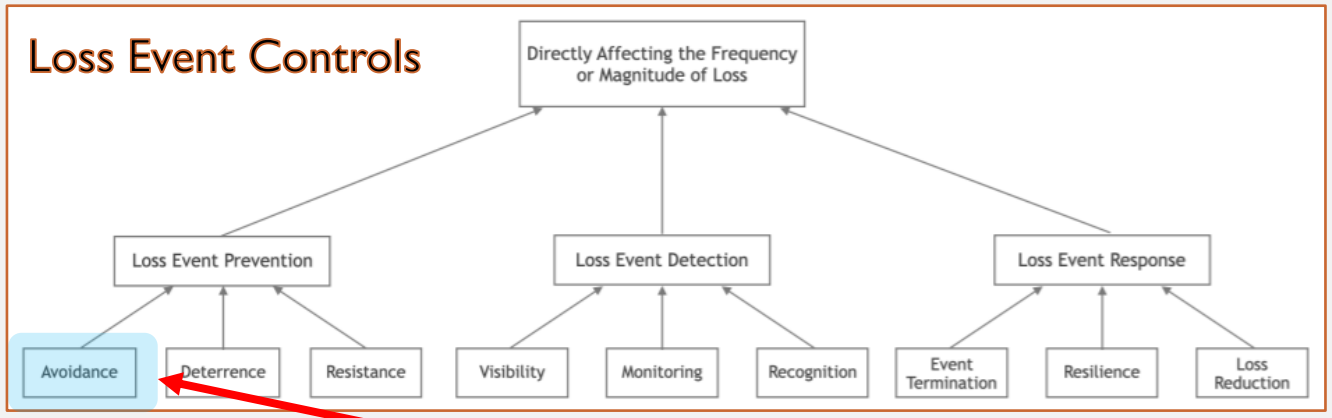


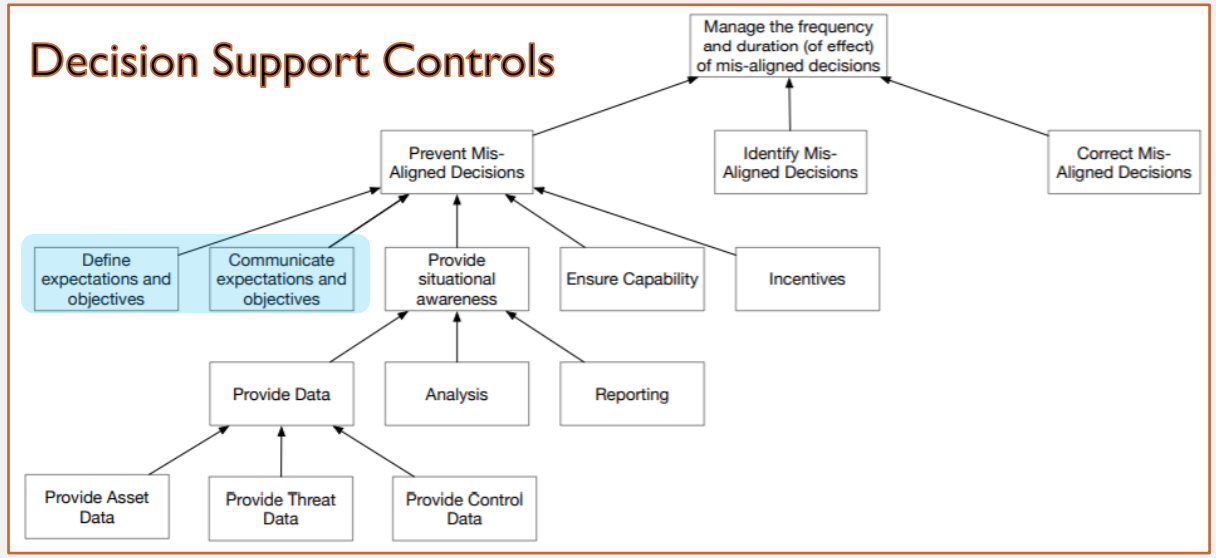


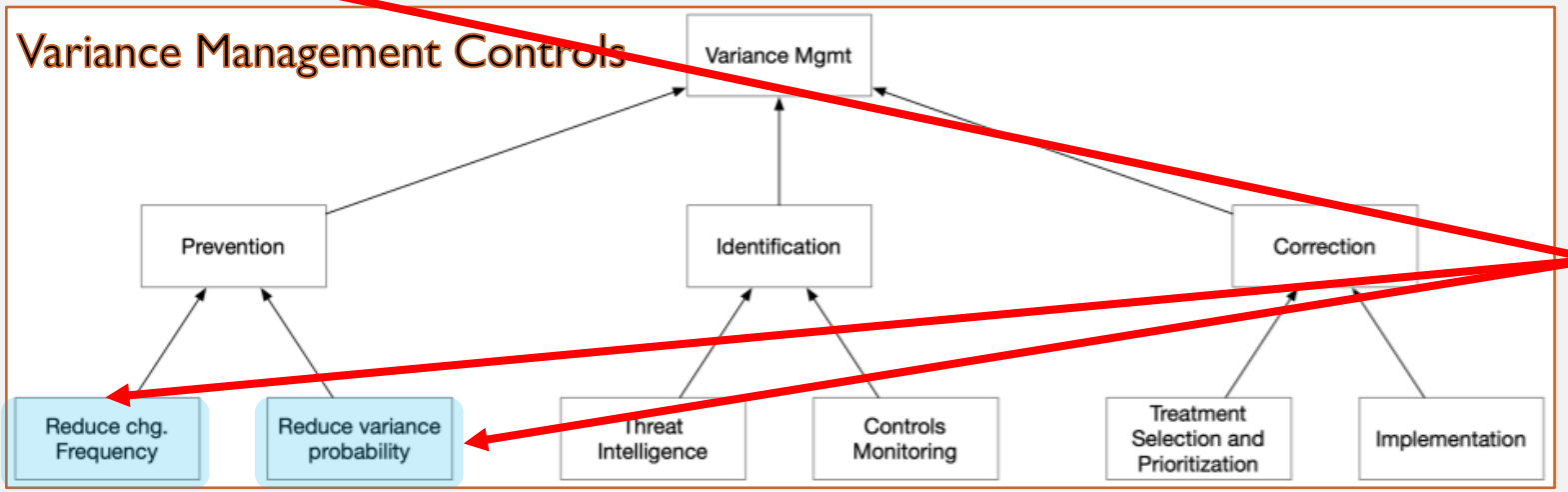
- Establish policies and communicate the policies for teleworking!

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking





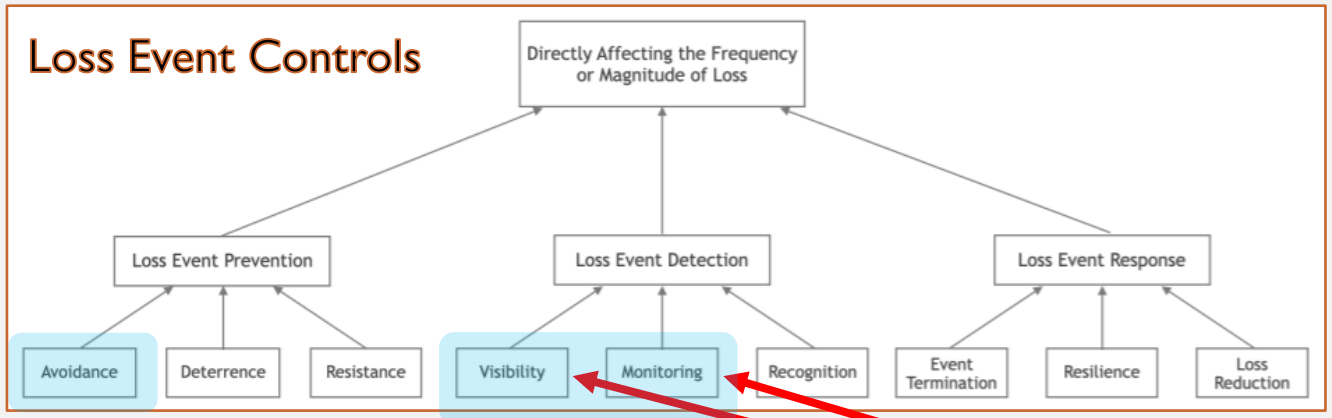


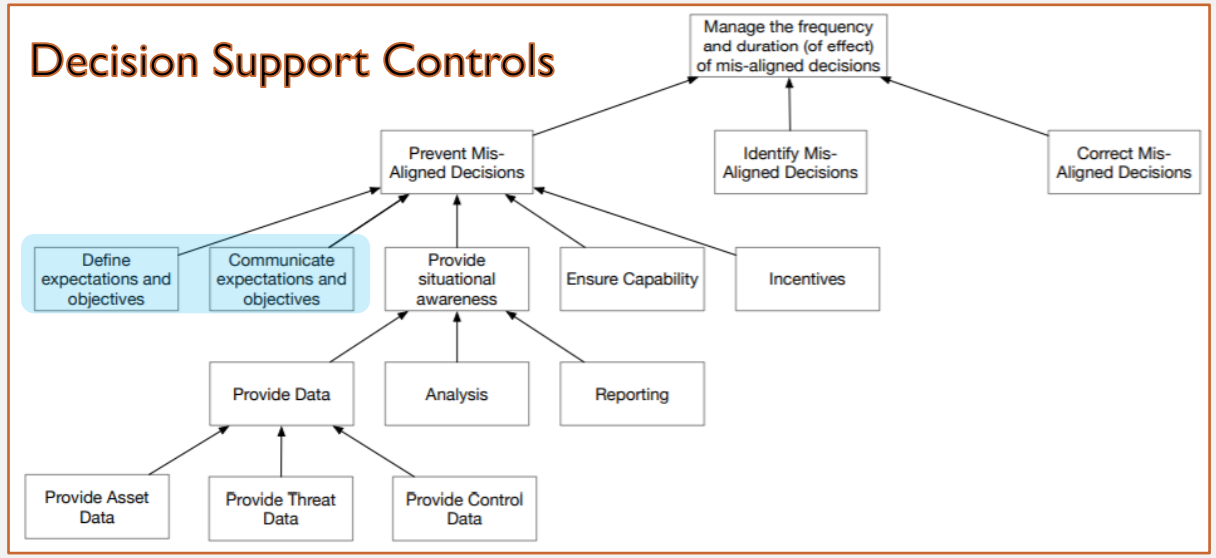
"The provision of virtual desktop access that prevents processing and storage of information on privately owned equipment"

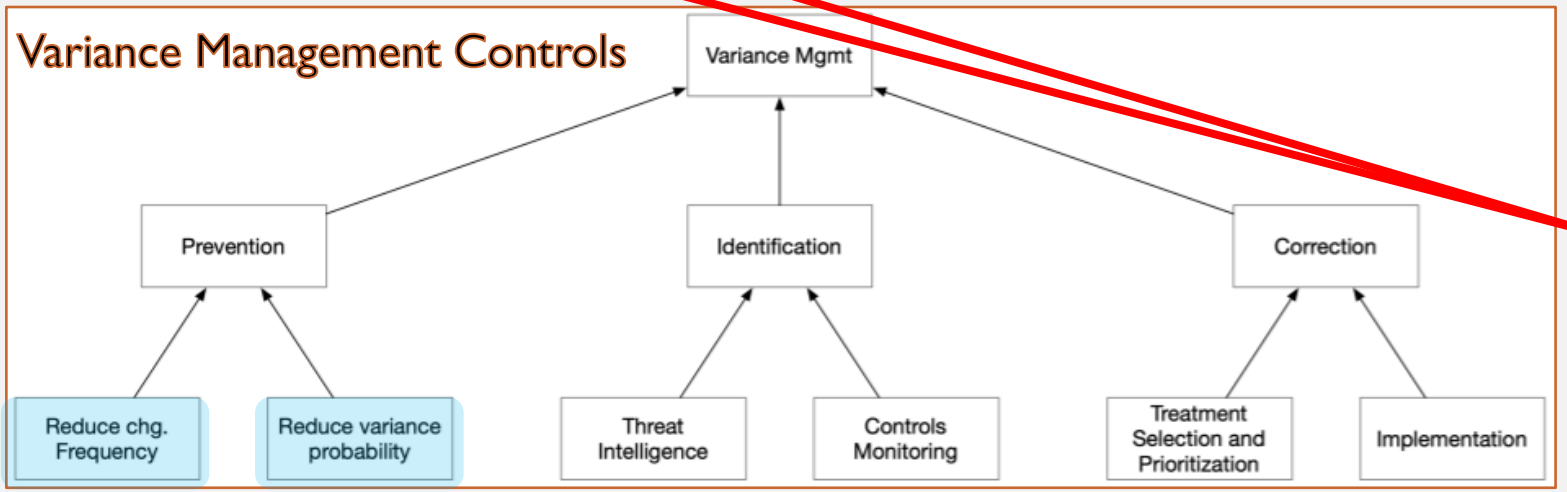
- Are we making prevention? Reducing the change frequency? Reducing the variance probability?

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking





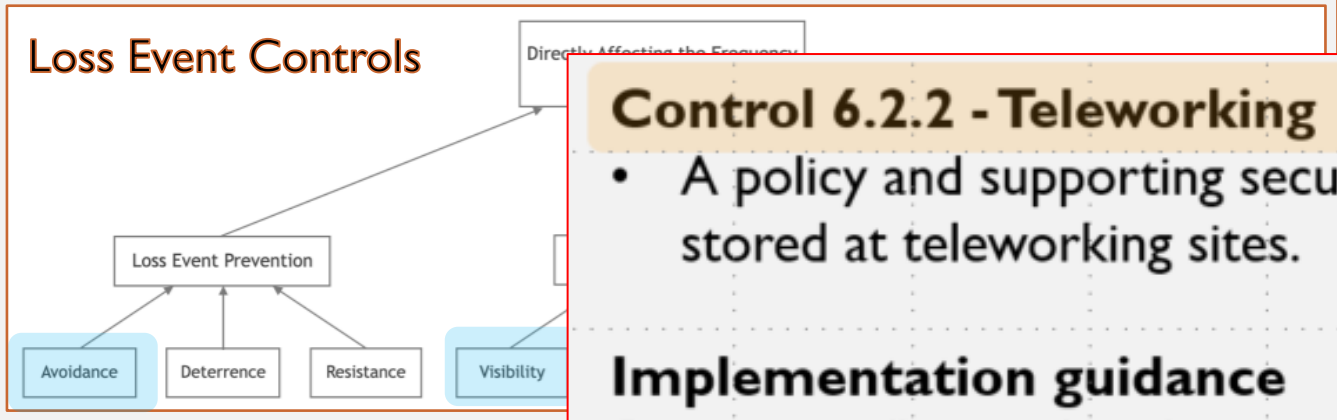


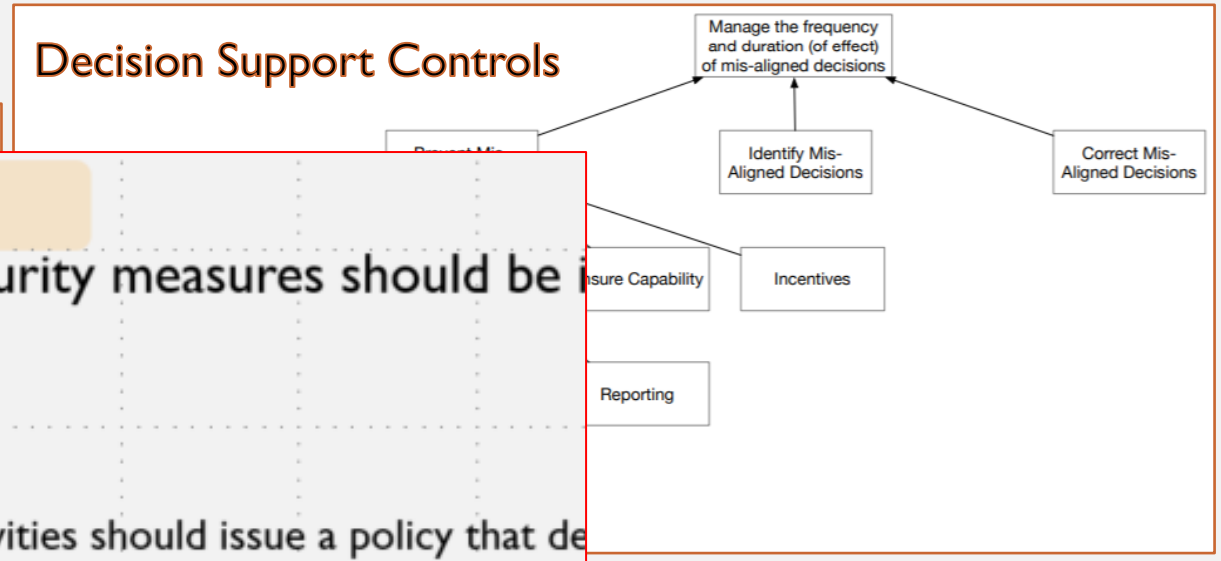
"The provision of virtual desktop access that prevents processing and storage of information on privately owned equipment"

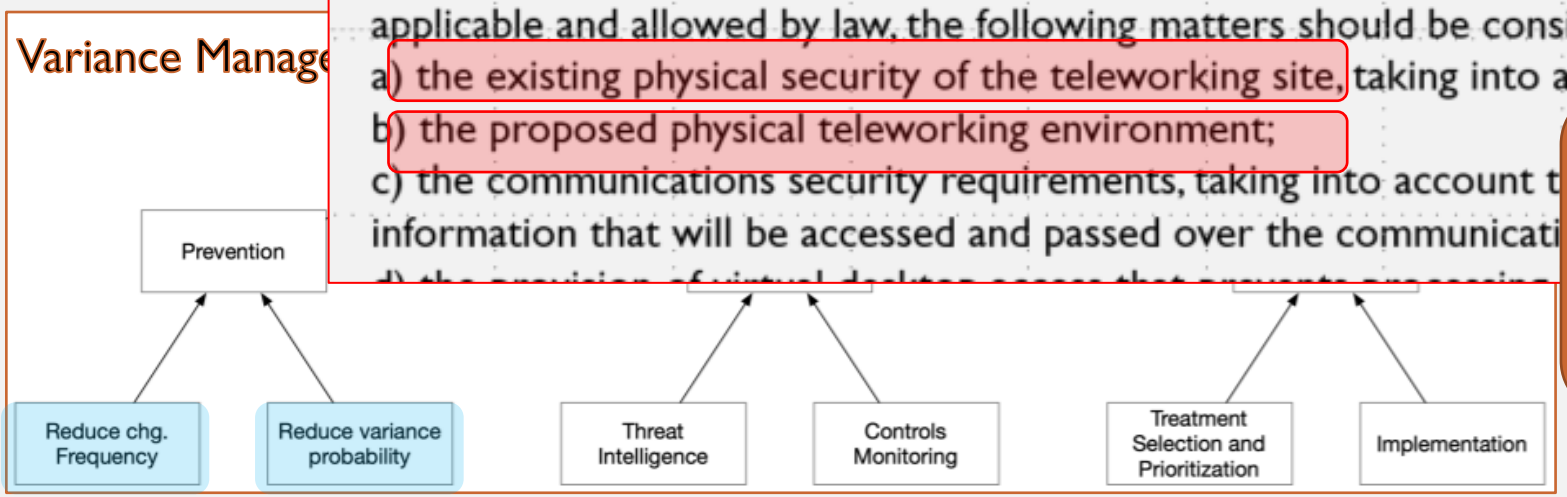
- Is the VDI infrastructure middleware providing visibility and monitoring functionalities?

MAPPING EXAMPLE #3

Control 6.2.2 - Teleworking







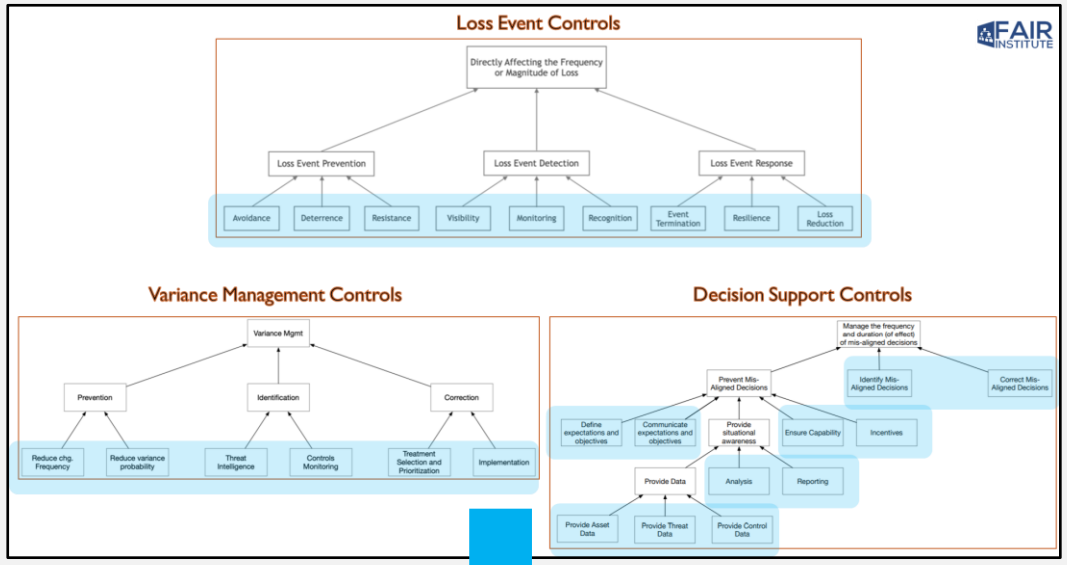
Further observations
- For some controls additional information from the context and scenario may help in the mapping

The third ingredient: the context

Why is important?

THE CONTEXT / THE SCENARIO

- It provides essential information about the physical and logical aspects, technological implementation, etc.
- The need to assess and quantify "how good a control acts" in a specific scenario
- Replacing the "x" with "numbers": the CMMI rating as input for the

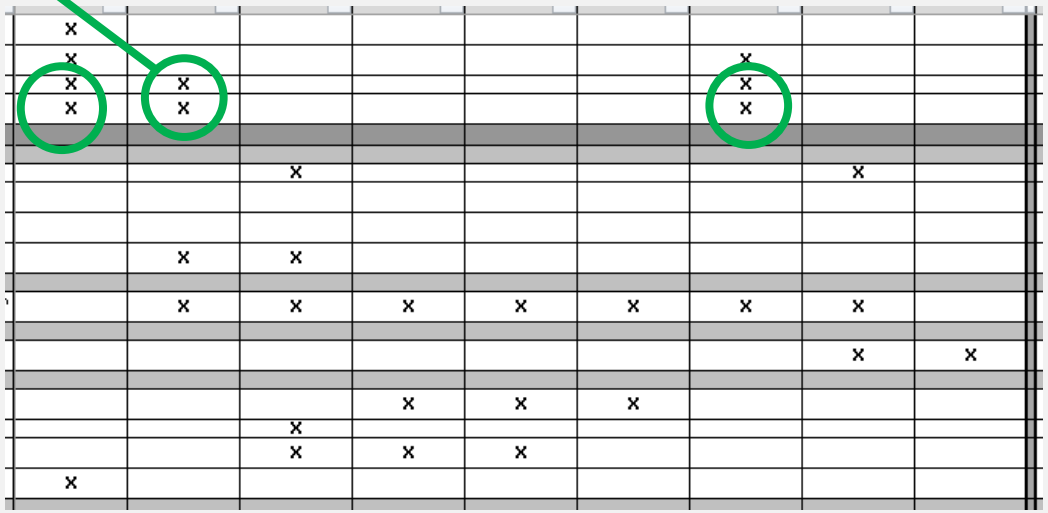


FAIR CAM CONTROL FUNCTIONS

ISO/IEC 27001:2013 CONTROLS

- ISO/IEC 27001 controls listed in Annex A (Reference control objectives) and detailed in ISO/IEC 27002 (Code of practice for information security controls)
- Total of 114 controls in the following domains:
  1. Information security policies
  2. Organization of information security
  3. Human resources security
  4. Asset management
  5. Access control
  6. Cryptography
  7. Physical and environmental security
  8. Operations security
  9. Communications security
  10. System acquisition, development and maintenance
  11. Supplier relationships
  12. Information security incident management
  13. Information security aspects of business continuity management
  14. Compliance

ISO 27001 CONTROLS



There is no perfect recipe!

Lessons learned:

- Aim to reduce uncertainty
- Precision in the mapping is not theoretically possible
- The mapping (at certain extent) can be defined without taking into account the context
- The mapping can be only valued for a specific scenario
- Threat scenario → ISO 27001 SOA → FAIR CAM → Risk quantification