2 parole di introduzione e prospettiva

La metodologia quantitativa è riconosciuta da ISACA , oltre che da altri, ed il metodo FAIR è un esempio, sempre riconosciuto da ISACA per fare delle analisi quantitative.

Non c'è discontinuità con i metodi qualitativi, si passa al quantitativo con sostituzioni uno-a-uno.

I metodi si imparano ed utilizzano progressivamente

Molti tool sono free

Lanciamo un gruppo di lavoro sull'argomento scrivere a g.bertocchi@isacaroma.it

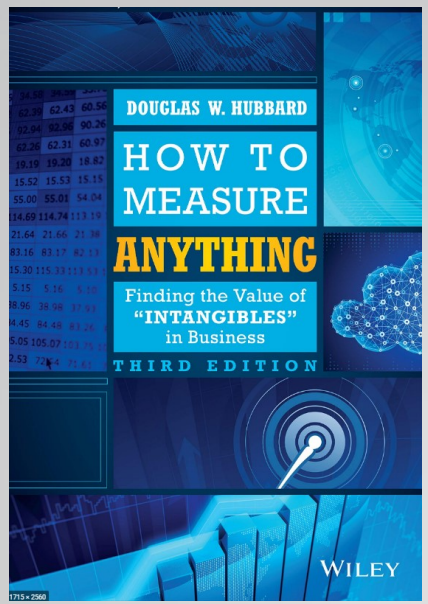
Abbiamo in programma dei corsi teorico-pratici tra alcuni mesi , vi terremo informati

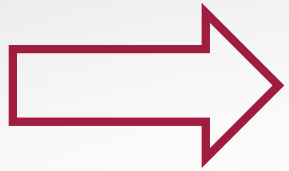
EVOLUZIONE DEL RISK MANAGEMENT
E
RISK QUANTIFICATION

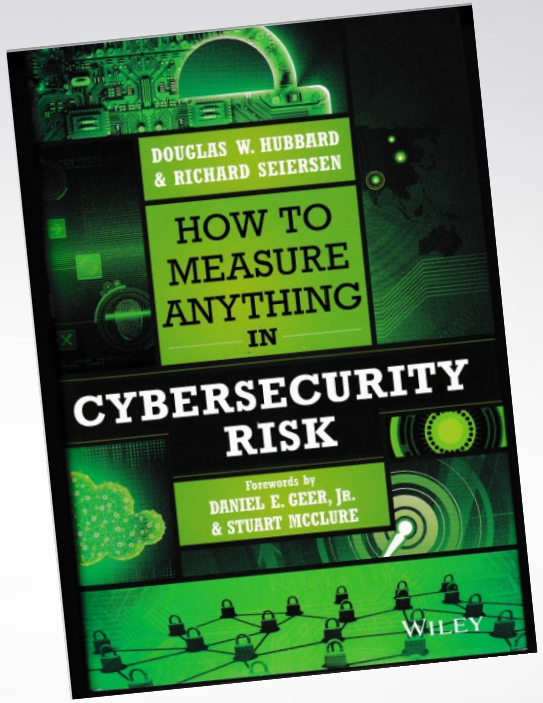
2° - DALLA TEORIA ALLA PRATICA

Alberto Piamonte

ISACA Roma







Più di 150.000 copie vendute, trad. in 8 lingue, testo universitario . . . .

- Si parte da una indagine sui metodi di analisi dei rischi IT che ha coinvolto circa 200 esperti del settore
- Si fa il punto teorico/pratico sullo stato dell'arte
- 1-2 giugno un corso sulle nuove metodologie organizzato da ISACA CHICAGO, con la partecipazione degli autori (*e del sottoscritto !*)

Agenda

- Gli standard e framework : posizionamento
- Il modello FAIR
- Un po’ di teoria
- Tools e pratica

ISACA NOW BLOG : Risk IT Revitalized

25 giugno 2020

ISACA

Search

SIGN IN SUPPORT JOIN CAREERS MYISACA

WHY ISACA? CREDENTIALING MEMBERSHIP TRAINING & EVENTS RESOURCES ENTERPRISE

Home / Resources / News and Trends / ISACA Now Blog / 2020 / Risk IT Revitalized

ISACA NOW BLOG

Risk IT Revitalized

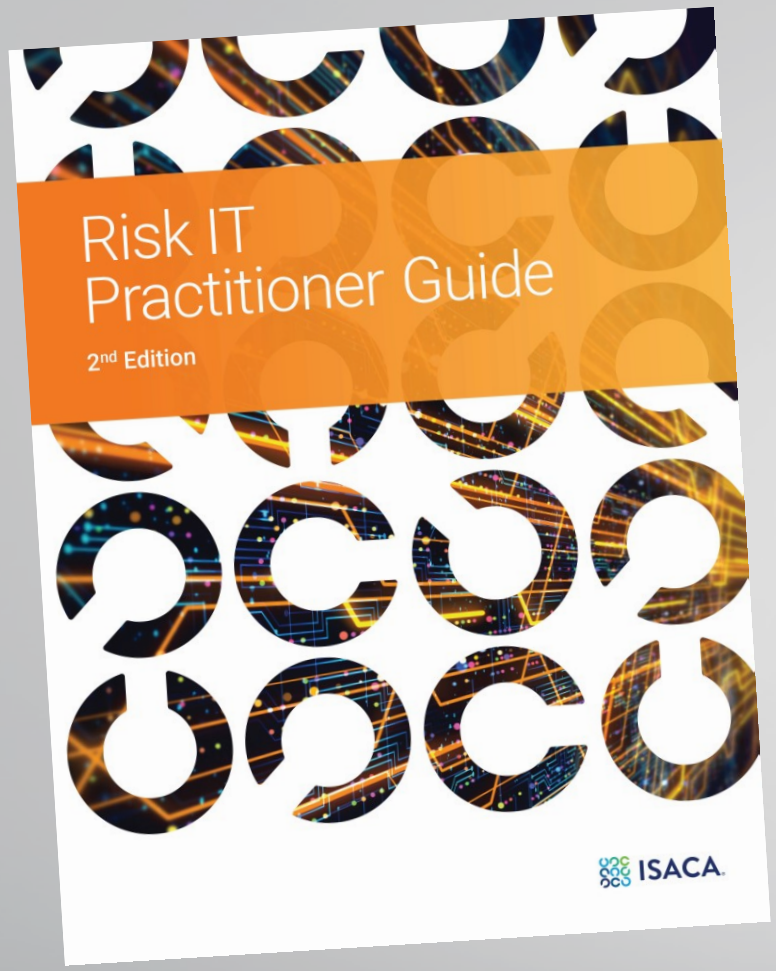
Author: Jack Jones, Chairman of the FAIR Institute and Chief Risk Scientist at RiskLens
Date Published: 25 June 2020

I had the privilege of being on the task force that created the original version of ISACA's Risk IT Framework several years ago. At the time, I felt Risk IT was an important contribution to the profession, as it provided an explicitly risk-focused context from which information security, audit, and technology professionals could think and operate. But, as with the first draft of anything, room for improvement existed. Furthermore — especially in today's dynamic risk landscape — periodic updates are necessary in order to maintain the value of any framework. With that in mind, ISACA recently put together a task force to update and refine Risk IT, and once again I was invited to take part — this time as a reviewer.

ISACA NOW BLOG : Risk IT Revitalized

25 giugno 2020

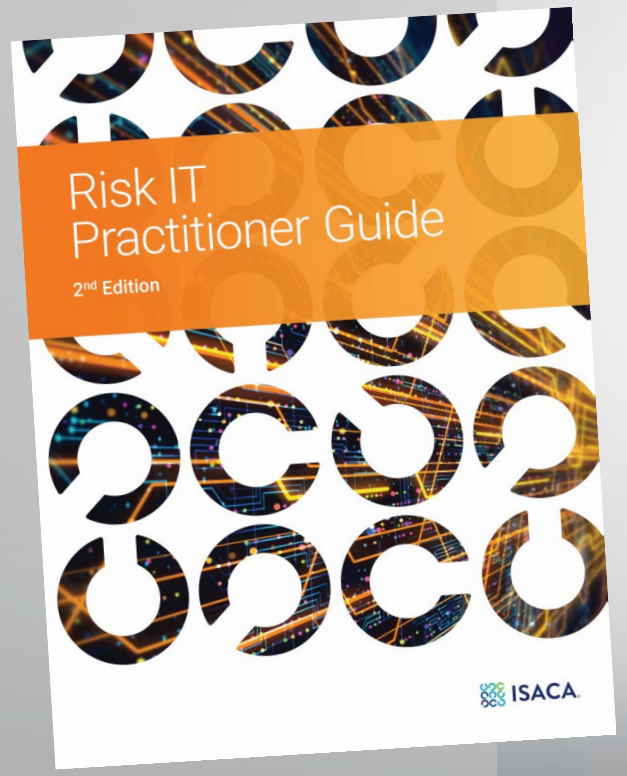
- …..
- I had the privilege of being on the task force that created the original version of ISACA's Risk IT Framework several years ago. . . .
- Another significant area of improvement in the second edition of Risk IT is the updates to the section on risk assessment — particularly **risk measurement**. Guidance related to **quantitative versus qualitative** measurement is significantly improved, which will help readers to have a clearer and more accurate understanding of the differences. Also, the risk analysis scoping section in the Practitioner' s Guide is much improved, reflecting better consistency and alignment with what's required to measure risk reliably.
- Of particular importance to me is the fact that **Risk IT remains highly compatible with the FAIR risk measurement model**. If anything, it is even more closely aligned, which further strengthens the utility of both frameworks.
- Despite a percentage of users who dislike using **heat maps** for communicating risk, Risk IT still advocates their use. Given that their use is still common and many executives are accustomed to them, to ignore them would not reflect the current state of the profession.

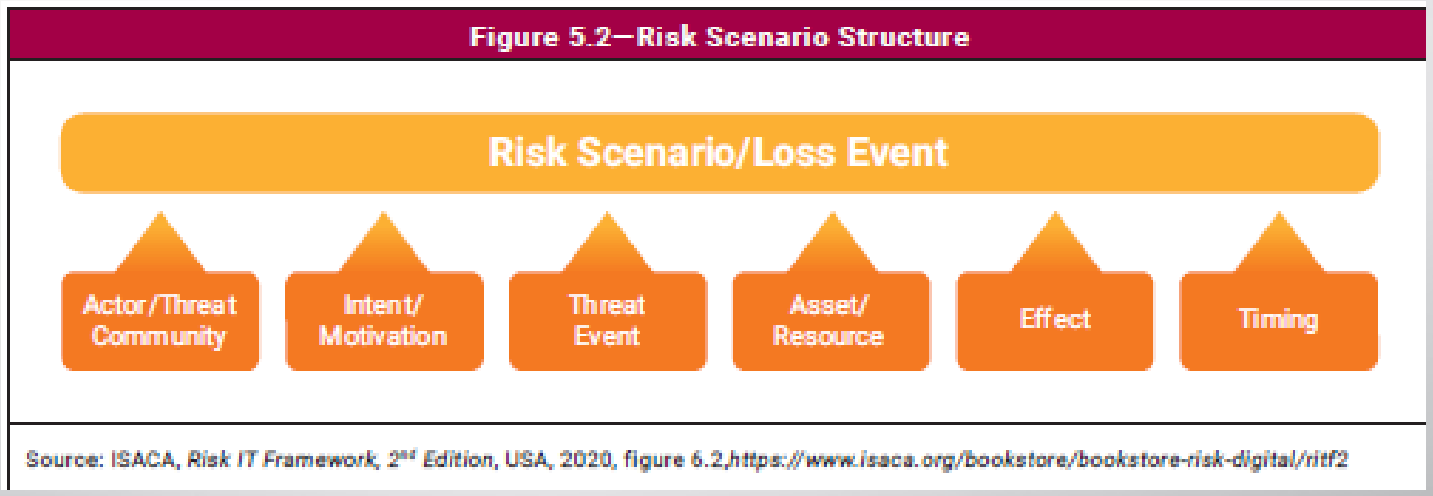


Dal nuovo Risk IT.....

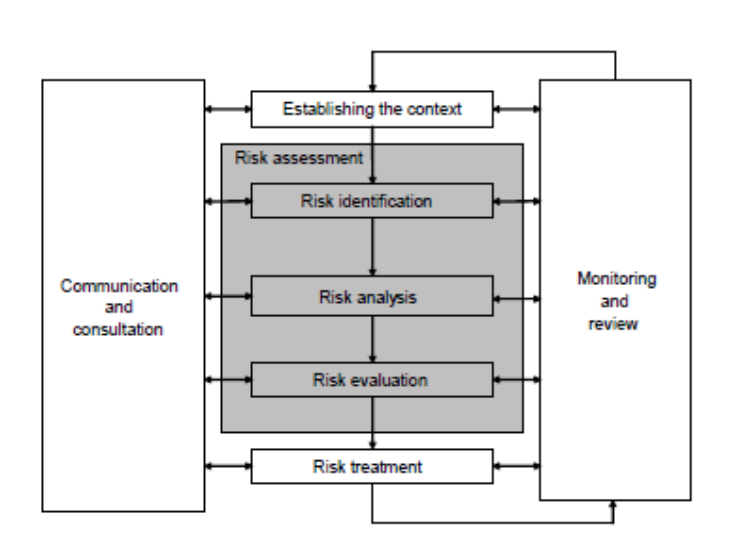
- ....
- If a risk is identified, enter it into a list, sometimes called a risk register, and determine the next step in analysis or response. This step in the risk management process often needs further analysis of the **risk factors** to determine an effective course of action or cost-justification for a plan of remediation.
  - A recommended decision analysis process is to use Monte Carlo[17] 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 Factor Analysis of Information Risk[18] (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.**
- ....

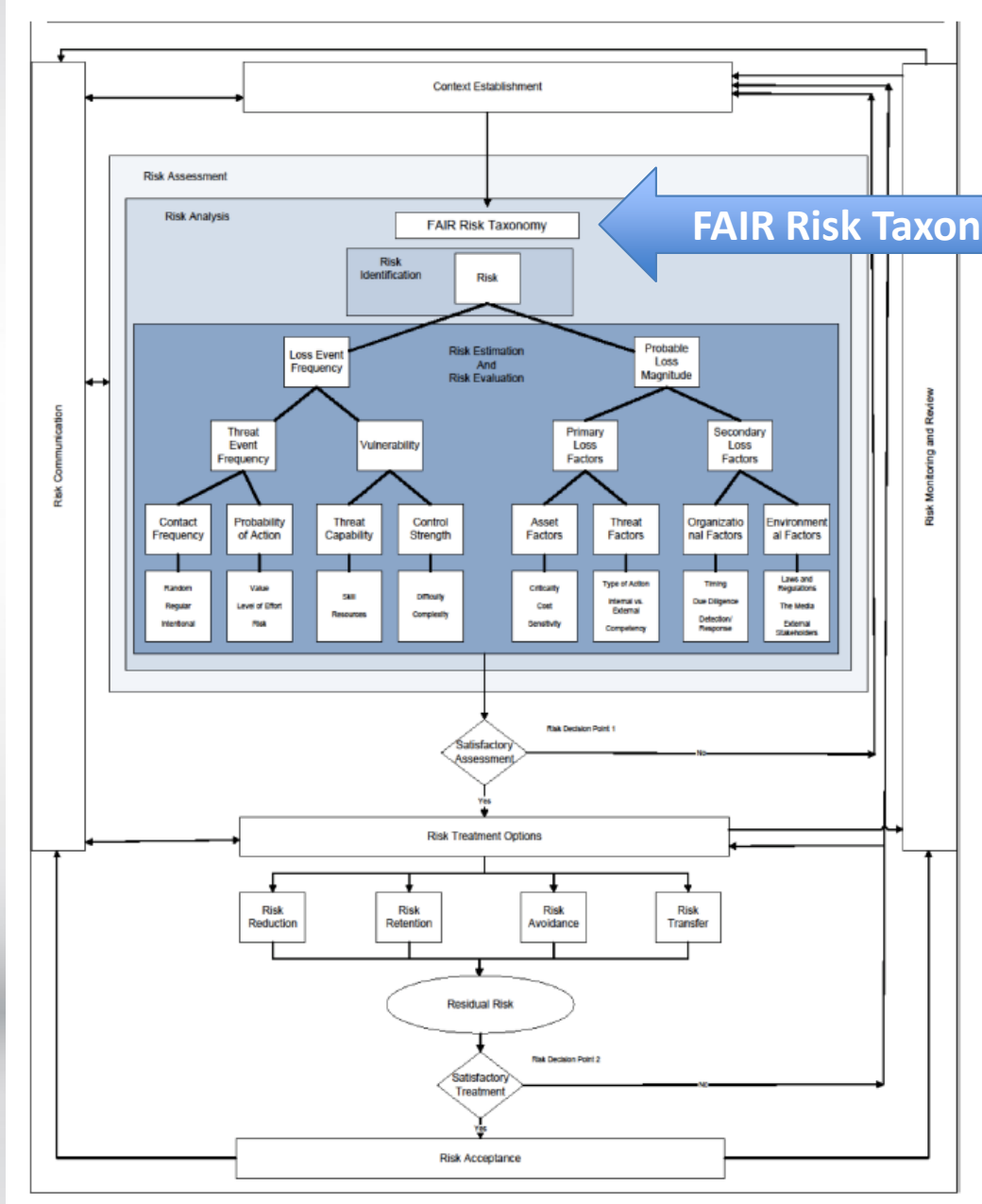
The following structure for risk scenarios is proposed, based on a review of current risk methodologies (Risk IT, COBIT 2019, **FAIR,** Committee of Sponsoring Organizations of the Treadway Commission [COSO] Enterprise Risk Management [ERM] 2017). The structure indicates all elements that should be described to have a full, analyzable risk scenario.





ISO 31000





FAIR Risk Taxonomy

NIST-CSF

Member Login

FAIR INSTITUTE

ABOUT ▾ GET INVOLVED LEARN FAIR ▾ EVENTS ▾ AWAR

NIST Maps FAIR to the CSF - Big Step Forward in Acceptance of Cyber Risk Quantification

Nov 19, 2019 2:36:00 PM / by **Jeff B. Copeland**

Tweet Share Like 12 Share

It's official: NIST has formally published FAIR as an Informative Reference to the NIST CSF, the most widely used cybersecurity framework in the U.S, a major milestone in the history of FAIR. This means that there is mapping between FAIR and the NIST CSF standard in the sections covering risk analysis and risk management.

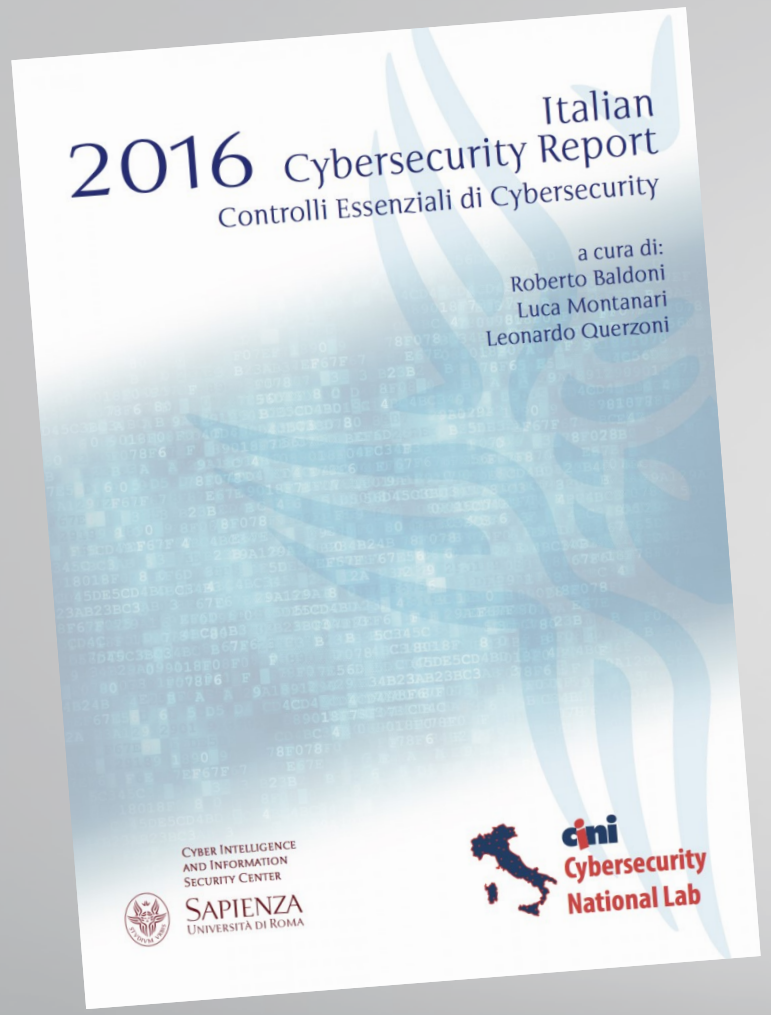
*See FAIR officially listed in the **Informative Reference Catalog** on the NIST CSF website.*

The FAIR Institute has long since held that FAIR is a complementary standard to other information security frameworks. This is confirmation that organizations can be confident employing FAIR for their risk analyses alongside the other NIST CSF framework processes.

Jack Freund, PhD, co-author with Jack Jones of the FAIR book, ***Measuring and Managing Information Risk*** and Risk Science Director for RiskLens, worked with NIST on behalf of the FAIR Institute to gain this recognition. Jack also moderated a panel discussion at the 2019 FAIR Conference entitled **Building a Cybersecurity Program with a Risk Management Framework and FAIR.** The panel included Ian Amit, CSO of Cimpress, recently **cited by NIST as a "success story"** in integrating FAIR and NIST CSF.

The CSF is essentially a very thorough, step-by-step walk-through of defensive measures for cybersecurity, including risk assessment (RA) and risk management (RM).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management



- Negli ultimi anni le minacce cyber sono ulteriormente evolute in qualità e quantità. Oggi un problema fondamentale è rappresentato dai *data breach* che sottraggono in modo fraudolento dati, anche sensibili, dalle banche dati di industrie, enti pubblici ed organizzazioni di ogni genere. I data breach rappresentano un danno spesso ingente per le organizzazioni e oggi, alla luce delle norme previste dal Regolamento Generale sulla Protezione dei Dati (GDPR), possono essere causa di consistenti multe.
- In questo contesto viene oggi introdotta una nuova versione del Framework Nazionale per la Cybersecurity e la Data Protection, uno strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. Rispetto alla versione presentata nel 2015, sono stati introdotti contributi volti a cogliere gli aspetti fondamentali legati alla protezione dei dati secondo quanto previsto nel GDPR.

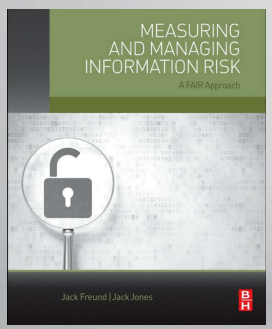
ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

IL MODELLO FAIR

1 1

1

Il metodo FAIR



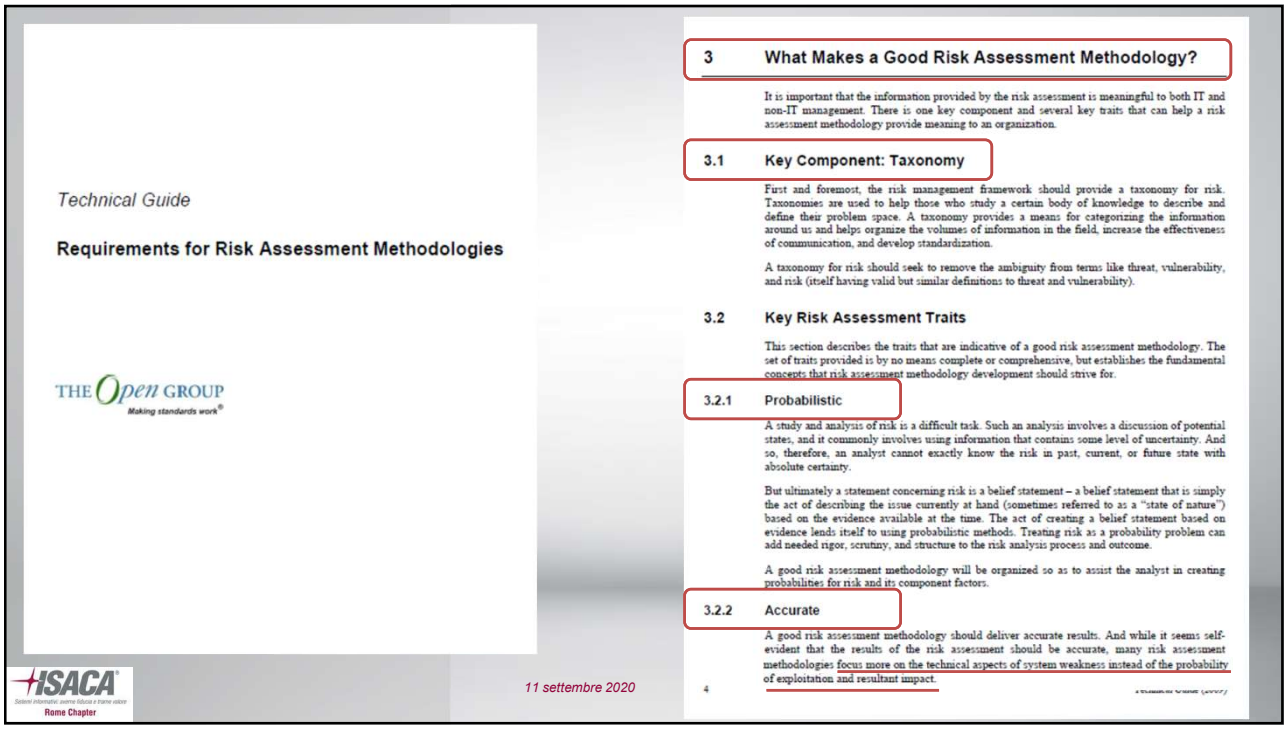
- Un'associazione ed uno standard documentato e riconosciuto
- Un testo completo, pratico ed efficace che:
  - Identifica i fattori che determinano il rischio
  - Individua le aree possibili di intervento
  - Spiega come procedere per livelli di dettaglio progressivi
  - Considera il «*come*» comunicare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

ISACA Rome Chapter

11 settembre 2020

2

2



Technical Guide

Requirements for Risk Assessment Methodologies

THE Open GROUP
Making standards work®

ISACA
Rome Chapter

11 settembre 2020

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

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.

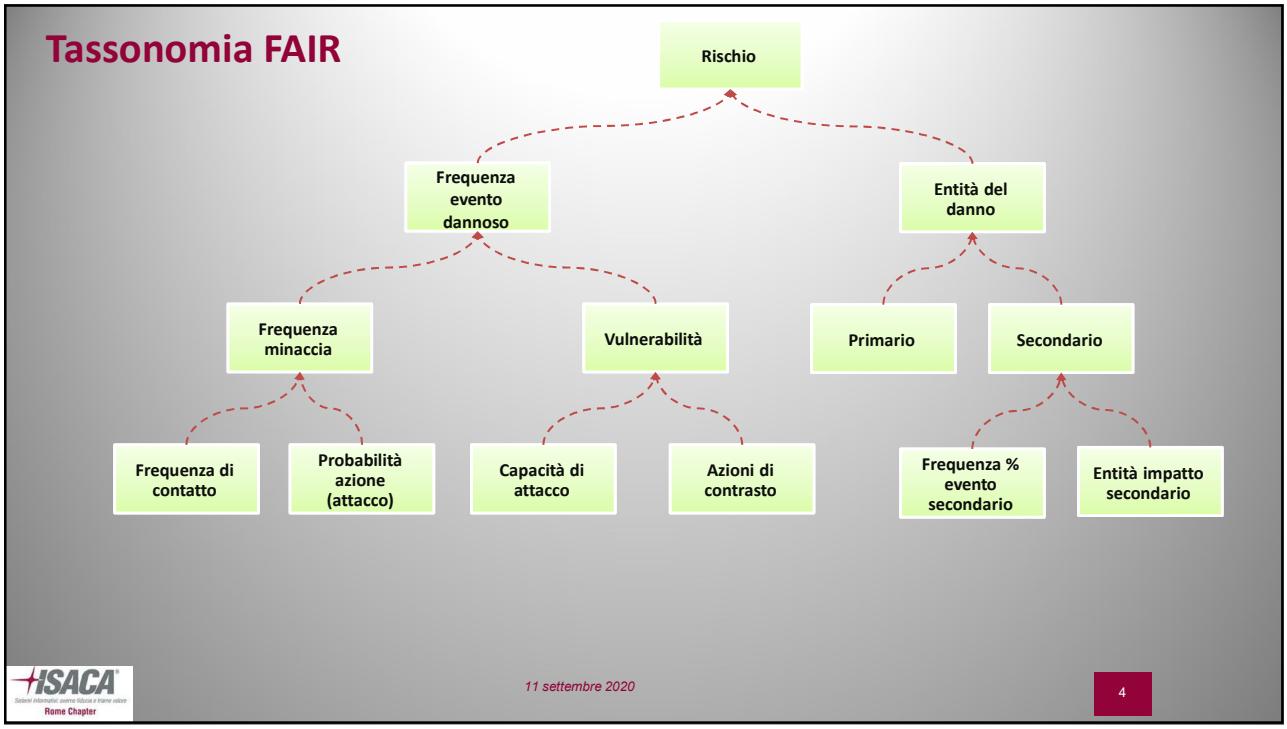
A good risk assessment methodology will be organized so as to assist the analyst in creating probabilities for risk and its component factors.

3.2.2 Accurate

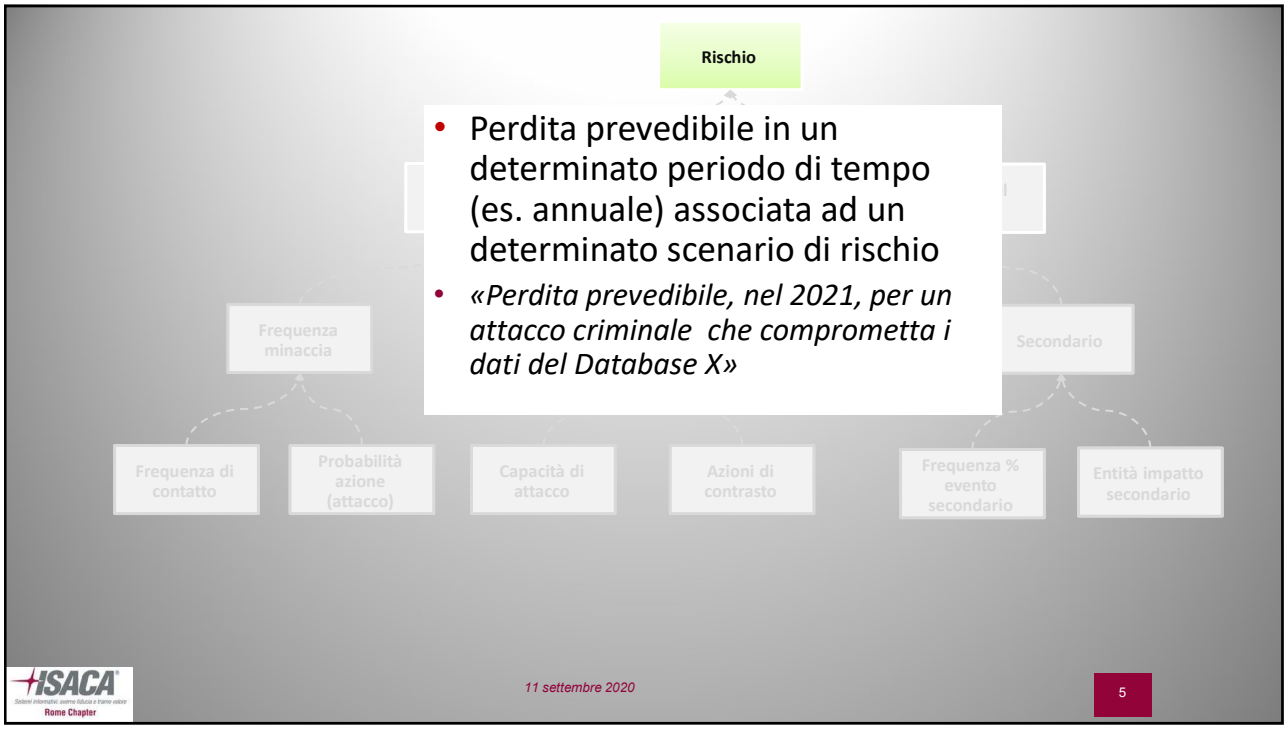
A good risk assessment methodology should deliver accurate results. And while it seems self-evident that the results of the risk assessment should be accurate, many risk assessment methodologies focus more on the technical aspects of system weakness instead of the probability of exploitation and resultant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

4

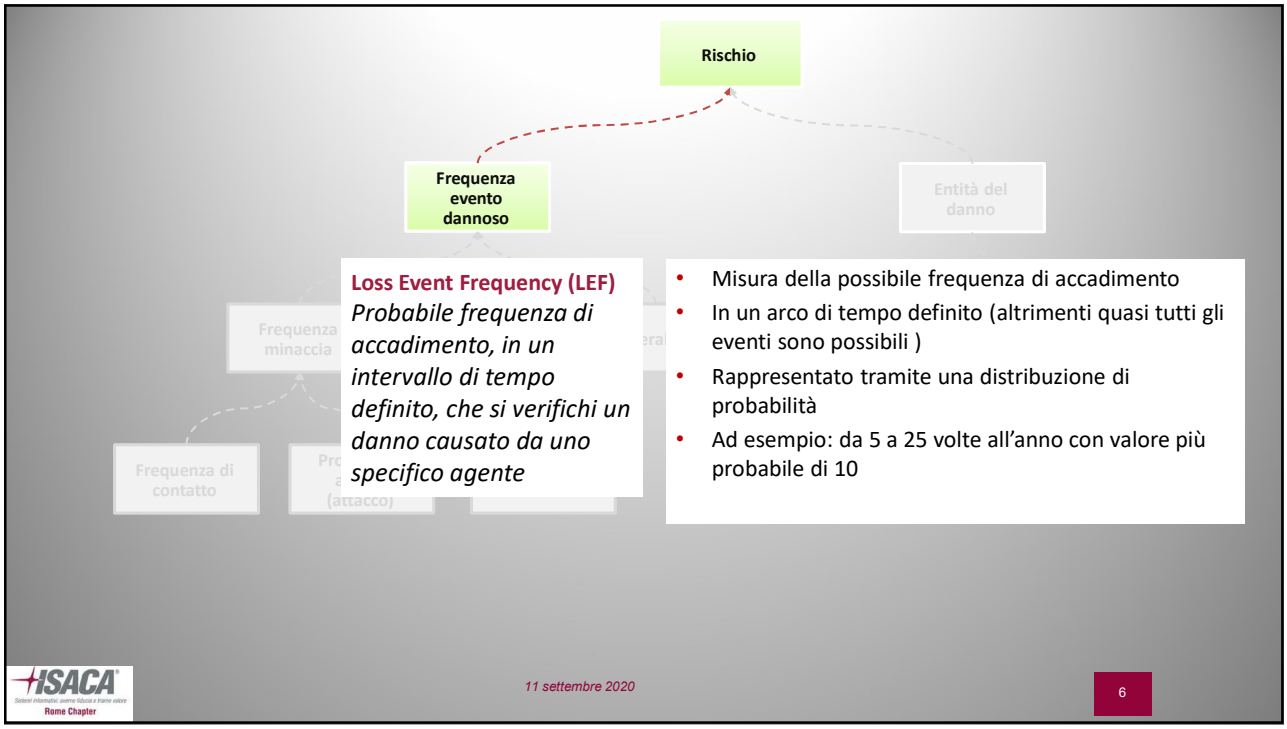
3



4


Rischio
Perdita prevedibile in un determinato periodo di tempo (es. annuale) associata ad un determinato scenario di rischio
«Perdita prevedibile, nel 2021, per un attacco criminale che comprometta i dati del Database X»
Frequenza minaccia
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
ISACA Rome Chapter
11 settembre 2020
5

5


Rischio
Frequenza evento dannoso
Entità del danno
Loss Event Frequency (LEF)
Probabile frequenza di accadimento, in un intervallo di tempo definito, che si verifichi un danno causato da uno specifico agente
Misura della possibile frequenza di accadimento
In un arco di tempo definito (altrimenti quasi tutti gli eventi sono possibili)
Rappresentato tramite una distribuzione di probabilità
Ad esempio: da 5 a 25 volte all'anno con valore più probabile di 10
Frequenza minaccia
Frequenza di contatto
ISACA Rome Chapter
11 settembre 2020
6

6

LOSS EVENT FREQUENCY (LEF)

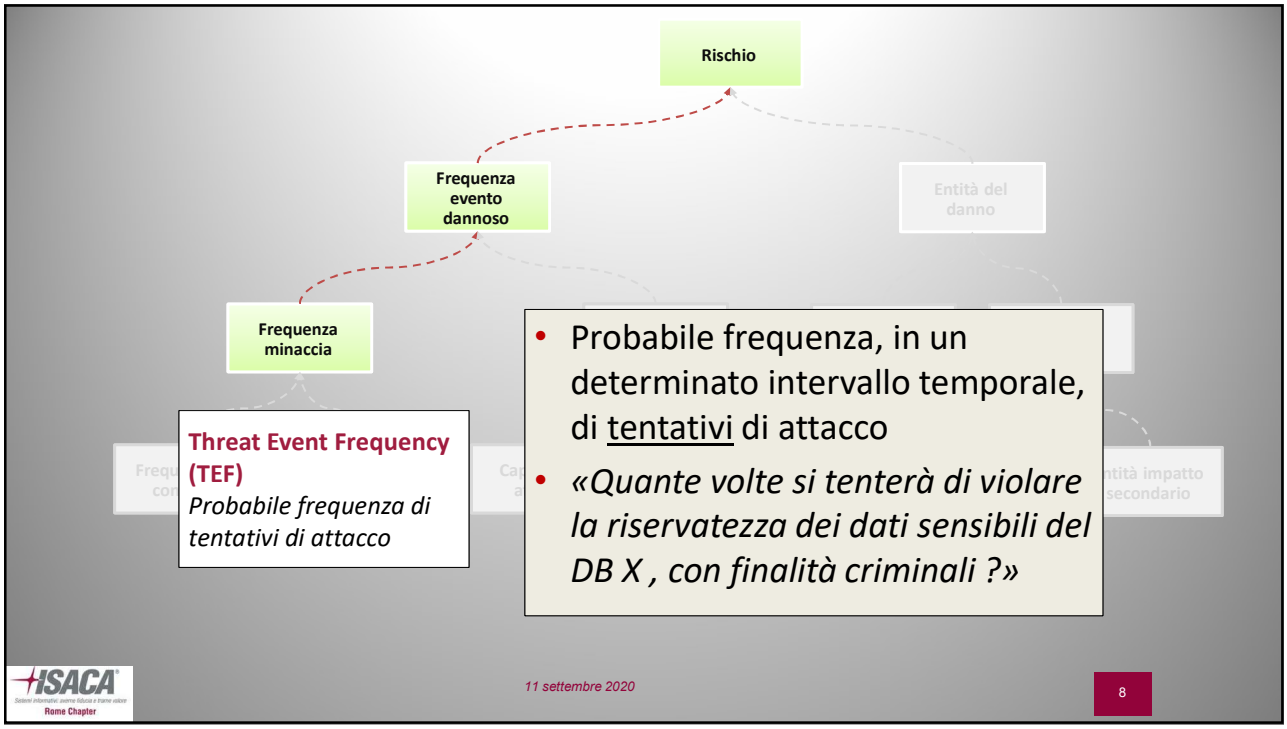
- FAIR usa frequenza piuttosto che probabilità
- Più facili ad capire e forzano la definizione dell'intervallo temporale.
- Ad esempio: «L'evento x ha una probabilità del 20 %»
- In alternativa : l'evento x si può verificare 2 volte in dieci anni (o una volta in 5 anni) è più chiaro ed immediato (e contiene un riferimento temporale)

ISACA Rome Chapter

11 settembre 2020

7

7



8

THREAT EVENT FREQUENCY (TEF)

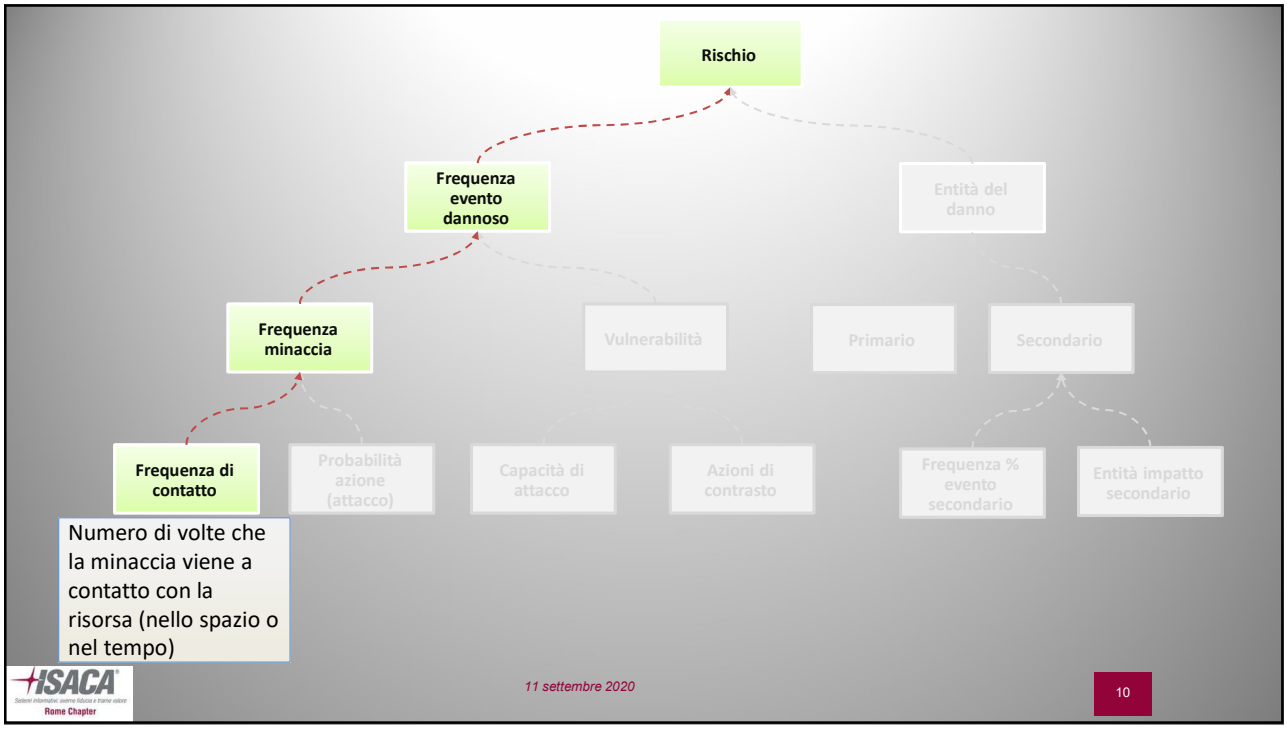
Threat Event	Loss Event
Attacco hacker ad un sito web	Un hacker danneggia o sottrae informazioni da un sito Web
Passaggio in produzione di un nuovo rilascio Sw	Il nuovo rilascio crea problemi di disponibilità, integrità, ecc.
Vengo minacciato con un'arma da taglio	Vengo ferito da un'arma da taglio

ISACA Rome Chapter

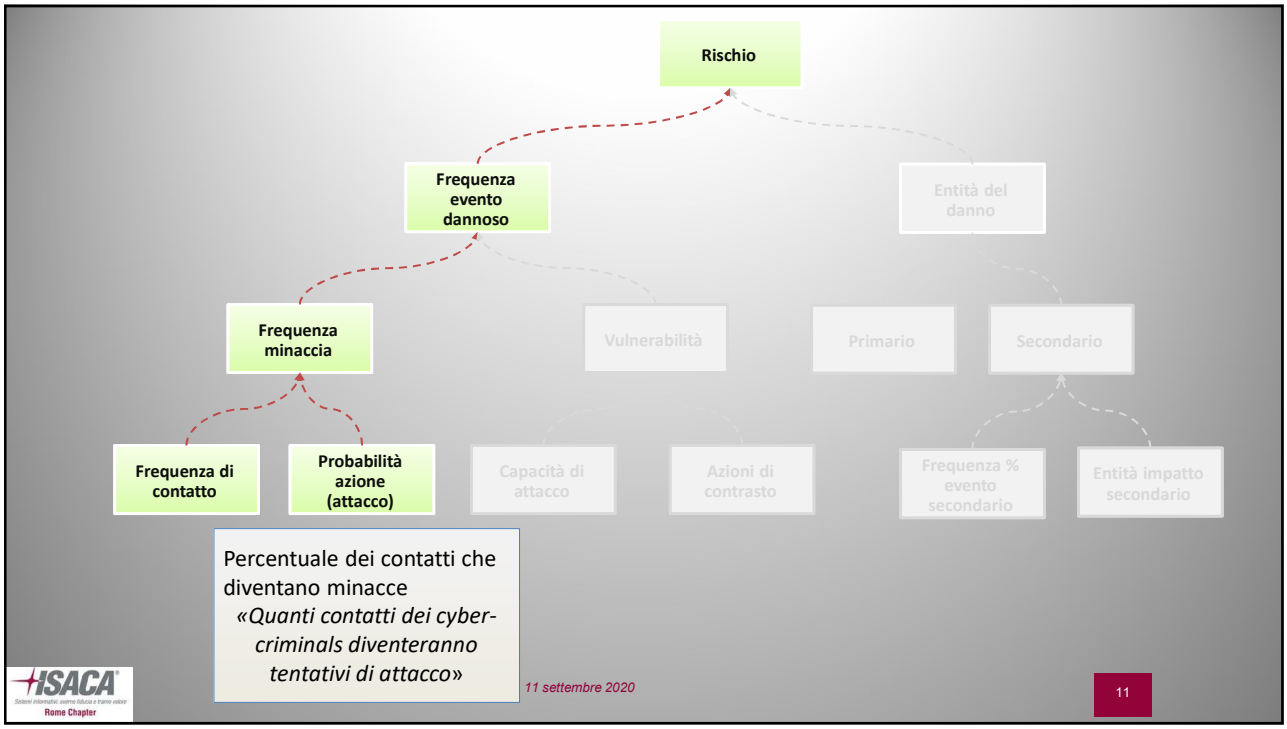
11 settembre 2020

9

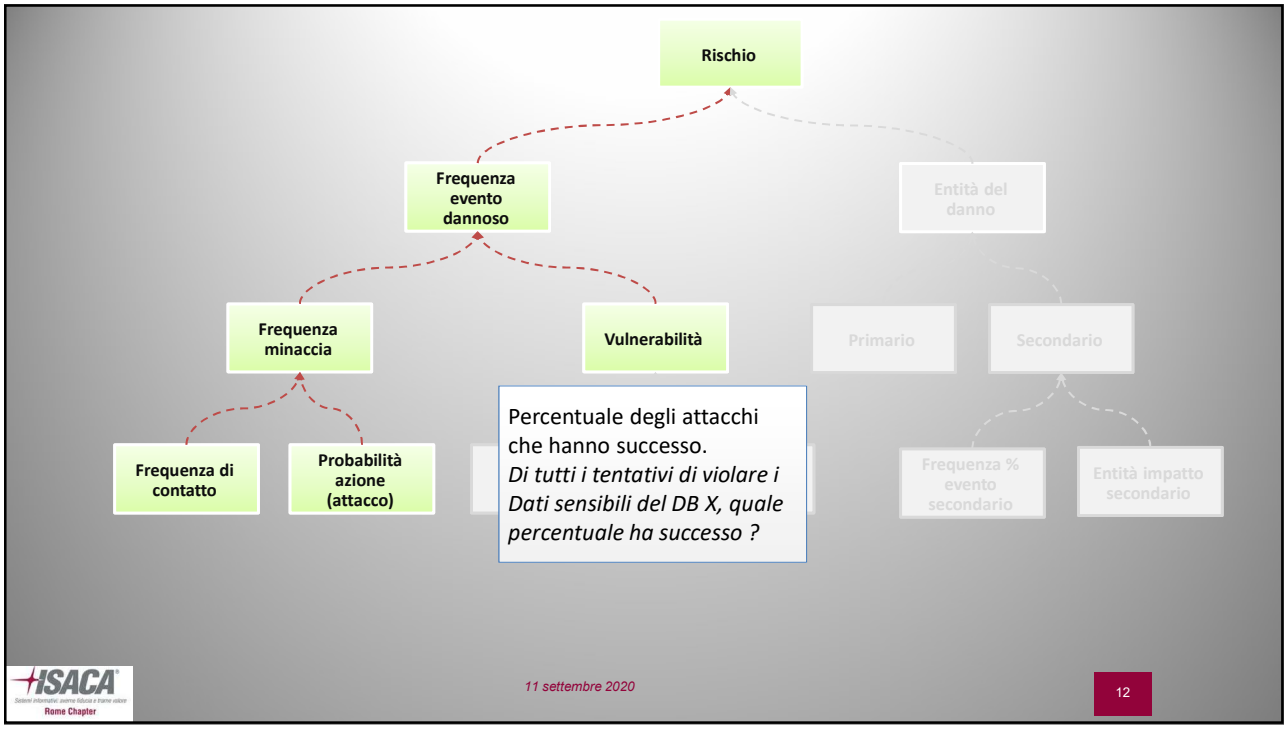
9



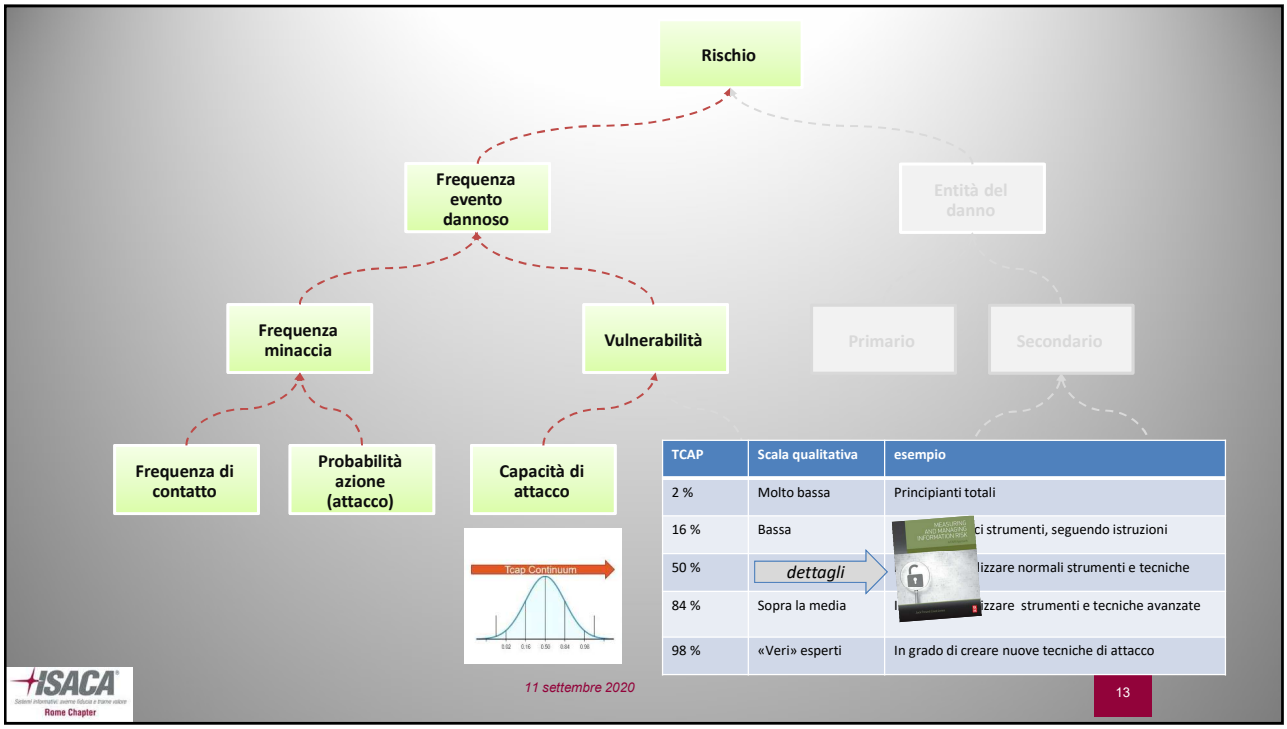
10


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
Percentuale dei contatti che diventano minacce
«Quanti contatti dei cyber-criminals diventeranno tentativi di attacco»
ISACA Rome Chapter
11 settembre 2020
11

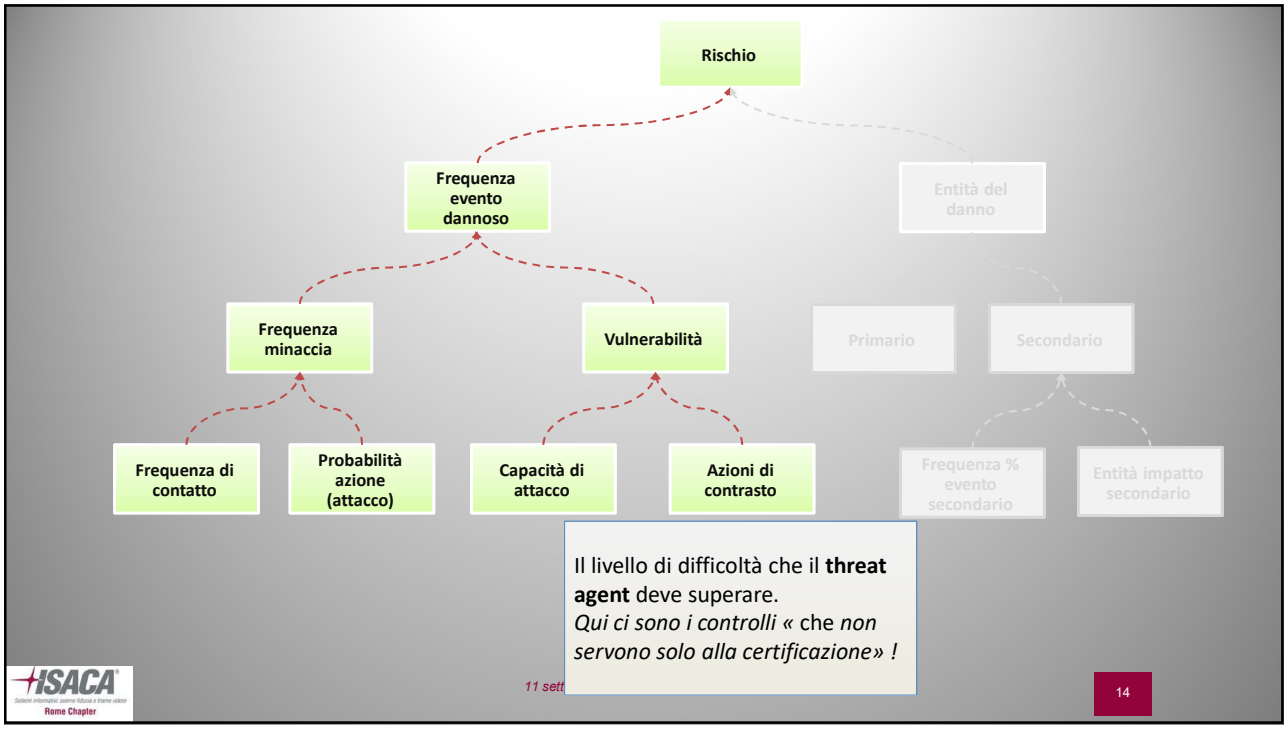
11


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Frequenza % evento secondario
Entità impatto secondario
Percentuale degli attacchi che hanno successo.
Di tutti i tentativi di violare i Dati sensibili del DB X, quale percentuale ha successo ?
ISACA Rome Chapter
11 settembre 2020
12

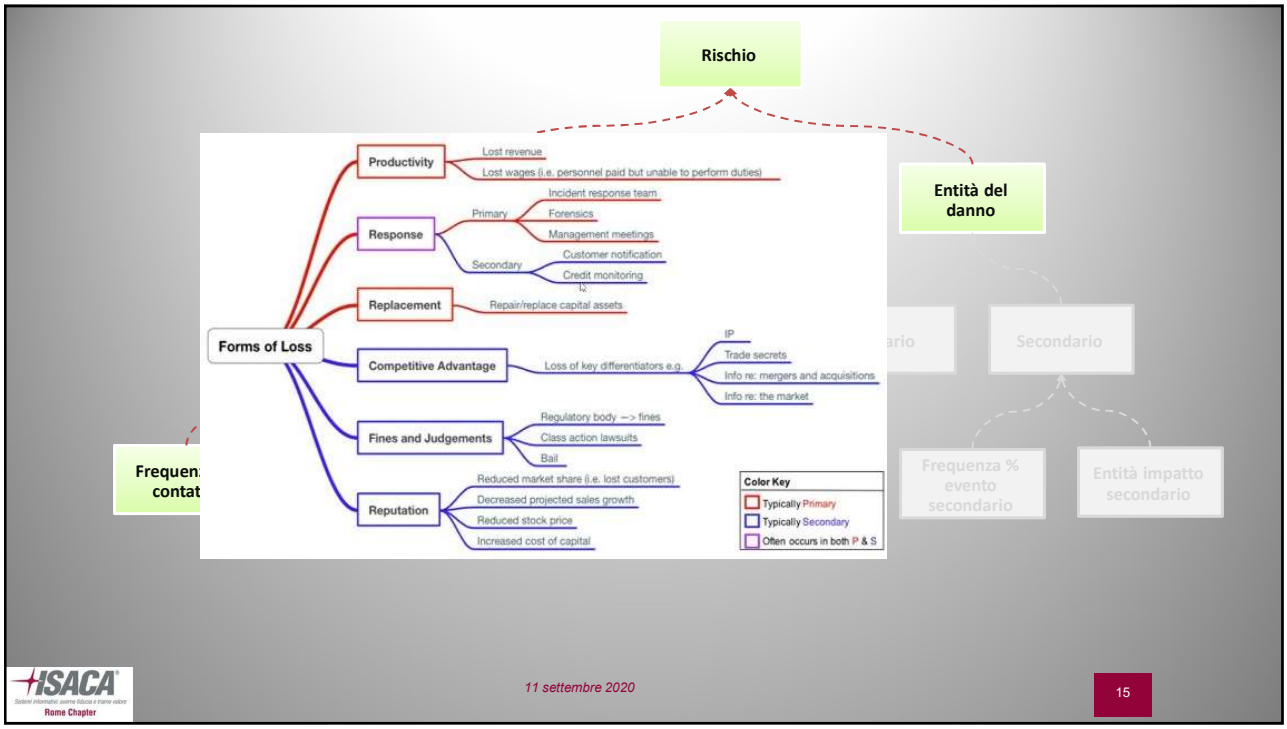
12


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Tcap Continuum
TCAP
Scala qualitativa
esempio
2 %
Molto bassa
Principianti totali
16 %
Bassa
ci strumenti, seguendo istruzioni
50 %
dettagli
lizzare normali strumenti e tecniche
84 %
Sopra la media
izzare strumenti e tecniche avanzate
98 %
«Veri» esperti
In grado di creare nuove tecniche di attacco
ISACA
Rome Chapter
11 settembre 2020
13

13

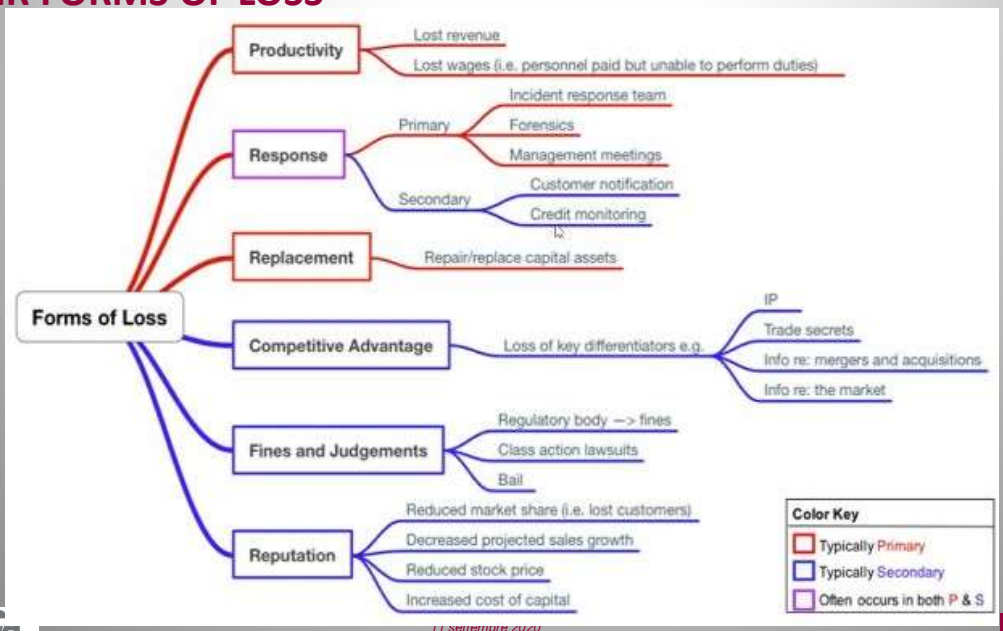

Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
Il livello di difficoltà che il threat agent deve superare.
Qui ci sono i controlli « che non servono solo alla certificazione» !
ISACA
Rome Chapter
14

14

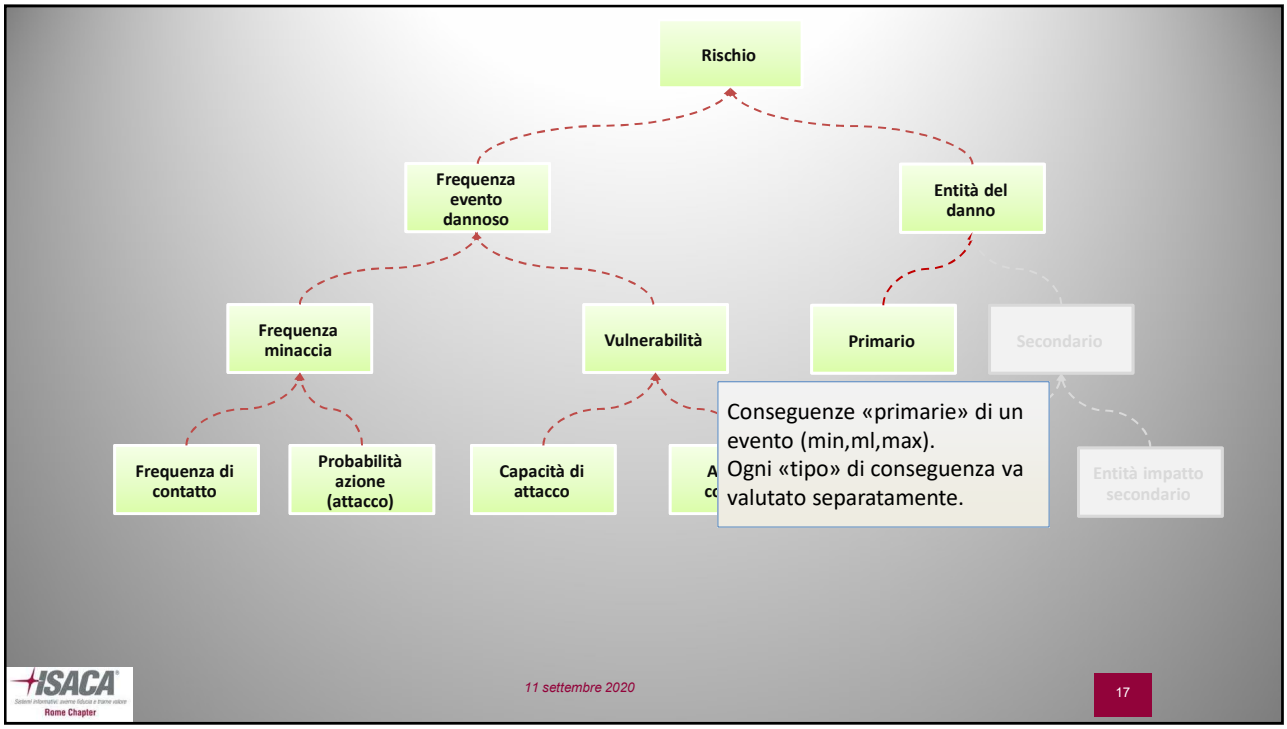


15

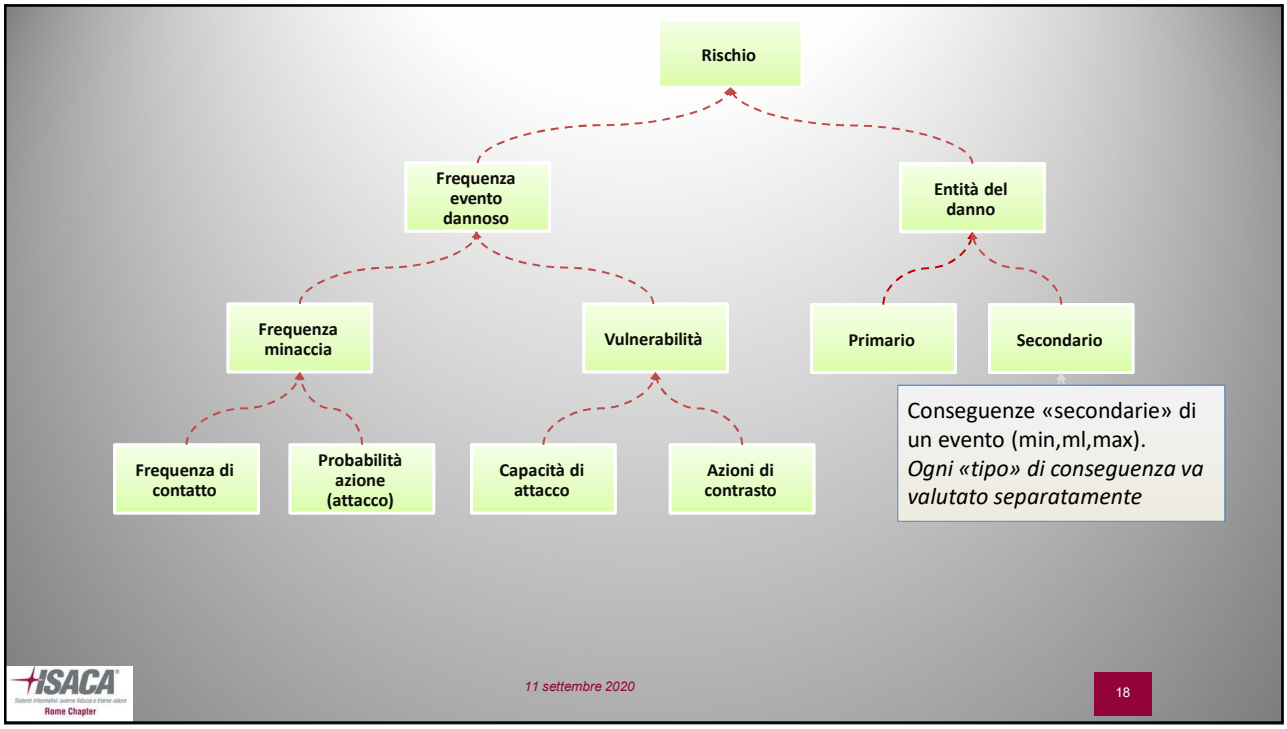
FAIR FORMS OF LOSS



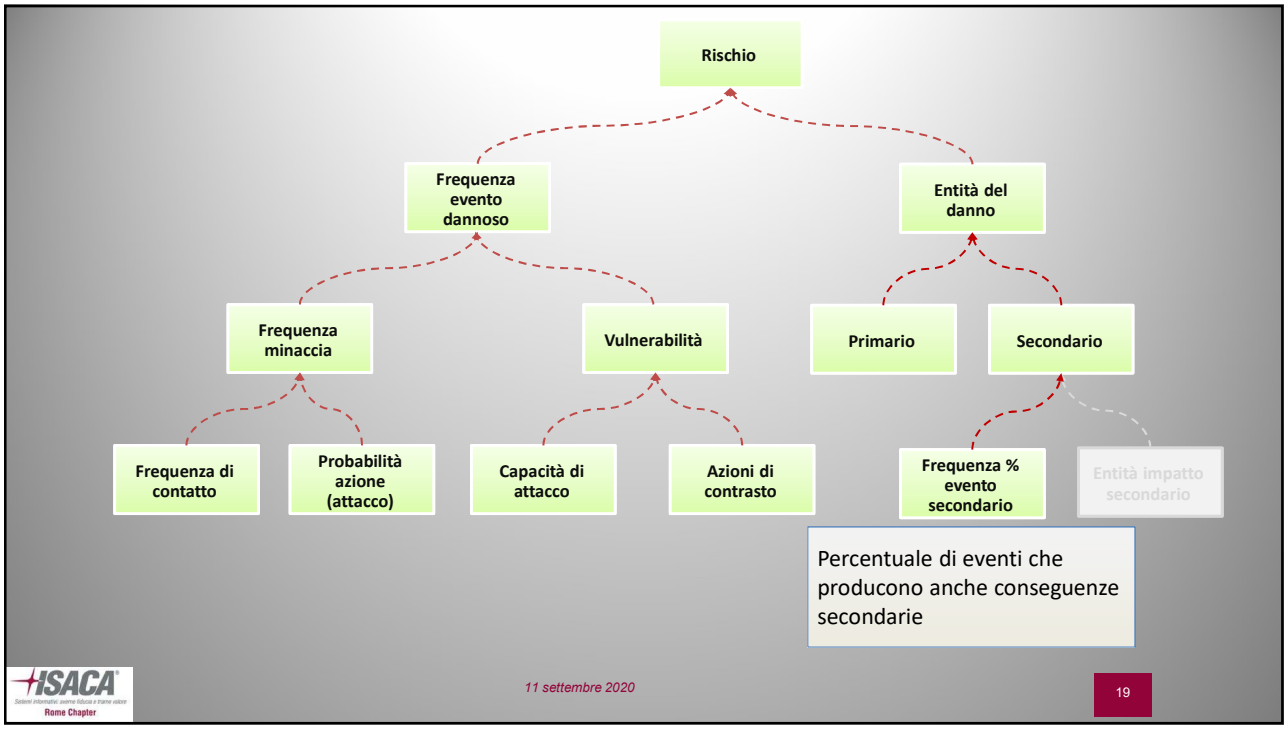
16


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Entità impatto secondario
Conseguenze «primarie» di un evento (min,ml,max).
Ogni «tipo» di conseguenza va valutato separatamente.
ISACA
Rome Chapter
11 settembre 2020
17

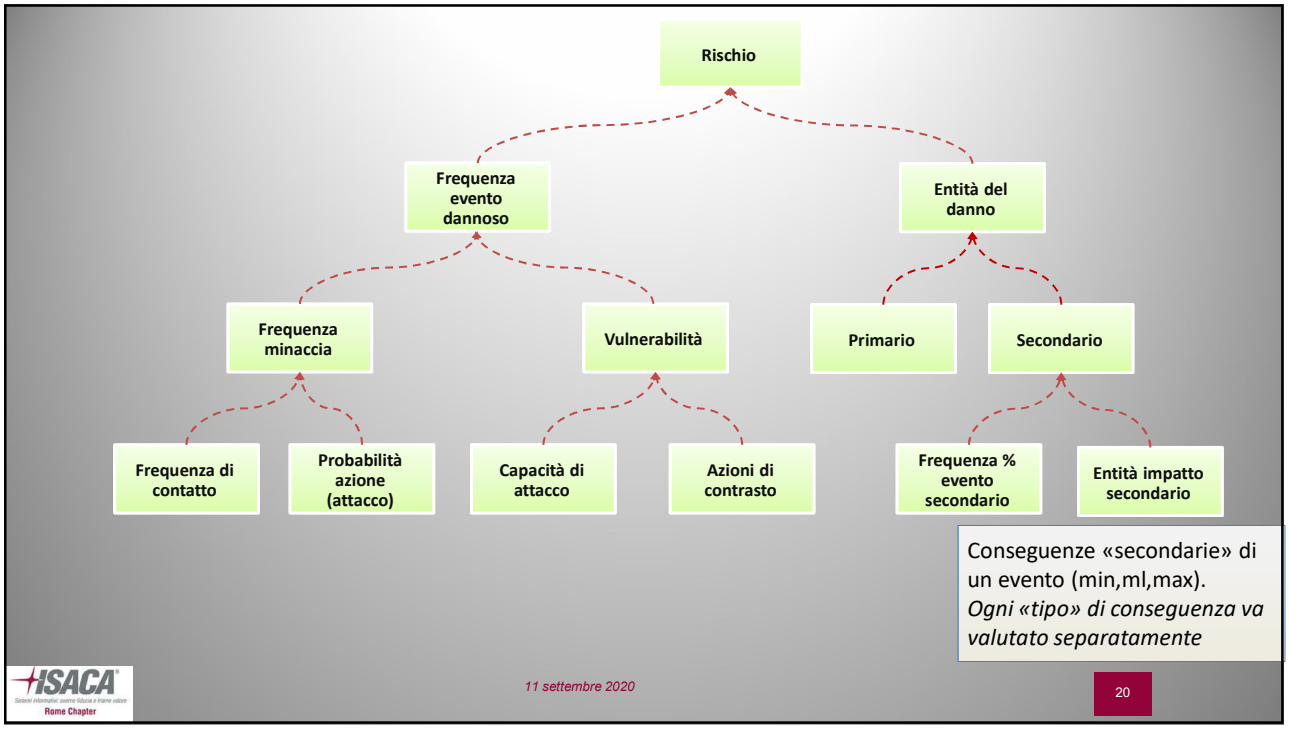
17


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Conseguenze «secondarie» di un evento (min,ml,max).
Ogni «tipo» di conseguenza va valutato separatamente
ISACA
Rome Chapter
11 settembre 2020
18

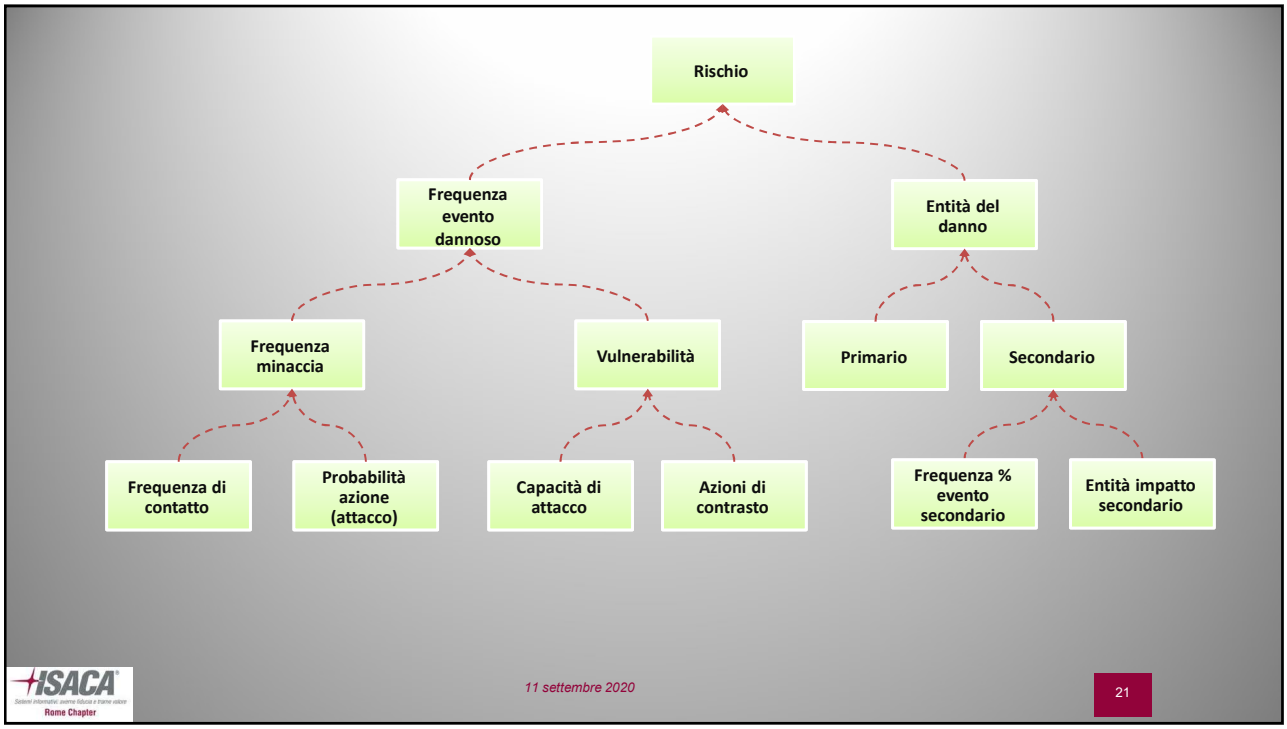
18


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
Percentuale di eventi che producono anche conseguenze secondarie
ISACA Rome Chapter
11 settembre 2020
19

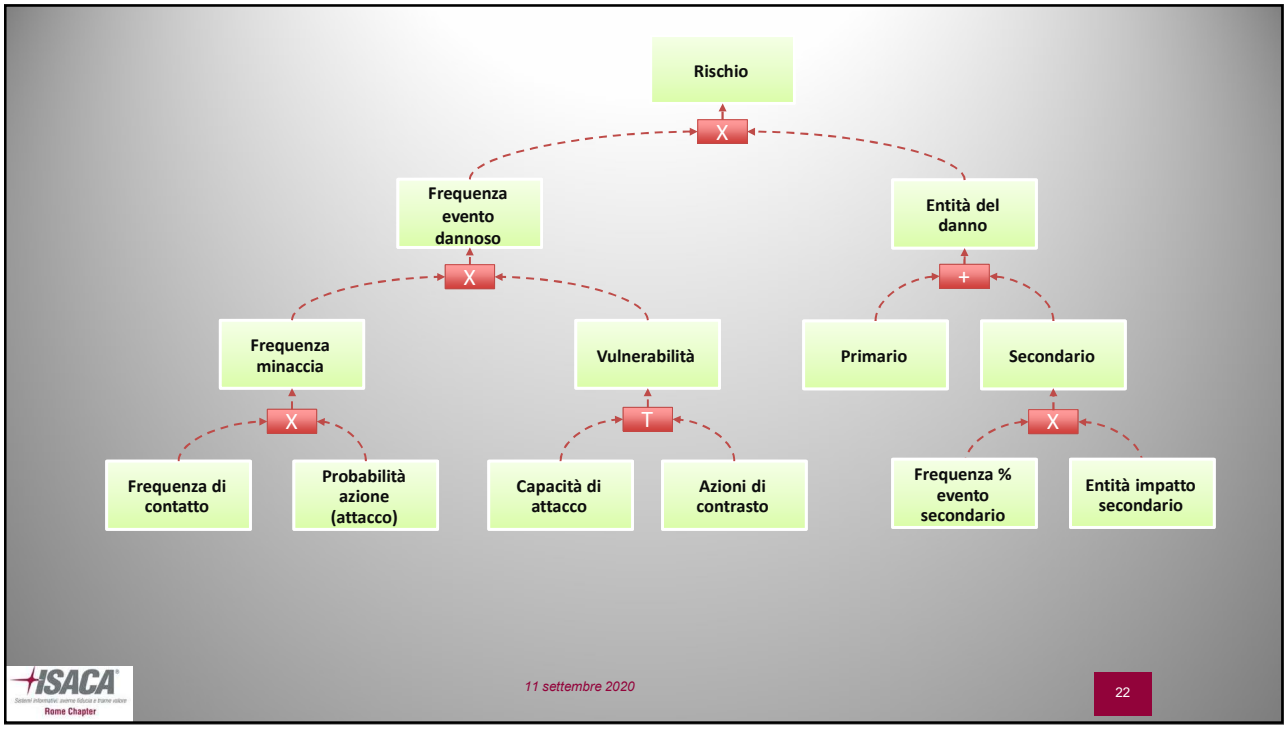
19


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
Conseguenze «secondarie» di un evento (min,ml,max).
Ogni «tipo» di conseguenza va valutato separatamente
ISACA Rome Chapter
11 settembre 2020
20

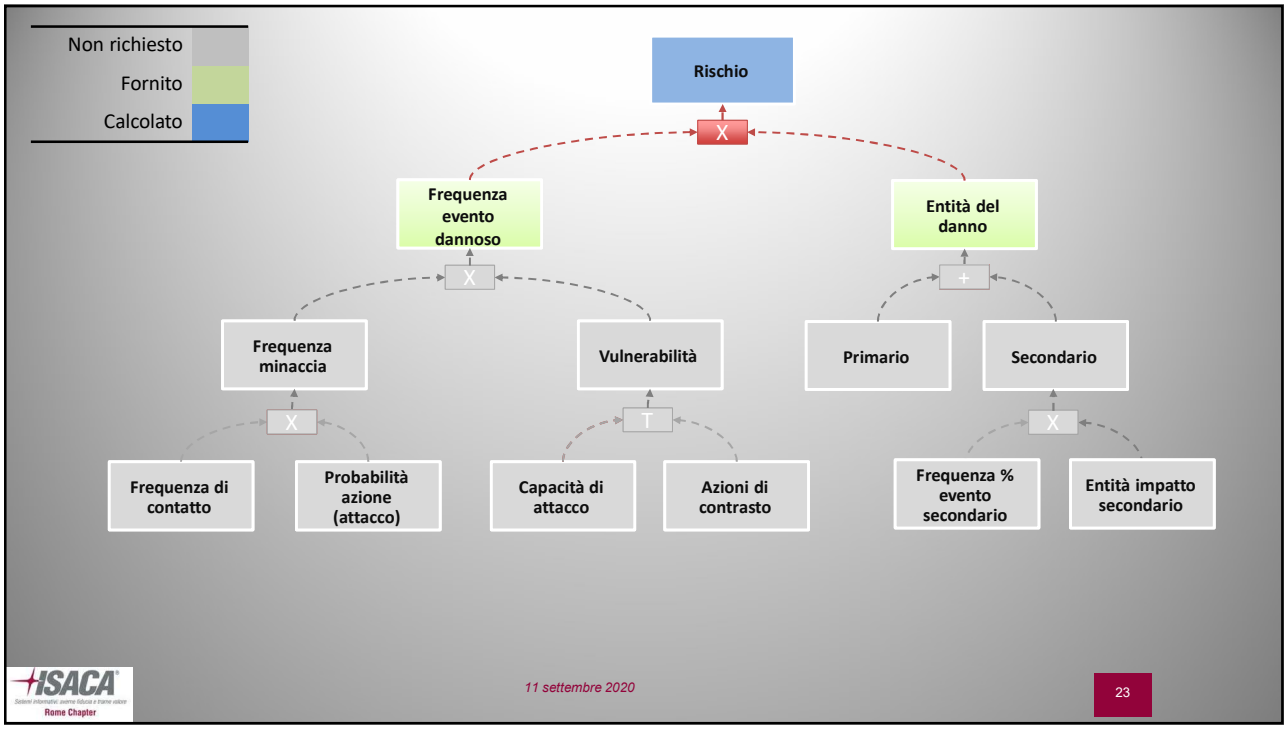
20


Rischio
Frequenza evento dannoso
Entità del danno
Frequenza minaccia
Vulnerabilità
Primario
Secondario
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
ISACA
Rome Chapter
11 settembre 2020
21

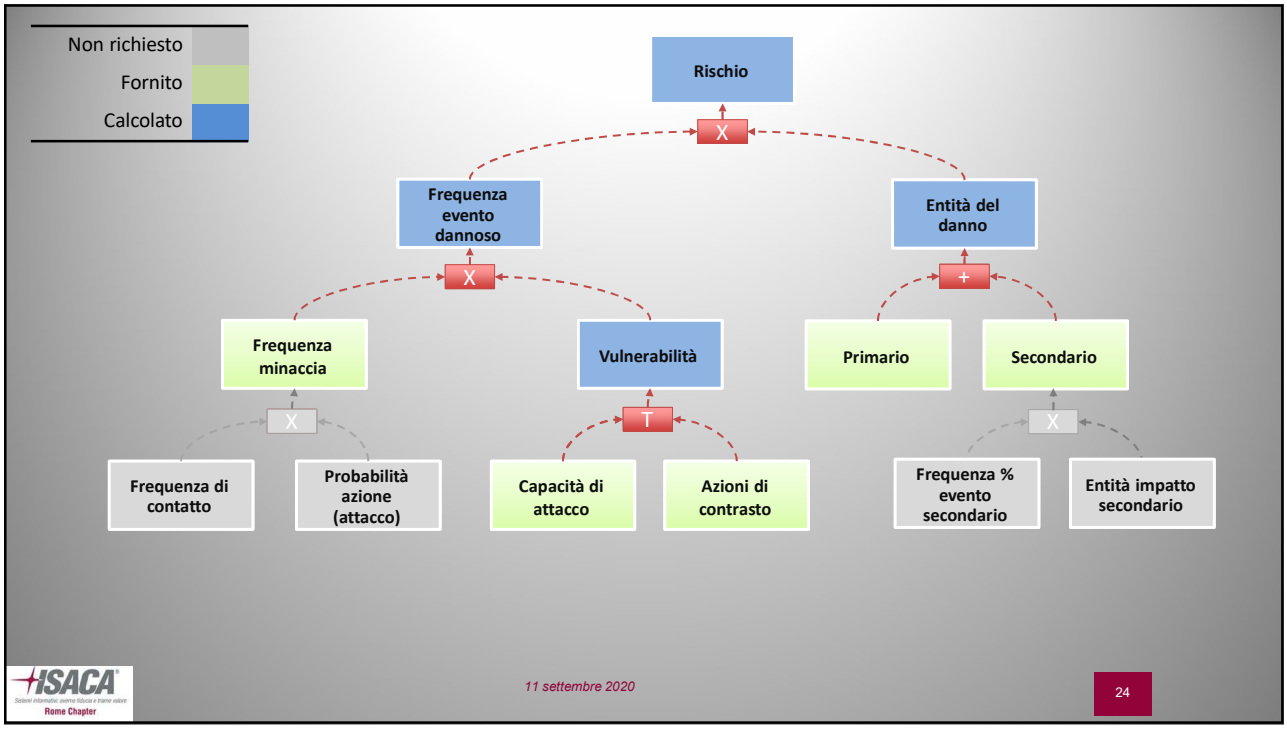
21


Rischio
X
Frequenza evento dannoso
Entità del danno
X
+
Frequenza minaccia
Vulnerabilità
Primario
Secondario
X
T
X
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
ISACA
Rome Chapter
11 settembre 2020
22

22


Non richiesto
Fornito
Calcolato
Rischio
X
Frequenza evento dannoso
Entità del danno
X
+
Frequenza minaccia
Vulnerabilità
Primario
Secondario
X
T
X
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
ISACA
Rome Chapter
11 settembre 2020
23

23


Non richiesto
Fornito
Calcolato
Rischio
X
Frequenza evento dannoso
Entità del danno
X
+
Frequenza minaccia
Vulnerabilità
Primario
Secondario
X
T
X
Frequenza di contatto
Probabilità azione (attacco)
Capacità di attacco
Azioni di contrasto
Frequenza % evento secondario
Entità impatto secondario
ISACA
Rome Chapter
11 settembre 2020
24

24

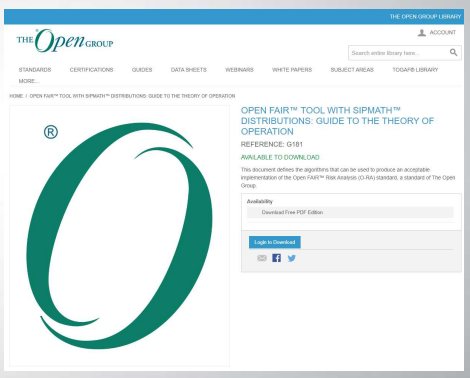
Dalla teoria alla pratica *(es: Excel®)*

Open Group Guide

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

THE Open GROUP

Scaricabile dal sito OpenGroup previa registrazione:



ISACA Rome Chapter

11 settembre 2020

25

25

Istruzioni dettagliate

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:

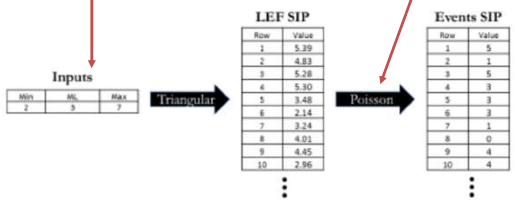
- Estimate – produce output based on direct user input
- Derive – produce output based only on data in the model

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

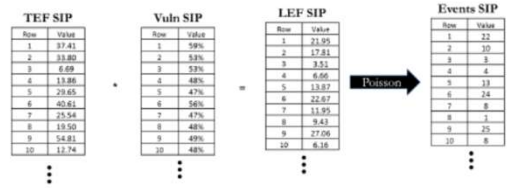
2.3.1 **Estimate LEF**

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.



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.



Or:

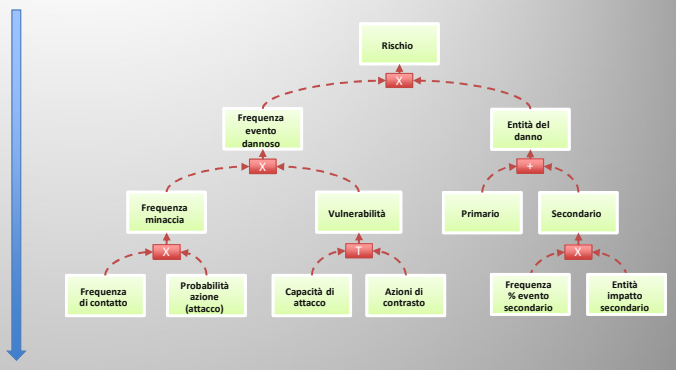
ISACA Rome Chapter

11 settembre 2020

26

Riassumendo

- Processo guidato e standardizzato di analisi e comunicazione
- Fornisce un modello strutturato del nostro livello di incertezza
- Evidenza i legami
- Ci si può fermare a qualsiasi livello
- Istruzioni pratiche dettagliate



ISACA Rome Chapter

11 settembre 2020

27

27

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

UN PO' DI TEORIA

1 1

1

Una 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.

ISACA Rome Chapter

11 settembre 2020

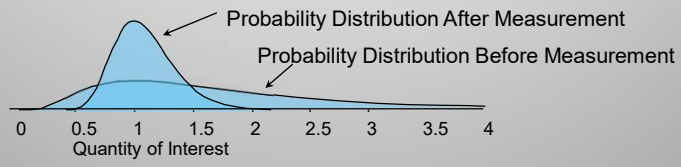
2

2

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.



ISACA Rome Chapter

11 settembre 2020

3

3

3

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.

ISACA Rome Chapter

4

4

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

ISACA Rome Chapter

11 settembre 2020

5

5

Due tipi di stima di probabilità

- Discreta (binaria) nell'arco di tempo
  - Lancio moneta
  - Data Breach
  - Blocco sistema
  - …
- Continua (Intervallo di confidenza: CI 90%)
  - Conseguenze Data Breach (€ $_{max-min}$)
  - Durata interruzione di servizio (t $_{max-min}$)
  - …

Due atteggiamenti

- **Ottimista**
- **Pessimista**

Il fenomeno è stato studiato (Psicologia delle Decisioni) a partire dagli anni '80: premio Nobel Scienze Economiche 2002.

Per ogni individuo l'atteggiamento relativo alle stime è abbastanza costante (prevale l'ottimismo)

Le ricerche hanno dimostrato che si può imparare a correggere la nostra attitudine «congenita», migliorando, in modo misurabile, la nostra capacità di stima

Esercizi di calibrazione (Corso ½ giornata)

ISACA Rome Chapter

11 settembre 2020

6

6

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

ISACA Rome Chapter

11 settembre 2020

7

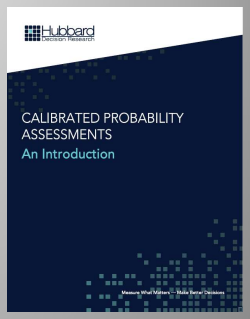
7

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

ISACA Rome Chapter

11 settembre 2020

8

8

Come esprimere l'incertezza ?

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

Oppure :

ma non :

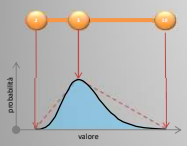
ISACA Rome Chapter

11 settembre 2020

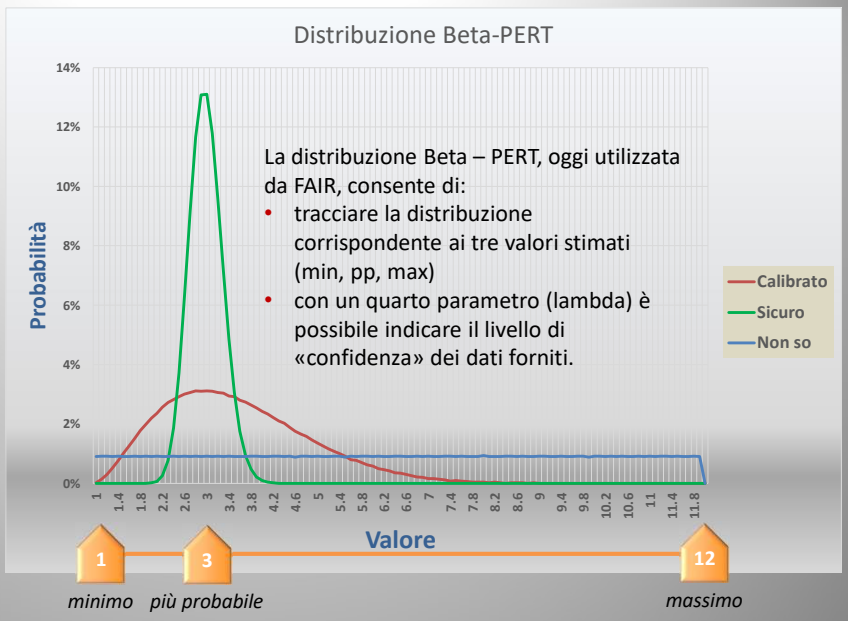
9

9

Da gamma a distribuzione



La distribuzione triangolare e la beta-Pert



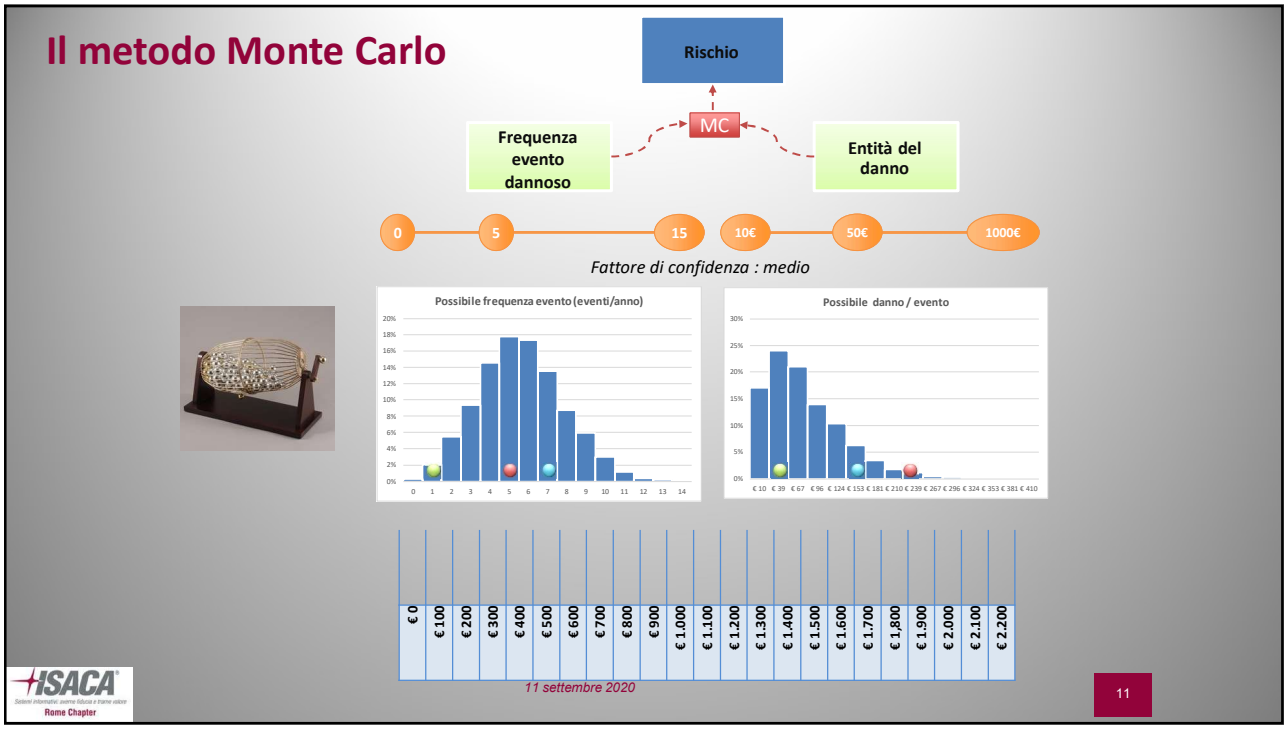
ISACA Rome Chapter

11 settembre 2020

10

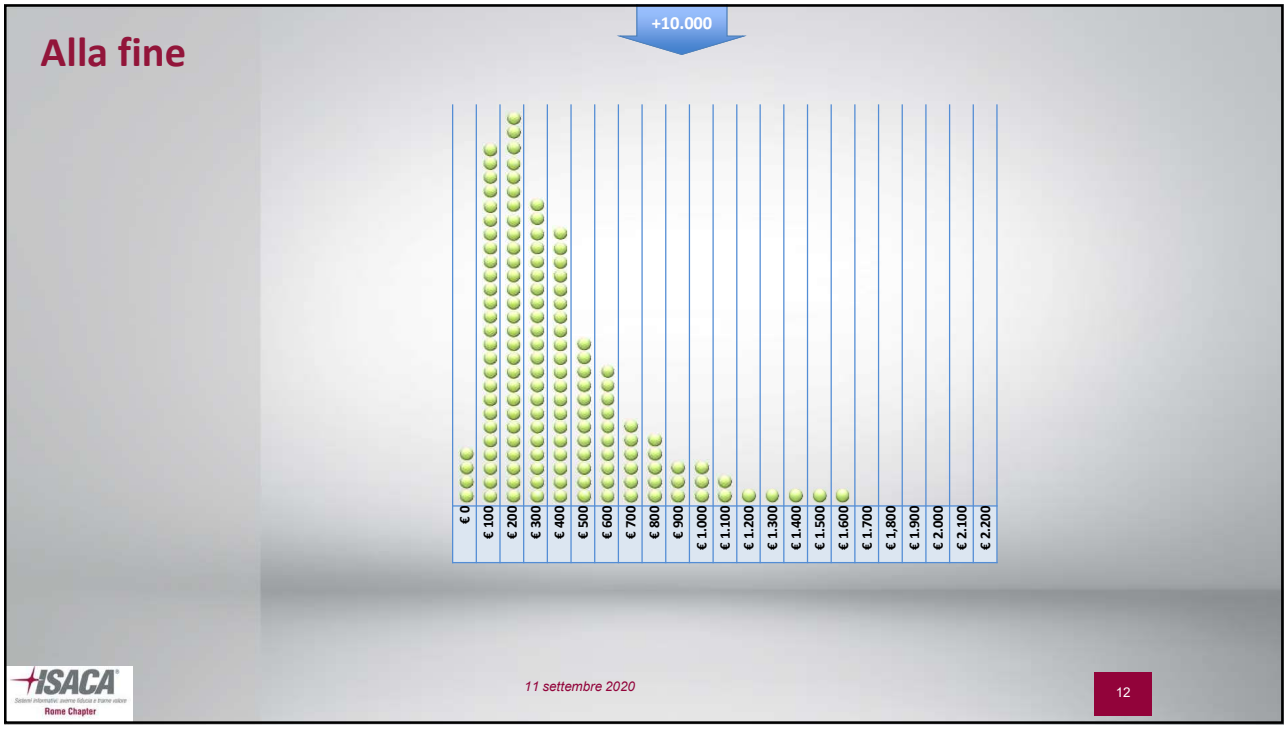
10

Il metodo Monte Carlo



11

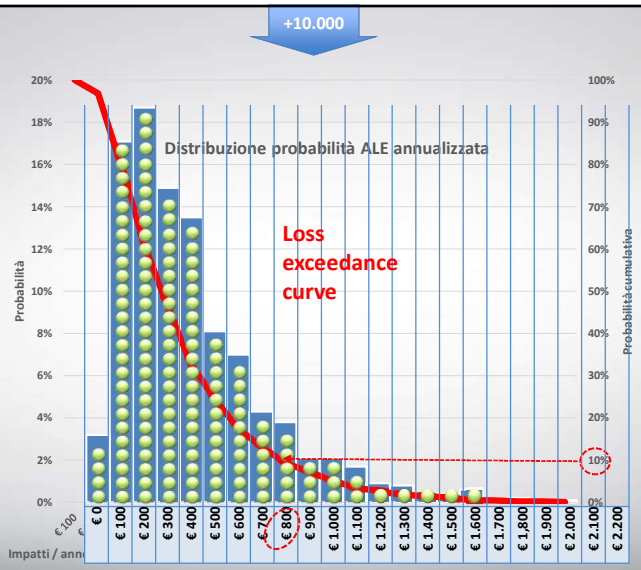
Alla fine



12

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



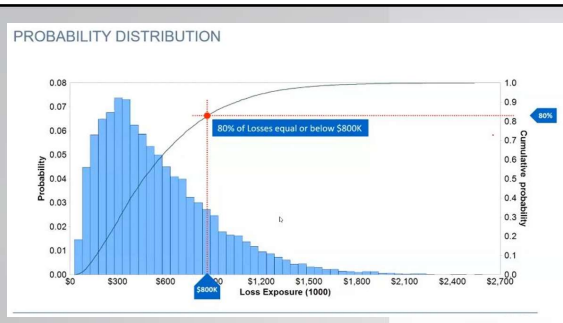
Analisi del rischio «quantitativa - statistica» !

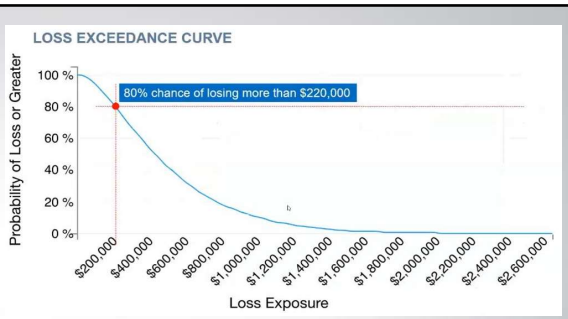
ISACA Rome Chapter

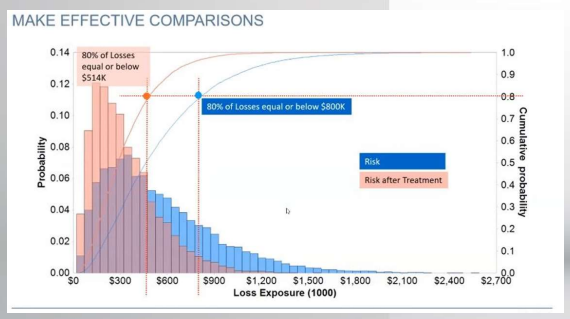
11 settembre 2020

13

13







ISACA Rome Chapter

Monte Carlo

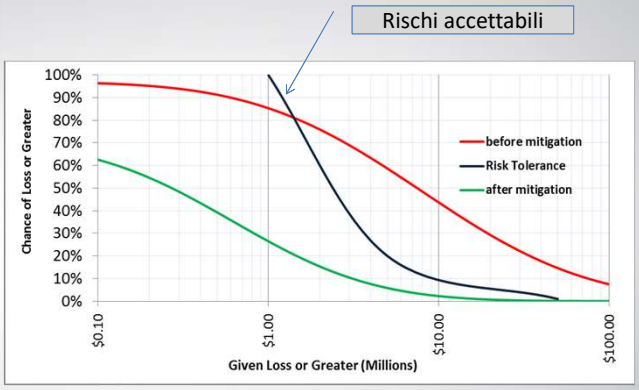
11 settembre 2020

14

14

Rischio accettabile

È esprimibile mediante una curva, confrontabile con le «Loss Exceedance curves»



ISACA Rome Chapter

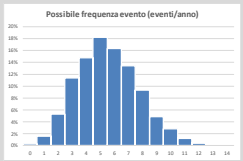
11 settembre 2020

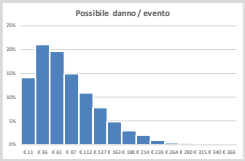
15

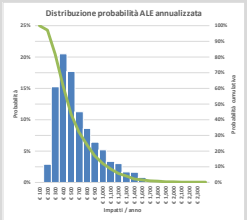
15

Il «costo» dell'incertezza

	Minimum	Most Likely	Maximum
Annualized Rate of Occurance	0	5	15
Single Loss Expectancy	€ 10	€ 50	€ 1,000



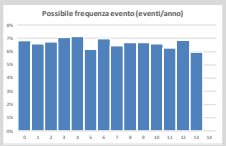


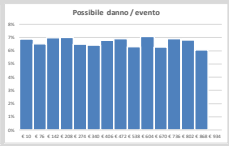


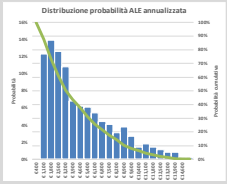
ALE annualizzato

min	€ 34
media	€ 485
in 10 anni >=	€ 954
in 10^2 anni >=	€ 1,580
in 10^3 anni >=	€ 1,977
in 10^4 anni >=	€ 2,288
in 10^5 anni >=	€ 2,290

Calibrato





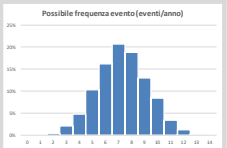


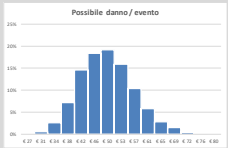
ALE annualizzato

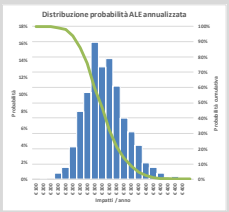
min	€ 1
media	€ 3,760
in 10 anni >=	€ 8,290
in 10^2 anni >=	€ 12,674
in 10^3 anni >=	€ 13,961
in 10^4 anni >=	€ 14,281
in 10^5 anni >=	€ 14,284

Incerto

Incompetente







ALE annualizzato

min	€ 127
media	€ 257
in 10 anni >=	€ 314
in 10^2 anni >=	€ 366
in 10^3 anni >=	€ 409
in 10^4 anni >=	€ 435
in 10^5 anni >=	€ 435

Sicuro

(dati storici ?)

La «non conoscenza» porta a scelte «cautelative»: che hanno un costo

ISACA Rome Chapter

11 settembre 20

6

16

Il Paradosso di AP

Si può dimostrare quantitativamente che una valutazione, almeno qualitativa, è necessaria

ISACA Rome Chapter

11 settembre 2020

17

17

Istruzioni dettagliate

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:

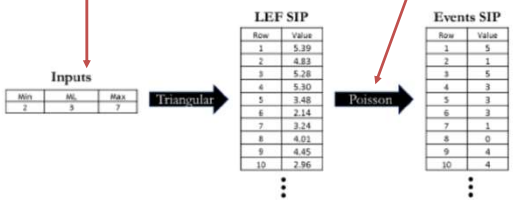
- Estimate – produce output based on direct user input
- Derive – produce output based only on data in the model

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

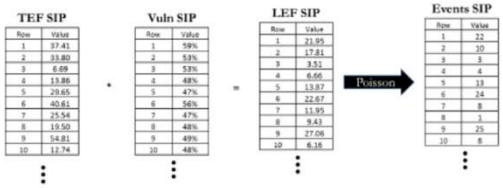
2.3.1 Estimate LEF

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.



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.

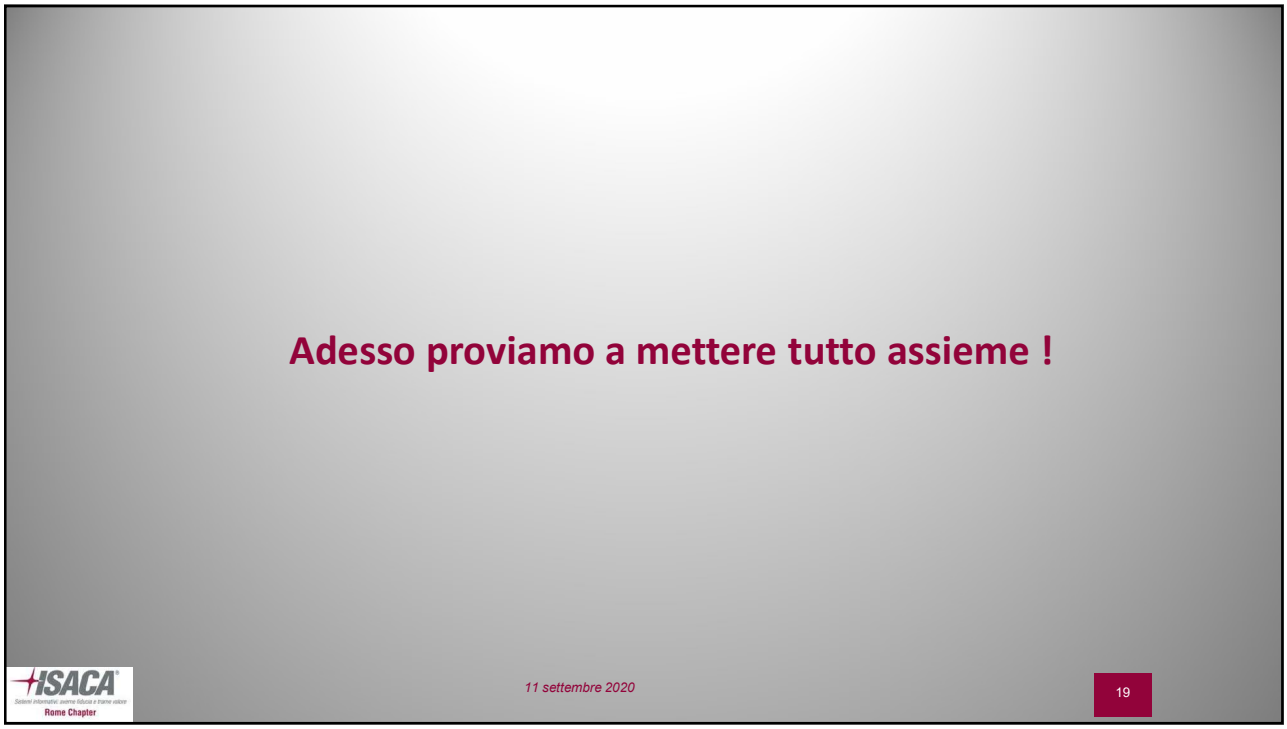


Or:

ISACA Rome Chapter

11 settembre 2020

18


Adesso proviamo a mettere tutto assieme !
ISACA
Rome Chapter
11 settembre 2020
19

19

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

T

IN PRATICA

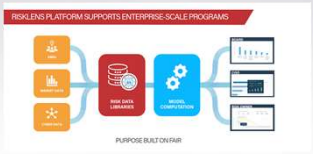
1 1

1

TOOLS FAIR

- RiskLens

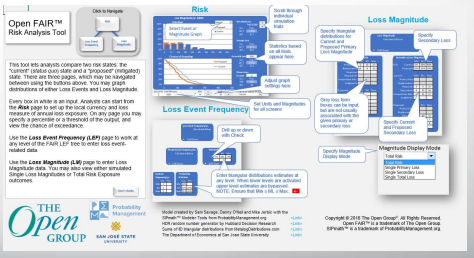
SaaS



Free training

- Open Group

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



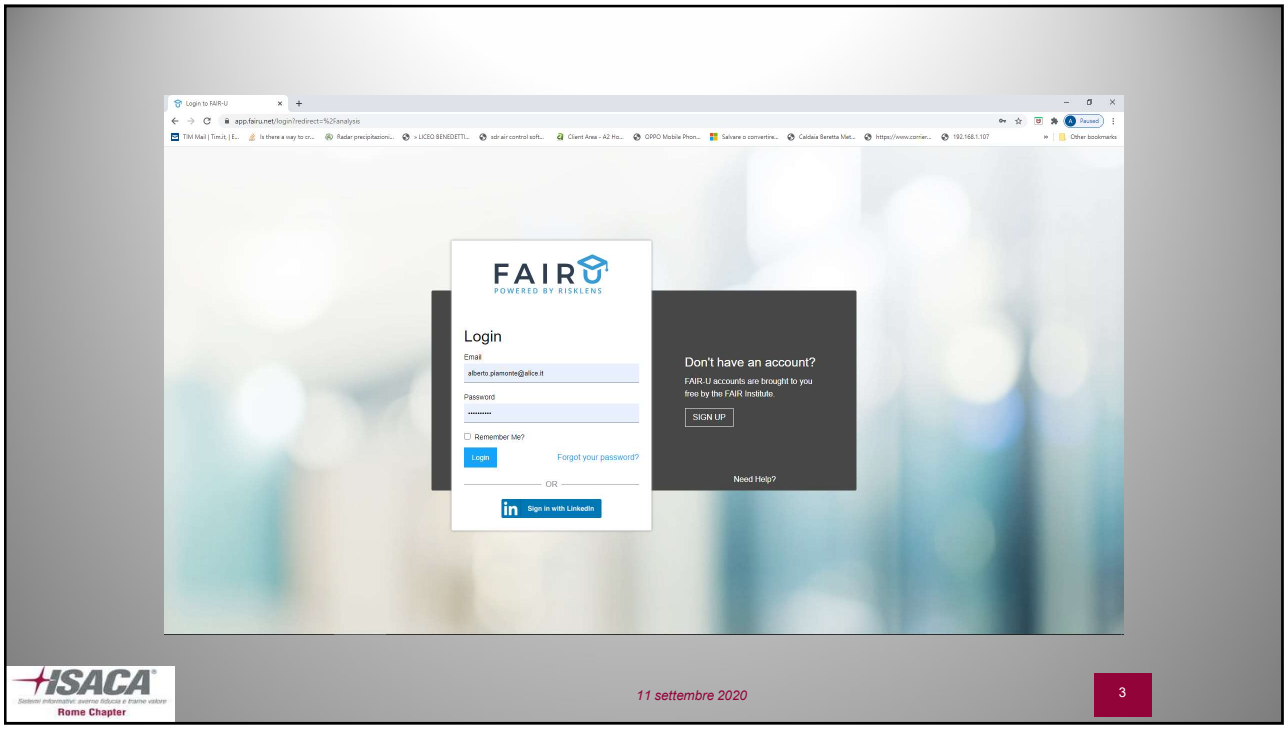
- Fogli EXCEL + tools (OPENPERT, ecc.)
- Python
- ……

ISACA Rome Chapter

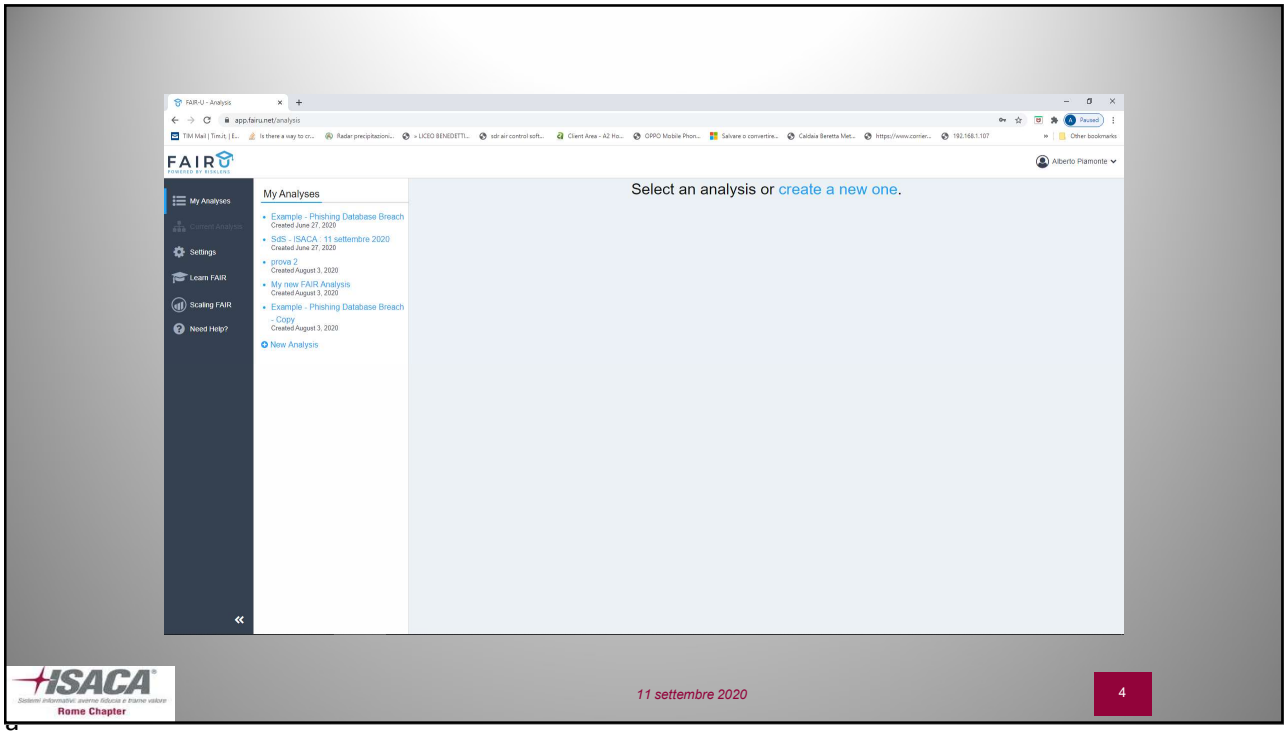
11 settembre 2020

2

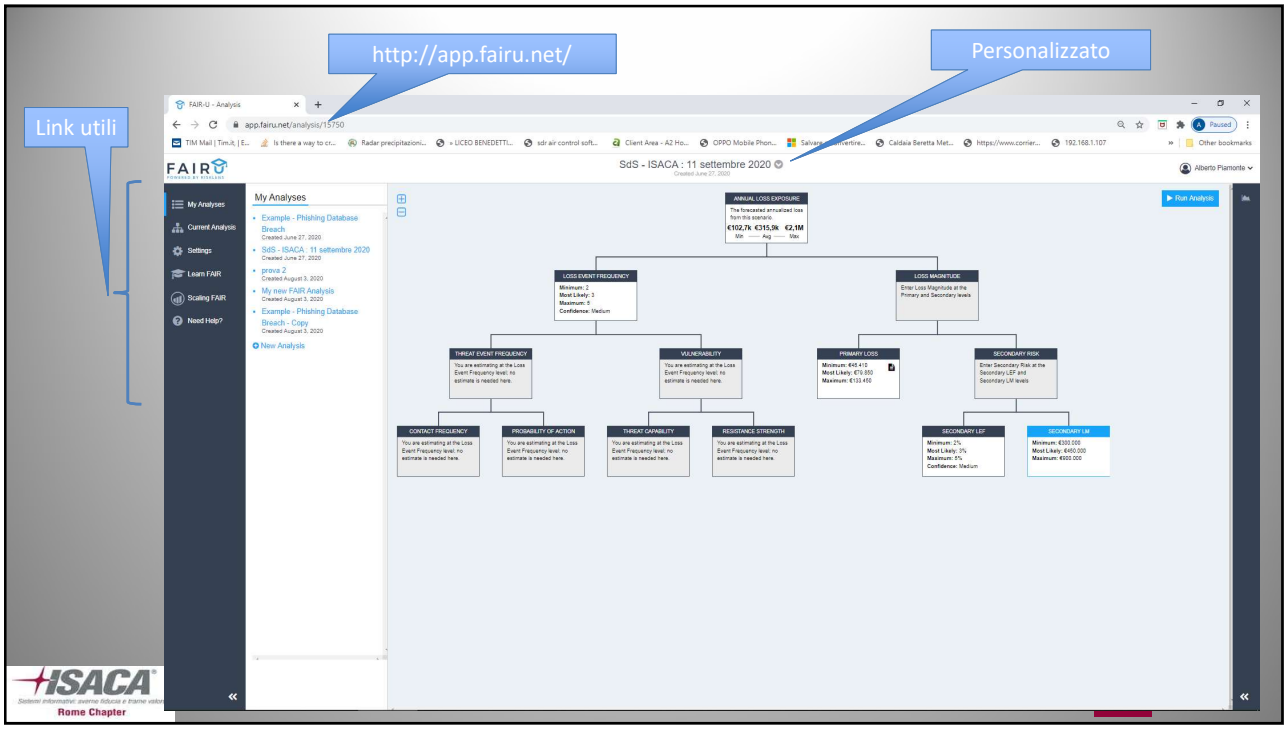
2


FAIR-U
POWERED BY RISKLENS
Login
Email
alberto.piamonte@alice.it
Password
Remember Me?
Login
Forgot your password?
OR
Sign in with LinkedIn
Don't have an account?
FAIR-U accounts are brought to you free by the FAIR Institute.
SIGN UP
Need Help?
ISACA
Rome Chapter
11 settembre 2020
3

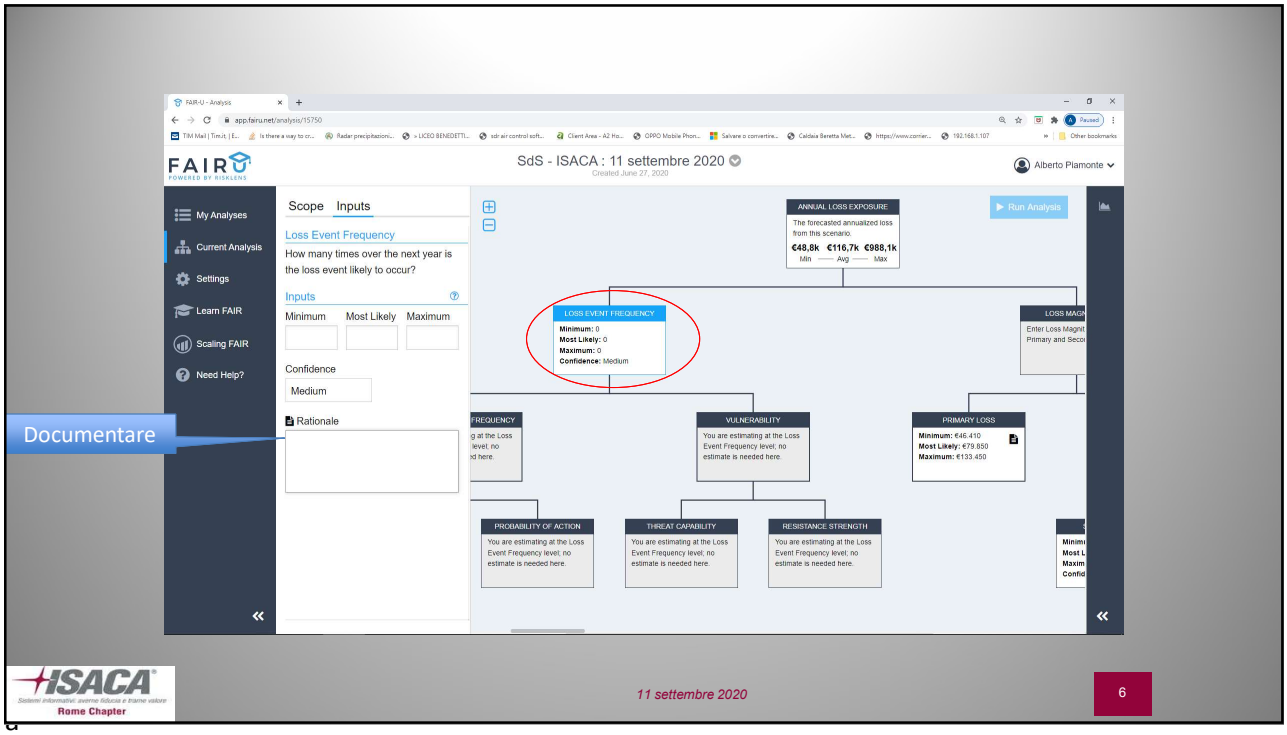
3


FAIR-U
Alberto Piamonte
My Analyses
Example - Phishing Database Breach
SdS - ISACA_11 settembre 2020
prova 2
My new FAIR Analysis
Example - Phishing Database Breach - Copy
New Analysis
Select an analysis or create a new one.
Settings
Learn FAIR
Scaling FAIR
Need Help?
ISACA
Rome Chapter
11 settembre 2020
4

4


http://app.fairu.net/
Personalizzato
Link utili
SdS - ISACA : 11 settembre 2020
My Analyses
Run Analysis
ANNUAL LOSS EXPOSURE
LOSS EVENT FREQUENCY
LOSS MAGNITUDE
THREAT EVENT FREQUENCY
VULNERABILITY
PRIMARY LOSS
SECONDARY RISK
CONTACT FREQUENCY
PROBABILITY OF ACTION
THREAT CAPABILITY
RESISTANCE STRENGTH
SECONDARY LEF
SECONDARY LM
ISACA
Rome Chapter

5


SdS - ISACA : 11 settembre 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Loss Event Frequency
How many times over the next year is the loss event likely to occur?
Inputs
Minimum
Most Likely
Maximum
Confidence
Medium
Rationale
Documentare
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€48,8k €116,7k €988,1k
Min Avg Max
Run Analysis
LOSS EVENT FREQUENCY
Minimum: 0
Most Likely: 0
Maximum: 0
Confidence: Medium
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
PROBABILITY OF ACTION
THREAT CAPABILITY
RESISTANCE STRENGTH
ISACA
Rome Chapter
11 settembre 2020
6

6

Stima del LEF

- Gli esperti hanno stimato che le probabilità di attacco Ransomware nei prossimi anni sono :

LEF		
Min	ML	Max
2	3	5

- Nella realtà si potrebbe sentire il parere di più SME's per mediare le loro stime:

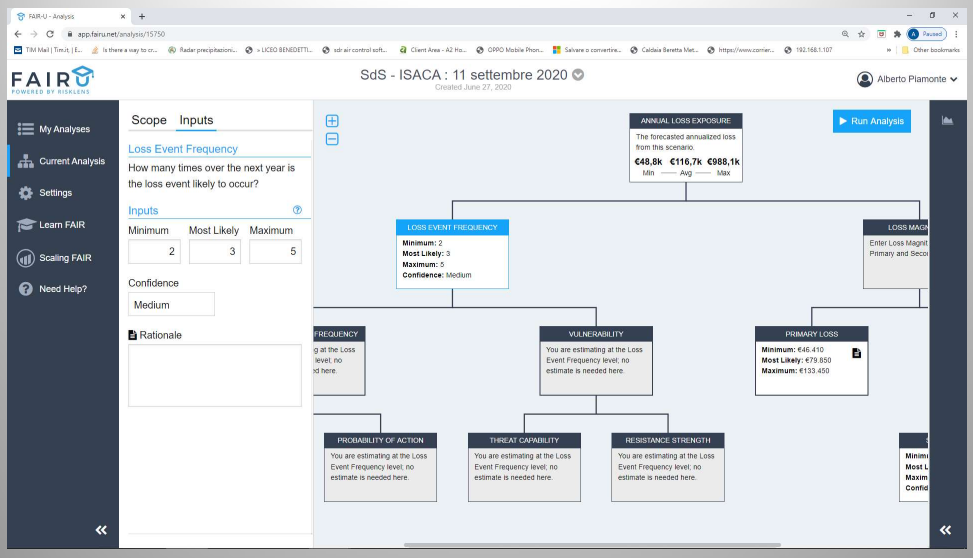
	Min	ML	Max
SME1	2	15	25
SME2	4	12	22
SME3	3	17	30
Media	3	14.6	25.6

ISACA Rome Chapter

11 settembre 2020

7

7



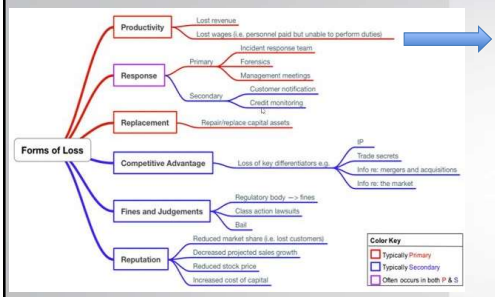
ISACA Rome Chapter

11 settembre 2020

8

8

Perdita di produttività impiegati non attivi

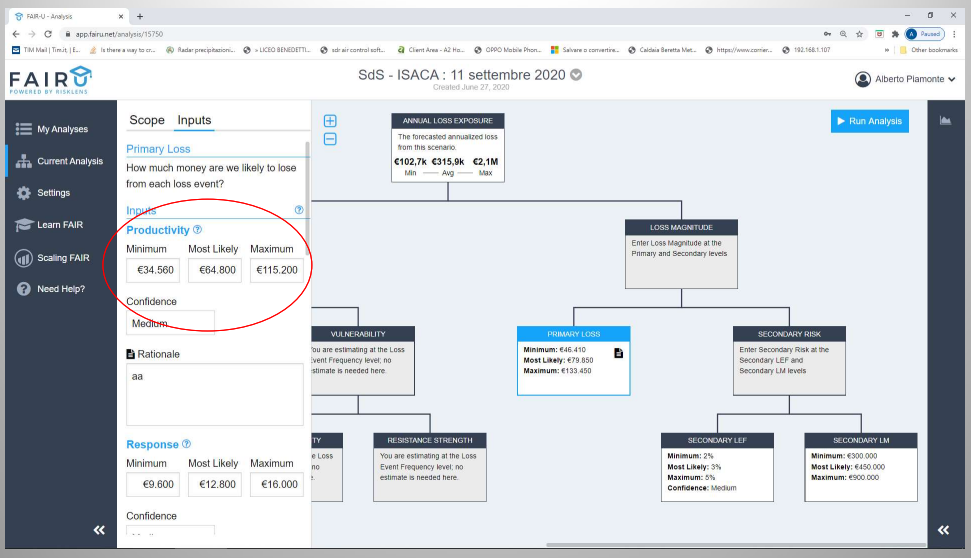


		Min	Più probabile	Max
Produttività (perdita)	Costo annuo	€ 50,000	€ 70,000	€ 100,000
	Giornate lavorative	260	260	260
	Costo/giorno	€ 192	€ 269	€ 385
	Perdita produttività %	60%	60%	60%
	# impiegati	50	50	50
	Costo giorno non produttività	€ 5,769	€ 8,077	€ 11,538
	Giorni non produttivi	6	8	10
	Totale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

ISACA Rome Chapter

11 settembre 2020 9

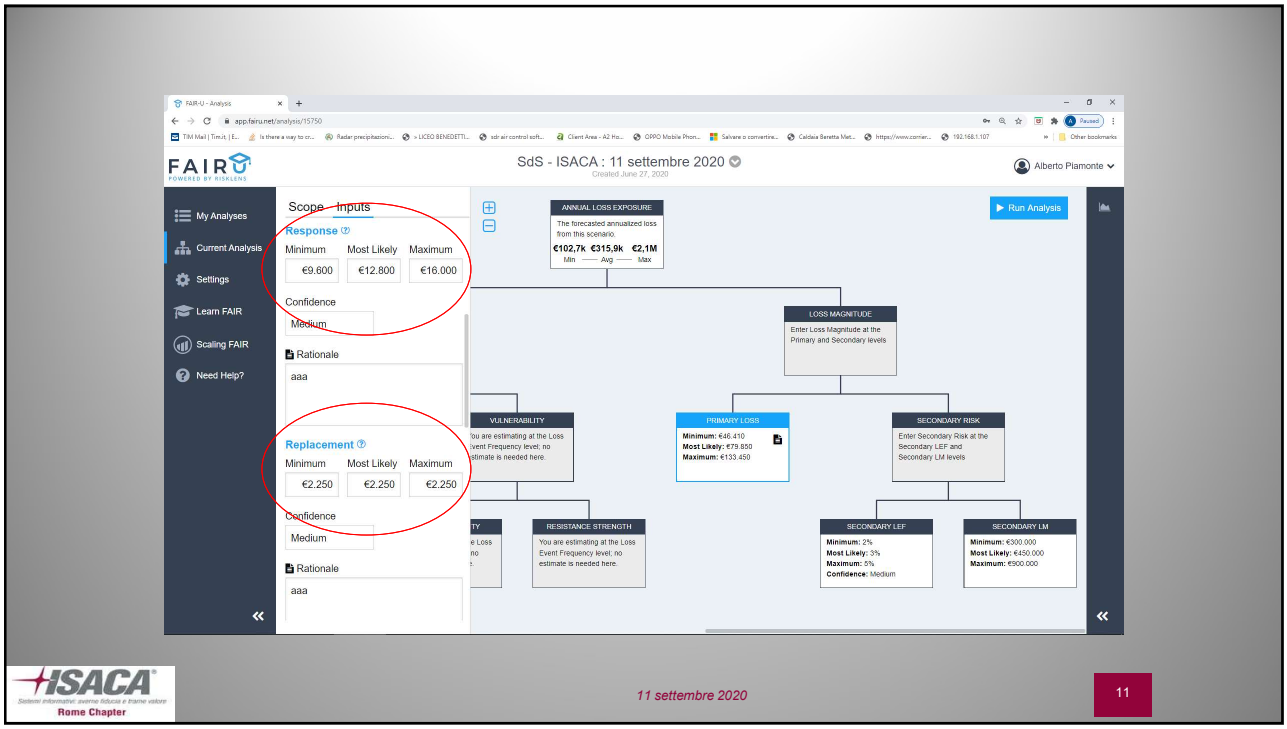
9



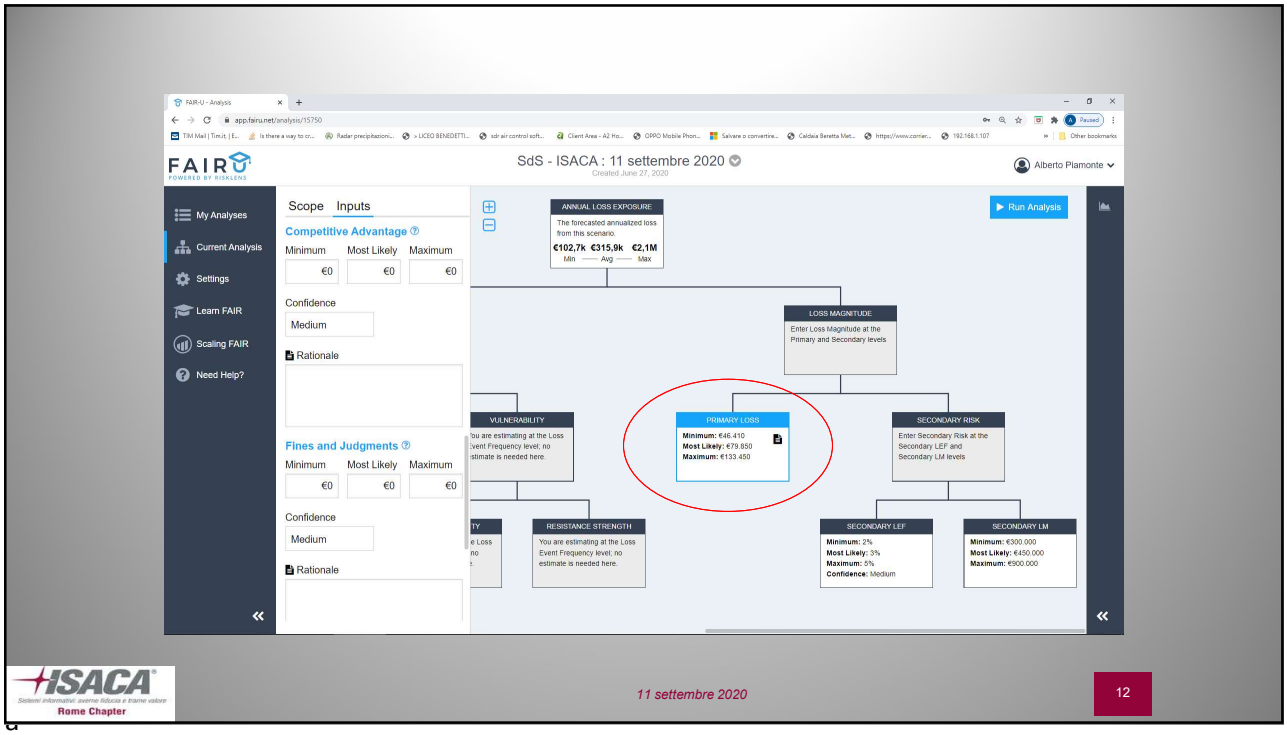
ISACA Rome Chapter

11 settembre 2020 10

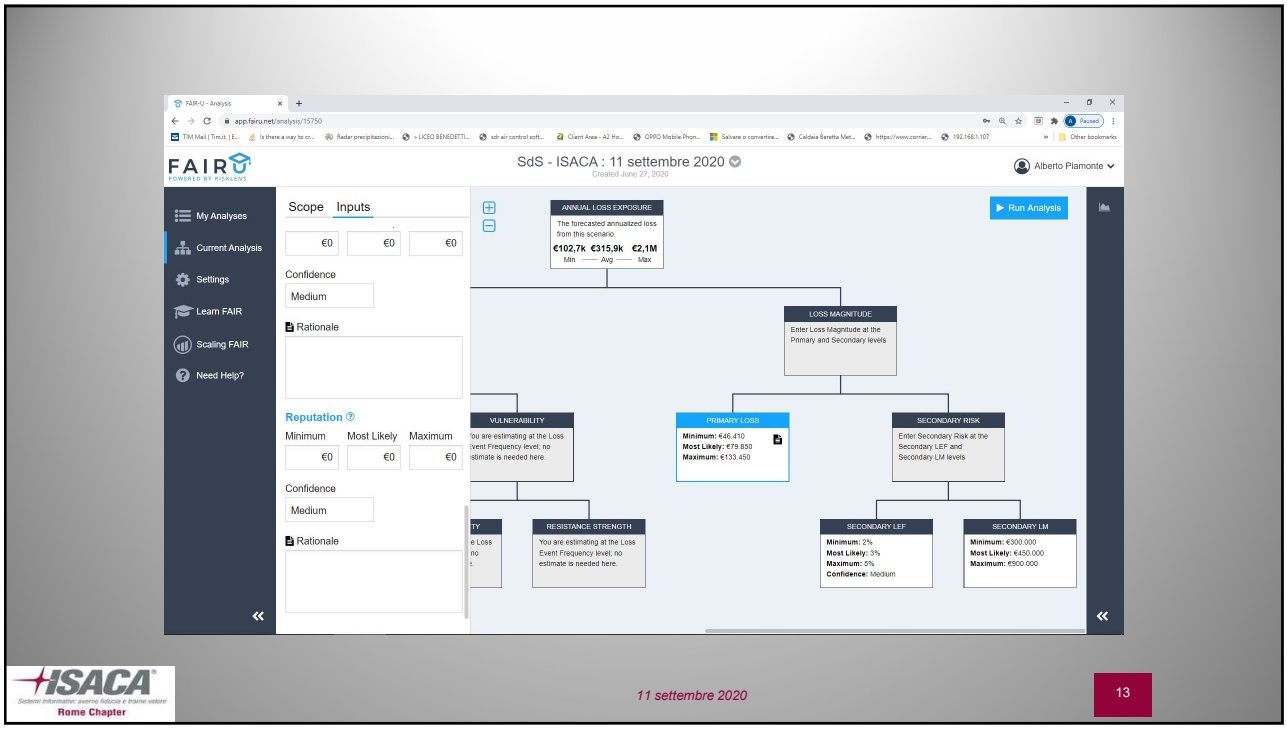
10


FAIR
SdS - ISACA : 11 settembre 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Response
Minimum
Most Likely
Maximum
€9.600
€12.800
€16.000
Confidence
Medium
Rationale
aaa
Replacement
Minimum
Most Likely
Maximum
€2.250
€2.250
€2.250
Confidence
Medium
Rationale
aaa
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€102,7k €315,9k €2,1M
Min Avg Max
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
VULNERABILITY
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
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
ISACA
Rome Chapter
11 settembre 2020
11

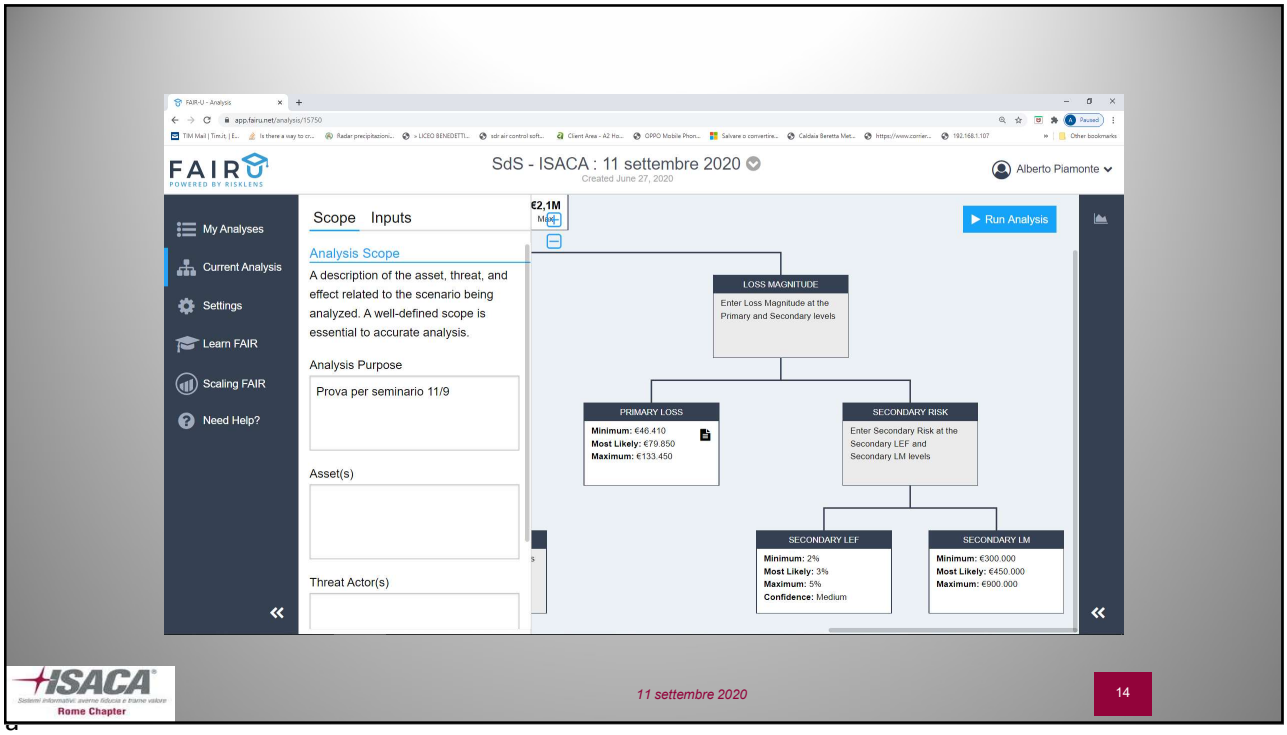
11


FAIR
SdS - ISACA : 11 settembre 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Competitive Advantage
Minimum
Most Likely
Maximum
€0
€0
€0
Confidence
Medium
Rationale
Fines and Judgments
Minimum
Most Likely
Maximum
€0
€0
€0
Confidence
Medium
Rationale
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€102,7k €315,9k €2,1M
Min Avg Max
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
VULNERABILITY
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
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
ISACA
Rome Chapter
11 settembre 2020
12

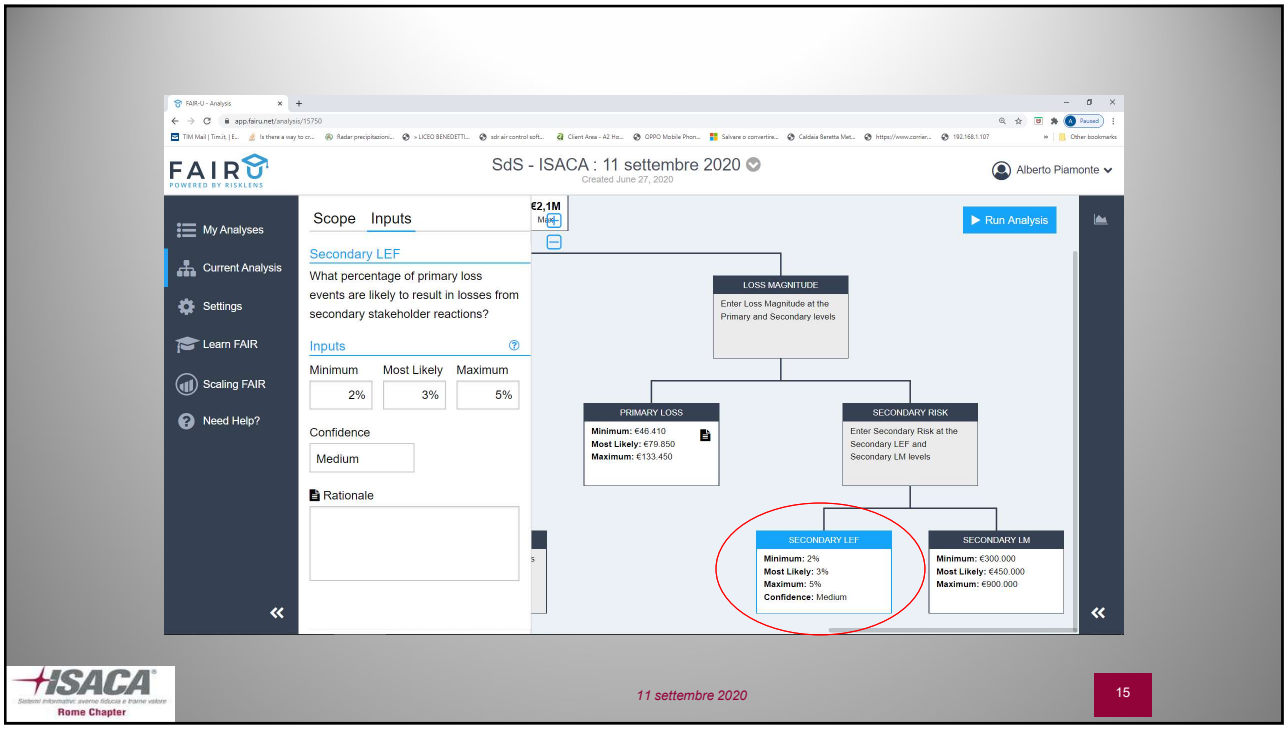
12


FAIR
SdS - ISACA : 11 settembre 2020
Created June 27, 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Confidence
Medium
Rationale
Reputation
Minimum
Most Likely
Maximum
Confidence
Medium
Rationale
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
€102,7k €315,9k €2,1M
Min Avg Max
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
VULNERABILITY
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
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

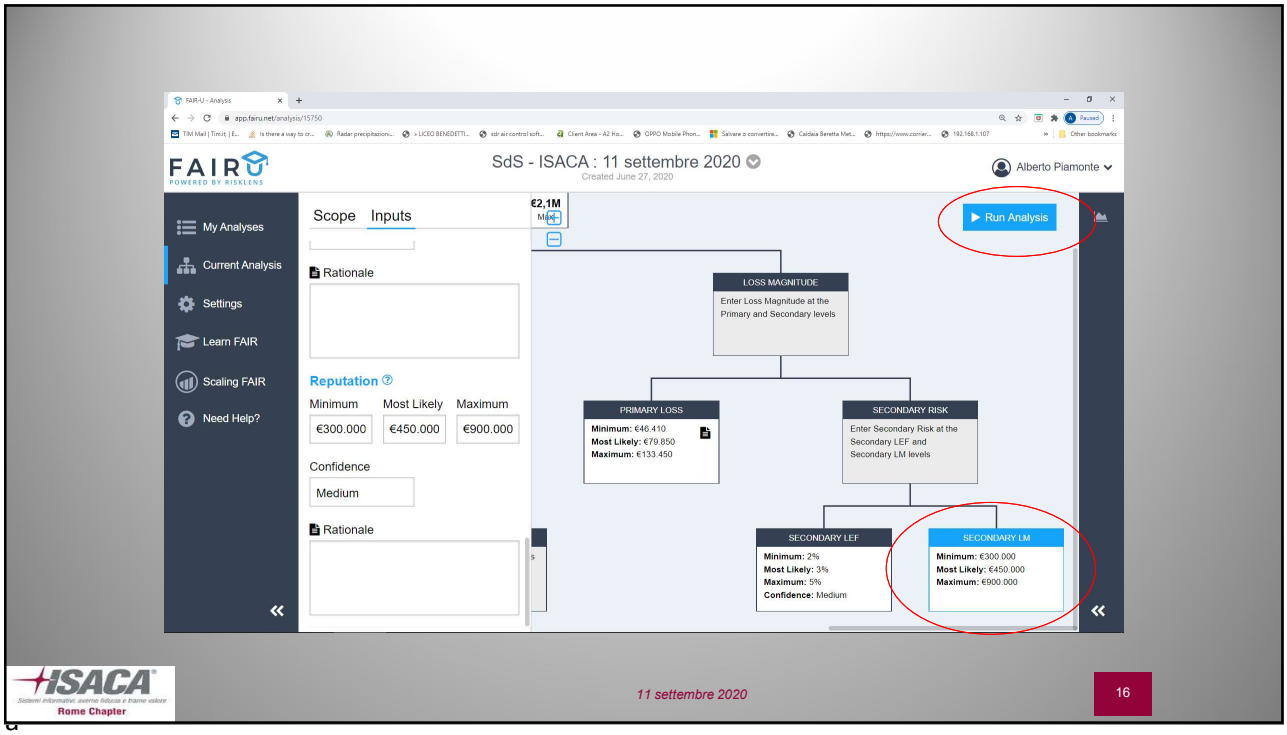
13


FAIR
SdS - ISACA : 11 settembre 2020
Created June 27, 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Analysis Scope
A description of the asset, threat, and effect related to the scenario being analyzed. A well-defined scope is essential to accurate analysis.
Analysis Purpose
Prova per seminario 11/9
Asset(s)
Threat Actor(s)
€2,1M
Max
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
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
SECONDARY LEF
Minimum: 2%
Most Likely: 3%
Maximum: 5%
Confidence: Medium
SECONDARY LM
Minimum: €300.000
Most Likely: €450.000
Maximum: €900.000

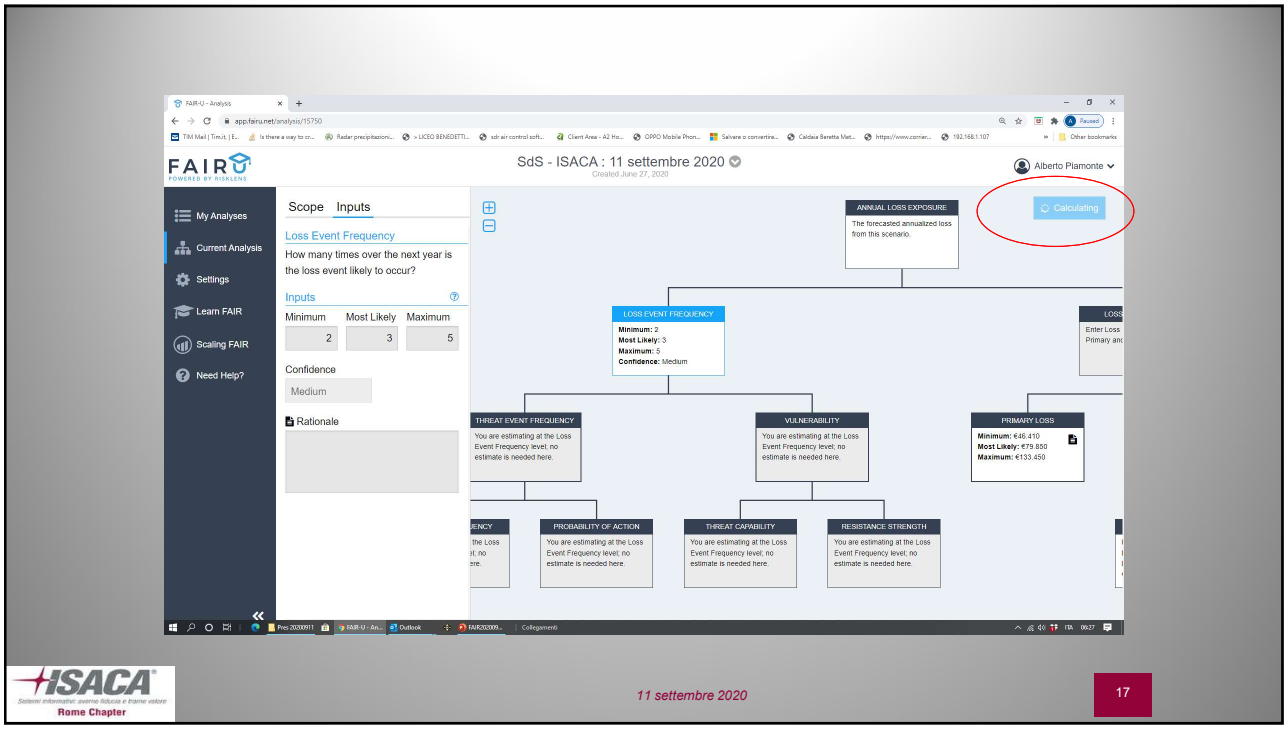
14


FAIR
SdS - ISACA : 11 settembre 2020
Created June 27, 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Secondary LEF
What percentage of primary loss events are likely to result in losses from secondary stakeholder reactions?
Inputs
Minimum
Most Likely
Maximum
2%
3%
5%
Confidence
Medium
Rationale
€2,1M
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
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
SECONDARY LEF
Minimum: 2%
Most Likely: 3%
Maximum: 5%
Confidence: Medium
SECONDARY LM
Minimum: €300.000
Most Likely: €450.000
Maximum: €900.000
ISACA
Rome Chapter
11 settembre 2020
15

15

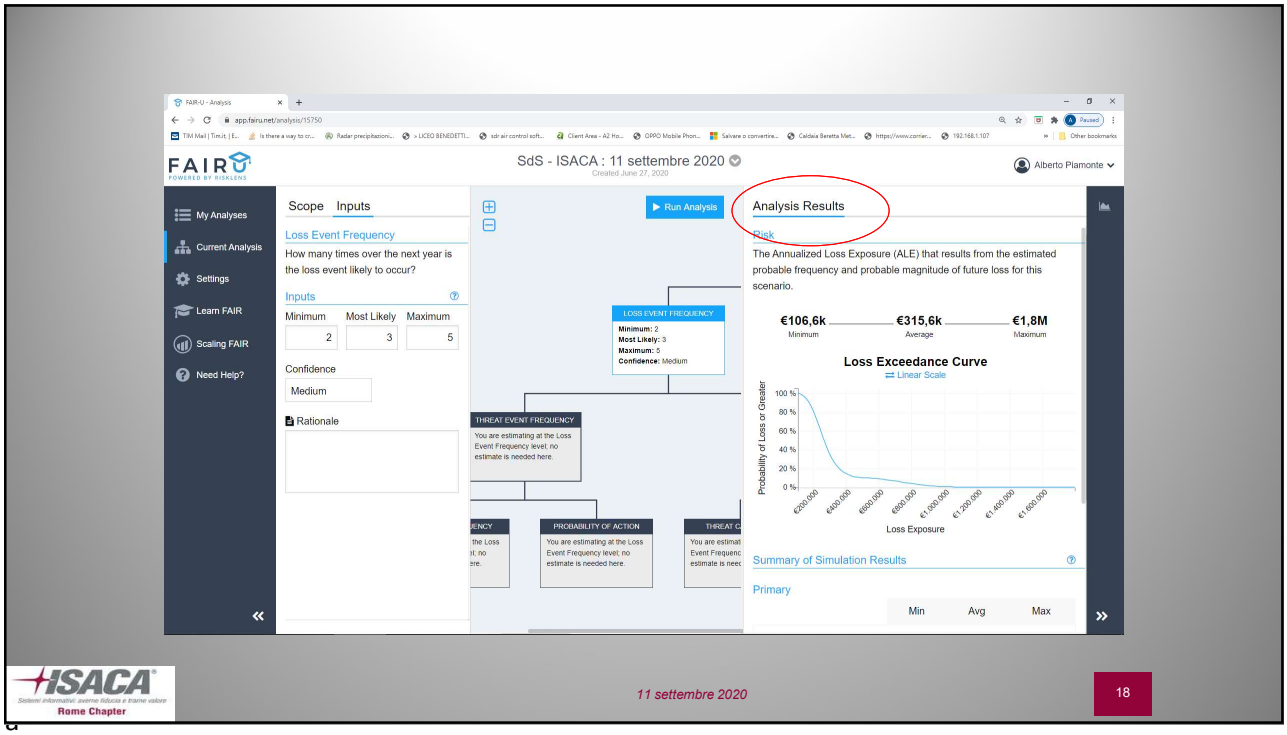

FAIR
SdS - ISACA : 11 settembre 2020
Created June 27, 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Rationale
Reputation
Minimum
Most Likely
Maximum
€300.000
€450.000
€900.000
Confidence
Medium
Rationale
€2,1M
Run Analysis
LOSS MAGNITUDE
Enter Loss Magnitude at the Primary and Secondary levels
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
SECONDARY LEF
Minimum: 2%
Most Likely: 3%
Maximum: 5%
Confidence: Medium
SECONDARY LM
Minimum: €300.000
Most Likely: €450.000
Maximum: €900.000
ISACA
Rome Chapter
11 settembre 2020
16

16



ISACA Rome Chapter

17



ISACA Rome Chapter

18

Sommario risultati analisi

Analysis Results

€98,7k	€314,4k	€1,8M
Minimum	Average	Maximum

Loss Exceedance Curve

Linear Scale

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	2	3,17	5
Loss Magnitude	€49,3k	€83,1k	€126,6k

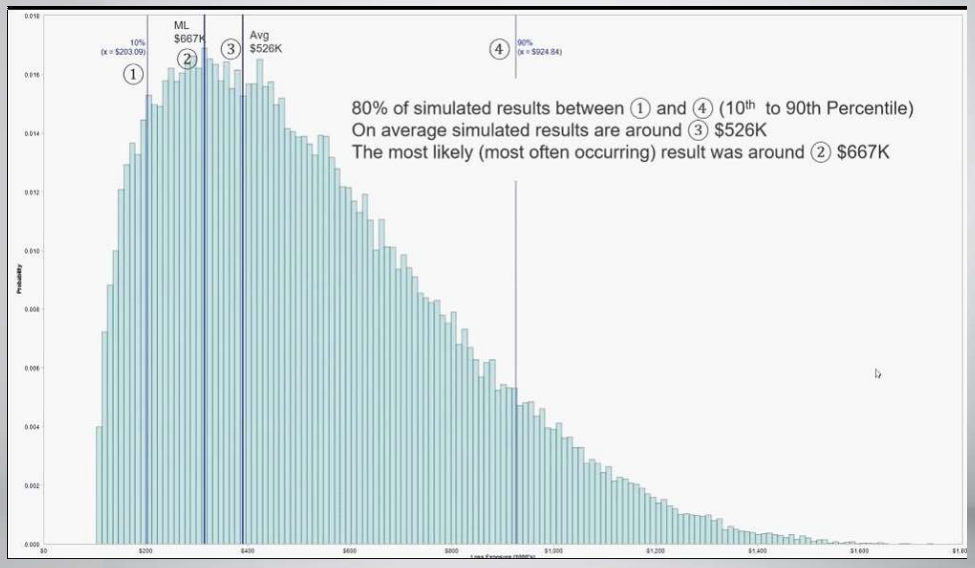
Secondary

	Min	Avg	Max
Loss Events / Year	0	0,1	2
Loss Magnitude	€300,7k	€498,5k	€860,1k

ISACA Rome Chapter

19

19



ISACA Rome Chapter

11 settembre 2020

20

20

TREATMENT OPTION 1: UPGRADE ENDPOINT SECURITY

- Replacing AV with "Next generation Endpoint protection" will have what impact?

ISACA Rome Chapter

21

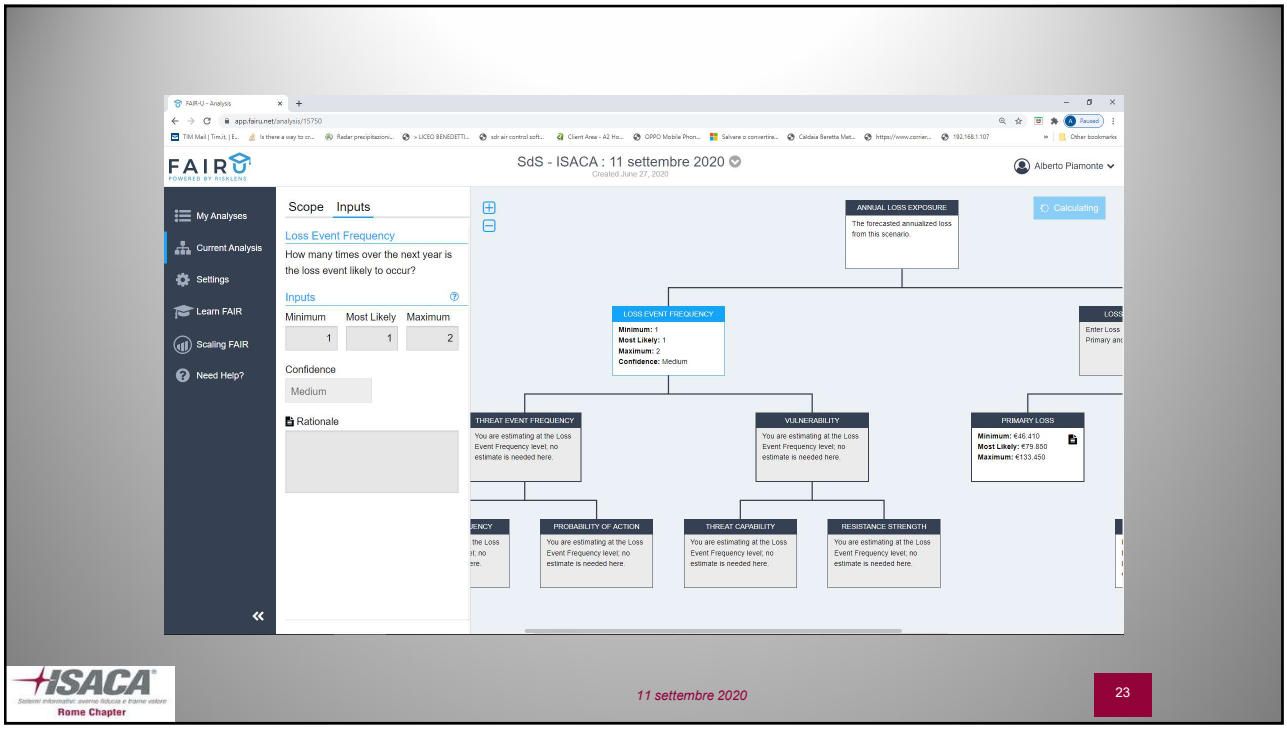
Pianifichiamo un miglioramento

- Proviamo a sostituire gli antivirus attuali (AV) con quelli di nuova generazione (NGAV) e stimiamo la riduzione della LEF

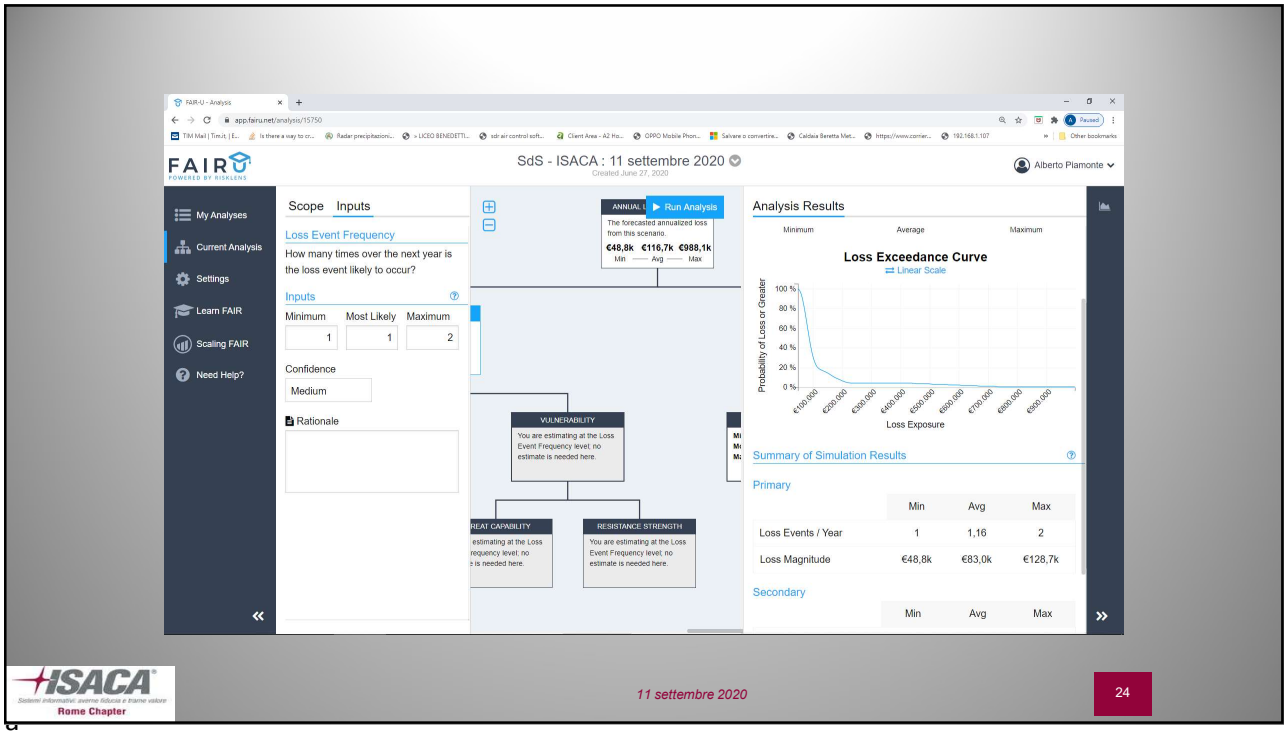
LEF		
Min	ML	Max
2	3	5
1	1	2

ISACA Rome Chapter

22


FAIR
SdS - ISACA : 11 settembre 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Loss Event Frequency
How many times over the next year is the loss event likely to occur?
Inputs
Minimum
Most Likely
Maximum
1
1
2
Confidence
Medium
Rationale
ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
Calculating
LOSS EVENT FREQUENCY
Minimum: 1
Most Likely: 1
Maximum: 2
Confidence: Medium
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
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.
ISACA
Rome Chapter
11 settembre 2020
23

23


FAIR
SdS - ISACA : 11 settembre 2020
Alberto Piamonte
My Analyses
Current Analysis
Settings
Learn FAIR
Scaling FAIR
Need Help?
Scope
Inputs
Loss Event Frequency
How many times over the next year is the loss event likely to occur?
Inputs
Minimum
Most Likely
Maximum
1
1
2
Confidence
Medium
Rationale
Run Analysis
The forecasted annualized loss from this scenario.
€48,8k €116,7k €988,1k
Min Avg Max
VULNERABILITY
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.
Analysis Results
Minimum
Average
Maximum
Loss Exceedance Curve
Linear Scale
Probability of Loss or Greater
100 %
80 %
60 %
40 %
20 %
0 %
€100.000
€200.000
€300.000
€400.000
€500.000
€600.000
€700.000
€800.000
€900.000
Loss Exposure
Summary of Simulation Results
Primary
Min Avg Max
Loss Events / Year 1 1,16 2
Loss Magnitude €48,8k €83,0k €128,7k
Secondary
Min Avg Max
ISACA
Rome Chapter
11 settembre 2020
24

24

Current State				After treatment			
$96.4k Minimum	$314.3k Average		$1.8M Maximum	$48.2k Minimum	$116.3k Average		$990.1k Maximum
Primary				Primary			
	Min	Avg	Max		Min	Avg	Max
Loss Events / Year	2	3.18	5	Loss Events / Year	1	1.17	2
Loss Magnitude	$47.7k	$83.2k	$127.7k	Loss Magnitude	$48.2k	$83.3k	$128.7k
Secondary				Secondary			
	Min	Avg	Max		Min	Avg	Max
Loss Events / Year	0	0.1	2	Loss Events / Year	0	0.04	1
Loss Magnitude	$301.9k	$501.4k	$864.8k	Loss Magnitude	$302.3k	$501.5k	$849.4k

ISACA Rome Chapter

11 settembre 2020

25

25

Potremmo analizzare altre soluzioni che agiscono anche sull'entità del danno

- Servizio Cloud per *restore* istantaneo

		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

Si riducono i giorni non produttivi a 1h max

- *«Controlled folder»* (accessibile solo da processi autorizzati)

ISACA Rome Chapter

11 settembre 2020

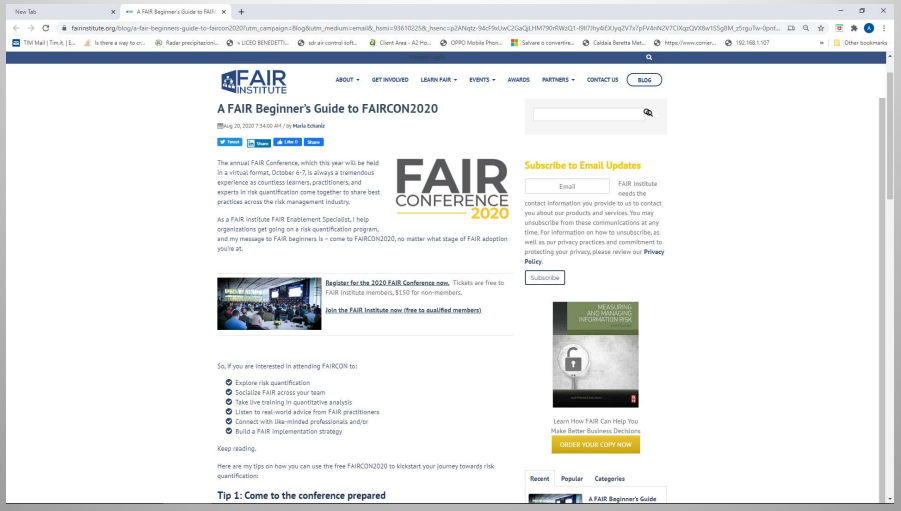
26

Suggerimenti

- Iniziare con modelli semplici ed usando «excel»
- Tradurre i termini «qualitativi» cui si è abituato da:
  - alto / medio / basso

  a:
  - Alto = Probabilità 10% di danno >= € 1.500.000 / anno
  - Medio = Probabilità 2% di danno <= € 300.000 / anno
  - Basso = Probabilità 0.1% di danno <= € 50.000 / anno

6-7 ottobre 2020

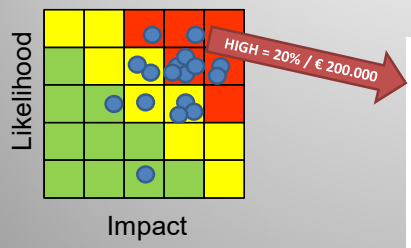


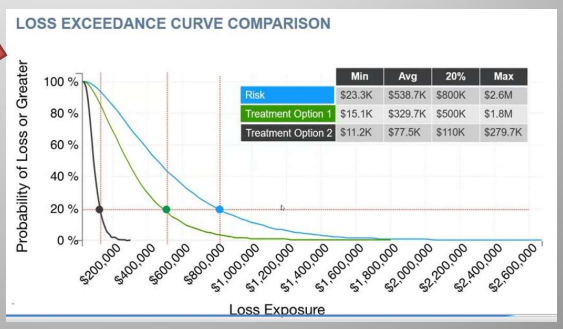
Conclusioni

FAIR consente di capire meglio

- Come nasce lo scenario di rischio (fattori)
- Dove è possibile intervenire
- Come valutare gli impatti
- Quali aree approfondire
- È semplice da usare (v. prossima slide)
- .....

Non è un'alternativa e si integra con un approccio qualitativo





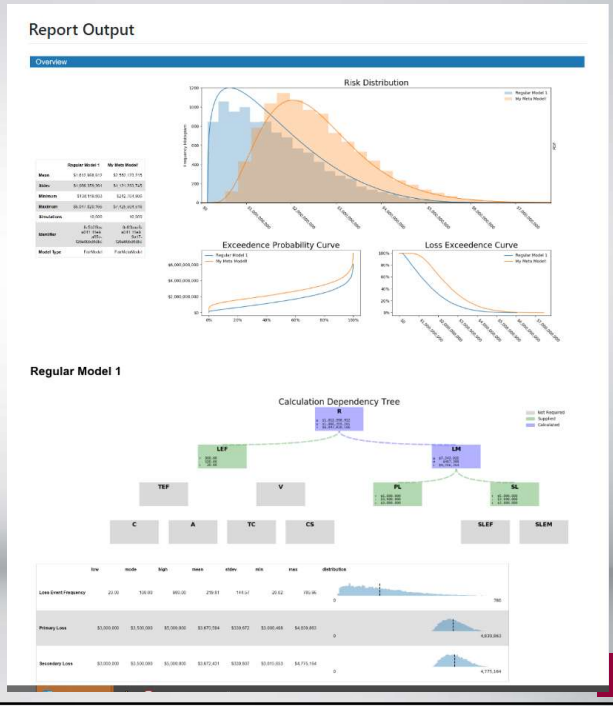
ISACA Rome Chapter

29

Excel

ALE

Python . . .



ISACA Rome Chapter

30

Grazie per l'attenzione

alberto.piamonte@alice.it

31