

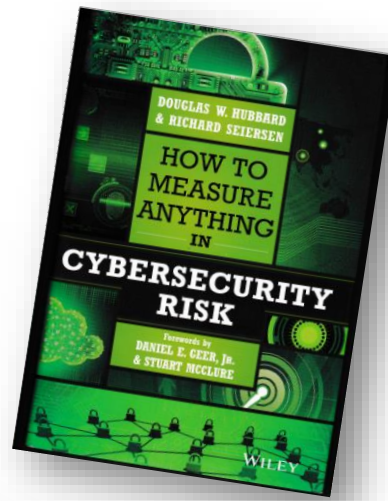
***USE OF FRAMEWORKS (ISO 2700X, NIST, ECC) AND  
QUANTITATIVE RISK ANALYSIS.  
A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.***

***WG ISACA ROMA***

# The Biggest Cybersecurity Risk

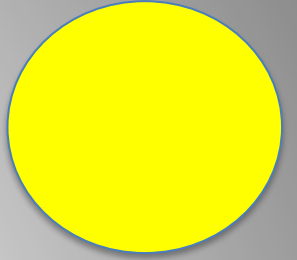
**Question: What is Your Single Biggest Risk in Cybersecurity?**

**Answer: How You Measure Cybersecurity Risk**



3

# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - **INTRODUCTION**
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

## Working group participants

- *Coordinators*
- Alberto Piamonte
- Glauco Bertocchi
- *Contributors*
- Giuseppe Cagnetta
- Francesca Della Mea
- Luca Fei
- Maurizio Pagano
- Mario Taddonio
- Alessia Valentini



# Guidelines for this presentation

- This presentation follows the development of our work.
- We believe that the **main mistakes** and **dead ends** found during our journey are **lessons learned** and therefore as important as the positive results, so we will also share few, the most relevant, of these drawbacks
- Some difficulties can be overcome by making assumptions, a usual fact in risk analysis. We have made many assumptions and will make you aware of them.
- The main goal of this presentation is to take you through a 2-year journey (we will be brief, I promise) and then make you aware of the main facts that enabled us to achieve what we call first results toward a transition from compliance to effectiveness

# OUR MAIN OBJECTIVE

- WHEREAS an **ISMS** (Information Security Management System) implemented according to a **framework such as ISO27001 (or NIST)** represents a **(costly)- asset** that is essentially used for **compliance**, the main objective of our work was to answer the **following question** :
- **Can we measure the effectiveness of ISMS controls and use it with quantitative risk analysis methods?**

## Our sub-goals as a Working Group

1. Identifying the role and use of ISO 27001 controls for quantitative risk analysis
2. Seek to build a BRIDGE or a MAPPING between ISO 27001 and quantitative risk analysis method (FAIR-Factor Analysis Information Risk)

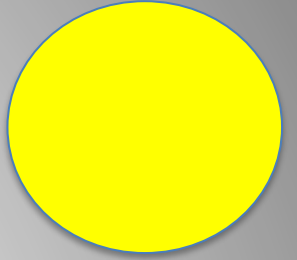
It appears that so far no one has addressed this

3. Use of threat scenarios with quantitative methods.

# How can the risk analysis be improved?

- **It is possible to greatly improve on the existing methods.**  
Many aspects of existing methods have been measured and found wanting.
- **Cybersecurity can use the same quantitative language of risk analysis used in other problems.**  
There are plenty of fields with massive risk, minimal data, and profoundly chaotic actors that are regularly modelled using traditional mathematical methods. We do not need to reinvent terminology or methods from other fields that also have challenging risk analysis problems.
- **Methods exist that have already been measured to be an improvement over expert intuition.**
- **These improved methods are entirely feasible.**
- **You can improve further on these models with empirical data.**  
You have more data available than you think from a variety of existing and newly emerging sources. Even when data is scarce, mathematical methods with limited data can still be an improvement on subjective judgment alone.
- **We have chosen to use FAIR, a quantitative method, it is not the only one, but it is a standard defined by Open Group and has some important features**

# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - **INTRODUCTION TO FAIR**
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

## Requirements for Risk Assessment Methodologies

### 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.

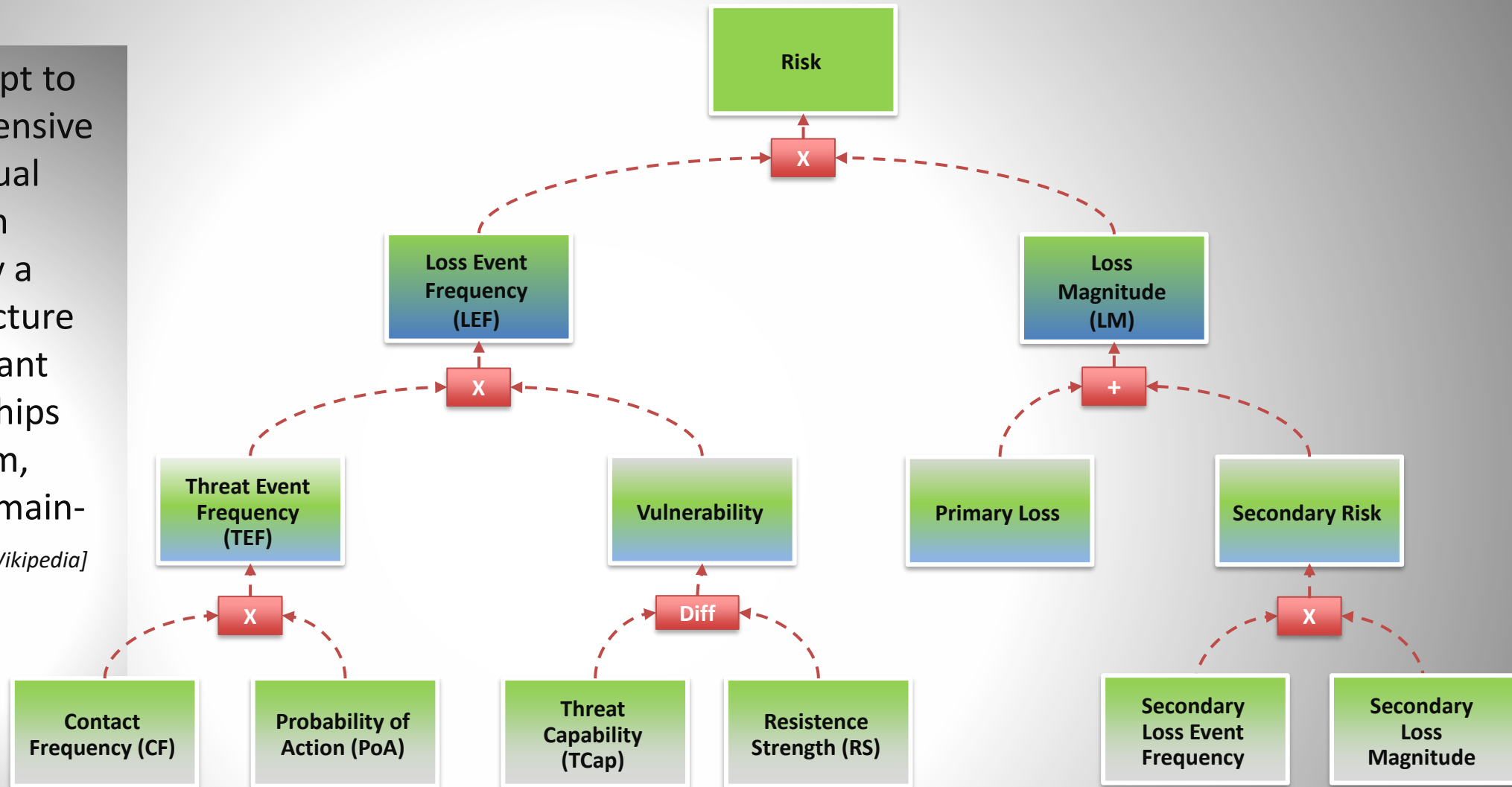
##### 3.2.2 Accurate

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.

# Ontology

Ontology is the attempt to formulate a comprehensive and rigorous conceptual scheme within a given domain; it is generally a hierarchical data structure that contains all relevant entities, the relationships existing between them, rules, axioms, and domain-specific constraints. *[Wikipedia]*





## 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.

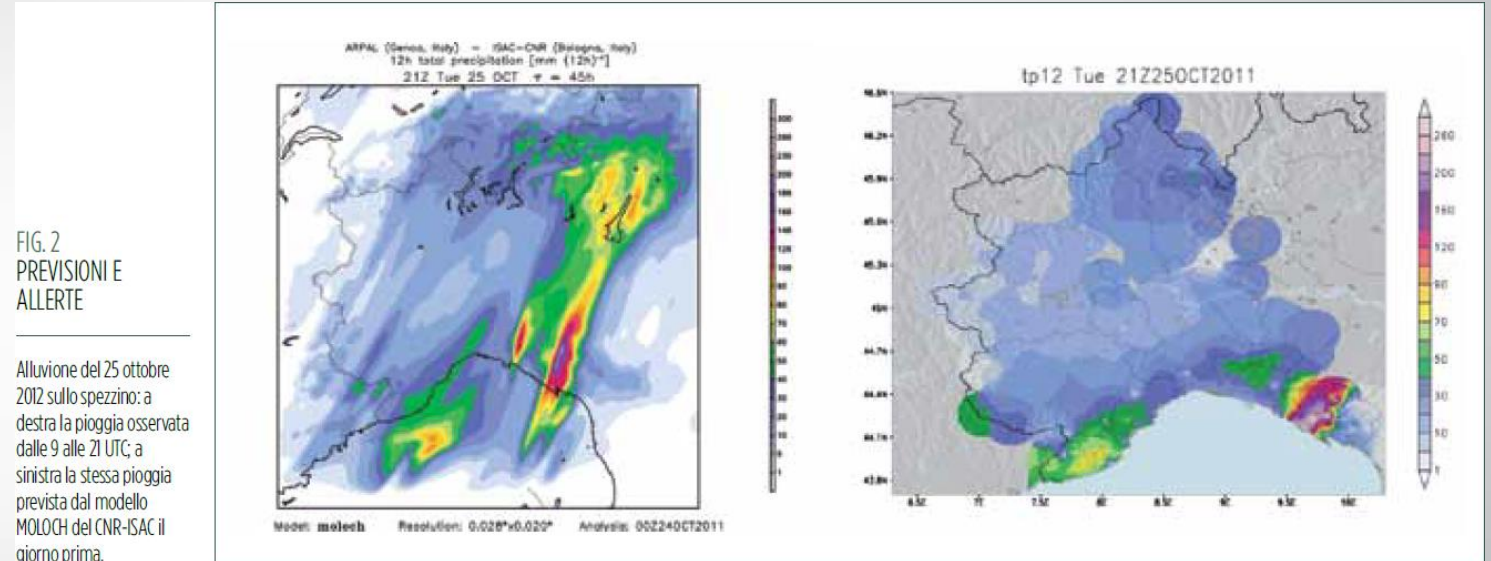


# Accuracy and Precision

- Accuracy and precision are two terms often misused in the context of measurement, so it is important to know the difference well.
- **Accuracy** indicates how close a measurement is to the true value, and thus, **describes a property of the result**.
- Precision, on the other hand, quantifies how effectively measurements were made, or how well calculations were performed.
- **Precision** says something **about the measurement process** or calculation but says nothing about the measurement result or calculated value.

# The value of prediction, that is, not only quality, but also utility

If quality is measured through the "difference" between prediction and observation, value indicates the ability of a prediction to affect the decision-making processes of the users who use it: a forecast will be of high value if it enables a decision maker to make the most correct decision in a given context.



Previsione



Realtà

# FAIR Ontology

## How to measure the quantities involved ? A fundamental concept:

### Definition of Measurement

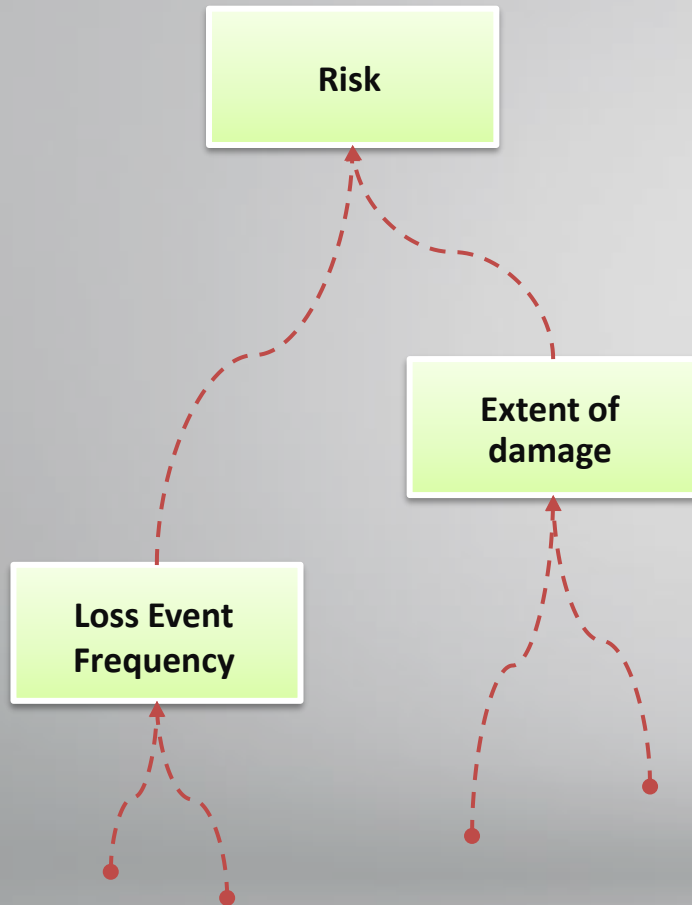
**Measurement:** A quantitatively expressed reduction of uncertainty based on one or more observations.

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.

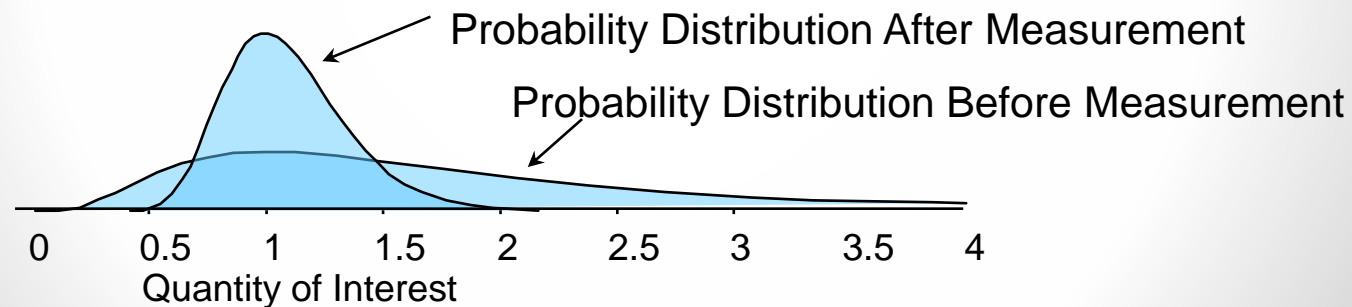




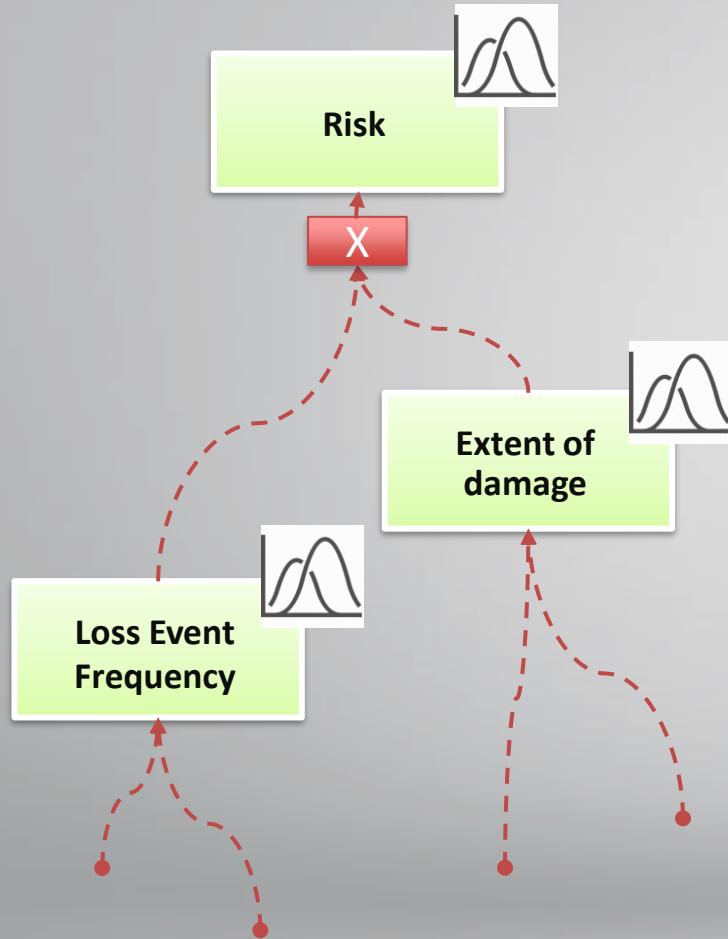
# The Concept of Measurement

**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.



# Uncertainty Math



## 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.

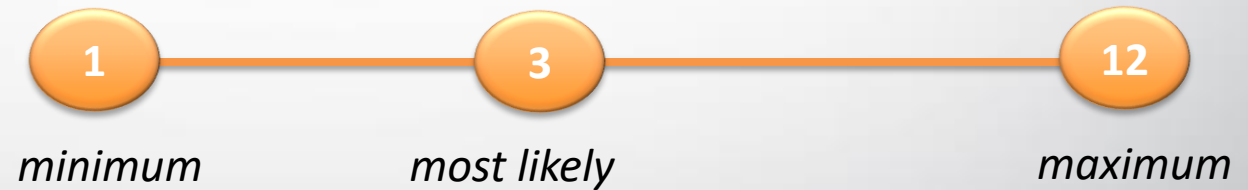


# How to express uncertainty ?

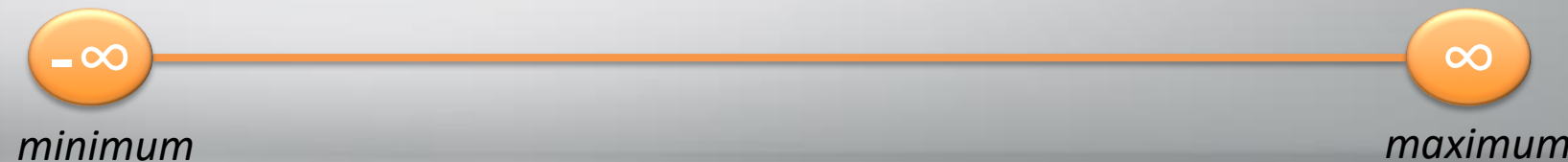
The range (extent of possible values) allows us to express our level of uncertainty numerically:



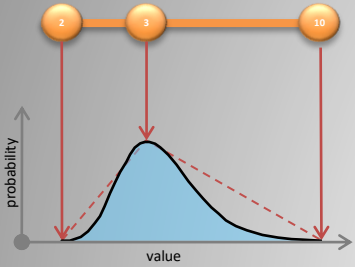
Or :



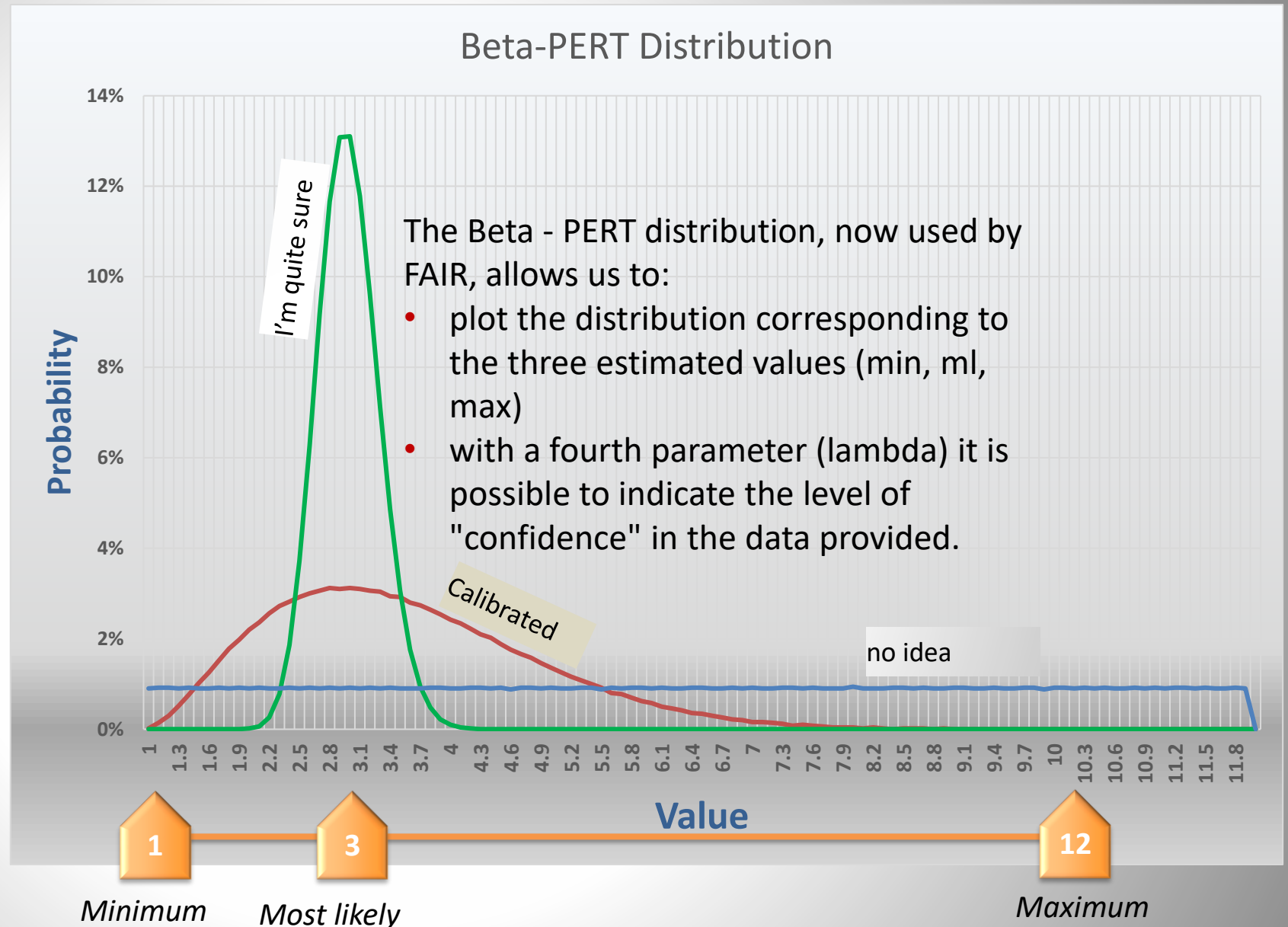
But no :



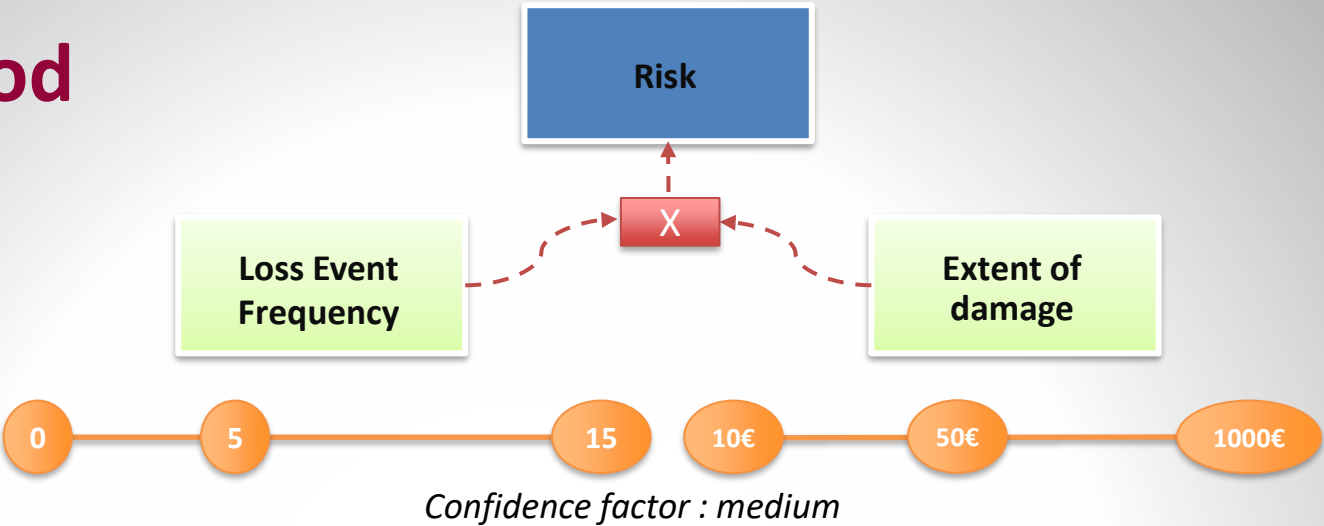
# From Range to Distribution



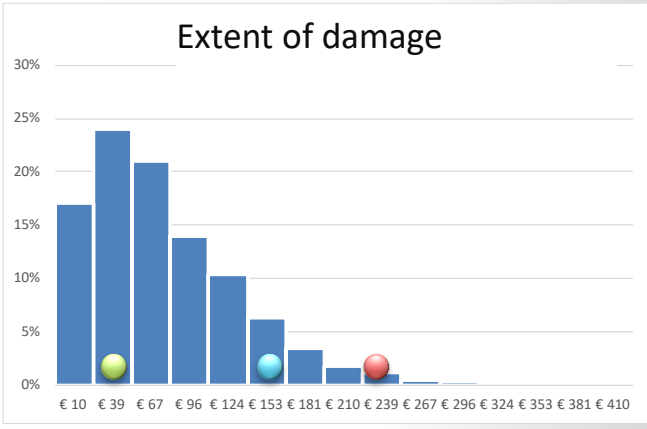
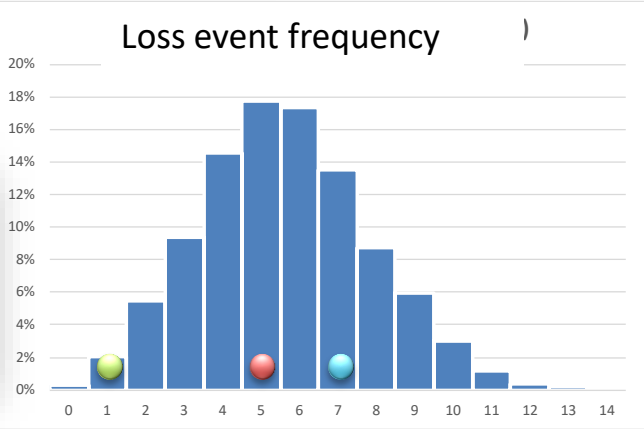
The triangular and Beta-Pert distribution



# Monte Carlo method



The number of spheres with a certain value follows the probability curve of the simulated magnitude



Simulated operation:

- Sum
- Mult
- Compare
- etc

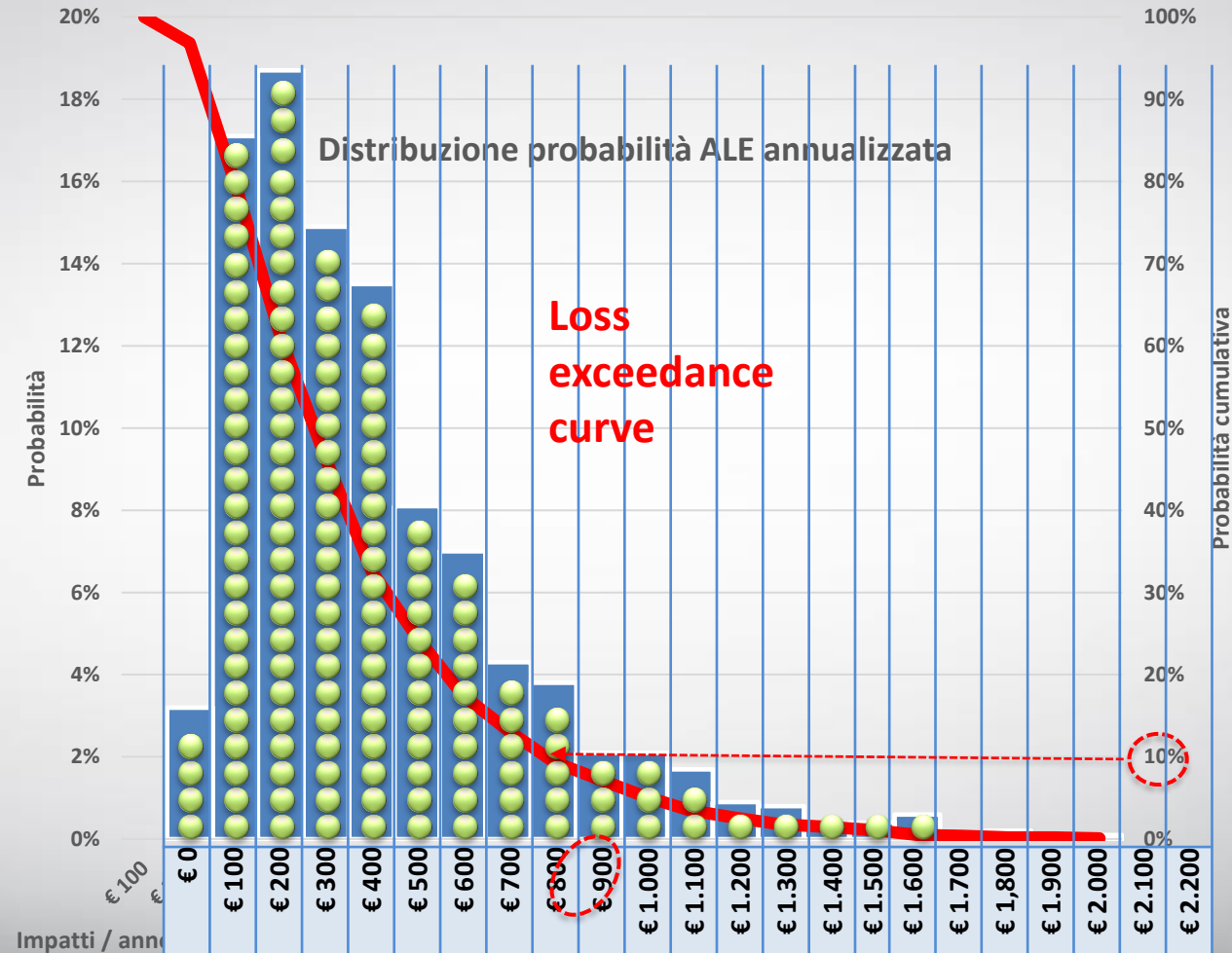
€ 0	€ 100	€ 200	€ 300	€ 400	€ 500	€ 600	€ 700	€ 800	€ 900	€ 1.000	€ 1.100	€ 1.200	€ 1.300	€ 1.400	€ 1.500	€ 1.600	€ 1.700	€ 1.800	€ 1.900	€ 2.000	€ 2.100	€ 2.200
-----	-------	-------	-------	-------	-------	-------	-------	-------	-------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.



+10.000

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



0

5

15

10€

50€

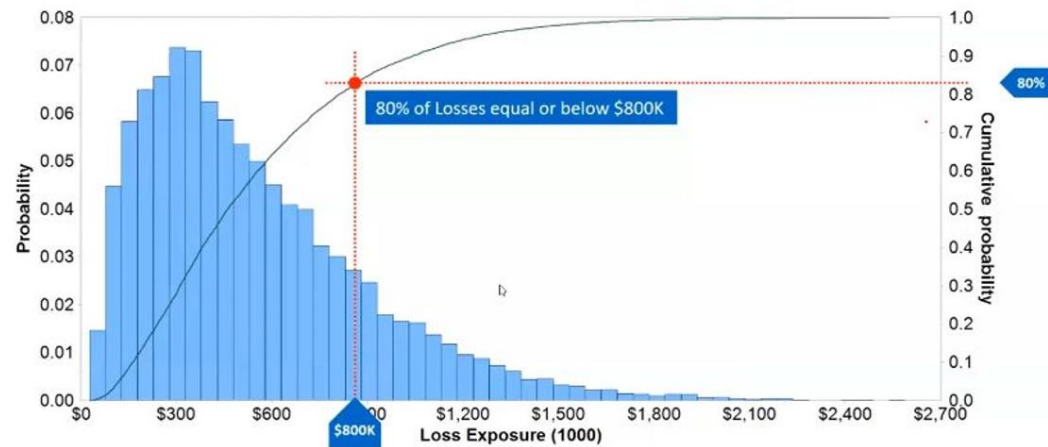
1000€

Fattore di confidenza : medio

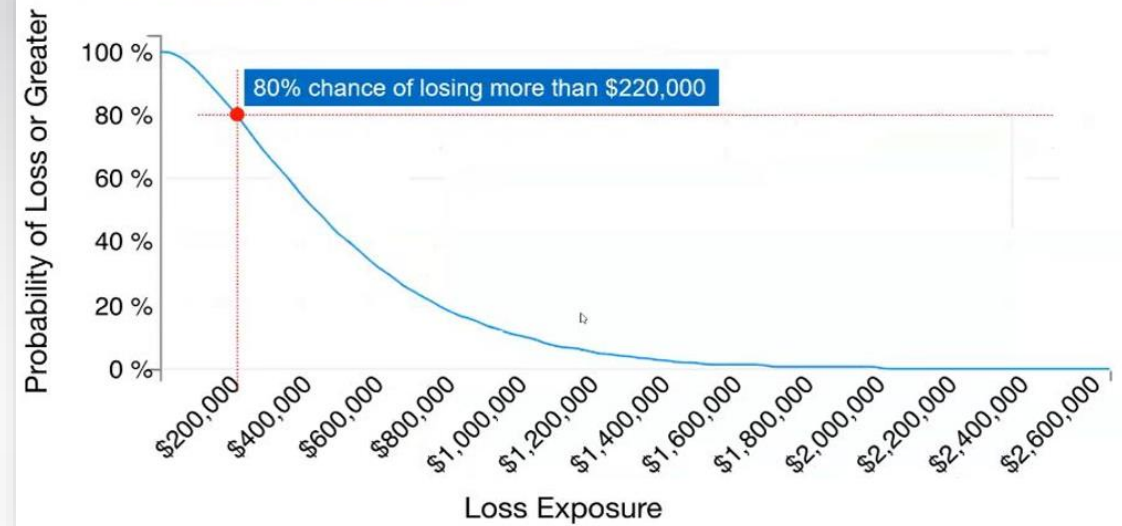
## «Quantitative - statistical» Risk Analysis !

USE OF FRAMEWORKS (ISO 2700X, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

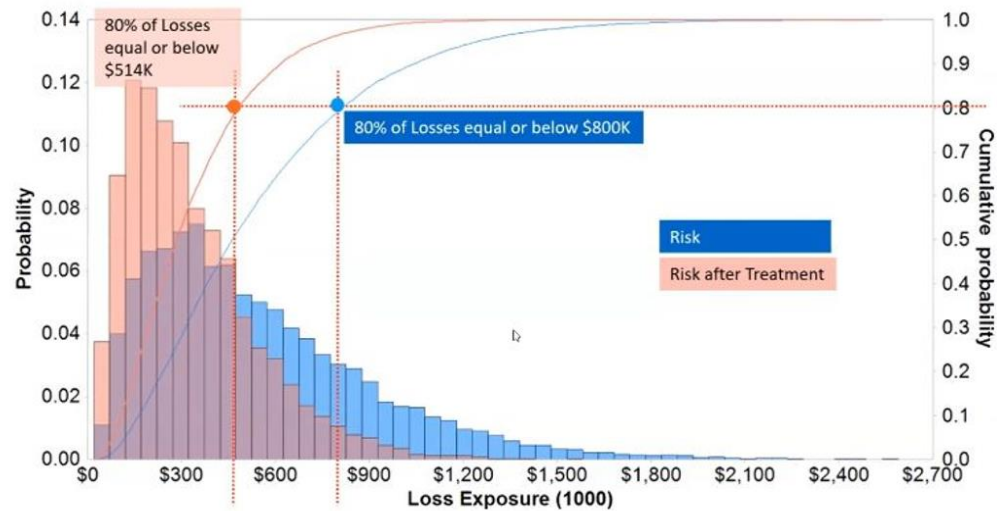
## PROBABILITY DISTRIBUTION



## LOSS EXCEEDANCE CURVE



## MAKE EFFECTIVE COMPARISONS



## LOSS EXCEEDANCE CURVE COMPARISON



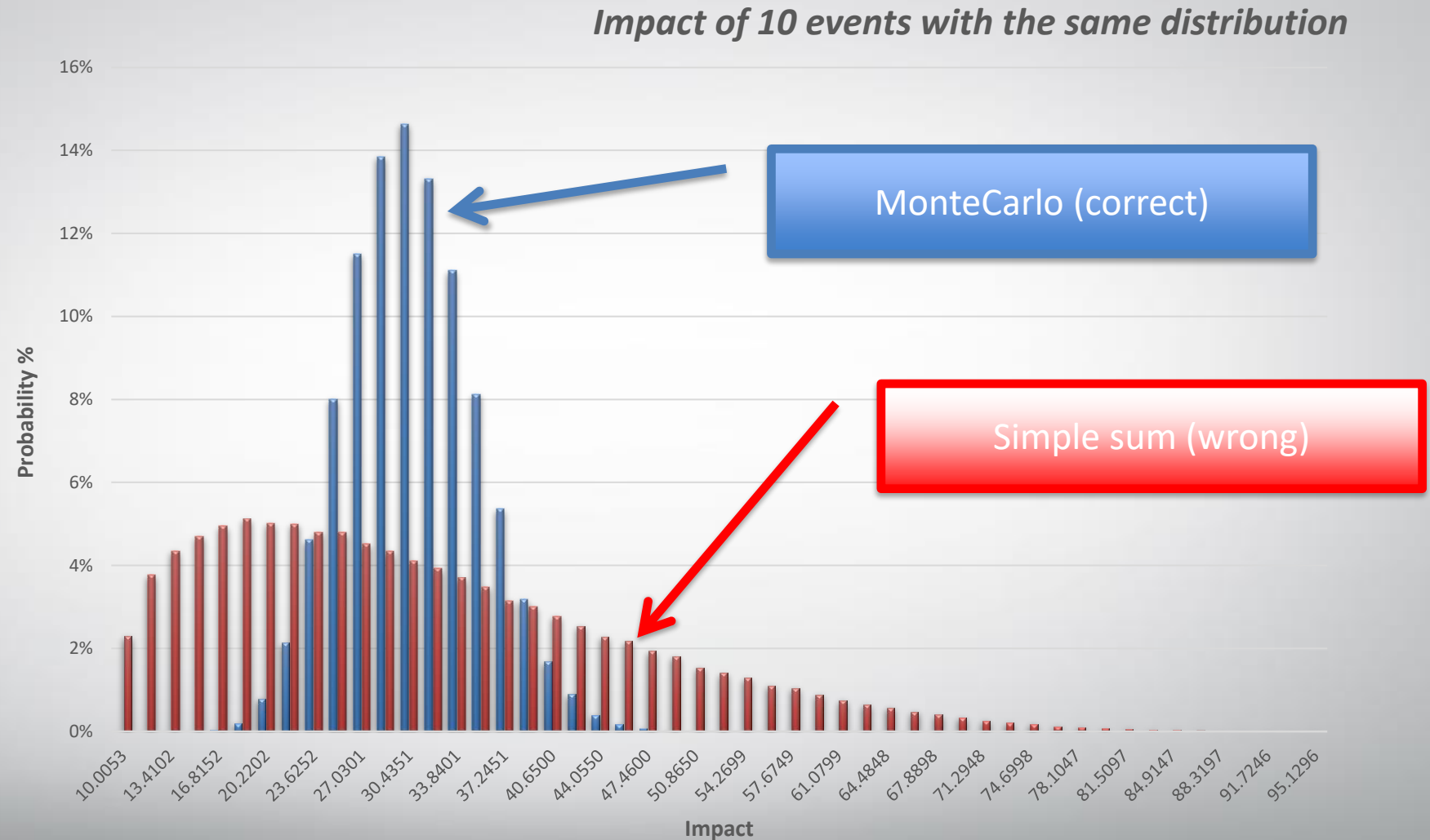
**Operations requiring the Monte Carlo method**

**Always when we have to operate on values defined by distributions**

**The result is also a distribution, which can be used as input to Monte Carlo**

- Risk = Loss Event Frequency  $\times$  Extent of Total damage
- Extent of Total damage =  $\sum$  Extent of damages
- Vulnerability = Threat Capability (TCap)  $>$  Resistance Strength
- Etc.

# What if we don't use Monte Carlo ?



***Wrong data: wrong decisions !***

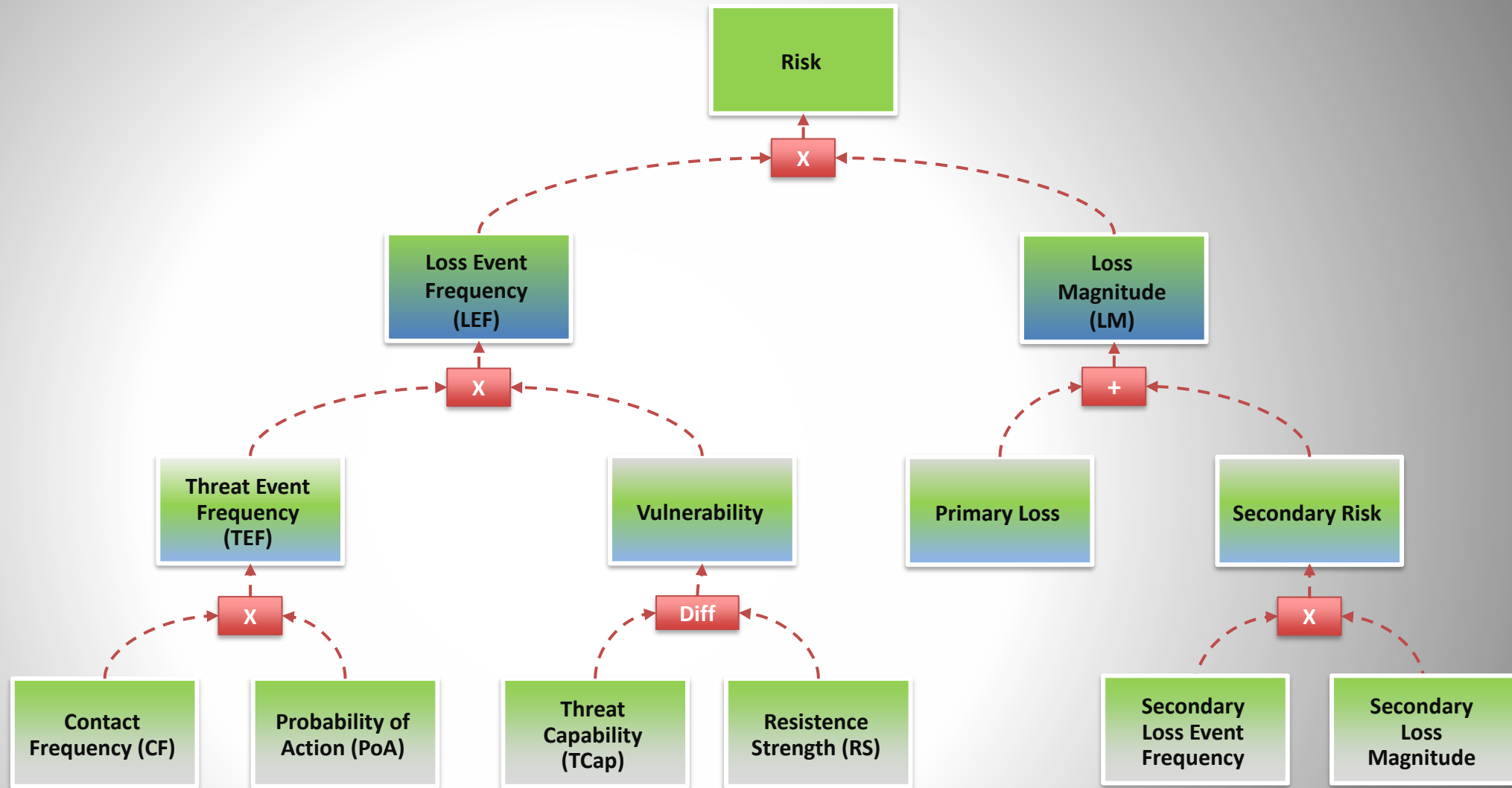
USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A  
FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

## Modeling LEF

There are different formulae to use to model Loss Event Frequency depending on the circumstance:

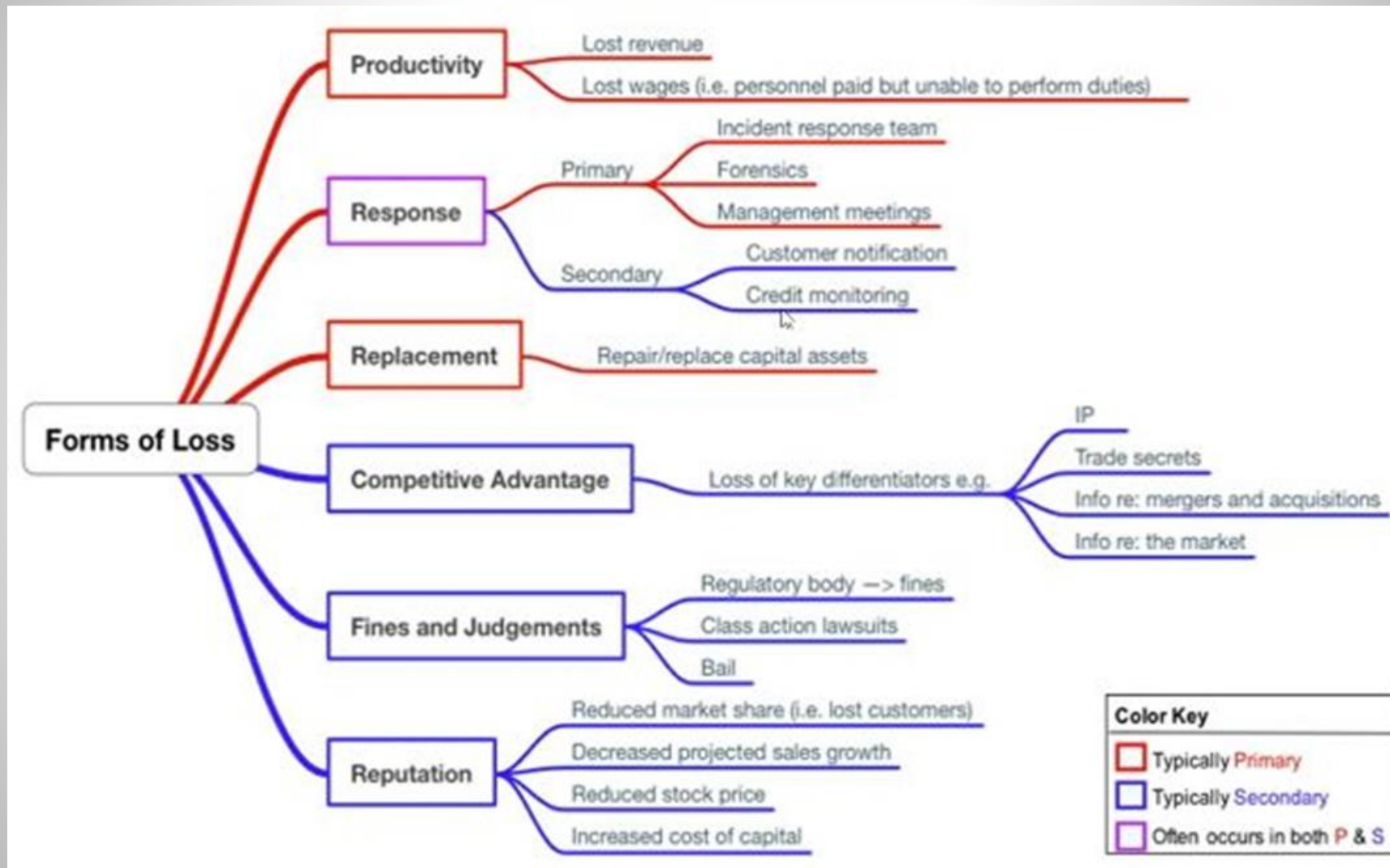
- $LEF = Ber(p_{LEF})$  : if the **Loss Event can only occur once**, LEF follows a **Bernoulli distribution**, where  $p_{LEF}$  is the probability of the event occurring during the time horizon
- $LEF = Bin(n_{LEF}, p_{LEF})$  : if the **Loss Event has a finite number of opportunities to occur**, and each opportunity has a  $p_{LEF}$  probability of resulting in the Loss Event, then LEF follows a **Binomial distribution**
- $LEF = Poi(\lambda_{LEF} * t)$  : if the Loss Event **can occur independently multiple times**, LEF follows a **Poisson distribution**, where  $\lambda_{LEF}$  is the expected number of times the event might occur per year (or day, month, etc.) and is the length of the time horizon in years (or days, months, etc. to match  $\lambda$ )

# Ontology





# FAIR Approach-Forms of loss



# No Data? No Problem

by Jack Jones

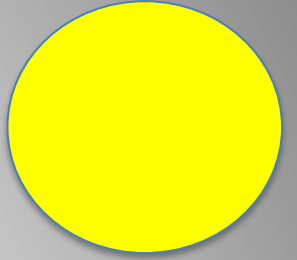


- .....
- Start with an absurd estimate (e.g., less than an inch or greater than ten feet tall). It breaks the ice and gets people out of the “I have no idea” mindset.
- Use references and logical reasoning to begin narrowing the range.
- Challenge your reasoning along the way, and consciously look for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



# Agenda



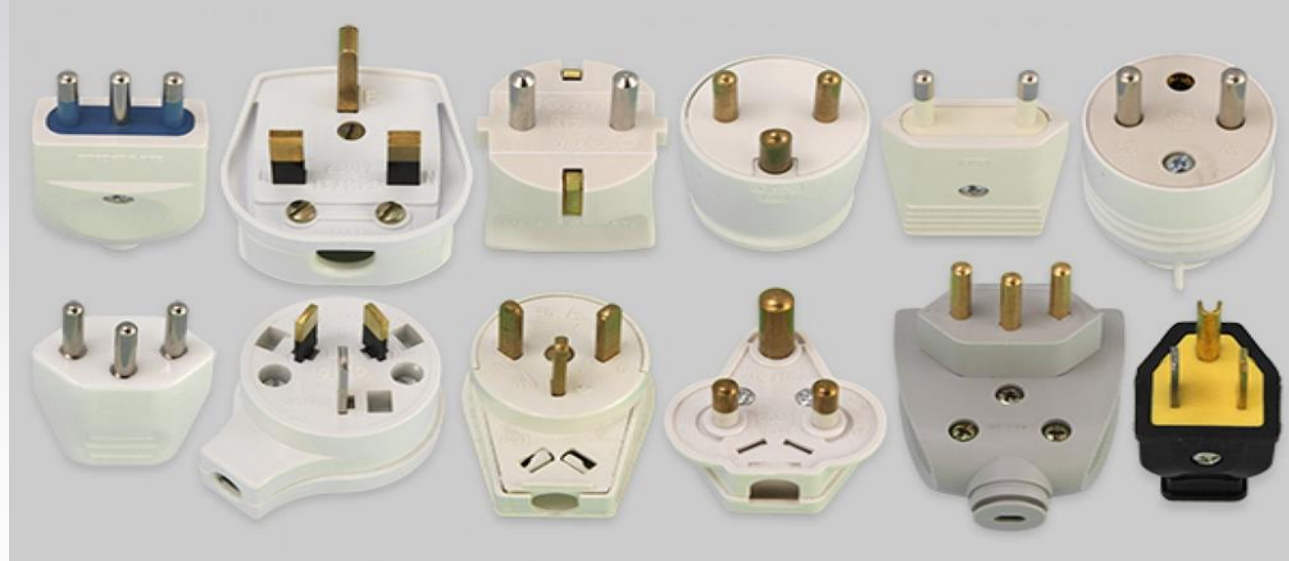
- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - **WG ISO-FAIR @ISACA ROMA**
    - **MAPPING ISO27001 to FAIR**
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

## How have we proceeded?

- *Trying to define terms and concepts (shared meanings)\**
- *By studying, doing exercises "at home," discussing differences of opinion*
- *Experimenting with a mathematical model to deepen concepts and consolidate choices*
- *With many Working Group meetings*

*\* This is the most complex and absolutely unresolved part also at international level.*

What did we think  
we needed to make  
as BRIDGE or  
MAPPING? An  
adaptation between  
plugs and sockets?



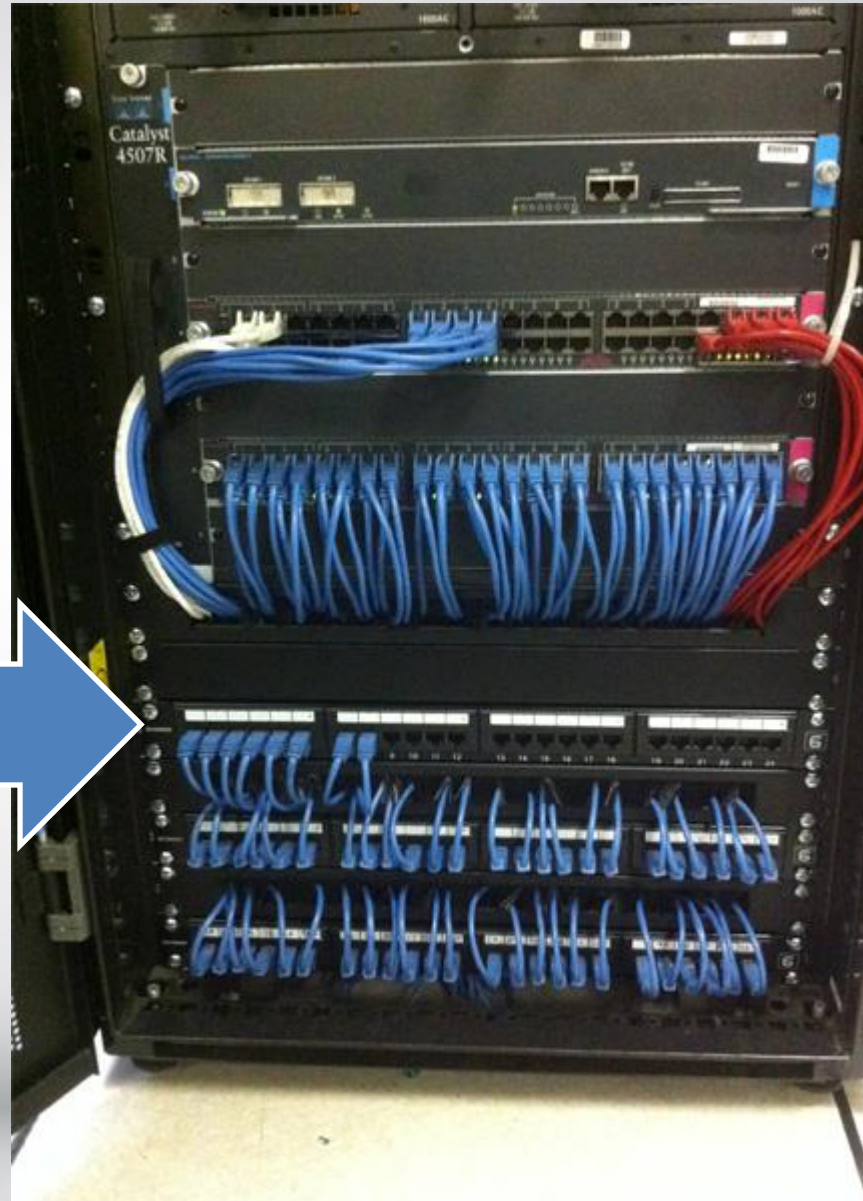
Could the solution have been a universal adapter, a set of adapters? Or what?





This is what we  
imagined we would  
get

ISO



FAIR

## Asking the right questions to set goals

### The first (of three) question

- It is necessary to **define the scope** in which to build **a bridge** (and thus a model) to "connect" ISO 27k and FAIR
- **The first question to answer is: which parts of ISO 27k and FAIR do we want to bridge?**
- Since our scope is **risk analysis** we will have to choose the part of ISO 27k that contains that scope. **The Statement of Applicability (SOA)** lists the application status of the controls in Annex A of the ISO 27001 standard.
- On **the FAIR side**, the equivalent is the **ontology of controls** described in Ch. 11 of The Handbook of FAIR (2015).

## The second question

- The second question is: **what are the "dimensions" of the problem ?**
- The first assumption was to consider modeling all ISO controls listed in Annex A in the corresponding FAIR ontology.
- There are at least 114 ISO 27001:2013 controls, each consisting of N sub-controls with N depending on the various ways a single control is implemented (see for example ISO 27002 standard), on FAIR side we could have about 30 controls for each sub-control on the ISO side.
- In case of defense in depth the situation would multiply for each defense level.
- **114xNx30x defense levels (with N probably <100)**
- The resulting set of combinations is probably computationally addressable, though very complex.
- **BUT ... perhaps it is better to ask a few more questions.**

## The third question

- The third question is, **what are the utility, manageability, and validation requirements of the "bridge"?**
- The **bridge** must be useful and manageable in application to concrete cases, as well as produce meaningful and possibly "validatable" results.
- For a **complete modeling one would have to evaluate thousands of "estimates" of ISO controls**
- **How would we validate such a complex model and what would be the reliability of the results?**



As we developed the project, we had the distinct feeling that we were in danger of ending up like this.

Our approach has to be changed.



## Let's change the approach: what was FAIR designed for and what goals is ISO useful for?

- The FAIR methodology has a top-down approach and the ability to use scenarios and assessments on aggregate factors, even without having detailed data.
- ISO 27001 aims to define an information security management system (ISMS) that is certifiable and therefore auditable. The ISO objective is for compliance and comprehensiveness of the company's security processes (controls) with respect to an overall analysis of the risks to which the organization is exposed.
- **Assessment of a real ISMS (controls) could be used to indicate the organization's posture toward security in terms of effectiveness and efficiency of processes?**

## Changed approach



## new type of questions

- If my organization **suffers an attack** (e.g., ransomware) what is the **likely damage in economic terms** and what are **the factors I can most affect to reduce the damage** and **how do I economically compare the alternatives?"** .
- To answer the **first part of the question**, I need to put the threat in context with the cyber defense already in place in the enterprise. Then **use data from the ISO 27k ISMS, which contains information about the controls in place , their implementation and effectiveness.**
- To answer **the second and third part of the question**, I need to use a **tool that allows quantitative analysis (amounts and probabilities)** of the threat scenario using advanced statistical techniques such as, for example, probability distributions and Monte Carlo type simulations.

## Some possible outcomes that result from the change in approach

- ISO -FAIR **modeling** is useful, and is **limited in complexity, to analyze a threat scenario**, and make a quantitative assessment of its risks . For this purpose we also **use some controls of the ISMS, those that are of interest** in the scenario considered .
- We have exemplified the ISMS with ISO 27001 but **believe that the methodology can be applied**, obviously with detailed adaptations, for a **similar system such as, for example, NIST800-53r4, based on the definition and application of families of controls.**
- From **the controls** (ISO 27k scope) and their **effectiveness we derive mitigation estimates** for the risk factors in the FAIR ontology.

## The first hypothesis of methodology (spring 2021)

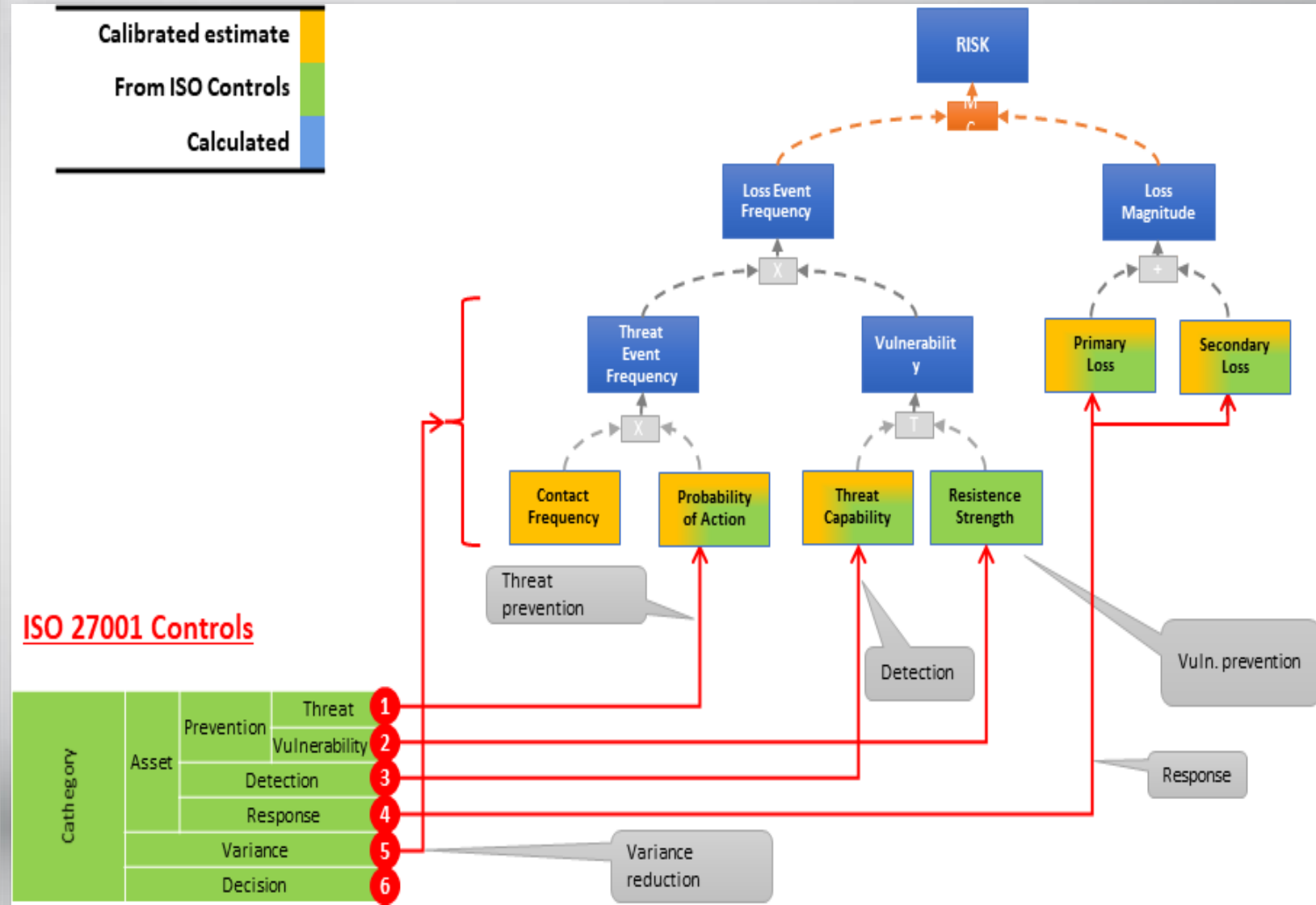
The following is a first hypothesis of methodology to **use controls (ISO 27k or similar)** to mitigate the risks of a **threat scenario analyzed with FAIR**:

1. Identification of the **ISO controls that are affected by the scenario under analysis.**
2. **For each of the identified ISO controls, modeling against the FAIR ontology controls is performed; that is, the ISO controls are evaluated,** using methods described later in the presentation.
3. **FAIR controls, modeled and valorized with the ISO controls,** are used for the quantitative analysis of the threat scenario.



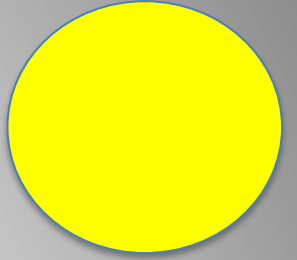
# Phase I - Schema

- Designed a schema to evaluate ISO 27001 system controls and calculate their contribution in the FAIR factors
- The ISO controls were mapped into categories that would then contribute to the determination of the various FAIR factors
- This working model allows us to calculate the effect of the contribution of ISO controls on FAIR factors and to produce the classic FAIR curves (ALE; LEE, etc.)





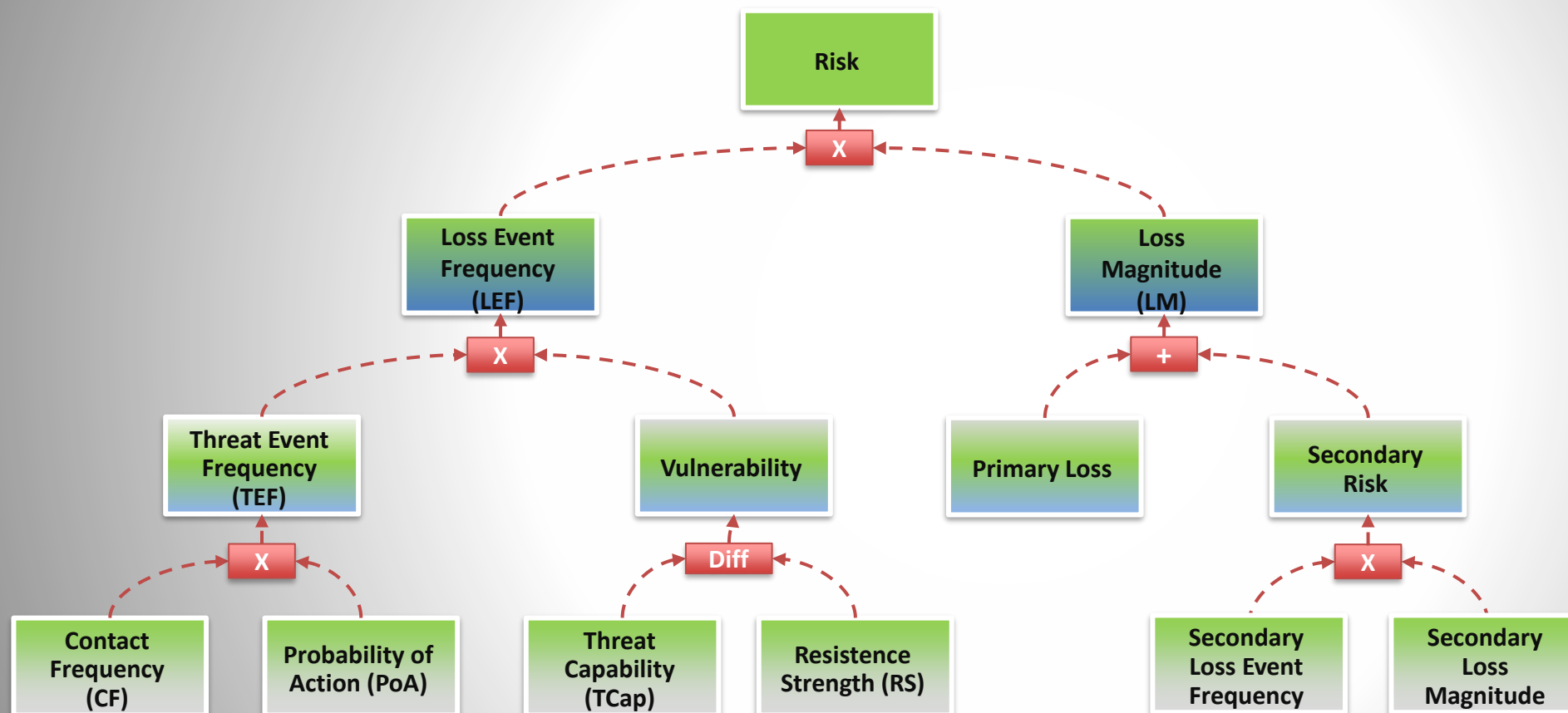
# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - **DEMO**
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

# FAIR Approach- The Ontology – The Tool

Not used	
Calibrated Estimate	
Computed value	



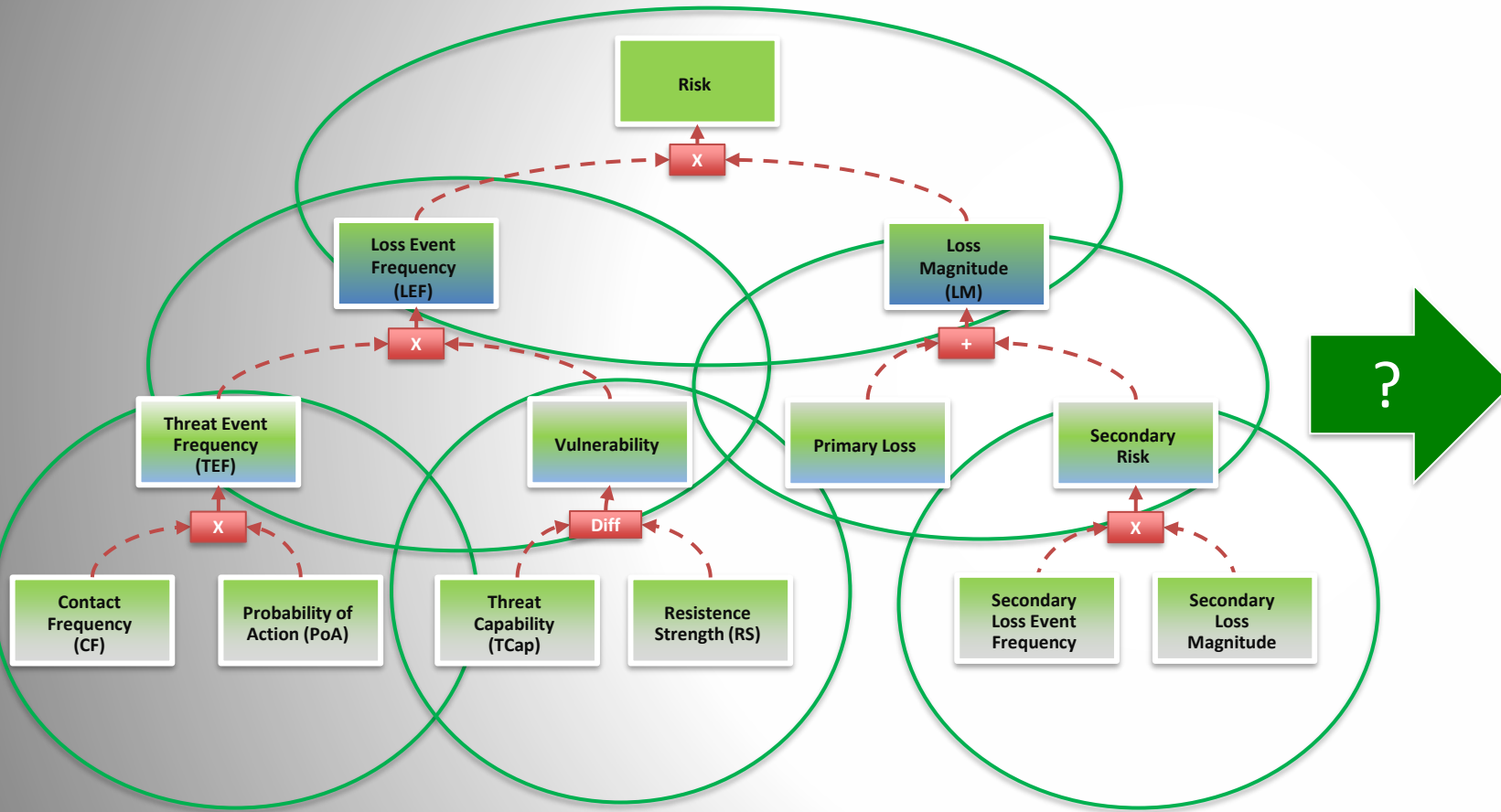
# The Tool

We soon realized that an open and flexible tool for understanding, and testing hypotheses and solutions would be very useful and almost indispensable. And so. And so . . . .

## Developing DIY solutions with Excel

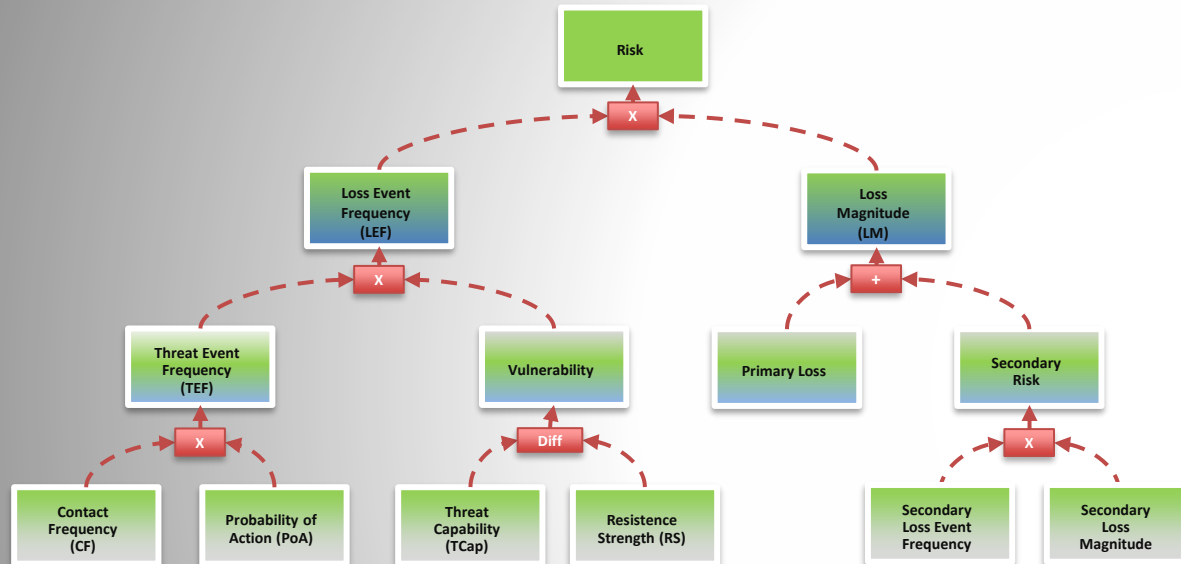
- ✓ The standard is very well documented in terms of the calculation algorithms to be used in the various steps.
- ✓ EXCEL has excellent performance in more complex calculations (Monte Carlo), possible implementations of the method are well documented
- ✓ The necessary statistical functions (Beta-Pert, Poisson, Binomial, etc.) are available.
- ✓ Autonomous development requires no special skills and allows the ontology to be extended to meet specific needs (ISO mapping!).

# The Excel Model



# Ontology

# Excel® Model



- Open
- Easily interfaced (in and out)
- Modifiable
- Performance
- Programmable

An Excel sheet for each FAIR factor

Dim.	min	pp	max	Conf	Nome	Descrizione
In 1	€ 0,000			7	ALE primario	
In 2	€ 0,000			7	ALE secondario	
Operazione	+					
Out	€ 0,000				ALE	Impatto totale annuo

Dim.	min	pp	max	Conf	Nome	Descrizione
In 1	€ 0,000			7	PLMR	Loss magnitude ridotta
In 2	€ 0,000			7	LEF	LEF frequency
Operazione	+					
Out	€ 0,000				ALEP	Impatto Primario totale annuo

Dim.	min	pp	max	Conf	Nome	Descrizione
In 1	€ 0,000			7	SLEF	Loss event frequency ridotta
In 2	€ 0,000			7	SLEF	Loss event frequency ridotta
Operazione	+					
Out	€ 0,000				ALES	Impatto secondario totale annuo

Dim.	min	pp	max	Conf	Nome	Descrizione
In 1	€ 0,000			7	TCR	Threat Capability ridotta
In 2	€ 0,000			7	RS	Resistance Strength
Operazione	+					
Out	€ 0,000				VULN	Vulnerability

Dim.	min	pp	max	Conf	Nome	Descrizione
In 1	€ 0,000			7	TTTb	Perdita produttività
In 2	€ 0,000			7	TTTc	Sostituzione
In 3	€ 0,000			7	TTTc	Risposta
Operazione	+					
Out	€ 0,000				PLM	Impatto primario totale per evento



Model	Prova 01
Date	29/10/2021
Default Confidence	M
n. of iterations	10.000

S = Simple
F = Fitting

**Generate  
Distribution  
Description**

CLEAR  
DESCRIBE

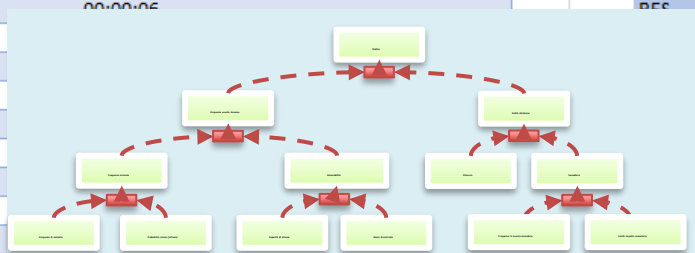
Distr. list update

## CLEAR DISTRIBUTIONS

## Process Model

**Update !**

Worksheet	Time	Message
1 TCR	00:00:03	
2 RES	00:00:05	
3 TEF	00:00:06	
4 VUL		
5 LEF		
6 SLF		
7 PLM		
8 PLMR		
9 ALEP		
10 ALES		
11 ALE		
12		
13		
14		
15		
16		
Tot time	00:00:34	



Distrib.	Options
RESMin	SF
RESMax	SF
RES	SF

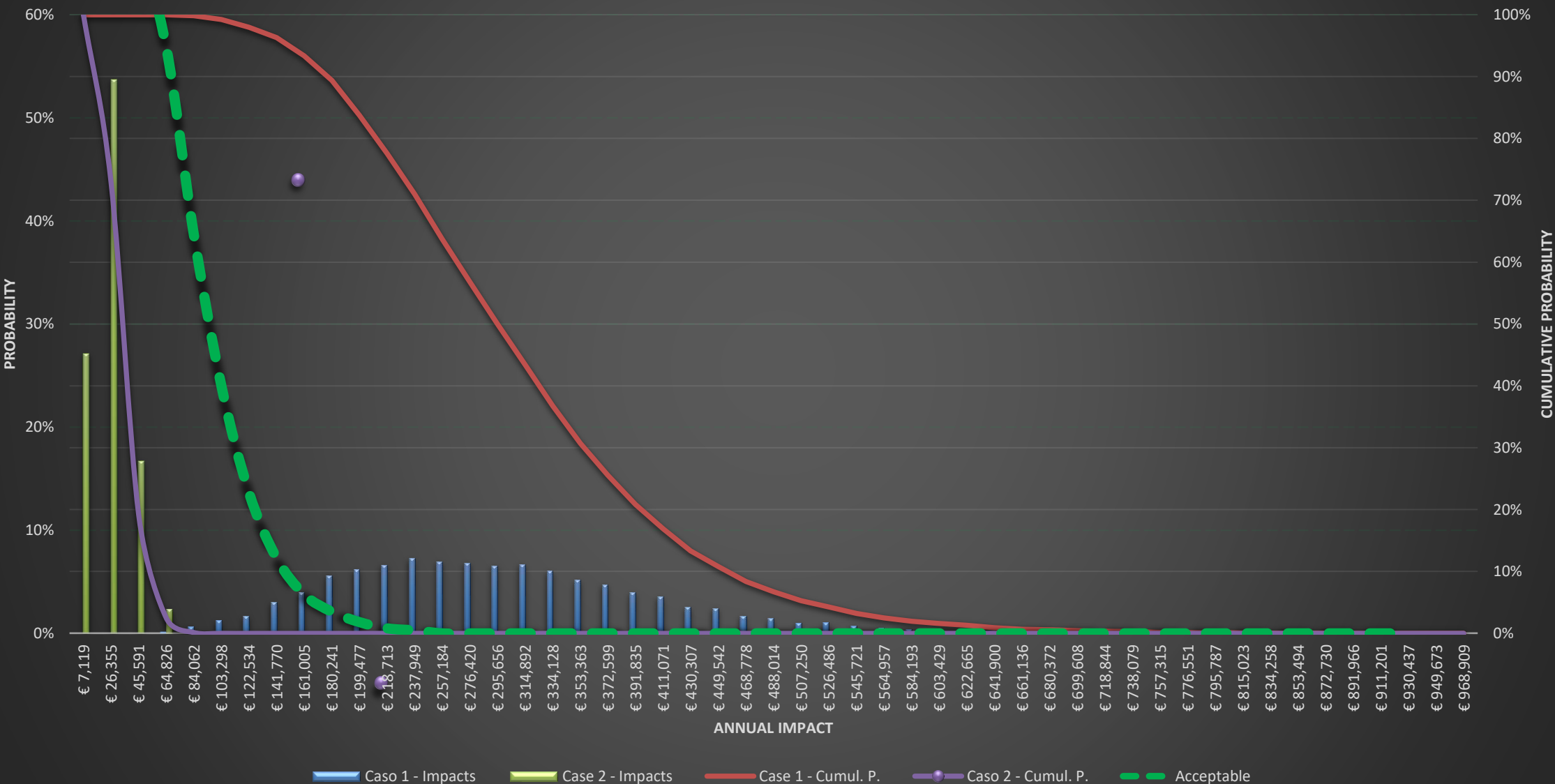
Name	Definition	Where defined	Format
ALE	Impatto totale annuo	=ALE!\$L\$4:\$L\$10003	€ #,##0
ALEP	Impatto Primario totale annuo	=ALEP!\$L\$4:\$L\$10003	€ #,##0
ALES	Impatto secondario totale annuo	=ALES!\$L\$4:\$L\$10003	€ #,##0
DET	Detection	=TCR!\$K\$4:\$K\$10003	0.00%
LEF	Loss event frequency	=LEF!\$L\$4:\$L\$10003	#,##0.00
PLM	Impatto primario totale per evento	=PLM!\$M\$4:\$M\$10003	€ #,##0
PLMmin	Perdita Minima	=PLMR!\$K\$4:\$K\$10003	€ #,##0
PLMR	Perdita ridotta primaria	=PLMR!\$M\$4:\$M\$10003	€ #,##0
PoA	Probability of Action	=TEF!\$L\$4:\$L\$10003	0.00%
R_PLM	Response	=PLMR!\$L\$4:\$L\$10003	0%
RES	Resistance	=RES!\$M\$4:\$M\$10003	0.00%
RESIN	Resistance	=RES!\$L\$4:\$L\$10003	0.00%
RESMax	RES Max	=RES!\$J\$4:\$J\$10003	0.00%
RESMin	RESMin	=RES!\$K\$4:\$K\$10003	
SLEF	Secondary loss event frequency	=SLF!\$L\$4:\$L\$10003	#,##0.00
SLF	Percentuale eventi secondari	=SLF!\$K\$4:\$K\$10003	#,##0.00
SLM	SLM perdita reputazionale (secondaria)	=ALES!\$J\$4:\$J\$10003	€ #,##0
TC	Threat Capability (Criminals)	=TCR!\$J\$4:\$J\$10003	0.00%
TCR	TC Reduced	=TCR!\$L\$4:\$L\$10003	0.00%
TEF	Threat Event Freq	=TEF!\$M\$4:\$M\$10003	0.00
TEFMax	TEF Max (Criminals)	=TEF!\$J\$4:\$J\$10003	0.00
TEFMin	TEF Min	=TEF!\$K\$4:\$K\$10003	0.00
TTTa	Perdita produttività	=PLM!\$J\$4:\$J\$10003	€ #,##0
TTTb	Sostituzione	=PLM!\$K\$4:\$K\$10003	€ #,##0
TTTc	Risposta	=PLM!\$L\$4:\$L\$10003	€ #,##0
VUL	Vulnerability	=LEF!\$K\$4:\$K\$10003	#,##0.00
VULN	Vulnerability 1	=VUL!\$L\$4:\$L\$10003	0

**Compare graph**

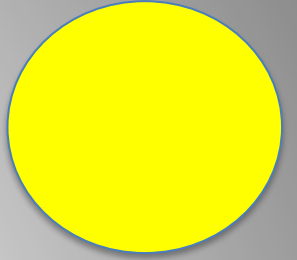
	Name	Notes
COPY 1	ALE	ALE 1
COPY 2	ALE	ALE 3 (ISO P)

*All the defined distributions as Excel® names*

Case 2 : Planned ISO Controls



# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - **ISSUES IN MAPPING ISO to FAIR**
  - **TRANSITION**
    - **CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM**
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

# Phase 1 – VALUES AND PROBLEMS

After defining the high level schema, we searched for a quantification of values to accurately map ISO to FAIR:

- "Precision" mapping trials: the most accurate assessment of controls, use of sub controls and how to calculate their weights
- How to evaluate the impact of sets of ISO controls on FAIR factors

Results at this stage:

- Difficulties in defining an accurate and detailed mapping, impossible to overcome without a clear approach definition with FAIR support and update on new criteria

We contacted FAIR and, having had access to the early draft version of FAIR-CAM, we were able to start with new elements

Phase 2.

ISO/IEC 27002 section	Control	Category					
		Asset				Variance	Decision
		Prevention		Detection	Response		
6	Organization of information security						
6.1	Internal Organization	60%	80%	0%	60%	100%	60%
6.1.1	Information security roles and responsibilities		✓		✓	✓	✓
6.1.2	Segregation of duties					✓	✓
6.1.3	Contact with authorities	✓	✓		✓	✓	✓
6.1.4	Contact with special interest groups	✓	✓		✓	✓	
6.1.5	Information security in project management	✓	✓			✓	
6.2	Mobile devices and teleworking	100%	100%	100%	100%	100%	100%
6.2.1	Mobile device policy	✓	✓	✓	✓	✓	✓
6.2.2	Teleworking	✓	✓	✓	✓	✓	✓

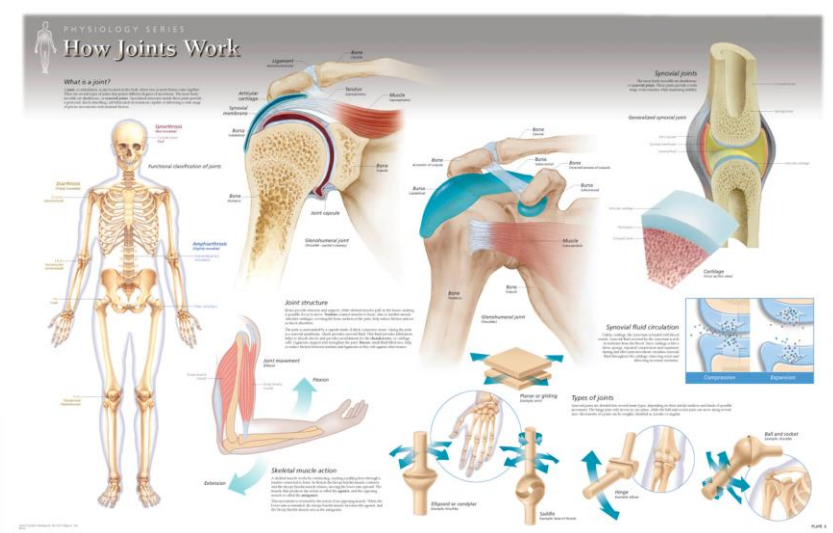
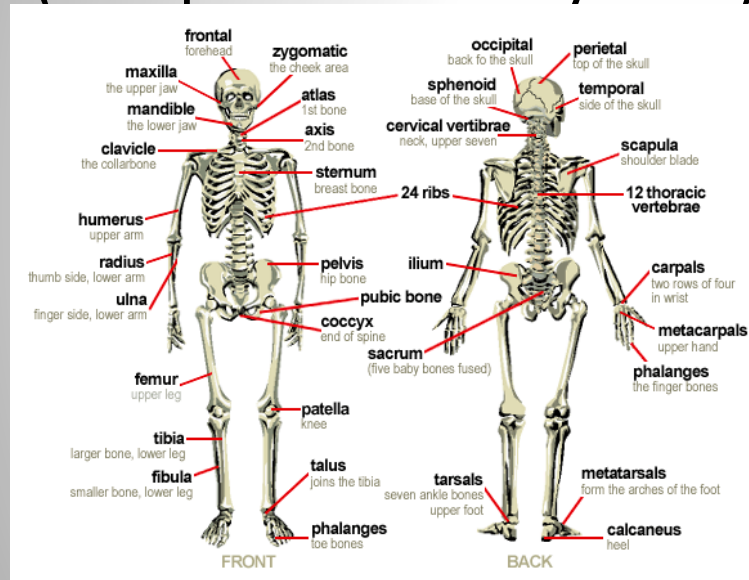
# What's been missing...

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.

# FAIR-CAM (FAIR-Controls Analytics Model) Objectives

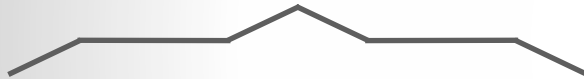
- Describe controls physiology so that we can:
  - Bridge the gap between controls “anatomy” and risk
  - Properly account for individual control functionality as well as systemic functionality
  - Reliably forecast, measure, and validate control efficacy and value
  - Enable better use of security telemetry
  - 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



# Clarifying terms (FAIR-CAM)

## Controls:

*“Anything used to directly or indirectly affect the frequency or magnitude of loss.”*

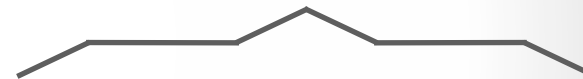


## Examples:

Policies  
Passwords  
Patching  
Data backups  
Auditing  
etc...

## Control Functions:

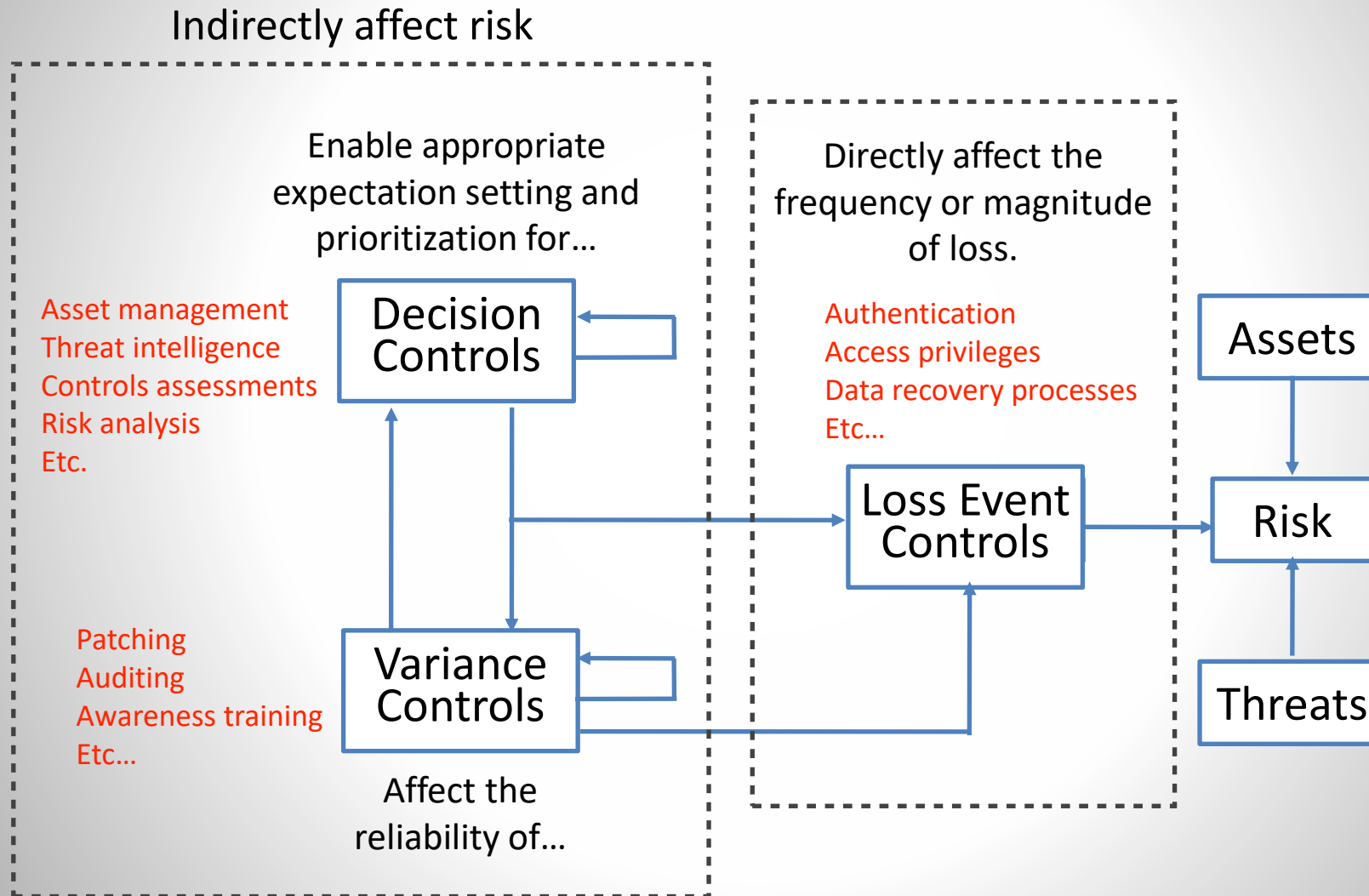
*“How a control directly or indirectly affects the frequency or magnitude of loss.”*



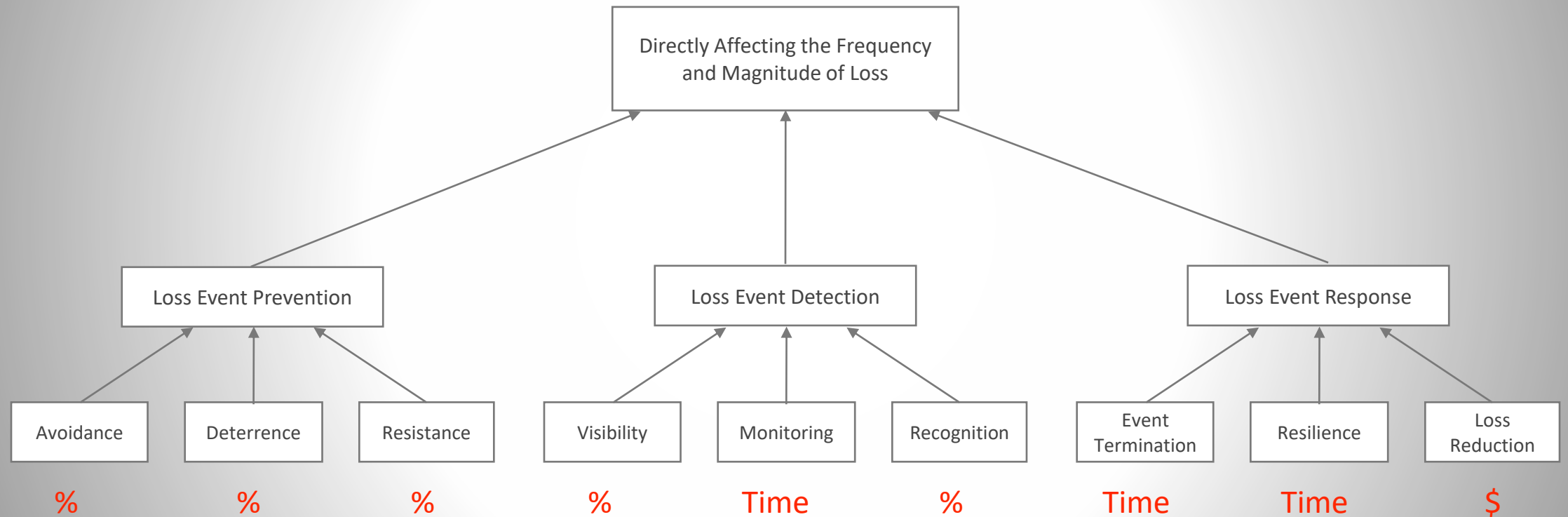
## Examples:

Loss Event Prevention  
Loss Event Detection  
Variance Prevention  
Variance Correction  
etc...

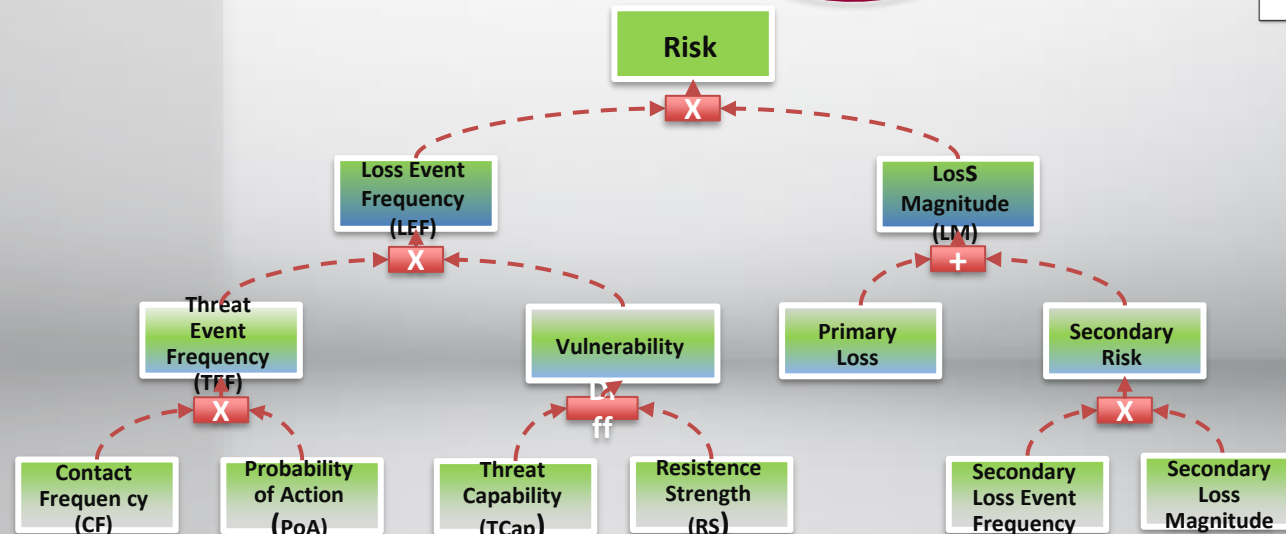
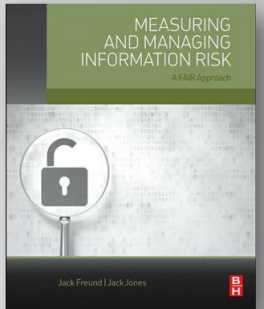
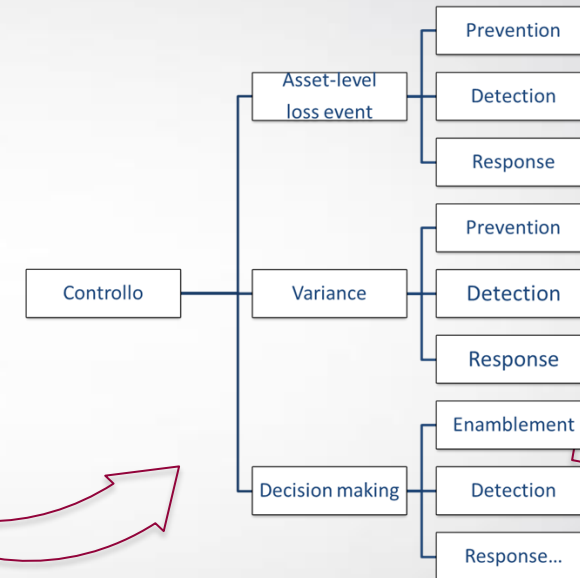
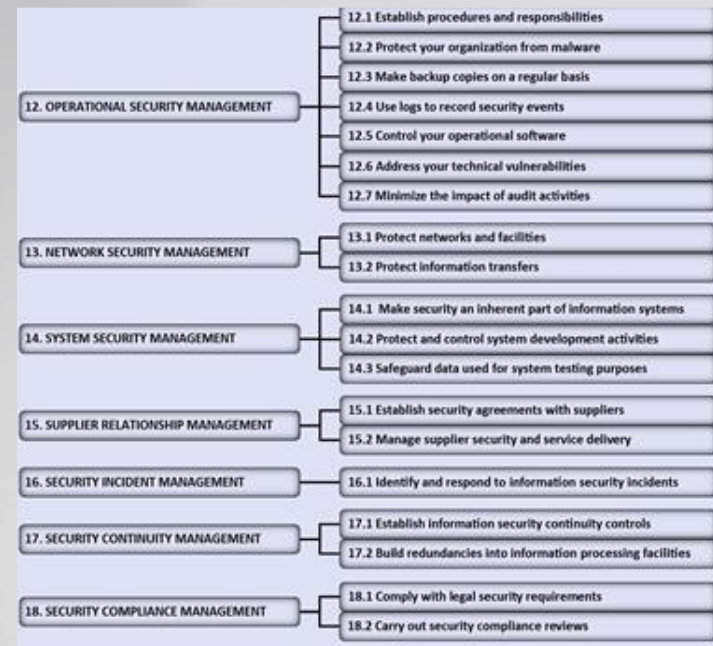
# Control Functional Domain Relationships (FAIR-CAM)



# Loss Event Control Functions (FAIR-CAM)

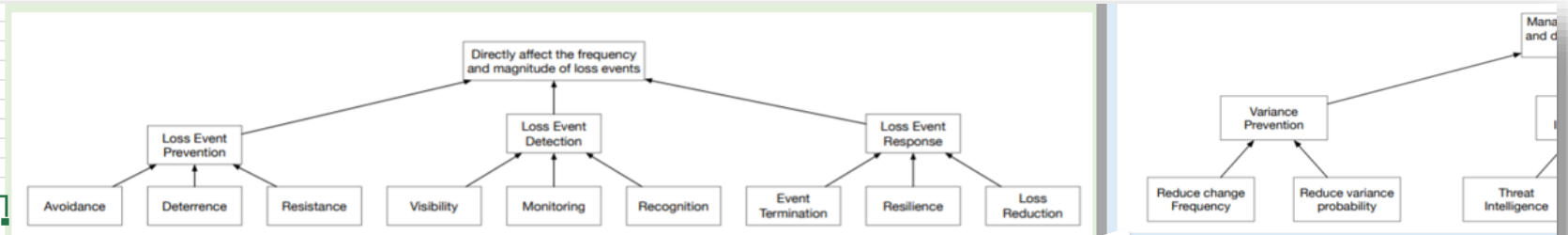


# ISO controls and FAIR factors



USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

# PHASE 2: ISO 27001 TO FAIR CAM: A MAPPING TRIAL

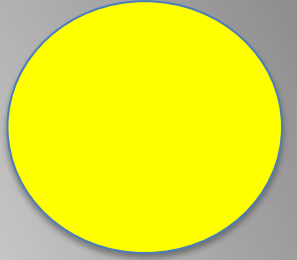


Ref #	Control Framework Elements	Loss Event Control Functions							Variance Manager		
		Prevention			Detection			Response	Prevention		Ident
		Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Event termination	Change Chg Freq	Reduce Var Prob	Threat Intel
8	Asset Management										
8.1	Responsibility for assets										
8.1.1	Inventory of assets										
8.1.2	Ownership of assets										
8.1.3	Acceptable use of assets										
8.1.4	Return of assets										
8.2	Information classification										
8.2.1	Classification of information										

Work in progress!

- One-To-Many mapping
- Direct and "indirect" mapping ISO 27001 <> FAIR CAM
  - Direct mapping (ISO to FAIR): for each ISO control it is determined which categories of FAIR CAM are affected.
  - "Indirect" (or reverse) mapping (FAIR to ISO): for each FAIR CAM category, using its description and available examples, we determine which ISO controls contribute to the category.
- The two mappings are complementary in reducing the uncertainty deriving from the interpretation of ISO and FAIR CAM controls

# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - **ADJUSTMENT OF PROJECT GOALS**
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A



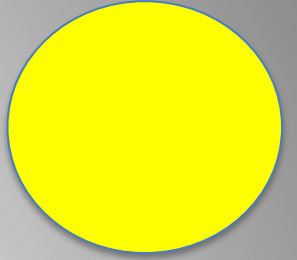
# Adjustment of the project goals

In the context of a **defined risk scenario**, **estimate the effectiveness of ISO controls** mapping them to **FAIR-CAM**.

Meanwhile, ISO 27002:2021 has reached the final stage of approval and is in the process of becoming ISO 27002:2022.

**WE HAVE** decided to adopt ISO 27002:2022 as the basis of our work

# Agenda

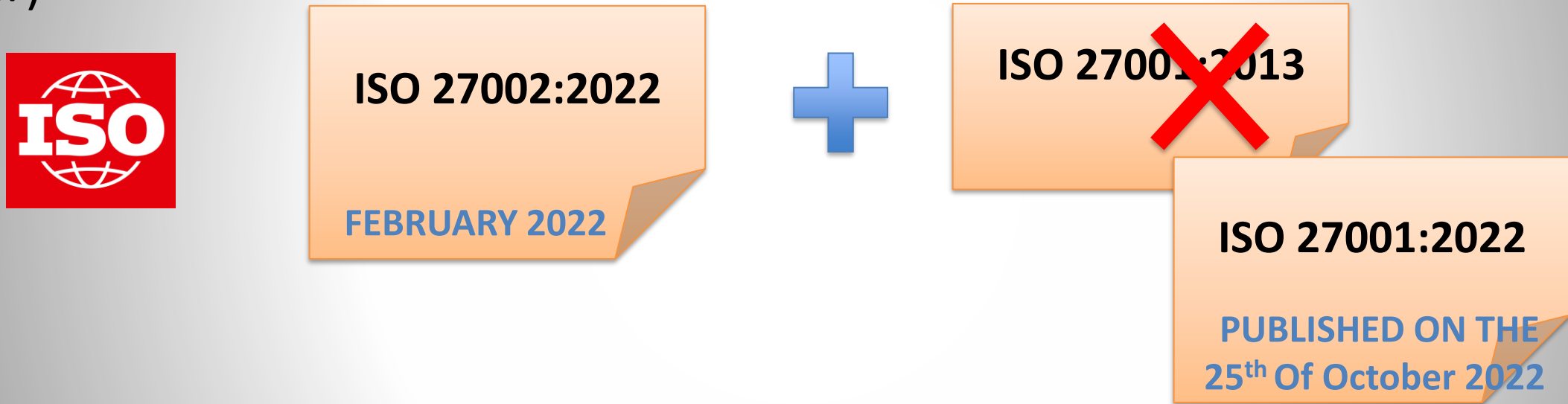


- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - **THE NEW ISO27002:2022**
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

# THE NEW ISO 27002:2022

## An uncommon process of publication

ISO27002 already published, has been followed by the new 27001 (8 months later)



And the other standards linked to ISO 27002?

ISO/IEC  
27017:2015

ISO/IEC  
27018:2019

ISO/IEC  
27701:2019

USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A  
FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

# THE NEW ISO 27002:2022

## Major changes in ISO27002 for mapping purposes (1/2)

### TITLE

- The ‘**Code of Practice**’ has been **dropped** from the title => reflects the intended use of the 2022 version as a **reference set** of generic information security controls and guidance.
- Its full title is now ‘**Information security, cybersecurity, and privacy protection — Information security controls.**’ which reflects a broader context and that **preventing, detecting, and responding** to cyberattacks is now **considered as well as protecting data**.

### CONTROLS

- The ISO 27002:2022 update consists of 93 controls rather than the previous 114.
  - 58 have been updated
  - 24 controls represent the merging of previous controls
  - 11 new controls have been introduced

### THEMES

- The controls are now grouped in 4 ‘themes’ rather than the previous 14 clauses:
  - Organisational (37 controls)
  - Technological (34 controls)
  - Physical (14 controls)
  - People (8 controls)

# THE NEW ISO 27002:2022

## Major changes in ISO27002 for mapping purposes (2/2)

### ATTRIBUTES

- Another significant change is the introduction of 5 + 'attributes' where you can assign hashtags to controls to enable you to filter, sort, or present controls in different ways, i.e., by:
  - **Control type**, (e.g., preventive, detective, corrective, etc).
  - **Information security properties** (relating to confidentiality, integrity, availability).
  - **Cybersecurity concepts** (following ISO 27110, like the NIST CSF approach, with identify, protect, detect, respond, recover)
  - **Operational capabilities** (e.g., governance, asset management, information protection, human resource security, physical security, system and network security, application security, secure configuration, identity and access management, threat and vulnerability management, continuity, supplier relationships security, legal and compliance, information security event management, security assurance).
  - **Security domains**. (e.g., governance and ecosystem, protection, defence, resilience).

Users have the freedom to **create their attributes** to meet the specific needs of their organization. For example, if you have defined risk treatment plans, you could associate a **risk scenario** attribute with each affected control.

It is **not mandatory** to use attributes, however, it is argued their use will make an organization's controls categorization process easier.

# THE NEW ISO 27002

## Attributes (1/5)

### A) Control Type (#preventive, #detective, #corrective)

- Control type is an attribute to view controls from the perspective of **when and how the control changes the risk** with respect to the occurrence of an information security incident
- Attribute values consist of
  - Preventive (the control that aims to prevent the occurrence of an information security incident)
  - Monitoring (control acts when an accident occurs information security)
  - Corrective (control acts after an information security incident has occurred)





# THE NEW ISO 27002

## Attributes (2/5)

### B) Information security properties

- The information security properties are an attribute to display the controls in consideration of the **characteristic** of the information that **you want to preserve**.
- Attribute values consist of:
  - Confidentiality
  - Integrity
  - Availability



# THE NEW ISO 27002

## Attributes (3/5)

### C) Concepts of information security

- Cybersecurity concepts are an attribute to display controls from the point of view of the **association of controls to cybersecurity concepts defined in the cybersecurity framework** as described in TS 27110\*.
- Attribute values consist of:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover



\* ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection —Cybersecurity framework development guidelines

# THE NEW ISO 27002

## Attributes (4/5)

### D) Operational capabilities

- Operational capabilities are an attribute for viewing controls from the **perspective of the information security capability practitioner**.




- Attribute values consist of:
  - Governance
  - Asset\_management
  - Information\_protection
  - Human\_resource\_security
  - Physical\_security, System\_and\_network\_security
  - Application\_security
  - Secure\_configuration
  - Identity\_and\_access\_management
  - Threat\_and\_vulnerability\_management
  - Continuity
  - Supplier\_relationships\_security
  - Legal\_and\_compliance
  - Information\_security\_event\_management
  - Information\_security\_assurance

# THE NEW ISO 27002

## Attributes (5/5)

## E) Security domains

- Security domains are an attribute for viewing controls from the perspective of information security domains, skills, services, and products.
- 
- Attribute values consist of:
    - Governance\_and\_Ecosystem
    - Protection
    - Defense
    - Resilience
- 
- The image shows a stylized world map in dark blue. Overlaid on the map is a complex network of glowing nodes and connecting lines. The nodes are represented by various icons such as airplanes, factories, mailboxes, and people, all enclosed in circular frames. Some nodes are illuminated with bright blue light, while others have a reddish glow. The lines connecting the nodes form a web-like pattern across the continents, suggesting a global network or data flow.



# THE NEW ISO 27002

## Moving from compliance to effectiveness evaluation

The changes in ISO 27002:2022 represent a significant evolution



The **reduction in the number of controls** has been accompanied by a migration of **controls toward greater complexity**, i.e., most controls are processes and not individual operations.

Analysis of the **controls** shows that they are **often** not a single process but there **are several subprocesses**.

**Triggering** of processes and their subprocesses can occur by other processes or due to events detected by other controls; triggering is also activated by time deadlines such as, for example, periodic ISMS reviews.

This is a **dynamic mechanism**, composed of various entities some of which are triggered independently or on a time basis while others act on **"dependency" relationships** with other controls.

The categorizations of controls according to Themes and **the introduction of Attributes** allow the "reading" of the standard according to "viewpoints" that enable its use aimed at user needs (e.g., Operational Capabilities) or a **better interface with other frameworks** (NIST CSF, ISO 27110) as in the case of Cybersecurity Concepts.

This evolution of the standard, in our opinion:

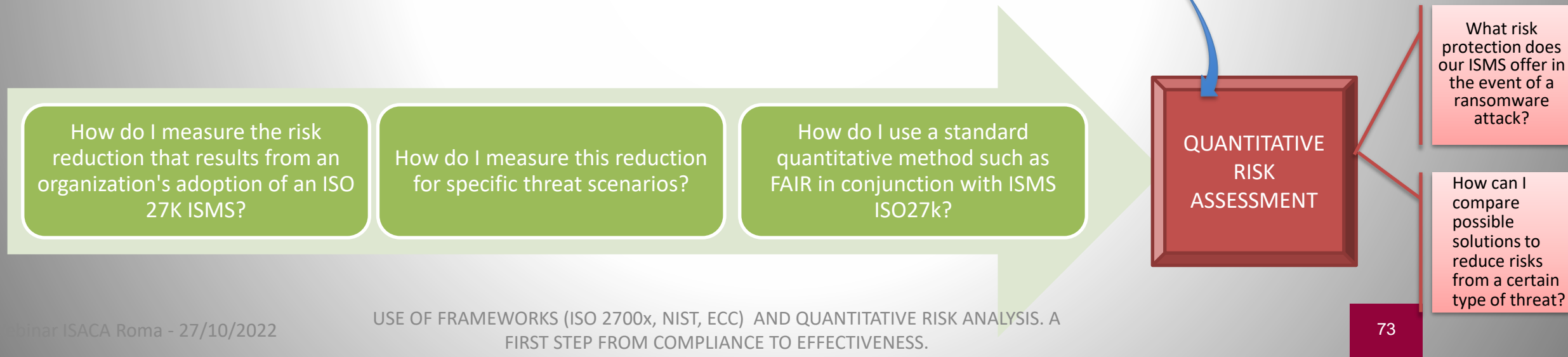
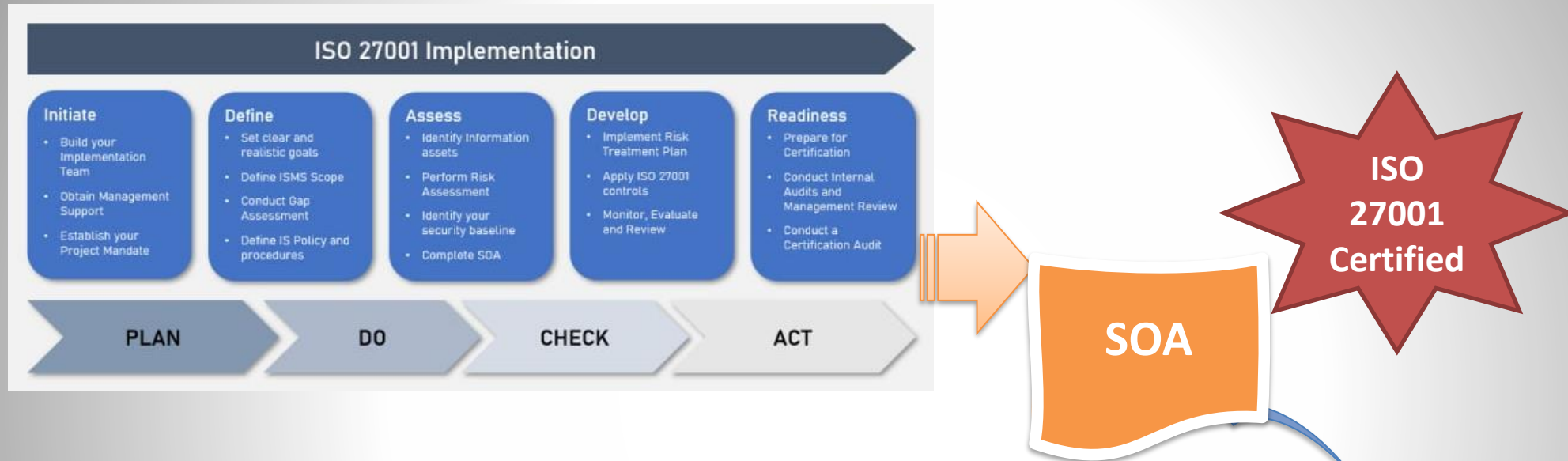
- has changed its nature by making it a **complex system**
- composed of **numerous processes**
- that are **interconnected**
- by various types and **degrees of "dependencies."**

This change has made some assessments such as, for example, measuring the effectiveness of the controls, i.e., the processes and subprocesses contained in them, very complex.



# THE NEW ISO 27002

## Certification, Compliance, Controls Effectiveness





# THE NEW ISO 27002 – The controls relationship

- The ISO 27002:2022 standard is also distinguished by the large number of references that are contained to indicate that a control refers to other controls.
- In addition to the relationships explicitly expressed in the Standard, we added several relationships that can be easily derived by reading the text of the Standard for each control.

## 5.4 Management responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

### Control

Management should be a role model for information security and require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

### Guidance

Management should demonstrate support of the information security policy, topic-specific policies, procedures and controls for information security.

- d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see 6.3);



## 6.3 Information security awareness, education and training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

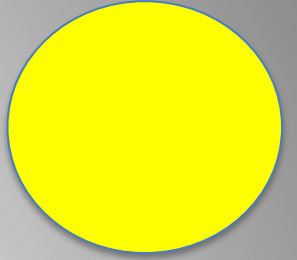
### Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of organizational policies and procedures, as relevant for their job function.

### Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - **ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS**
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

# Compliance, SOA, risk evaluation

Among the main merits of the ISO 27k standard is the **third-party certification of the ISMS**. The certification process is essentially based on **compliance with** the standard and primarily on the **Statement of Applicability (SoA)**.

**But compliance is not sufficient to answer** the typical questions that require a quantitative risk assessment such as:

- **What risk protection**, in terms of direct and indirect damage, **does our ISMS offer in the event of a ransomware attack?**
- **How can I compare, from the perspective of damage reduction in terms of lower expenses, possible solutions** to reduce risks from a certain type of threat?

We are therefore **back to the initial questions viz:**

- **How do I measure the risk reduction that results from an organization's adoption of an ISO 27K ISMS?**
- **How do I measure this reduction for specific threat scenarios?**
- **How do I use a standard quantitative method such as FAIR in conjunction with ISMS ISO27k?**

# Effectiveness of ISO 27k controls?

Therefore, to answer these questions, we need to analyze the ISO 27k standard from a different perspective, namely, trying to evaluate the **effectiveness of the controls**.

Due to the **complex relationships among controls, we cannot just evaluate controls individually** but must consider the set of relationships that exist between them and how these relationships affect the effectiveness of the controls.

The questions we must answer to evaluate the overall effectiveness of the controls in an ISMS are:

- how do we identify the types of relationships among the various controls?
- how can we assess the "strength" of these relationships?
- how can we "calculate" the combined effect of multiple controls distributed across multiple levels of interactions?

# Interdependent systems some considerations

- Baruch Spinoza, the famous Dutch philosopher who lived more than three centuries ago, urged(\*) that each unit of a system be considered interdependent on the others;
- The complex system represented by an ISMS can be described, in a simplified way, **as a fishing net**. Each **control** is related to **several other controls** that "influence" its "capabilities" by enhancing or decreasing them. As a first approximation, the rule that "the whole is greater than the sum of its individual components" applies, although,...
- Following the comparison of the fishing net, we will then have to assess **whether our ISMS has those characteristics of completeness and integrity that allow its use and make an initial assessment of its "strength."**
- At this point we have a **net that we know is complete and "strong", but we have no idea if it will be suitable for the type of fish we want to catch**. That is, ending the comparison with fishing, **we need to define the scenario in which we want to measure the actual capacity**.



(\*) Baruch Spinoza, letter 32 to Henry Oldenburg, November 1665  
USC OF CRIMINAL JUSTICE, EDU AND QUANTITATIVE RISK ANALYSIS. A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.



# References among controls of ISO 27002:2022

- The ISO 27002:2022 standard is also distinguished by the large number of references that are contained to indicate that a control refers to other controls.
- In addition to the relationships explicitly expressed in the Standard, we added some relationships that can be easily derived by reading the text of the Standard for each control.

## 5.4 Management responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

### Control

Management should be a role model for information security and require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

### Guidance

Management should demonstrate support of the information security policy, topic-specific policies, procedures and controls for information security.

- d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see 6.3);



## 6.3 Information security awareness, education and training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

### Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of organizational policies and procedures, as relevant for their job function.

### Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

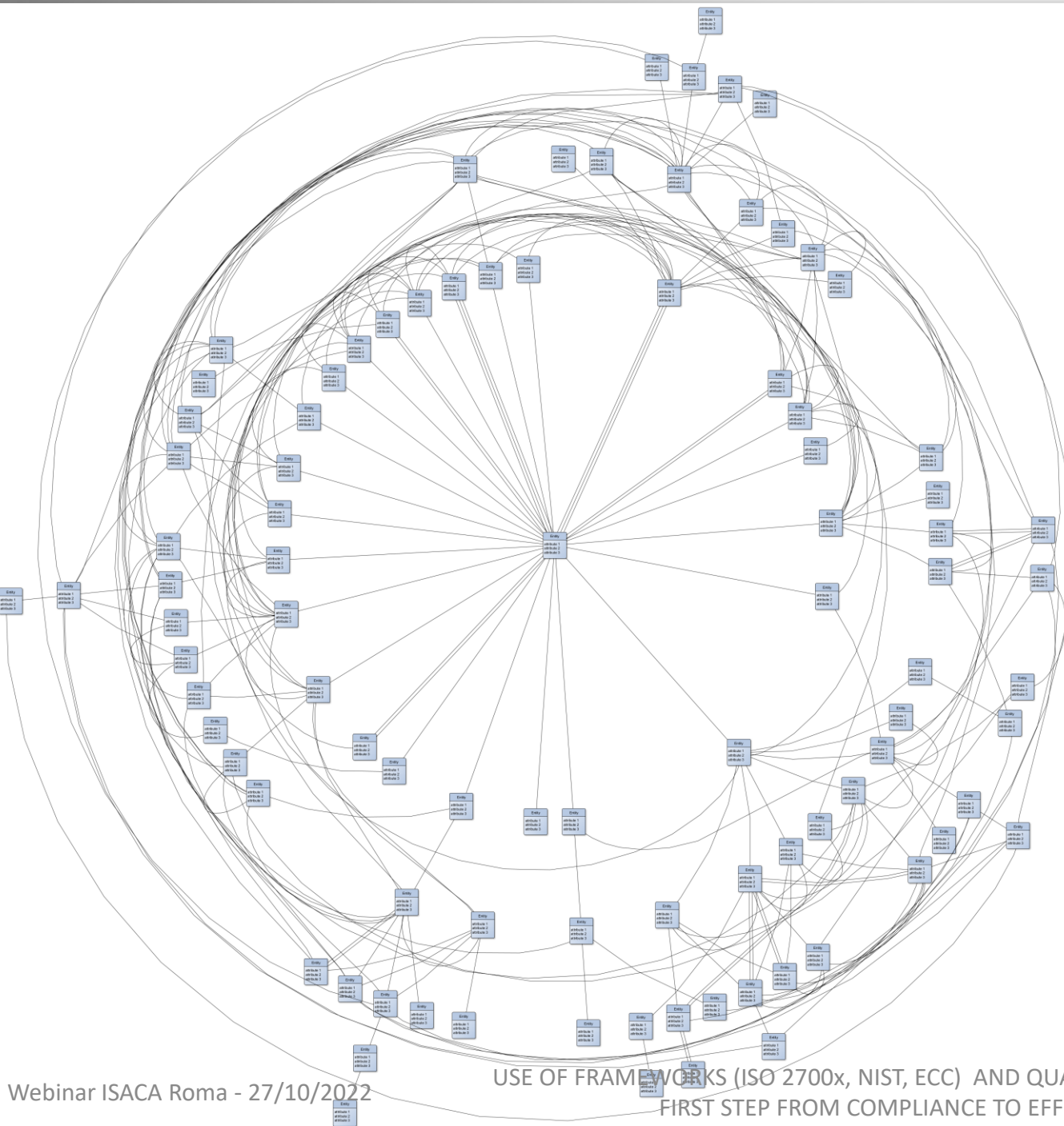


# How to model the set of ISO 27k relations?

- To represent this set of relations **we built a graph**, having as **nodes the individual ISO controls** and as **edges the relationship that exists between a control A and a control B**. This choice also **allows us to "explore" the ISO 27002 standard** by using the relationships between the controls.
- We derived the relationships **semi-automatically from the text of the standard**.
- We built a tool that would check graphs for **completeness and absence of loops** because they provoke the impossibility of stopping the chain of relations.

# ISO Controls Physiology

- 93 Controls
- 285 dependency relations



USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A  
FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

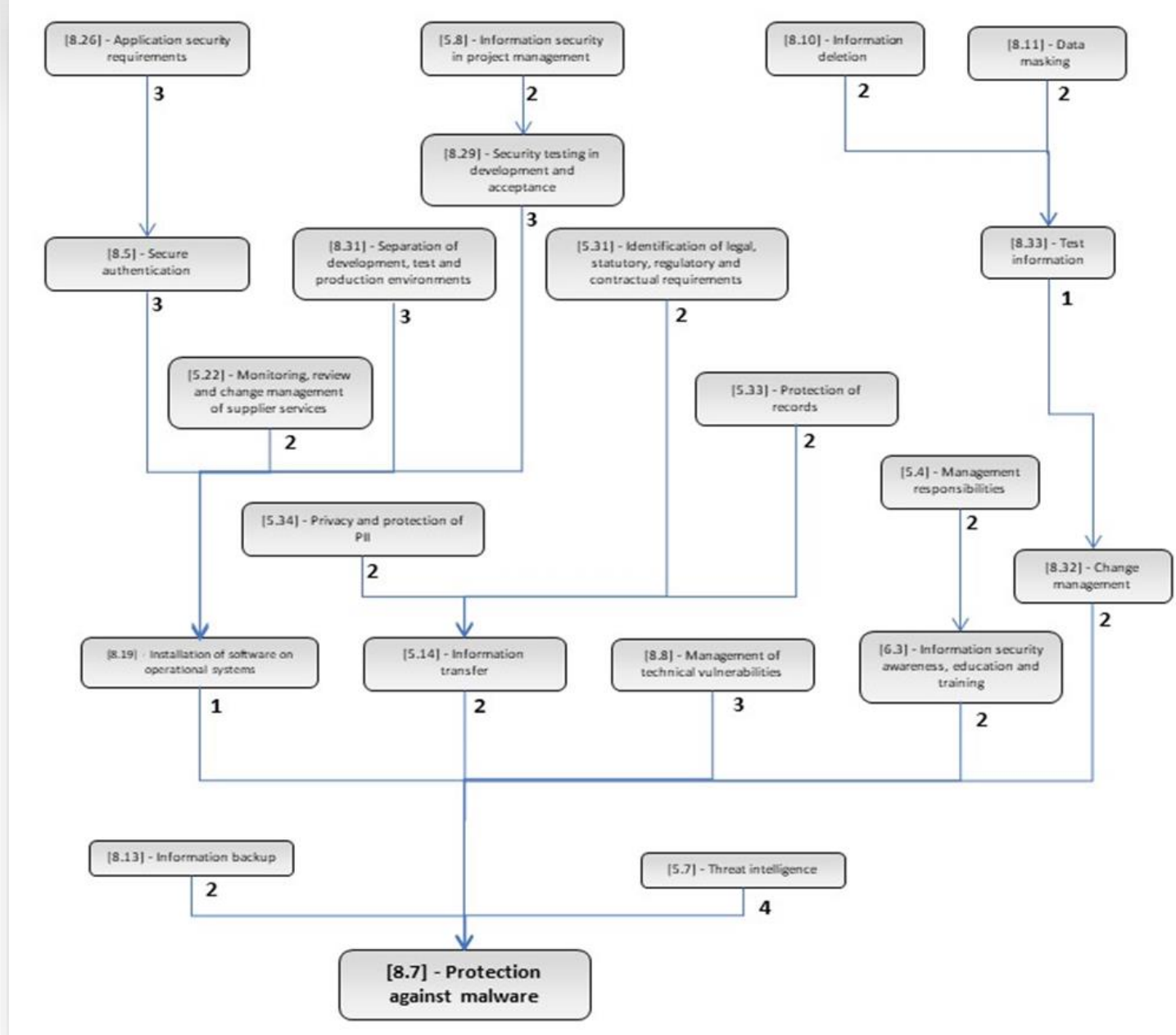
# How to model the set of ISO 27k relations?

To define the type of relationship, we find that a very simple paradigm could be adopted.

1. Some controls have “dependent” controls, e.g., *5.4 Management responsibilities* and *6.3 Information security awareness, education and training* **are in a relationship in which 6.3 “depends” on 5.4.**
2. Controls that **have only “dependents” controls are origin nodes** in the graph.
3. Controls that **have no “dependents” are terminal nodes.**

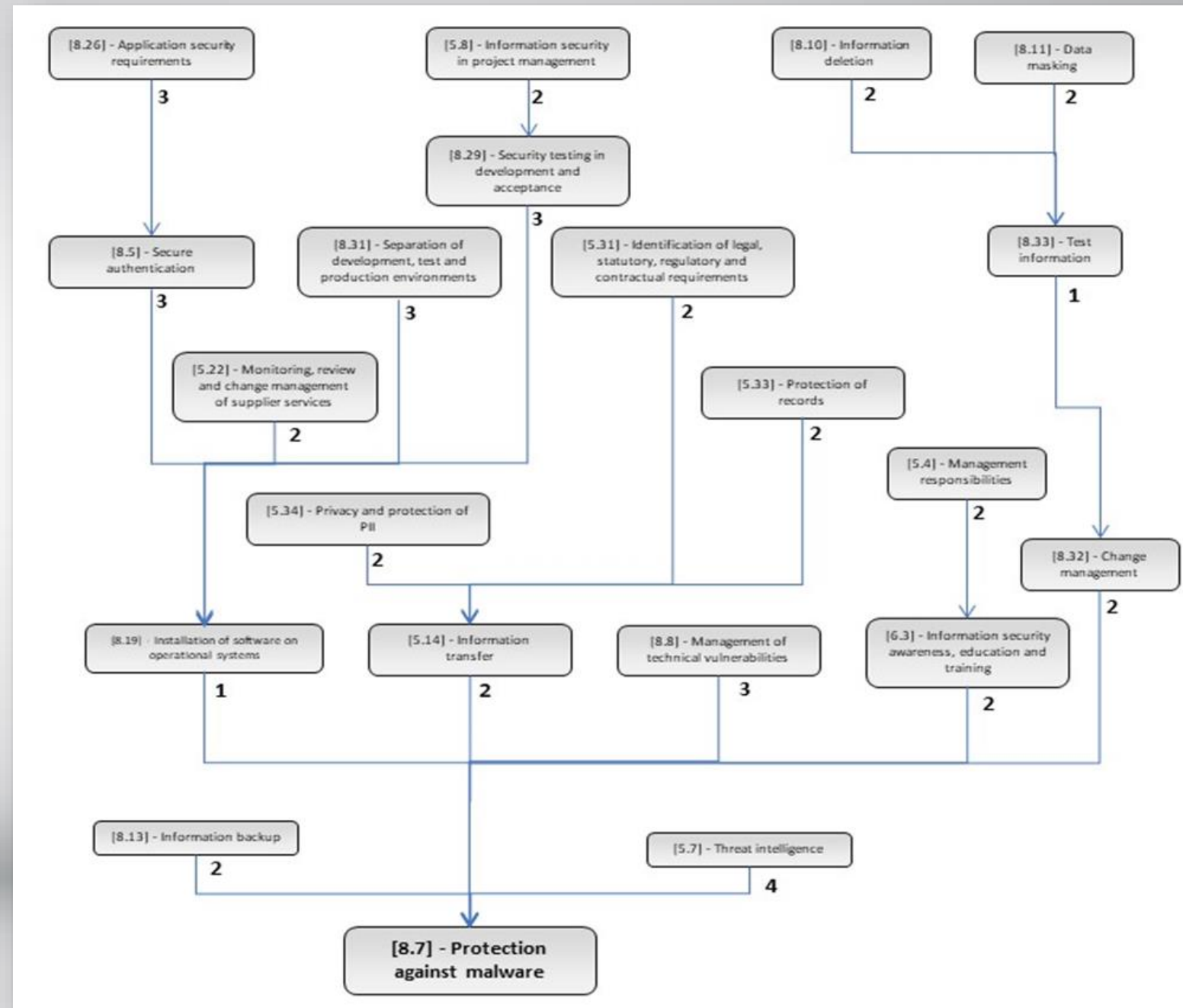
# Example of part of the graph

- Many interesting considerations can be derived from the “exploration” of the graph, they are relevant to experts that want to analyse ISO 27002 in-depth.
- To give an idea of the complexity of the Standard it is interesting to look at this schema which presents a part of the graph, not the most complex one.



Once the graph of relationships between controls is defined, the problem arises of **understanding how these relationships operate**, i.e., we need to find a satisfactory answer to the following observations:

- 1) the relationships between the controls are not all the same, concerning previous example it is quite evident, based on the simple experience of an expert, that the "influence" of control [5.7] - *Threat intelligence* on [8.7] - *Protection against malware* is "greater" than control [5.14] - *Information transfer* which defines the general rules by which information is to be transferred; therefore, we need to determine a method for expressing this difference.
- 2) it is evident from the example that control [8.7] - *Protection against malware* is the terminal point of many relationships that are articulated on different levels. Therefore, we need to define a method to evaluate the contribution of all these relationships.





## Control to control weight of the relationship

- The first step in understanding and evaluating the combined effect of the controls from the relationships (which represent the edges that connect the nodes, the controls) **is to define a scale of values that allows weight to be given to the relationships between two controls** that are connected according to the graph.
- **No ISO documentation indicates** the importance of such relationships. Consequently, the **authors have included their evaluation as experts** in the Excel tool; it relates to the type of controls and is intended to best define the degree of dependence between the controls
- To indicate **the weight of the relation among controls** **we defined the following scale of values:**
  1. the two controls are completely independent (**logical OR**)
  2. there is a very weak relationship between the 2 controls
  3. there is a weak relationship between the 2 controls
  4. there is a dependence between the 2 controls
  5. the 2 controls are related by a strong dependence
  6. the 2 controls are closely dependent (**logical AND**)



A1W2 Update

Controls iterative  
adjustment

5 Iterations

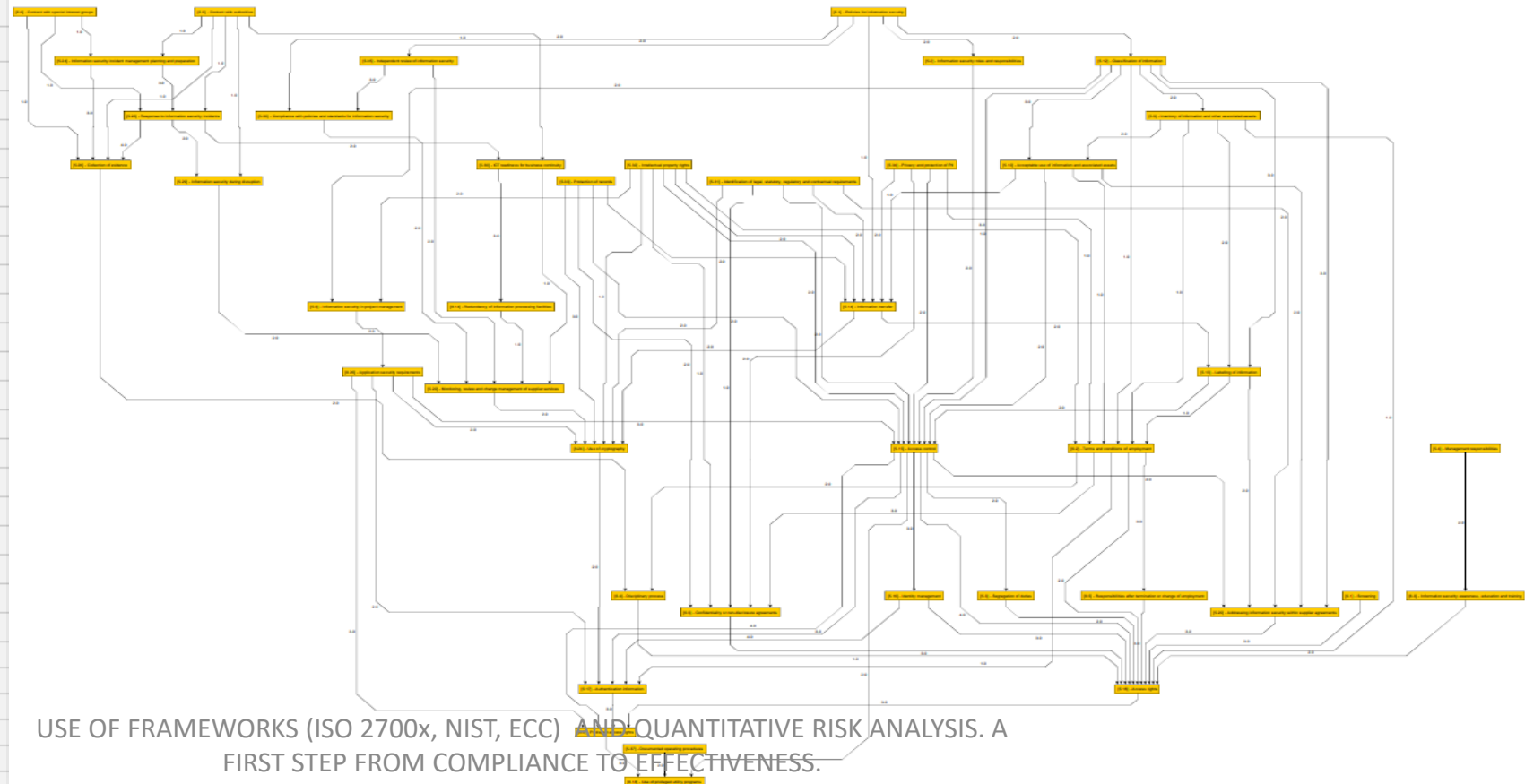
Gen. Links list

Gen. Ctl. Tree

		Depend.	Lnks/ Ctls
Control ID	8.18	D	Ctls
max dist	10		

## 8.18: Capability Tree

Use of privileged utility programs



USE OF FRAMEWORKS (ISO 2700x, NIST, ECC) AND QUANTITATIVE RISK ANALYSIS. A FIRST STEP FROM COMPLIANCE TO EFFECTIVENESS.

### Operational Capabilities & Risk Scenarios

	Governance
	Asset_management
	Information_protection
	Human_resource_security
X	Physical_security
	System_and_network_security
	Application_security
	Secure_configuration
	Identity_and_access_management
	Threat_and_vulnerability_management
	Continuity
	Supplier_relationships_security
	Legal_and_compliance
	Information_security_event_management
	Information_security_assurance
	Risk Scenario 1
	Risk Scenario 2
	Risk Scenario 3
	Risk Scenario 4
	Risk Scenario 5

## How to refine the controls' capability within an ISO 27k ISMS.

Following our approach to give the Expert the highest flexibility in reducing uncertainty, **we defined a tool to refine the ISO 27k controls' capability estimates initially expressed by the Expert using the SoA**

- **Initial Expert's capability estimates** are given using a **value between 0 and 5 according to a scale based on the CMMI scale with the option of associating a Confidence value** to indicate the level of confidence the expert attributes to his or her estimate.
- The **Expert's initial estimates** are expressed on a **control-by-control** basis and **will not consider** the ISMS ISO27k complex relationships that exist between controls.
- The purpose of **this step is to give the Expert the opportunity to refine his or her assessments to make them "consistent" with an computation that includes the relationships among the various controls** and then "adjusts" the capability of each ISO control.
- This step uses the graph derived from the Standard and it provides an assessment, according to a viewpoint definable as *ISO internal*, of the combined effect of the controls, giving the Expert the possibility to confirm or modify the initial estimate.

## A little insight into the refinement process

- The refinement algorithm explores the graph using a classical method for Direct Acyclic Graph (DAG) type graphs.
- The overall capability value of each control is calculated by weighing the individual contributions of the controls that are related to it. The formula behave as a probabilistic OR for independent controls and progressively become an AND in the case of a closely dependent relationship.
- The formula is the result of choosing, among several alternatives, a "simple" tool that would allow for uncertainty reduction and would not involve defining other parameters and variables that would require further evaluation by the Expert.
- The proposed algorithm and formula reflect our approach to reducing uncertainty; the Expert may define an algorithm and formula that he deems most appropriate.



# Example of the overall consistency of ISO controls

**CMMI 1** are the Expert's initial values

**CMMI2** are the values computed using the internal relationships of the ISMS

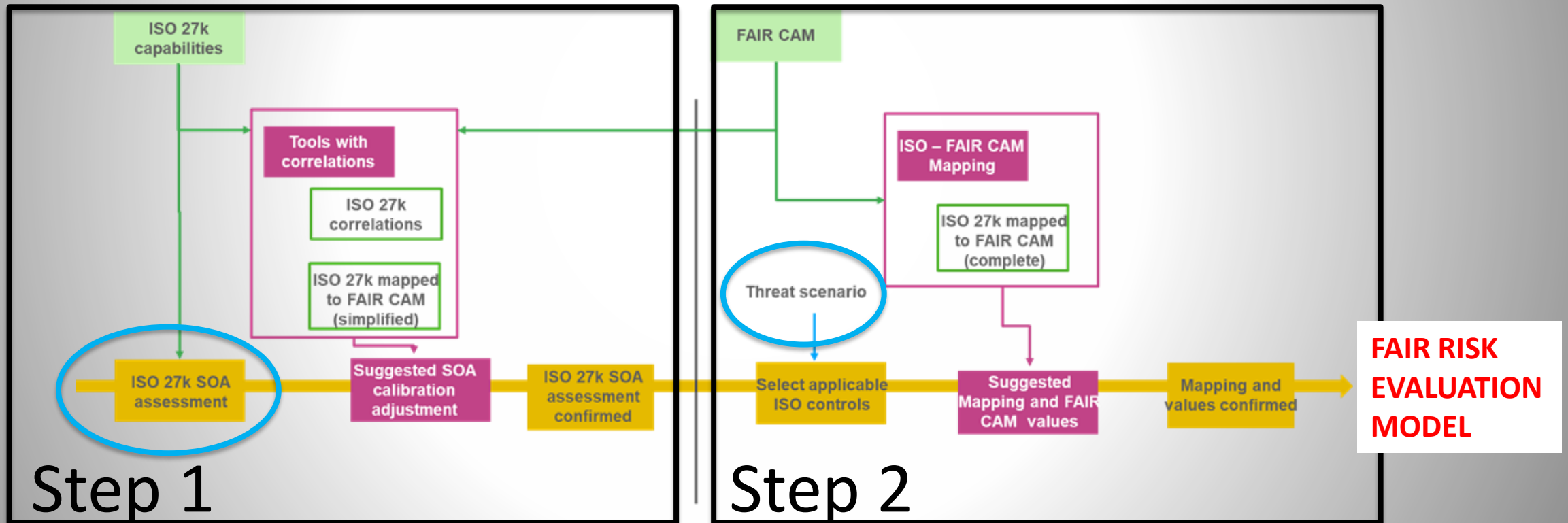
ID	Control Name	CMMI 1	CMMI 2	Suggested CMMI correction	
5.1	Policies for information security	3,00	3,00	→	0,00
5.2	Information security roles and responsibilities	2,00	2,94	→	0,94
5.3	Segregation of duties	0,00	2,05	↑	2,05
5.4	Management responsibilities	2,00	2,00	→	0,00
5.5	Contact with authorities	5,00	5,00	→	0,00
5.6	Contact with special interest groups	0,00	0,00	→	0,00
5.7	Threat intelligence	3,00	3,00	→	0,00
5.8	Information security in project management	3,00	1,47	↓	-1,53
5.9	Inventory of information and other associated assets	3,00	2,88	→	-0,13
5.10	Acceptable use of information and associated assets	1,00	2,85	↑	1,85
5.11	Return of assets	3,00	2,12	→	-0,88
5.12	Classification of information	2,00	2,94	→	0,94
5.13	Labelling of information	3,00	2,64	→	-0,36
5.14	Information transfer	3,00	2,14	→	-0,86
5.15	Access control	1,00	2,21	↑	1,21
5.16	Identity management	5,00	2,36	↓	-2,64
5.17	Authentication information	3,00	2,09	→	-0,91
5.18	Access rights	3,00	2,16	→	-0,84
5.19	Information security in supplier relationships	3,00	2,57	→	-0,43
5.20	Addressing information security within supplier agreements	1,00	2,32	↑	1,32
5.21	Managing information security in the ICT supply chain	4,00	4,00	→	0,00
5.22	Monitoring, review and change management of supplier ser	3,00	3,37	→	0,37
5.23	Information security for use of cloud services	4,00	3,66	→	-0,34
5.24	Information security incident management responsibilities a	3,00	2,51	→	-0,49
5.25	Assessment and decision on information security events	4,00	2,63	↓	-1,37
5.26	Response to information security incidents	0,00	2,49	↑	2,49
5.27	Learning from information security incidents	2,00	2,41	→	0,41
5.28	Collection of evidence	0,00	2,49	↑	2,49
5.29	Information security during disruption	1,00	3,70	↑	2,70
5.30	ICT readiness for business continuity	2,00	3,71	↑	1,71

# Mapping: two different steps

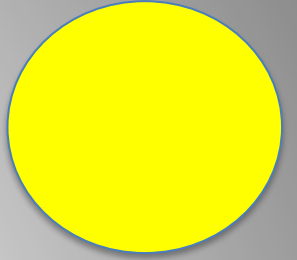
The approach allows two different steps of evaluation:

1. Comprehensive ISO 27k-based assessment and first FAIR CAM evaluation(simplified mapping)
2. Specific risk scenario evaluation in terms of quantitative risk as for the FAIR-CAM model (complete mapping)

For each step, one or more tools are available



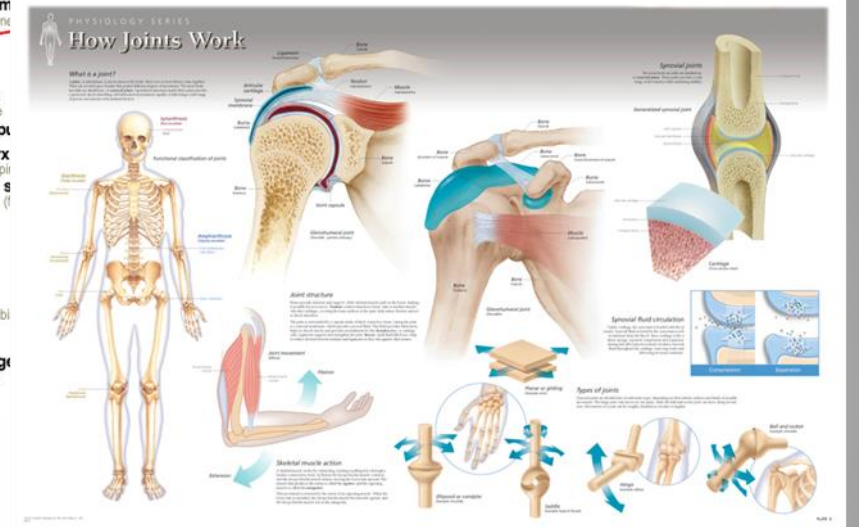
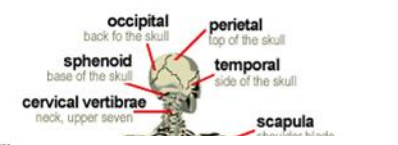
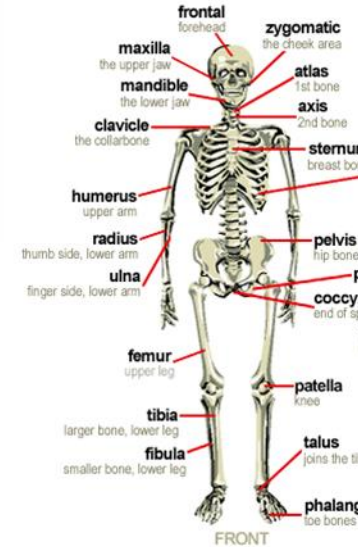
# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - **SIMPLIFIED MAPPING and SOAs**
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A



# Where we are now



ISMS  
SOA information

Adding:

- Relationships
- Relative strengths
- Coherence checks

An image of the working system that is behind it

# Bridge, caution!

- Assigning a correspondence between the elements of one set and those of another:
  - Controls of the ISMS
  - Control categories of the FAIR-CAM model (Loss Event Controls- LEC, Variance Management Controls- VMC, Decision Support Controls-DSC)



# ISO to FAIR-CAM

- Qualitative or quali-quantitative inputs
- Single level (type) of controls
- Subsystems
- Some relationships explained

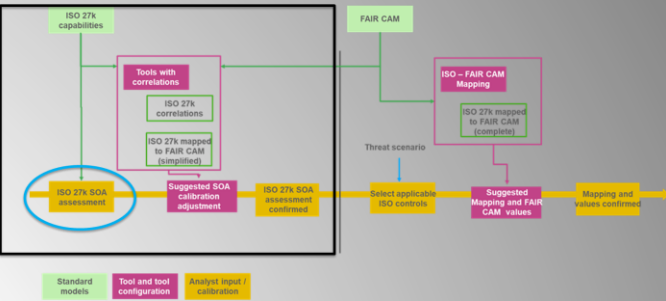


- Distributions
- Three categories (types) of controls
- Functions
- Relationships are integral parts of the model

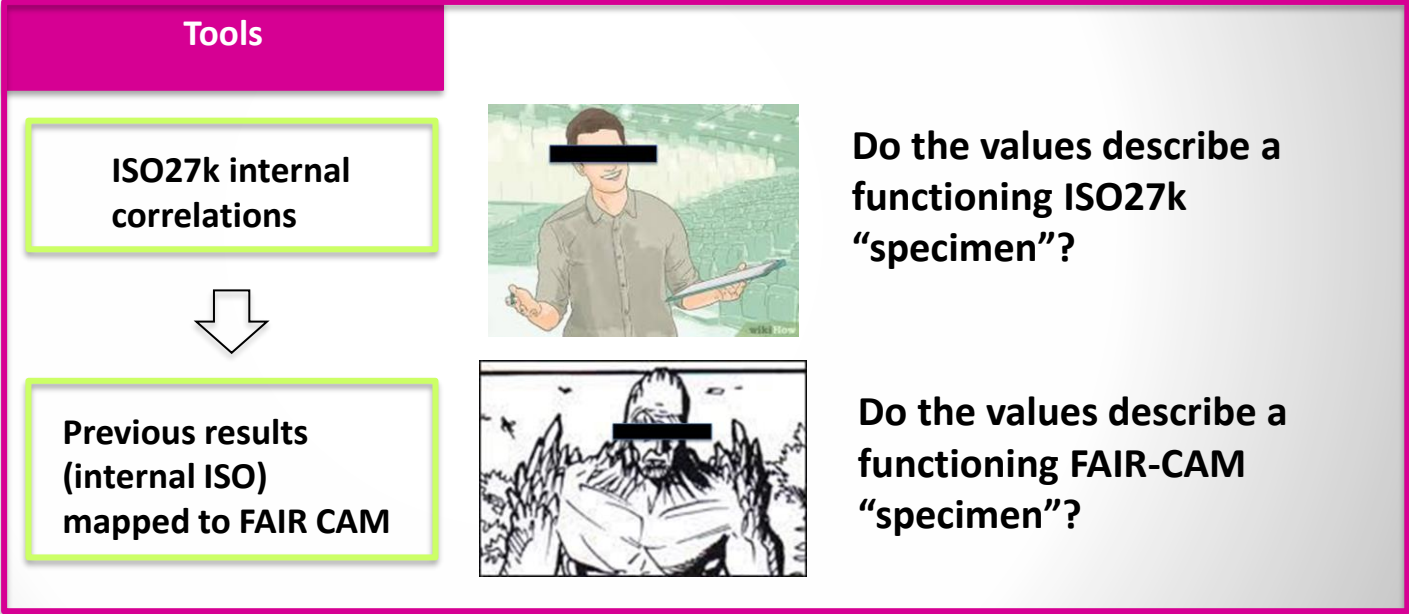


Quantum man, Bonelli Editore

# ISO to FAIR-CAM: correlation analysis



ISO27k SOA  
- Assessment -



ISO27001

FAIR-CAM



# ISO to FAIR-CAM: simplified mapping

For this step:

- ISO controls are **classified according to FAIR-CAM ontology and model**
  - FAIR-CAM categories of controls (LEC, VMC, DSC) are associated to ISO controls
  - FAIR-CAM subcategories (functions) are not used here

We call it **simplified mapping**

# ISO to FAIR-CAM: controls to control functions

ISO/IEC 27002 control identifier	Control name	Control function		
		LEC	Variance	Decision
<a href="#">5.1</a>	Policies for information security		x	x
<a href="#">5.2</a>	Information security roles and responsibilities		x	x
<a href="#">5.3</a>	Segregation of duties	x		x
<a href="#">5.4</a>	Management responsibilities		x	x
<a href="#">5.5</a>	Contact with authorities		x	x
<a href="#">5.6</a>	Contact with special interest groups		x	x
<a href="#">5.7</a>	Threat intelligence		x	x
<a href="#">5.8</a>	Information security in project management	x	x	x
<a href="#">5.9</a>	Inventory of information and other associated assets		x	x
<a href="#">5.10</a>	Acceptable use of information and associated assets		x	x
<a href="#">5.11</a>	Return of assets	x		
<a href="#">5.12</a>	Classification of information		x	x
<a href="#">5.13</a>	Labelling of information		x	x
<a href="#">5.14</a>	Information transfer	x	x	x
<a href="#">5.15</a>	Access control			x
<a href="#">5.16</a>	Identity management	x	x	x
<a href="#">5.17</a>	Authentication information	x	x	x
<a href="#">5.18</a>	Access rights	x	x	x
<a href="#">5.19</a>	Information security in supplier relationships	x	x	x
<a href="#">5.20</a>	Addressing information security within supplier agreements		x	x
<a href="#">5.21</a>	Managing information security in the ICT supply chain	x	x	x
<a href="#">5.22</a>	Monitoring, review and change management of supplier services		x	x
<a href="#">5.23</a>	Information security for use of cloud services		x	x
<a href="#">5.24</a>	Information security incident management responsibilities and preparation		x	x
<a href="#">5.25</a>	Assessment and decision on information security events		x	x
<a href="#">5.26</a>	Response to information security incidents	x	x	x
<a href="#">5.27</a>	Learning from information security incidents		x	x
<a href="#">5.28</a>	Collection of evidence		x	x
<a href="#">5.29</a>	Information security during disruption	x	x	x
<a href="#">5.30</a>	ICT readiness for business continuity	x	x	x
<a href="#">5.31</a>	Identification of legal, statutory, regulatory and contractual requirements		x	x
<a href="#">5.32</a>	Intellectual property rights	x	x	x

- All the mappings have been run through different experts to define an average profile
- A special focus is on ISO controls that are mapped as LECs, since these contribute as a direct input to the risk calculation.



# ISO to FAIR-CAM: simplified mapping considerations

The simplified mapping shows that most ISO controls belong to more than one FAIR-CAM category

FAIR-CAM Functional Domain	Number of mapped ISO controls
Loss Event Control Functions (only)	17
Variance Management Control Functions (only)	0
Decision Support Control Functions (only)	1
Variance <i>AND</i> Decision (not LOSS)	33
Loss <i>AND</i> Variance (not Decision)	5
Loss <i>AND</i> Decision (not Variance)	5
Loss <i>AND</i> Variance <i>AND</i> Decision	32
<b>Total</b>	<b>93</b>

## Multilayering and granularity

- Most ISO controls are associated to multiple FAIR-CAM categories of controls, this confirms the richness of ISO controls
- More than 66 % of them that include the decision-making, monitoring, and correction processes of the controls themselves (Variance and Decision)
- Coarseness of ISO controls hinders mapping – need to define an approach!

# Why “calibration of the schema”?

First, we tried a manual mapping between ISO and FAIR

- Various project pitfalls emerged (complex ISO controls that contain processes and asset-level measures, correlation between controls, not vectorial factors, required accuracy of estimates, identification of calibrating anchors and parameters)

The main issue was that we needed a granular description of how the control impact on risk, at a smaller level of granularity than the ISO description

ISO List	Compilato da:		Prima					Poi														
Controllo ISO			Categoria					Categoria														
			Asset					Asset														
			Threat	Prevention	Vulnerability	Detection	Response	Variance	Decision	Threat	Prevention	Vulnerability	Detection	Response	Variance	Decision						
			Copertura funzionale					Maturità					Copertura funzionale					Maturità				
			38%	28%	58%	10.0%			53.0%	32.5%	58%	10.0%			Miglioramento							
A.12 Sicurezza delle attività operative	A.12.1 Procedure operative e responsabilità	A.12.1.1 - Procedure operative documentate			30.0%		x			30.0%		x		Miglioramento								
		A.12.1.2 - Gestione dei cambiamenti					x							x								
		A.12.1.3 - Gestione della capacità	40.0%				10.0%					10.0%										
		A.12.1.4 - Separazione degli ambienti di sviluppo, di test e produzione	50.0%	10.0%						10.0%												
	A.12.2 Protezione dal malware	A.12.2.1 - Controlli contro il malware	60.0%						80%													
	A.12.3 Backup	A.12.3.1 - Backup delle informazioni		50.0%			x			70%				Miglioramento								
		A.12.4.1 - Raccolta di log degli eventi			40.0%						40.0%											
		A.12.4.2 - Protezione delle informazioni di log	20.0%						20.0%													
		A.12.4.3 - Log di amministratori e di operatori			75.0%						75.0%											
		A.12.4.4 - Sincronizzazione degli orologi					x						x									
		A.12.5 Controllo del software operativo		50.0%						60%												
			A.12.5.1 - Installazione del software sui sistemi di produzione	40.0%						55%												
		A.12.6 Gestione delle vulnerabilità tecniche		40.0%						50%												
		A.12.6.2 - Limitazioni nell'installazione del software	40.0%							20%			x									
	A.12.7 Considerazioni sull'audit dei sistemi informativi	A.12.7.1 - Controlli di audit dei sistemi informativi		20.0%			x			20%			x									

The “schemas” of multiple, real life, **architectures** are included in the tools through the process we adopted to calibrate them



This step required a hypothesis of **architecture** (or “physiology”)  
But which kind of architecture? At which level of detail?

# What does the tool include?



## **Calibration** of the **correlation “schema”** or net

- All the mapping run by experts with different background to normalize results
- The schema may be considered expressions of how architectures (physiologies) appear in a SOA assessment

Proposal of minimum amount of data required (categories not subcategories) – we tested different level of details

## **Tool** and underlying **mathematics**

- Graph: WeakAND, WeakOr., Cumulative effect
- Distributions
- Procedural AI

# Logical elaboration in the tool

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
Type	Std. Pag	D/I	ID1	ID2	Ver 26/7/2022	W	Run	CID	Tot	D	I	Estim. CMMI				Calc. CMMI				ISO Internal Calc Data			FAIR CAM Informative Data			
					min							ml	max	Conf	min	ml	max	Conf	W	CMMI	WA	VAR	DSC	LEC		
A	24				5.18 Access rights			[5.18]	17	6	11					43,21%				VL	44,37%	M		56,48%	32,40%	18,92%
B	13	D	[5.18]	[5.11]	Return of assets	1																				
B	25	I	[5.18]	[5.15]	Access control	4	6														0,80	44,54%	24,31%	0,00%	24,31%	0,00%
B	22	I	[5.18]	[5.16]	Identity management	3	7														0,60	45,91%	30,27%	27,55%	30,27%	30,27%
B	25	I	[5.18]	[5.20]	Addressing information security within supplier agreement	3	7														0,60	46,98%	30,97%	28,19%	30,97%	0,00%
B	25	I	[5.18]	[5.3]	Segregation of duties	2	7														0,40	42,79%	33,07%	0,00%	33,07%	33,07%
B	24	I	[5.18]	[5.9]	Inventory of information and other associated assets	1	2														0,20	58,44%	51,80%	11,69%	51,80%	0,00%
B	25	I	[5.18]	[6.1]	Screening	3	0														0,60	20,00%	13,19%	0,00%	0,00%	13,19%
B	25	I	[5.18]	[6.2]	Terms and conditions of employment	2	6														0,40	48,14%	37,20%	19,25%	37,20%	0,00%
B	25	I	[5.18]	[6.3]	Information security awareness, education and training	2	1														0,40	40,63%	31,40%	16,25%	31,40%	31,40%
B	25	I	[5.18]	[6.4]	Disciplinary process	1	7														0,20	57,62%	51,08%	11,52%	51,08%	51,08%
B	25	I	[5.18]	[6.5]	Responsibilities after termination or change of employment	3	7														0,60	46,64%	30,74%	27,98%	30,74%	0,00%
B	25	I	[5.18]	[6.6]	Confidentiality or non-disclosure agreements	3	7														0,60	37,61%	24,79%	22,56%	24,79%	24,79%
B	62	D	[5.18]	[7.2]	Physical entry	3																				
B	25	D	[5.18]	[8.11]	Data masking	3																				
B	25	D	[5.18]	[8.2]	Privileged access rights	3																				
B	116	D	[5.18]	[8.27]	Secure system architecture and engineering principles	2																				
B	25	D	[5.18]	[8.3]	Information access restriction	3																				
A	26				5.19 Information security in supplier relationships			[5.19]	2	1	1					51,41%				VH	48,66%	VL		14,69%	44,20%	44,20%
B	21	I	[5.19]	[5.16]	Identity management	2	7														0,40	45,91%	36,99%	18,36%	36,99%	36,99%
B	87	D	[5.19]	[8.8]	Management of technical vulnerabilities	2																				
A	28				5.20 Addressing information security within supplier agreements			[5.20]	8	3	5					46,31%				H	46,98%	L		38,35%	37,49%	7,72%
B	28	I	[5.20]	[5.10]	Acceptable use of information and associated assets	2	3														0,40	58,27%	45,76%	23,31%	45,76%	0,00%
B	28	I	[5.20]	[5.12]	Classification of information	3	1														0,60	59,38%	40,25%	35,63%	40,25%	0,00%
B	28	I	[5.20]	[5.13]	Labelling of information	2	5														0,40	53,38%	41,92%	21,35%	41,92%	0,00%
B	21	I	[5.20]	[5.15]	Access control	2	6														0,40	44,54%	34,98%	0,00%	34,98%	0,00%
B	29	D	[5.20]	[5.18]	Access rights	3																				
B	44	I	[5.20]	[5.31]	Identification of legal, statutory, regulatory and contractual	2	0														0,40	20,00%	15,71%	8,00%	15,71%	0,00%
B	30	D	[5.20]	[8.29]	Security testing in development and acceptance	3																				
B	30	D	[5.20]	[8.8]	Management of technical vulnerabilities	2																				
A	30				5.21 Managing information security in the ICT supply chain			[5.21]	1	1	0					80,00%				M	80,0%					
B	31	D	[5.21]	[5.23]	Information security for use of cloud services	2																				
A	31				5.22 Monitoring, review, change management of supplier services			[5.22]	9	4	5					67,38%				L	71,92%	L		37,84%	53,77%	48,34%
B	33	D	[5.22]	[5.23]	Information security for use of cloud services	2																				
B	33	I	[5.22]	[5.29]	Information security during disruption	2	3														0,40	83,54%	72,64%	33,42%	72,64%	72,64%
B	33	I	[5.22]	[5.30]	ICT readiness for business continuity	1	3														0,20	83,63%	78,17%	16,73%	78,17%	78,17%

The elaboration of this logical phase involves:

- The use of interdependencies between controls of ISMS 27k, already used for previous assessments. The contributions to the FAIR-CAM categories (LEC, VMC, DSC) for which the control is mapped are calculated.
- The contributions to the categories (LEC, VMC, DSC) are computed separately.
- The calculation method for the VCM is slightly different to take into consideration the relationships between LEC and VCM



# Logical elaboration in the tool: results

At the end of the processing for each control, the following results are provided in the FAIR CAM Informative Data section:

- The **calculated (suggested) capability** value for that control, if the control is
  - LEC
  - DSC

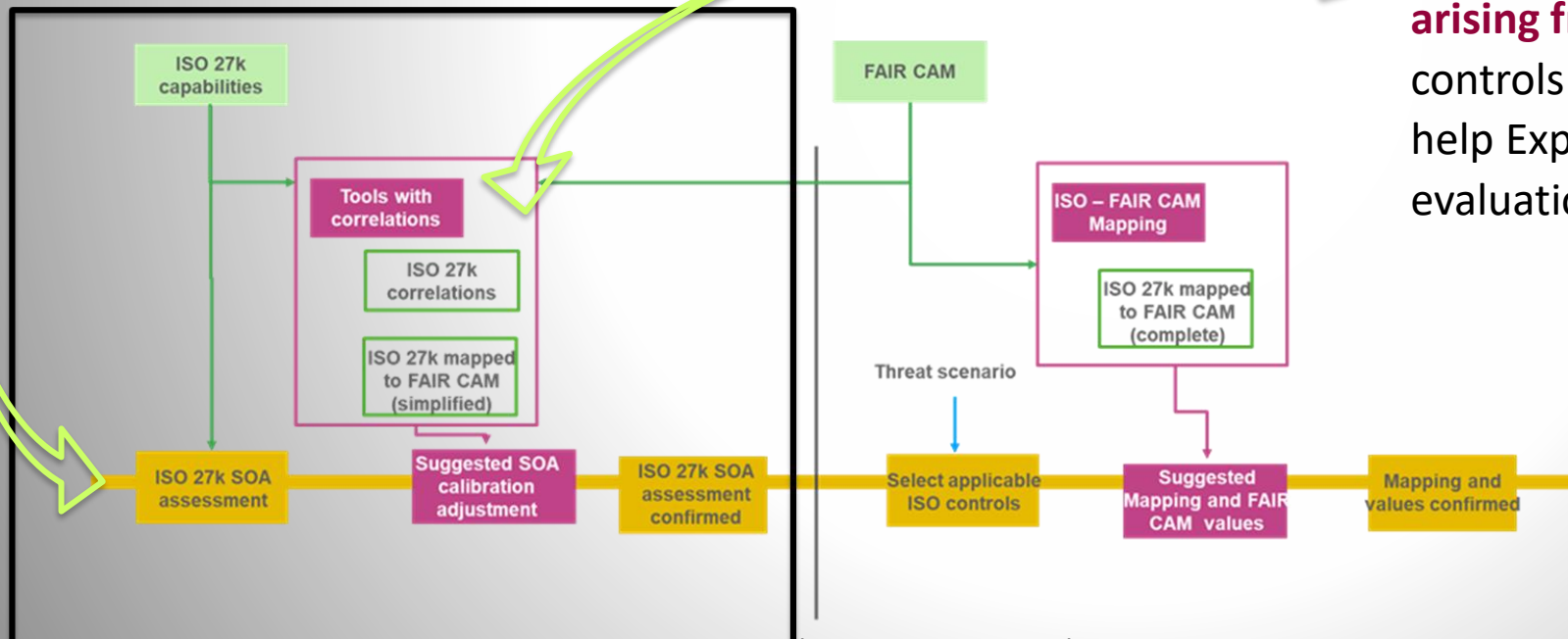
Tot	D	I	Estim. CMMI				Calc. CMMI				ISO Internal Calc Data			FAIR CAM Informative Data		
			min	ml	max	Conf	min	ml	max	Conf	W	CMMI	WA	VAR	DSC	LEC
17	6	11	60.00%			VL	43.05%			M				60.63%	98.89%	92.14%
											0.80	40.20%	27.34%	0.00%	27.34%	0.00%
											0.60	70.10%	53.28%	42.06%	53.28%	53.28%
											0.60	37.32%	28.36%	22.39%	28.36%	0.00%
											0.40	20.10%	16.89%	0.00%	16.89%	16.89%
											0.20	55.00%	50.60%	11.00%	50.60%	0.00%
											0.60	15.20%	0.00%	0.00%	15.20%	0.00%
											0.40	38.24%	18.21%	38.24%	0.00%	0.00%
											0.40	50.00%	42.00%	20.00%	42.00%	42.00%
											0.40	41.29%	37.98%	8.26%	37.98%	37.98%
											0.40	32.76%	24.90%	19.66%	24.90%	0.00%
											0.40	44.25%	33.63%	26.55%	33.63%	33.63%
2	1	1	60.00%			VH				L				22.43%	58.89%	58.89%
											0.40	70.10%	58.89%	28.04%	58.89%	58.89%
														33.18%	78.48%	0.00%
											0.40	41.67%	28.33%	16.67%	28.33%	0.00%
											0.60	50.00%	26.00%	30.00%	26.00%	0.00%
											0.40	52.02%	35.38%	20.81%	35.38%	0.00%
											0.40	40.20%	27.34%	0.00%	27.34%	0.00%
											0.40	20.00%	13.60%	8.00%	13.60%	0.00%
1	1	0	80.00%			M	80.0%									
9	4	5	60.00%			L	58.10%			L				35.09%	94.50%	86.32%

- A **calculated (suggested) confidence** value, which takes into consideration Variance controls' impacts:
  - Variance represents the ability of the ISMS to maintain ISO controls at the desired capability level.
  - A high Variance value implies a "stability" of the capability values of the affected controls and thus can, but need not, improve Confidence.
  - A low Variance value represents the inability of the ISMS to ensure capability stability and thus can reduce Confidence in capability evaluation.

# Why the simplified mapping step?

- The purpose of this step is to provide the Expert with a different point of view
  - i.e., to answer, in a simplified way the question: **what does the ISMS under consideration** look like from the point of view of **FAIR-CAM categories**?

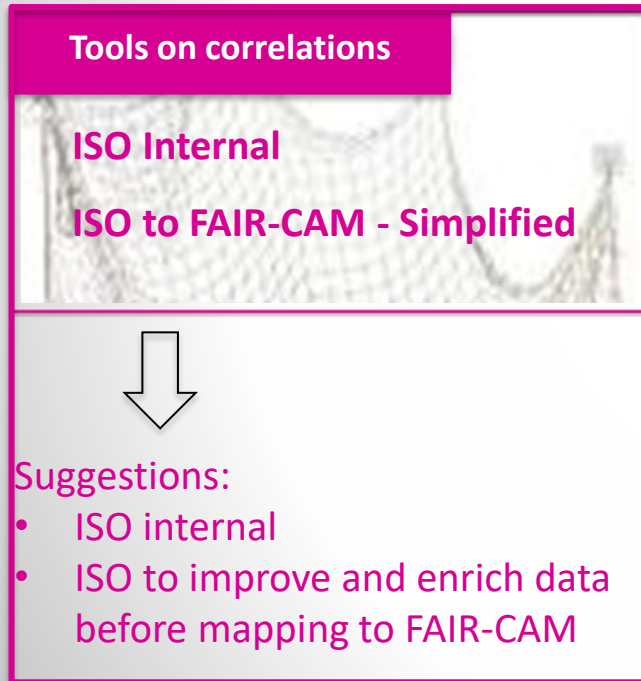
- The use of simplified mapping responds to the goals of **reducing the objective difficulties arising from the relationships** between ISO controls and multiple FAIR-CAM categories, to help Expert navigate through decisions and evaluations aimed to **reduce uncertainty**





# Inputs by the Analysts in the simplified mapping and SOA review

## ISO27k SOA - Assessment

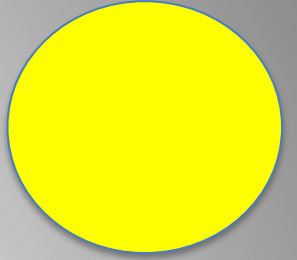


## SOA Assessment - Reviewed



- **Create SOA Assessment**  
=> may be imported from existing SOAs
- **(Optional) Review SOA Assessment**
- **(Optional) Modify tool configuration, if required to reflect specific conditions**

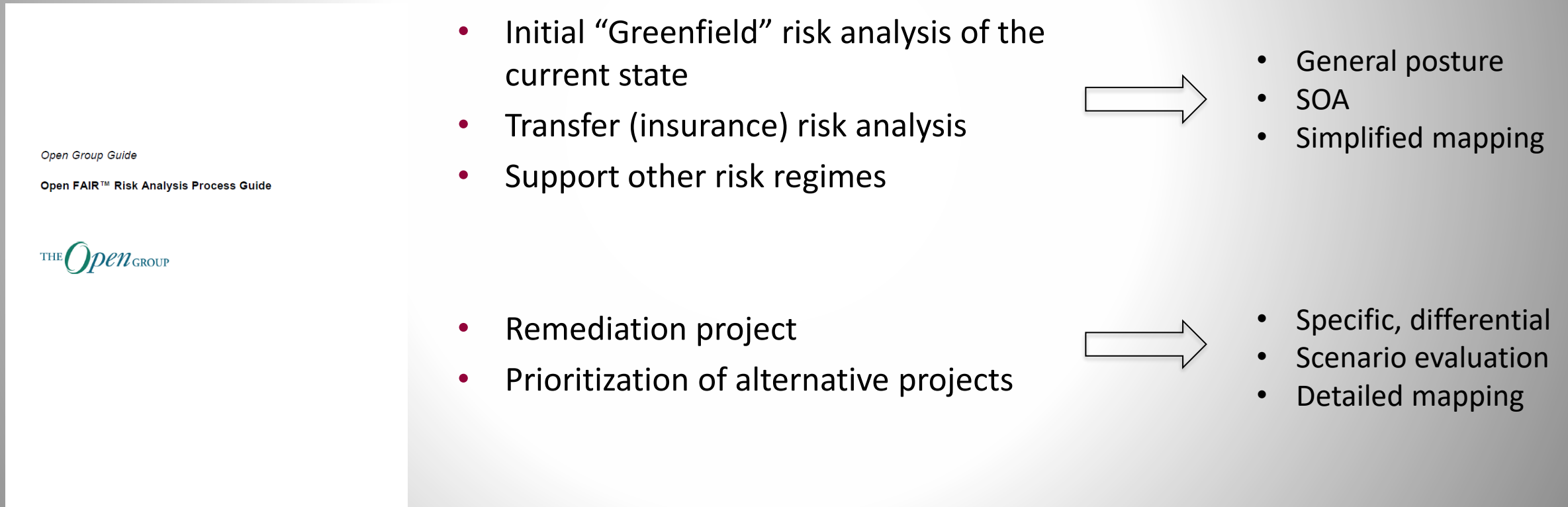
# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - **DETAILED MAPPING and SCENARIOS**
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

# Purpose of Risk Analysis

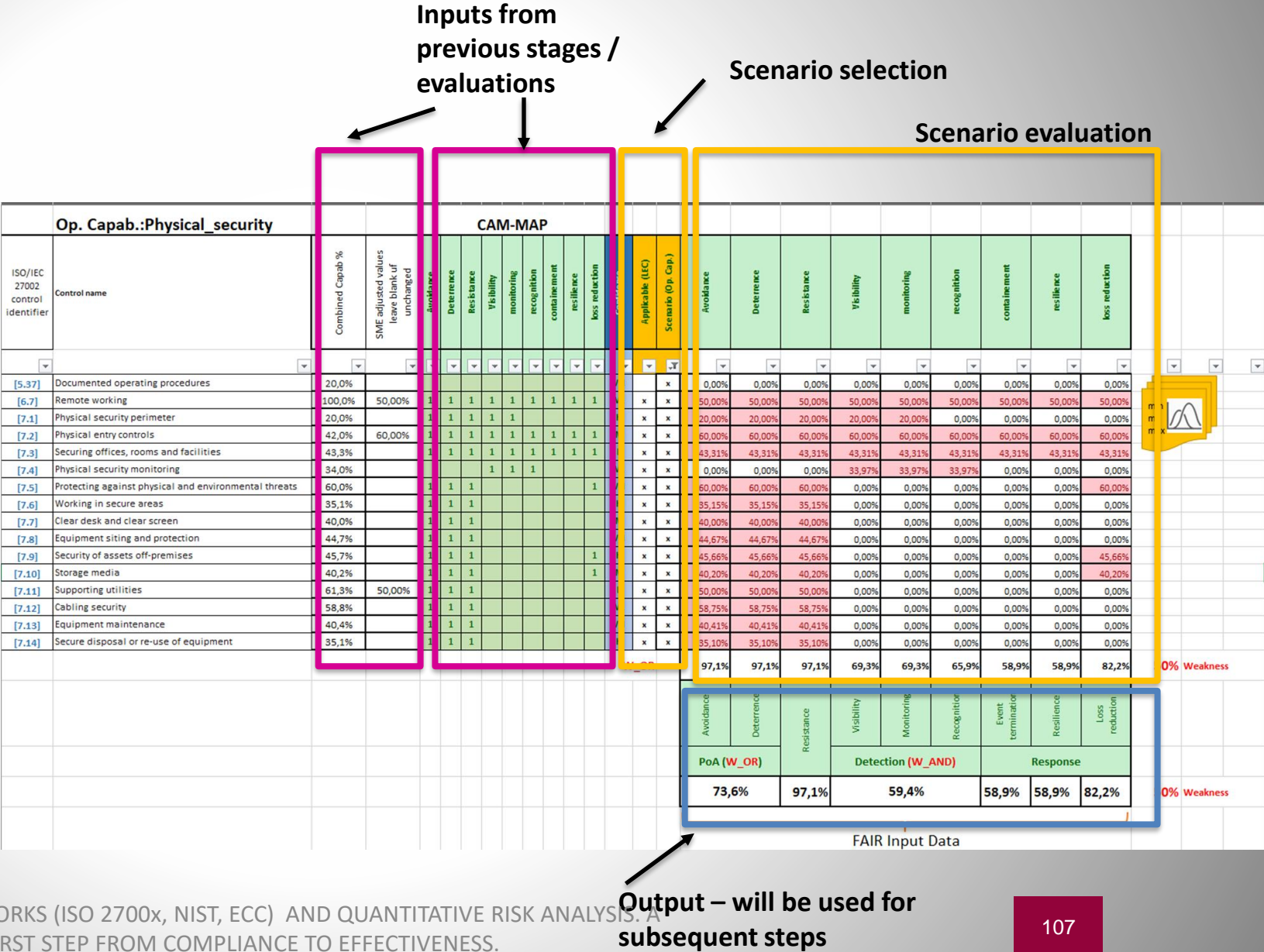
To perform a risk analysis, we must first understand the decision-maker's purpose requesting it. Typically there are five main purposes that sponsors have for requesting a risk analysis:



# Detailed mapping in scenario evaluation

Objective of this phase is the evaluation of the contribution of the controls of an ISO27 ISMS toward the factors of the FAIR-CAM functional domains and the LEC category and its subcategories.

A tool has been developed to support analyst's evaluations.





# Input for processing

This phase uses **as input**:

- The **capability and Confidence of the selected controls**, as resulting from the evaluations and processing of the previous procedures.
- The **detailed ISO 27002 FAIR-CAM mapping related** to the selected controls. As the simplified one, detailed mapping have been run through different experts to define an average profile

The input is organized so that it can be used with computational methods involving the **use of distributions** and in particular **Beta-Pert**

The **Analyst** can use the values proposed by the tool or make its adjustment

Op. Capab.:Physical_security			CAM-MAP																						
ISO/IEC 27002 control identifier	Control name	Combined Capab. % SAME adjusted values leave blank if unavailable	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Containment	Resilience	Loss reduction	Confidence	Applicable (ECC)	Score (by Gap)	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Containment	Resilience	Loss reduction		
[5.37]	Documented operating procedures	20,0%										H	+	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[6.7]	Remote working	100,0%	50,00%	1	1	1	1	1	1	1	1	M	+	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%		
[7.1]	Physical security perimeter	20,0%										M	+	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%		
[7.2]	Physical entry controls	42,0%	60,00%	1	1	1	1	1	1	1	1	M	+	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%		
[7.3]	Securing offices, rooms and facilities	43,3%										L	+	43,31%	43,31%	43,31%	43,31%	43,31%	43,31%	43,31%	43,31%	43,31%	43,31%		
[7.4]	Physical security monitoring	34,0%										M	+	0,00%	0,00%	0,00%	33,97%	33,97%	33,97%	0,00%	0,00%	0,00%	0,00%		
[7.5]	Protecting against physical and environmental threats	60,0%										M	+	60,00%	60,00%	60,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.6]	Working in secure areas	35,1%										M	+	35,15%	35,15%	35,15%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.7]	Clear desk and clear screen	40,0%										M	+	40,00%	40,00%	40,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.8]	Equipment siting and protection	44,7%										M	+	44,67%	44,67%	44,67%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.9]	Security of assets off-premises	45,7%										M	+	45,66%	45,66%	45,66%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.10]	Storage media	40,2%										M	+	40,20%	40,20%	40,20%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.11]	Supporting utilities	61,3%	50,00%	1	1	1	1	1	1	1	1	L	+	50,00%	50,00%	50,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.12]	Cabling security	58,8%										M	+	58,75%	58,75%	58,75%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.13]	Equipment maintenance	40,4%										M	+	40,41%	40,41%	40,41%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
[7.14]	Secure disposal or re-use of equipment	35,1%										M	+	35,10%	35,10%	35,10%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%		
W_OR														97,1%	97,1%	97,1%	69,3%	69,3%	65,9%	58,9%	58,9%	82,2%	50% Weakness		
														Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Event termination	Resilience	Loss reduction			
														PoA (W_OR)	Detection (W_AND)				Response						
														73,6%	97,1%		59,4%		58,9%	58,9%	82,2%		50% Weakness		
FAIR Input Data																									



# ISO 27002 to FAIR-CAM detailed mapping

- We propose a detailed mapping between ISO and FAIR-CAM model
- “Not-LEC” controls do not directly contribute to FAIR calculation (therefore analysts are not required to input them), but their contribution has been evaluated in the previous step through correlation analysis

ISO/IEC 27002 control identifier	Control name	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				Ensure Capability	Incentives	Identification	Correction	
																			Asset	Threat	Controls	Analysis	Reporting				
S.1	Policies for information security										1	1					1	1							1	1	
S.2	Information security roles and responsibilities										1	1					1	1							1	1	
S.3	Segregation of duties	1								1														1	1	1	
S.4	Management responsibilities										1	1		1			1	1						1	1	1	
S.5	Contact with authorities												1		1					1						1	
S.6	Contact with special interest groups												1							1							
S.7	Threat intelligence												1		1					1					1		
S.8	Information security in project management	1	1	1	1	1	1			1				1	1		1	1				1	1	1		1	
S.9	Inventory of information and other associated assets										1			1	1		1	1	1					1			
S.10	Acceptable use of information and associated assets										1	1		1	1		1	1	1		1						
S.11	Return of assets	1																									
S.12	Classification of information													1			1	1	1			1			1		
S.13	Labelling of information														1	1						1				1	
S.14	Information transfer	1	1	1						1		1		1			1	1						1		1	
S.15	Access control																1	1						1		1	
S.16	Identity management	1								1	1						1				1	1		1			
S.17	Authentication information	1								1	1								1			1		1			
S.18	Access rights	1								1	1			1			1	1	1			1				1	
S.19	Information security in supplier relationships	1	1							1	1	1		1			1	1		1				1		1	
S.20	Addressing information security within supplier agreements										1	1					1	1							1	1	
S.21	Managing information security in the ICT supply chain	1	1	1						1	1	1							1	1	1					1	
S.22	Monitoring, review and change management of supplier services										1	1		1					1			1				1	
S.23	Information security for use of cloud services													1	1		1	1								1	
S.24	Information security incident management responsibilities and preparation														1	1	1	1						1		1	
S.25	Assessment and decision on information security events													1	1	1				1	1	1	1			1	
S.26	Response to information security incidents							1	1	1				1	1	1	1	1	1							1	
S.27	Learning from information security incidents												1	1	1	1						1	1			1	
S.28	Collection of evidence													1	1	1			1	1	1	1	1				
S.29	Information security during disruption	1	1	1						1					1	1	1	1				1	1				
S.30	ICT readiness for business continuity			1				1	1	1				1	1	1	1	1				1	1		1		
S.31	Identification of legal, statutory, regulatory and contractual requirements											1	1				1	1				1	1			1	
S.32	Intellectual property rights	1								1	1			1			1	1	1			1				1	
S.33	Protection of records	1	1	1						1				1			1	1							1		
S.34	Privacy and protection of PII	1								1	1			1			1	1						1		1	
S.35	Independent review of information security										1	1		1	1				1	1	1	1	1				
S.36	Compliance with policies and standards for information security										1	1			1	1						1	1	1		1	

# Back to anatomy and physiology for a sec

- Focus on what matters more, that is to reduce uncertainty, while keeping in mind that there is (should be) a working system behind it. A long list of details may not help to reach the result
- Try to reflect reality and not what you hope it is – apply the calibration approach



# Scenario selection

For a specific risk scenario evaluation in terms of quantitative risk as for the FAIR-CAM model:

- Clear definition of one or more **risk scenarios**
- **Selection of ISO controls** that can counter-act the threats of the scenario.

It is applied the “Detailed ISO FAIR-CAM mapping” tool to appraise the contribution of the individual subcategories of the LEC category to determine suggested mapping and FAIR-CAM values

- Mapping and values are **confirmed or reviewed**

Op. Capab.:Physical_security			CAM-MAP																							
ISO/IEC 27002 control identifier	Control name	Combined Capab %	SME adjusted values leave blank if unchanged	Avoidance	Deterrence	Resilience	Visibility	Monitoring	Recognition	Containment	Resilience	Loss reduction	Applicable (LC)	Score (Op. Cap.)	Avoidance	Deterrence	Resilience	Visibility	Monitoring	Recognition	Event termination	Resilience	Loss reduction			
[5.37]	Documented operating procedures	20.0%											x	y	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[6.7]	Remote working	100.0%	50.00%	1	1	1	1	1	1	1	1	1	x	x	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%			
[7.1]	Physical security perimeter	20.0%		1	1	1	1	1	1	1	1	1	x	x	20.00%	20.00%	20.00%	20.00%	20.00%	0.00%	0.00%	0.00%	0.00%			
[7.2]	Physical entry controls	42.0%	60.00%	1	1	1	1	1	1	1	1	1	x	x	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%			
[7.3]	Securing offices, rooms and facilities	43.3%		1	1	1	1	1	1	1	1	1	x	x	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%			
[7.4]	Physical security monitoring	34.0%					1	1	1	1	1	1	x	x	0.00%	0.00%	0.00%	33.97%	33.97%	33.97%	0.00%	0.00%	0.00%			
[7.5]	Protecting against physical and environmental threats	60.0%		1	1	1						1	x	x	60.00%	60.00%	60.00%	0.00%	0.00%	0.00%	0.00%	60.00%	0.00%			
[7.6]	Working in secure areas	35.1%		1	1	1							x	x	35.15%	35.15%	35.15%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.7]	Clear desk and clear screen	40.0%		1	1	1							x	x	40.00%	40.00%	40.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.8]	Equipment siting and protection	44.7%		1	1	1							x	x	44.67%	44.67%	44.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.9]	Security of assets off-premises	45.7%		1	1	1						1	x	x	45.66%	45.66%	45.66%	0.00%	0.00%	0.00%	0.00%	0.00%	45.66%			
[7.10]	Storage media	40.2%		1	1	1						1	x	x	40.20%	40.20%	40.20%	0.00%	0.00%	0.00%	0.00%	0.00%	40.20%			
[7.11]	Supporting utilities	61.3%	50.00%	1	1	1							x	x	50.00%	50.00%	50.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.12]	Cabling security	58.8%		1	1	1							x	x	58.75%	58.75%	58.75%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.13]	Equipment maintenance	40.4%		1	1	1							x	x	40.41%	40.41%	40.41%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
[7.14]	Secure disposal or re-use of equipment	35.1%		1	1	1							x	x	35.10%	35.10%	35.10%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
															97,1%	97,1%	97,1%	69,3%	69,3%	65,9%	58,9%	58,9%	82,2%	50% Weakness		
															Avoidance	Deterrence	Resilience	Visibility	Monitoring	Recognition	Event termination	Resilience	Loss reduction			
															PoA (W_OR)		Detection (W_AND)			Response						
															73,6%		97,1%			59,4%			58,9%	58,9%	82,2%	50% Weakness
FAIR Input Data																										



# Inputs by the Analysts in the detailed mapping and scenario eval.



- (Optional) Review confidence value, imported from previous stages
- Select ISO controls that can counter-act the threats of the scenario
- Confirm or (Optional) review results

Op. Capab.:Physical_security		CAM-MAP											FAIR Input Data										
ISO/IEC 27002 control identifier	Control name	Combined Capab. %	SME adjusted values leave blank if unchanged	Avoidance	Deterrence	Resistance	Visibility	monitoring	recognition	containment	resilience	loss reduction	Applicable (IEC) Scenario (Op. Cap.)	Avoidance	Deterrence	Resistance	Visibility	monitoring	recognition	containment	resilience	loss reduction	
[5.37]	Documented operating procedures	20.0%		1	1	1	1	1	1	1	1	1	x	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[6.7]	Remote working	100.0%	50.00%	1	1	1	1	1	1	1	1	1	x	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	
[7.1]	Physical security perimeter	20.0%		1	1	1	1	1	1	1	1	1	x	20.00%	20.00%	20.00%	20.00%	20.00%	20.00%	20.00%	20.00%	20.00%	
[7.2]	Physical entry controls	42.0%	60.00%	1	1	1	1	1	1	1	1	1	x	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	
[7.3]	Securing offices, rooms and facilities	43.3%		1	1	1	1	1	1	1	1	1	x	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	43.31%	
[7.4]	Physical security monitoring	34.0%		1	1	1	1	1	1	1	1	1	x	0.00%	0.00%	0.00%	33.97%	33.97%	33.97%	0.00%	0.00%	0.00%	
[7.5]	Protecting against physical and environmental threats	60.0%		1	1	1	1	1	1	1	1	1	x	60.00%	60.00%	60.00%	0.00%	0.00%	0.00%	0.00%	0.00%	60.00%	
[7.6]	Working in secure areas	35.1%		1	1	1	1	1	1	1	1	1	x	35.15%	35.15%	35.15%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.7]	Clear desk and clear screen	40.0%		1	1	1	1	1	1	1	1	1	x	40.00%	40.00%	40.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.8]	Equipment siting and protection	44.7%		1	1	1	1	1	1	1	1	1	x	44.67%	44.67%	44.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.9]	Security of assets off-premises	45.7%		1	1	1	1	1	1	1	1	1	x	45.66%	45.66%	45.66%	0.00%	0.00%	0.00%	0.00%	0.00%	45.66%	
[7.10]	Storage media	40.2%		1	1	1	1	1	1	1	1	1	x	40.20%	40.20%	40.20%	0.00%	0.00%	0.00%	0.00%	0.00%	40.20%	
[7.11]	Supporting utilities	61.3%	50.00%	1	1	1	1	1	1	1	1	1	x	50.00%	50.00%	50.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.12]	Cabling security	58.8%		1	1	1	1	1	1	1	1	1	x	58.75%	58.75%	58.75%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.13]	Equipment maintenance	40.4%		1	1	1	1	1	1	1	1	1	x	40.41%	40.41%	40.41%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7.14]	Secure disposal or re-use of equipment	35.1%		1	1	1	1	1	1	1	1	1	x	35.10%	35.10%	35.10%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
														97,1%	97,1%	97,1%	69,3%	69,3%	65,9%	58,9%	58,9%	82,2%	
														0% Weakness									
														Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Event termination	Resilience	Loss reduction	
														PoA (W_OR)		Detection (W_AND)			Response				
														73,6%		97,1%			58,9%				
																59,4%			58,9%				
																			82,2%				
													0% Weakness										

FAIR Input Data

## Calculating process and outputs

The **tool-based calculating process** involves:

- The calculation of the contributions of ISO controls to the subcategories of FAIR-CAM controls; the calculation is done for LEC subcategories
- The contributions of each ISO control are then cumulated using a specific calculation method, that what we call a **Weak OR**. The motivation for this choice stems from the observation that there are no independent LEC-type controls in ISO whose contributions can be summed with a probabilistic OR.
- The Excel tool is set up to use **computational methods for distributions (typically Monte Carlo)**. The cumulative contributions of the subcategories are then calculated according to FAIR-CAM rules.

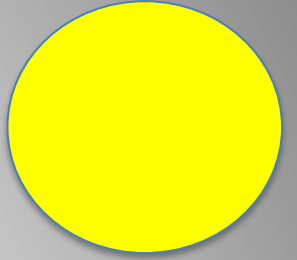
Op. Capab.:Physical_security		CAM-MAP																						
ISO/IEC 27002 control identifier	Control name	Combined Capab. %	SME adjusted values have blank if unchanged	Avoidance	Deterrence	Resistance	Viability	monitoring	recognition	containment	resilience	loss reduction	Confidence	Appraise (IGC Scenario Op.)	Avoidance	Deterrence	Resistance	Viability	monitoring	recognition	containment	resilience	loss reduction	
[5-37]	Documented operating procedures	20.0%											VI		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[6-7]	Remote working	100.0%	50.00%										VI		50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	50.00%	
[7-1]	Physical security perimeter	30.0%											H		30.00%	30.00%	30.00%	30.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-2]	Physical entry controls	42.0%	60.00%										M		60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	60.00%	
[7-3]	Securing offices, rooms and facilities	43.33%											L		43.33%	43.33%	43.33%	43.33%	43.33%	43.33%	43.33%	43.33%	43.33%	
[7-4]	Physical security monitoring	34.0%											VI		0.00%	0.00%	33.97%	33.97%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-5]	Protecting against physical and environmental threats	60.0%										1	VH		60.00%	60.00%	60.00%	0.00%	0.00%	0.00%	0.00%	60.00%	0.00%	
[7-6]	Working in secure areas	35.1%											H		35.13%	35.13%	35.15%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-7]	Clear desk and clear screen	40.0%											M		40.00%	40.00%	40.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-8]	Equipment siting and protection	44.7%											VH		44.67%	44.67%	44.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-9]	Security of assets off-premises	45.7%										1	H		45.66%	45.66%	45.66%	0.00%	0.00%	0.00%	0.00%	0.00%	45.66%	
[7-10]	Storage media	40.2%											M		40.20%	40.20%	40.20%	0.00%	0.00%	0.00%	0.00%	40.20%	0.00%	
[7-11]	Supporting utilities	61.3%	50.00%										L		50.00%	50.00%	50.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-12]	Cabling security	58.8%											VI		58.75%	58.75%	58.75%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-13]	Equipment maintenance	40.4%											VH		40.41%	40.41%	40.41%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
[7-14]	Secure disposal or re-use of equipment	35.1%											H		35.10%	35.10%	35.10%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	
W_OR															97.1%	97.1%	97.1%	69.3%	69.3%	65.9%	58.9%	58.9%	82.2%	0% Weakness
															Avoidance	Deterrence	Resistance	Viability	Monitoring	Recognition	Event termination	Resilience	Loss reduction	
															PoA (W_OR)									
															79.6%	97.1%		59.4%		58.9%	58.9%	82.2%	0% Weakness	
FAIR Input Data																								

## FAIR RISK EVALUATION MODEL

The **output** is the LEC values **expressed in the form appropriate to the FAIR model, i.e., as most likely, minimum, maximum, and Confidence values**. This mode also allows the use of distributions in the calculation of the FAIR model.



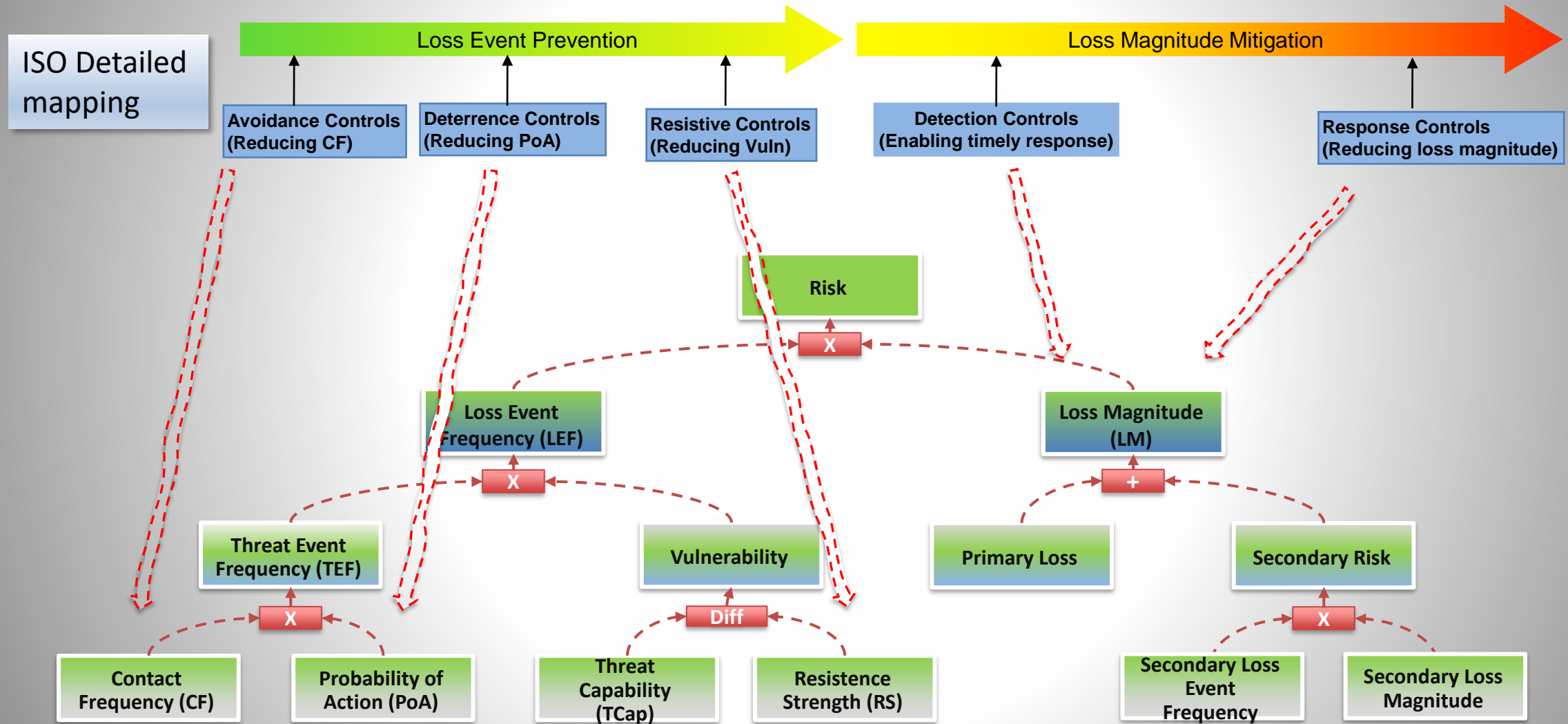
# Agenda



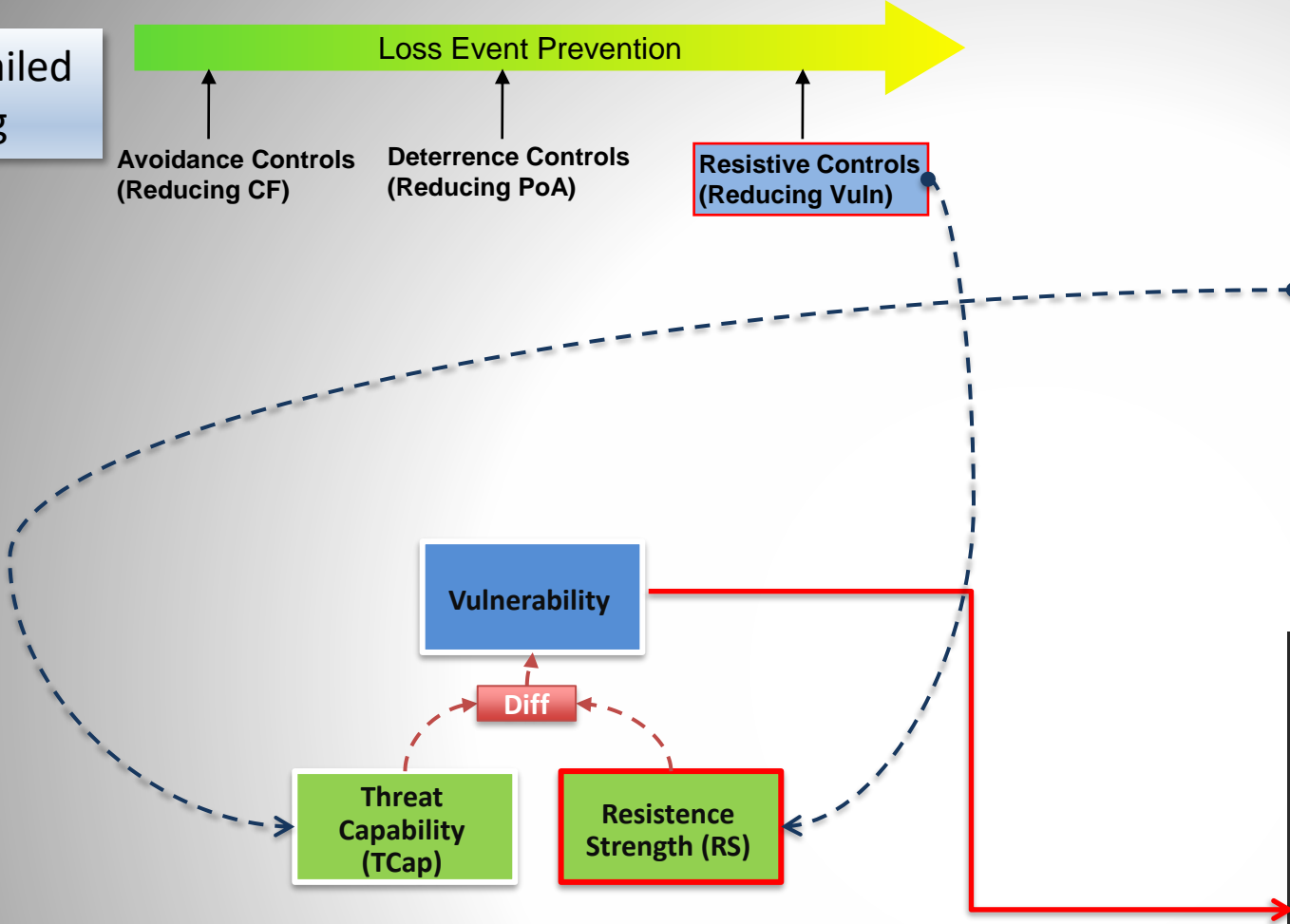
- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - **DEMO**
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - ROUND TABLE + Q&A

Op. Capab.:Physical_security		CAM-MAP																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																							
------------------------------	--	---------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

# Let's map the ISO Detailed mapping values . . .



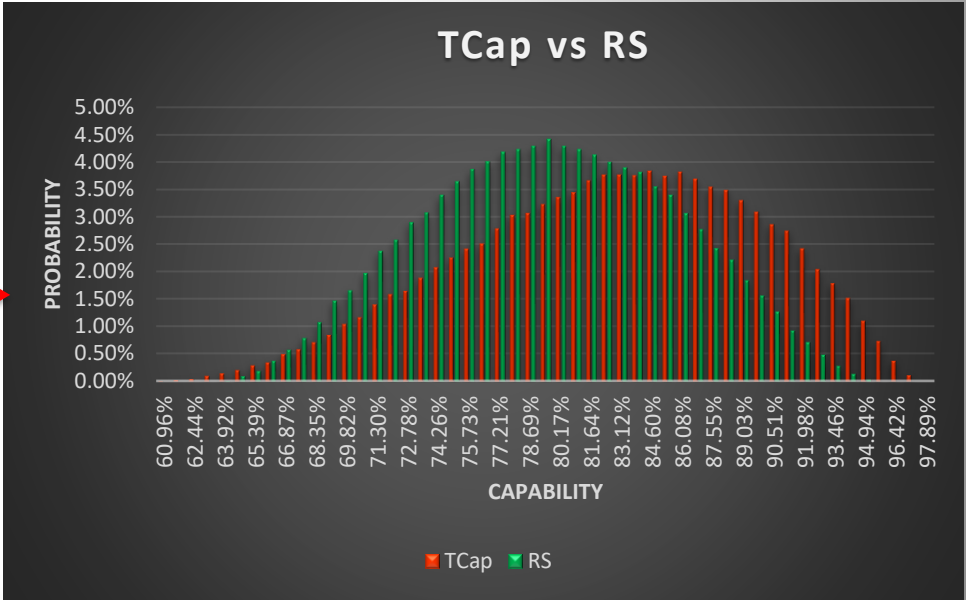
ISO Detailed mapping



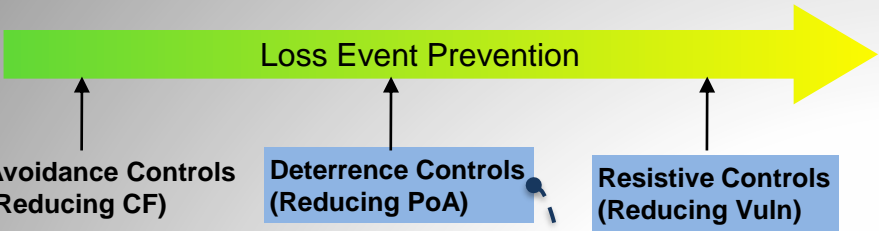
TCap	Min	ML	Max
Nation states	95	98	99
Cyber criminals	60	85	98
Privileged insider	98	99	99
Non-privileged insiders	40	50	95
Malware	40	60	95



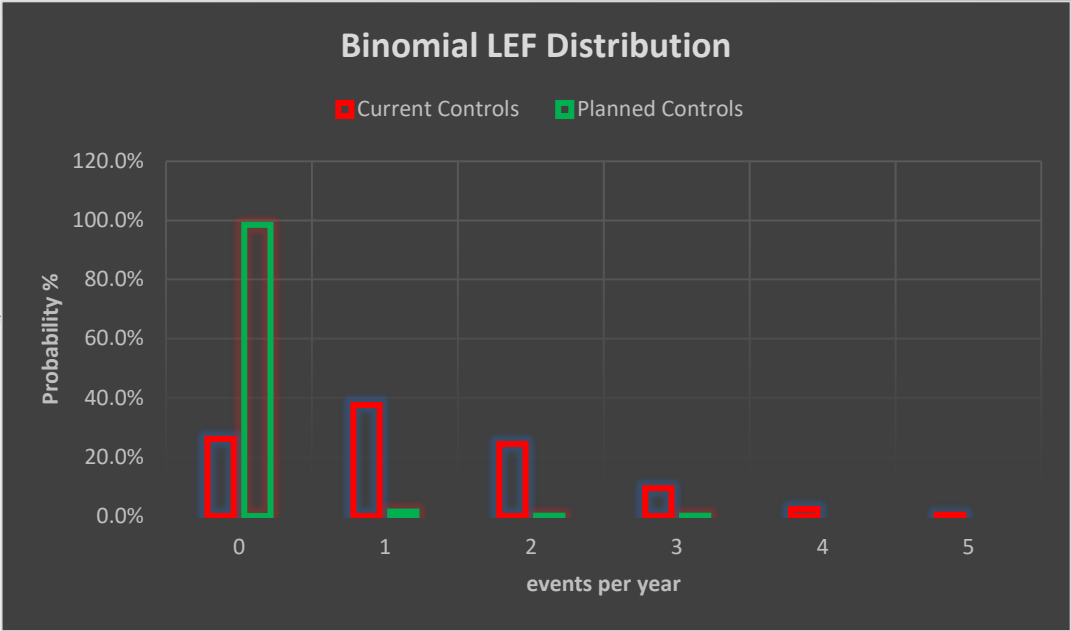
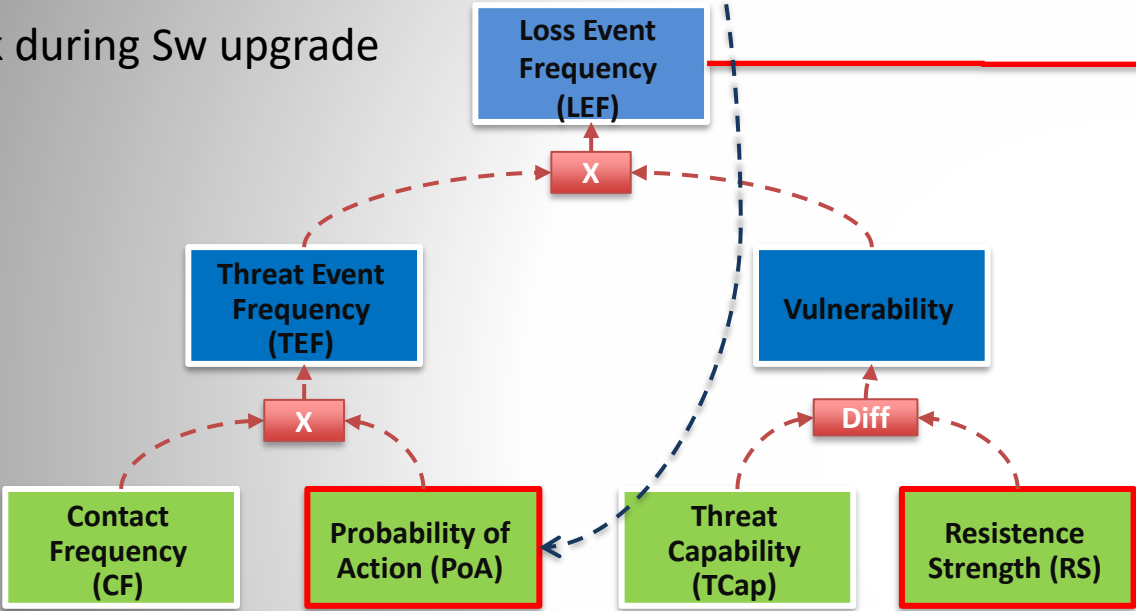
TCap	PERT(0.60, 0.85, 0.98, L)	Cyber criminals
RS	PERT(0.64, 0.80, 0.96, L)	ISO Mapping (± 20%)
Vulnerability	63,0 %	



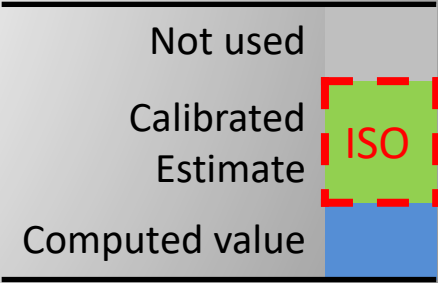
# ISO Detailed mapping



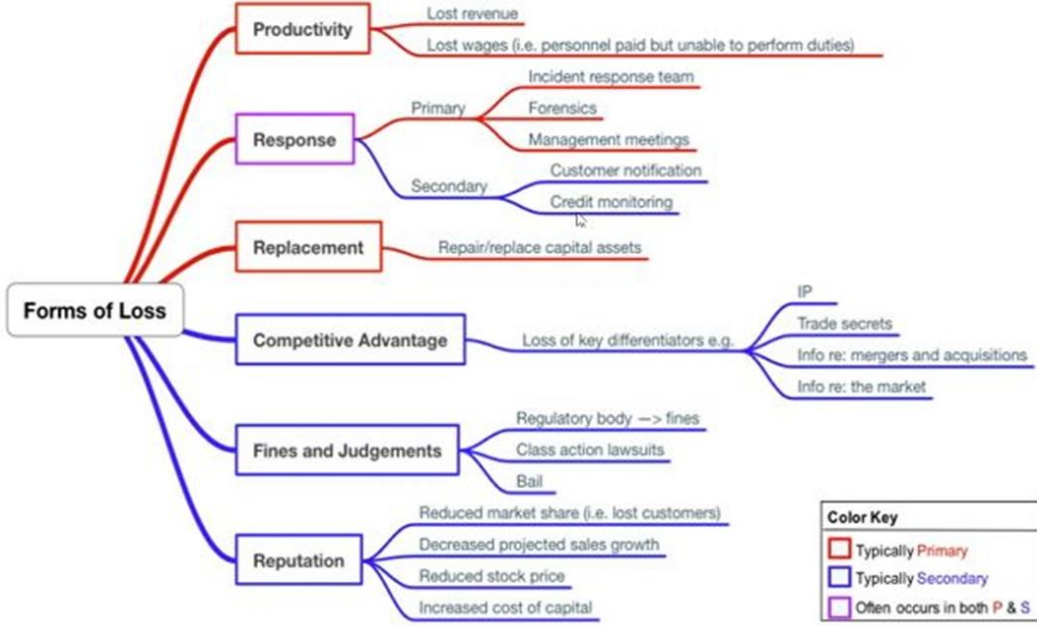
Attack during Sw upgrade



Threat events can occur	N times
Annual contact frequency	10
each with prob of	20%
PoA	5% → 95% ISO Mapping
Vulnerability	63 % ISO Mapping
LEF	Binomial (10; P)

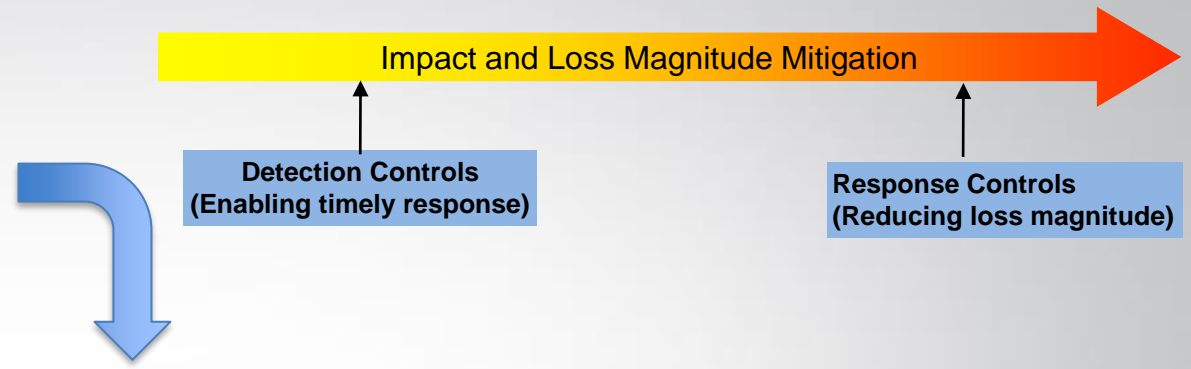






# Impact evaluation

For all applicable entries



Loss of productivity for inactive employees	min	most likely	max	confidence
Yearly cost	50.000 €	70.000 €	100.000 €	M
Working days	260	260	260	VH
cost/day	192 €	269 €	385 €	
loss of productivity %	60%	60%	60%	L
Number of employees	50	50	50	VH
non-productivity day cost	5.769 €	8.077 €	11.538 €	
non-productivity days	6	8	10	
Total losses	34.615 €	64.615 €	115.385 €	

## Impact reduction example

- Cloud service for instant restore

Loss  
Magnitude  
(LM)

Loss of productivity for inactive employees	min	most likely	max	confidence
Yearly cost	50.000 €	70.000 €	100.000 €	M
Working days	260	260	260	VH
cost/day	192 €	269 €	385 €	
loss of productivity %	60%	60%	60%	L
Number of employees	50	50	50	VH
non-productivity day cost	5.769 €	8.077 €	11.538 €	
non-productivity days	6	8	10	
Total losses	34.615 €	64.615 €	115.385 €	

Non-productive days are reduced to 1h max.

- "Controlled folder" (accessible only by authorized processes).

Loss Event  
Frequency  
(LEF)

Model Prova 01  
 Date 29/10/2021  
 Default Confidence M  
 n. of iterations 10.000

S = Simple  
 F = Fitting

Generate  
 Distribution  
 Description

CLEAR  
 DESCR

Distr. list update

CLEAR  
 DISTRIBUTIONS

Process Model

Update !

Wksheet	Message	Distrib.	Options
1 TCR		SF	
2 RES		SF	
3 TEF		SF	
4 VUL			
5 LEF			
6 SLF			
7 PLM			
8 PLMR			
9 ALEP			
10 ALES	00:00:03		
11 ALE	00:00:01		
12			
13			
14			
15			
16			
Tot time	00:00:34		

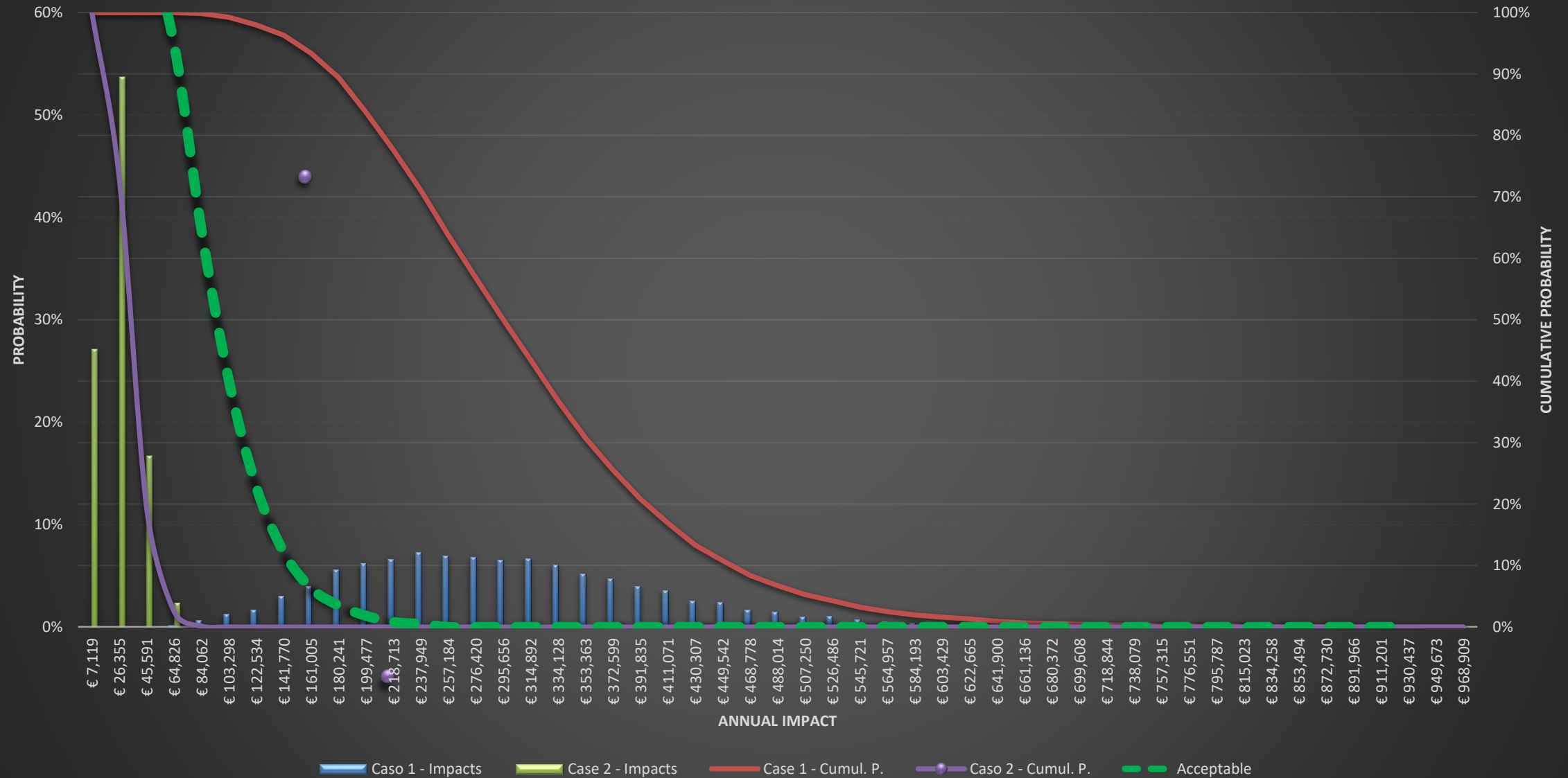
Compare graph

	Name	Notes
COPY 1	ALE	ALE 1
COPY 2	ALE	ALE 3 (ISO P)

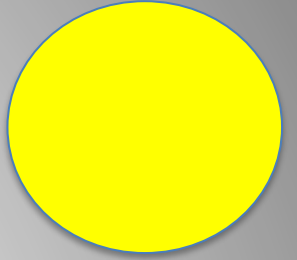
Update Data and :

Name	Definition	Where defined	Format
ALE	Impatto totale annuo	=ALE!\$L\$4:\$L\$10003	€ #,##0
ALEP	Impatto Primario totale annuo	=ALEP!\$L\$4:\$L\$10003	€ #,##0
ALES	Impatto secondario totale annuo	=ALES!\$L\$4:\$L\$10003	€ #,##0
DET	Detection	=TCR!\$K\$4:\$K\$10003	0.00%
LEF	Loss event frequency	=LEF!\$L\$4:\$L\$10003	#,##0.00
PLM	Impatto primario totale per evento	=PLM!\$M\$4:\$M\$10003	€ #,##0
PLMmin	Perdita Minima	=PLMR!\$K\$4:\$K\$10003	€ #,##0
PLMR	Perdita ridotta primaria	=PLMR!\$M\$4:\$M\$10003	€ #,##0
PoA	Probability of Action	=TEF!\$L\$4:\$L\$10003	0.00%
R_PLM	Response	=PLMR!\$L\$4:\$L\$10003	0%
RES	Resistance	=RES!\$M\$4:\$M\$10003	0.00%
RESIN	Resistance	=RES!\$L\$4:\$L\$10003	0.00%
RESMax	RES Max	=RES!\$J\$4:\$J\$10003	0.00%
RESMin	RESMin	=RES!\$K\$4:\$K\$10003	
SLEF	Secondary loss event frequency	=SLF!\$L\$4:\$L\$10003	#,##0.00
SLF	Percentuale eventi secondari	=SLF!\$K\$4:\$K\$10003	#,##0.00
SLM	SLM perdita reputazionale (secondario)	=ALES!\$J\$4:\$J\$10003	€ #,##0
TC	Threat Capability (Criminals)	=TCR!\$J\$4:\$J\$10003	0.00%
TCR	TC Reduced	=TCR!\$L\$4:\$L\$10003	0.00%
TEF	Threat Event Freq	=TEF!\$M\$4:\$M\$10003	0.00
TEFMax	TEF Max (Criminals)	=TEF!\$J\$4:\$J\$10003	0.00
TEFMin	TEF Min	=TEF!\$K\$4:\$K\$10003	0.00
TTTa	Perdita produttività	=PLM!\$J\$4:\$J\$10003	€ #,##0
TTTb	Sostituzione	=PLM!\$K\$4:\$K\$10003	€ #,##0
TTTc	Risposta	=PLM!\$L\$4:\$L\$10003	€ #,##0
VUL	Vulnerability	=LEF!\$K\$4:\$K\$10003	#,##0.00
VULN	Vulnerability 1	=VUL!\$L\$4:\$L\$10003	0

## Case 2 : Planned ISO Controls



# Agenda



- 15:00 – 15:55
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - GDL FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - DEMO
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- 16:00 – 16:55
  - PHASE 2 (1/2)
    - PROJECT GOALS
    - THE NEW ISO27002:2022
    - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
    - *DEMO*
- 17:00 – 17:55
  - PHASE 2 (2/2)
    - SIMPLIFIED MAPPING and SOAs
    - DETAILED MAPPING and SCENARIOS
    - DEMO
    - **TAKE AWAY + FUTURE EVOLUTIONS**
- 18:00 – 18:25
  - ROUND TABLE + Q&A



## Take away (1/2)

- The time for checklists is long gone. Frameworks (ISO, NIST, CIS, etc.) are composed of processes and subprocesses that are almost always interdependent and activated according to criteria (time, external factors, "internal" factors, etc.) that are highly articulated and complex. That is, they are systems of systems.
- Mapping between frameworks is no longer a one-to-one correspondence but presupposes the equivalence of processes and their measurement in terms of effectiveness. More complex issues like ontology equivalence can also be invoked.
- Despite these difficulties, it is possible to define an approach that allows creating a bridge with the goal of reducing uncertainty; we are not interested in being precise but accurate.

## Take away (2/2)

- It is possible to use the internal relationships of an ISMS to evaluate the effectiveness of the network of controls, not the individual control. This evaluation allows us to further investigate the validity of the controls in place.
- Defining a risk scenario allows us to identify the controls in the ISMS that are involved and then calculate their contribution to reducing risk factors according to the FAIR ontology.
- It is possible to build a tool, and we have demonstrated this, that allows a “bridge” between ISMS ISO and FAIR model, of course using the "right math."

# Future Developments (1/2)

- Existing relationships within frameworks such as ISO, NIST, etc., seem very interesting as a topic for further study with different objectives.
  - The definition of ontologies, common and shared, that allow easier mapping between frameworks and thus better definition of security regardless of the framework used.
  - A better definition of internal relationships in terms of type and relative weight
- The progressive definition of a "true" physiology such as, for example, the inclusion of trigger points in frameworks that allow for the activation of specific processes and thus a temporal development of the framework. Some suggestions are already in place, at least in ISO but, in our opinion, there is much work to be done in this area.
- The development of computational tools that enable an ever-improving ability to support the Expert's work seems to be a possible area of improvement.
- In our opinion enhancements are possible using AI (Artificial Intelligence) but a possible drawback is the lack of "transparency" of the process and thus, for the Expert, the inability to understand the process and the parameters by which the result is processed. However, this drawback is common to all AI applications, and many actions are underway to make AI applications more "transparent" to humans.

## Future Developments (2/2)

- There is a vast area of possible improvement in building more complex computational models using more refined computational methods and dynamic models.
- It is definitely desirable an evolution of frameworks (ISO, NIST,etc.) toward better definition of terms, processes, and their dynamics in terms of process activation/deactivation.
- *It has come a long way since the first definition in 1995 of BS 7799, the progenitor of the ISO27000 family, but, in our opinion, we are still in the early stages.*

# REFERENCES (very short list)

D. Vose- *Risk Analysis-A quantitative guide* - Wiley&Sons- 2008 Third edition

J. Freund, J. Jones – *Measuring and managing Information Risk- A FAIR approach*- ELSEVIER- 2015

D. Hubbard- R. Seiersen – *How to measure anything in Cybersecurity*- Wiley&Sons- 2016

The Open Group- *The Mathematics of the Open FAIR™ Methodology* - Document Number: G224 Sept 2022

<https://www.opengroup.org/>

[www.fairinstitute.org](http://www.fairinstitute.org)

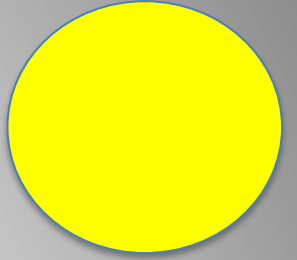
[www.isaca.org](http://www.isaca.org)

<https://www.yworks.com/products/yed> (graph editor)

•



# Agenda



- 15:00 –
  - PHASE 1: FAIR and ISO27001:2013
    - INTRODUCTION
    - INTRODUCTION TO FAIR
    - WG ISO-FAIR @ISACA ROMA
    - MAPPING ISO27001 to FAIR
    - *DEMO*
    - ISSUES IN MAPPING ISO to FAIR
  - TRANSITION
    - CONTROLS' "PHYSIOLOGY" AND THE NEW FAIR-CAM
- –PHASE 2 (1/2)
  - ADJUSTMENT OF PROJECT GOALS
  - THE NEW ISO27002:2022
  - ISO27002 CONTROLS – A TOOL-BASED ANALYSIS OF THE RELATIONSHIPS
- PHASE 2 (2/2)
  - SIMPLIFIED MAPPING and SOAs
  - DETAILED MAPPING and SCENARIOS
  - DEMO
  - TAKE AWAY +FUTURE EVOLUTIONS
- 18:00 – 18:25
  - **ROUND TABLE + Q&A**

*Vi ringraziamo per l'attenzione!*  
*We thank you for your attention!*

For info on the WG progress please contact

[alberto.piamonte@alice.it](mailto:alberto.piamonte@alice.it)

[glauco.bertocchi@gmail.com](mailto:glauco.bertocchi@gmail.com)