IT Security Controls Prioritization Using FAIR-CAM

December 16th 2024

FAIR-CAM Webinar

- Introductions
- FAIR-CAM Overview
- Practical Example
- Value in the field
- Questions

Introductions

IT Security Controls Prioritization Using FAIR™-CAM

Jack Jones
Chairman Emeritus, FAIR Institute

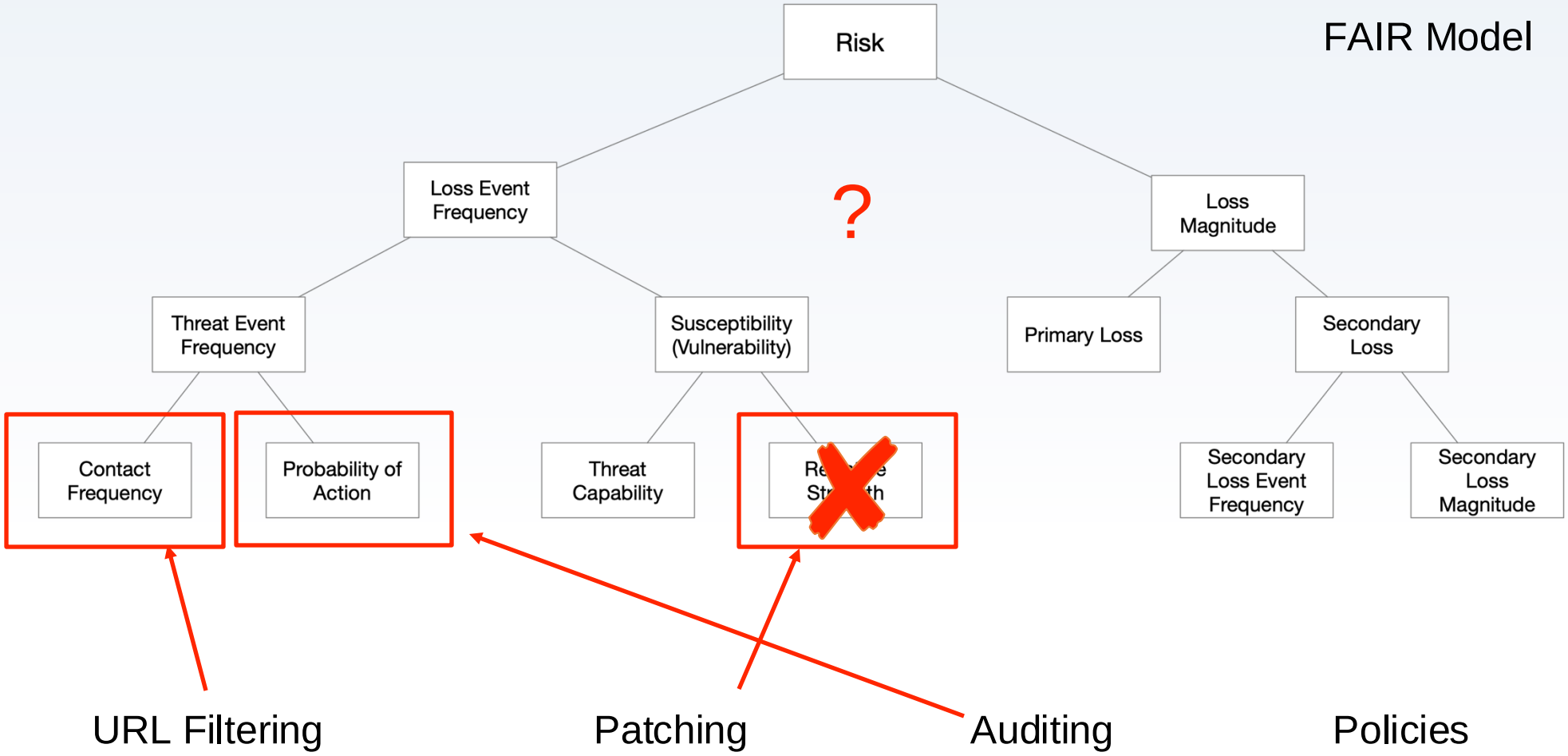
Rob Moore

VP Technology Risk Mgmt
Mastercard

Tom Callaghan

C-Risk Co-Founder
FAIR Institute Advisory Board

How do controls affect risk?



The Objectives:

Understand how the control landscape works

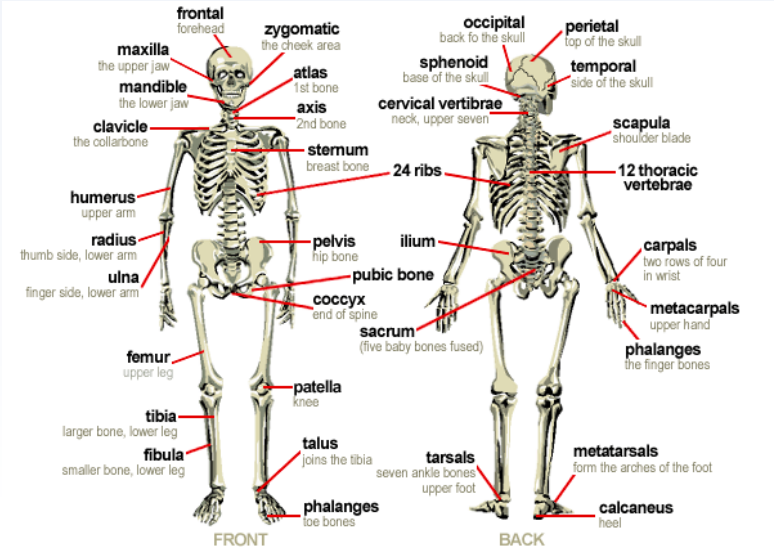
Enable empirical measurement of control efficacy and risk reduction value

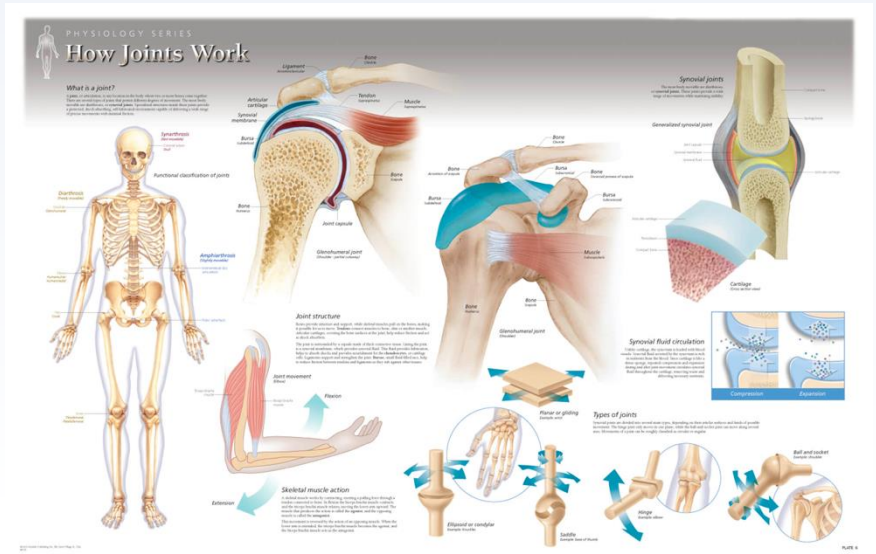
In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)



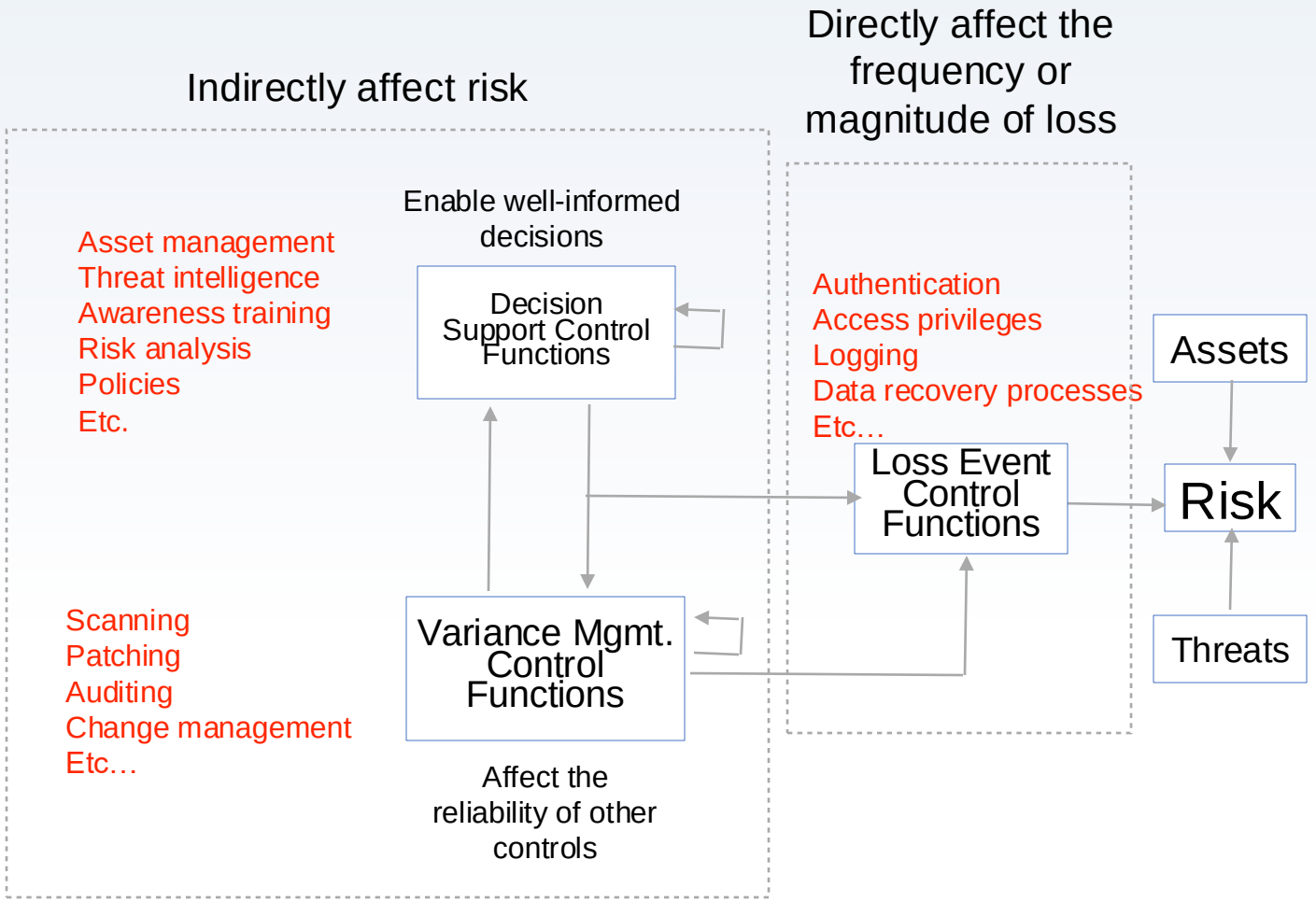


Neither. You need to know both.

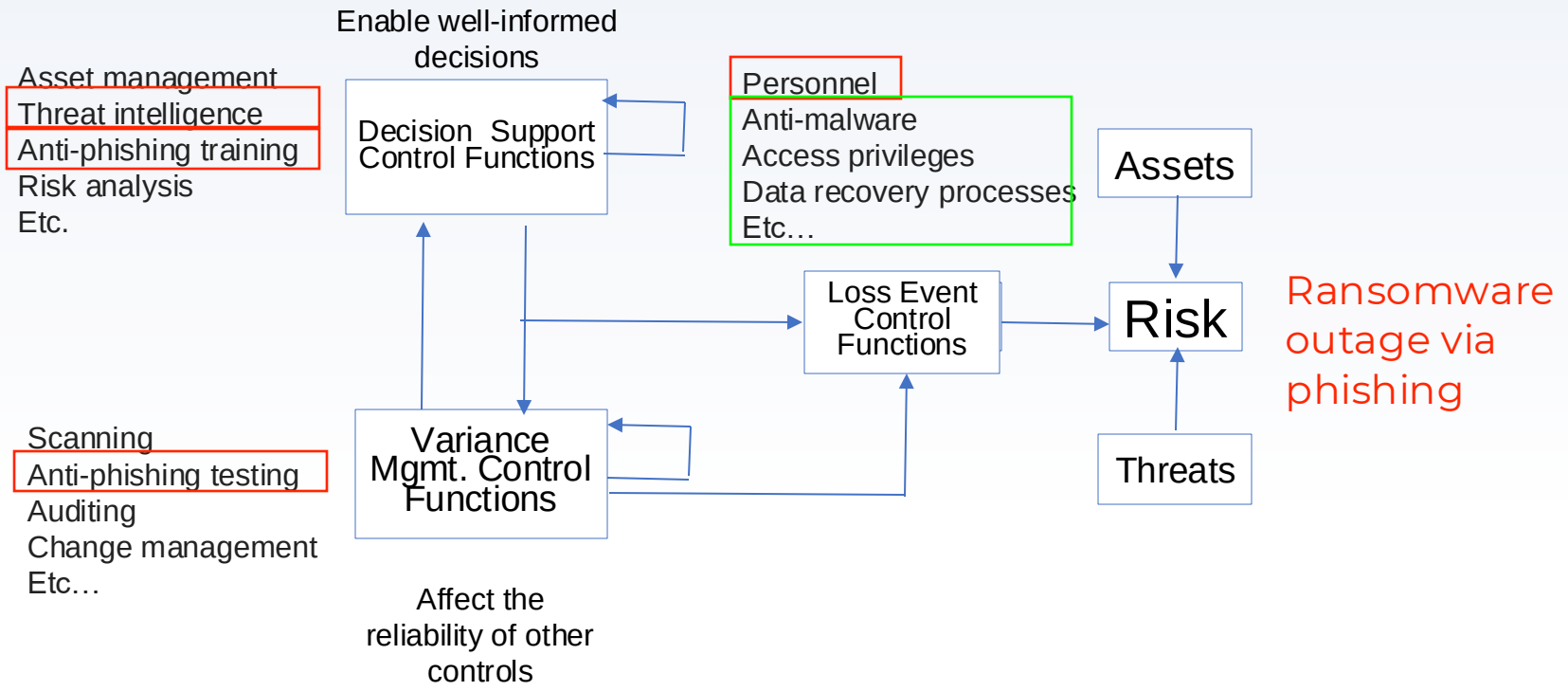
Cybersecurity anatomy vs. physiology

- Anatomy (controls)
  - Policies
  - Auditing
  - Patching
  - Authentication
- Physiology (control functions)
  - Define expectations
  - Identify control deficiencies
  - Correct control deficiencies
  - Resistance (or avoidance)

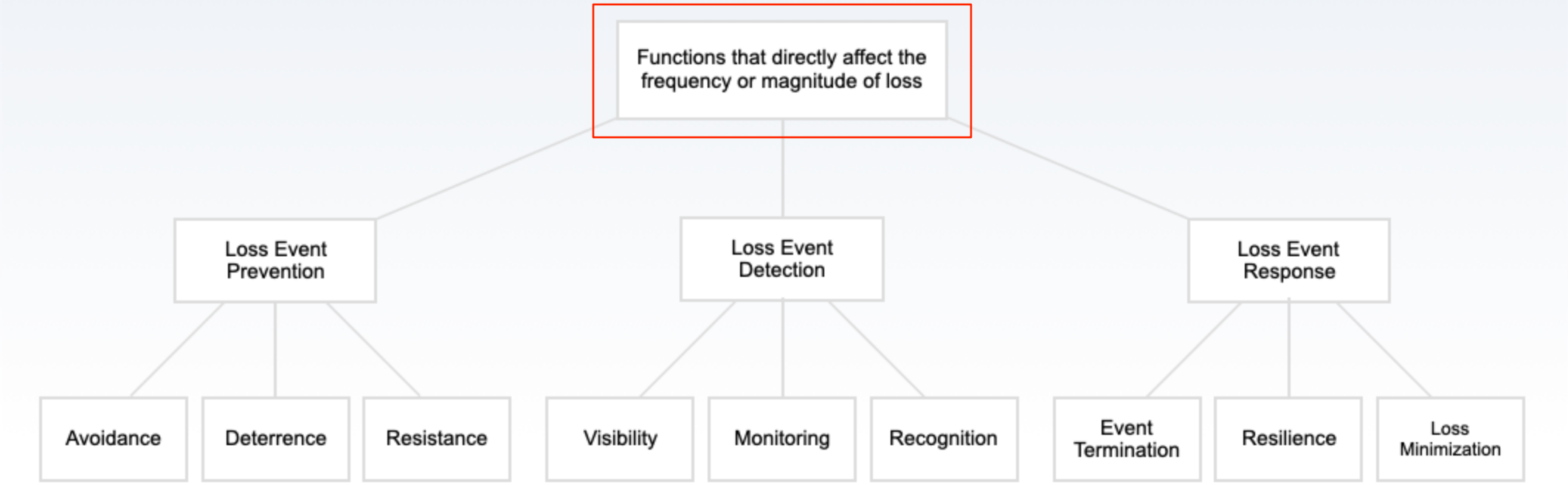
FAIR-CAM Functional Domains:
Direct vs. indirect effect on risk



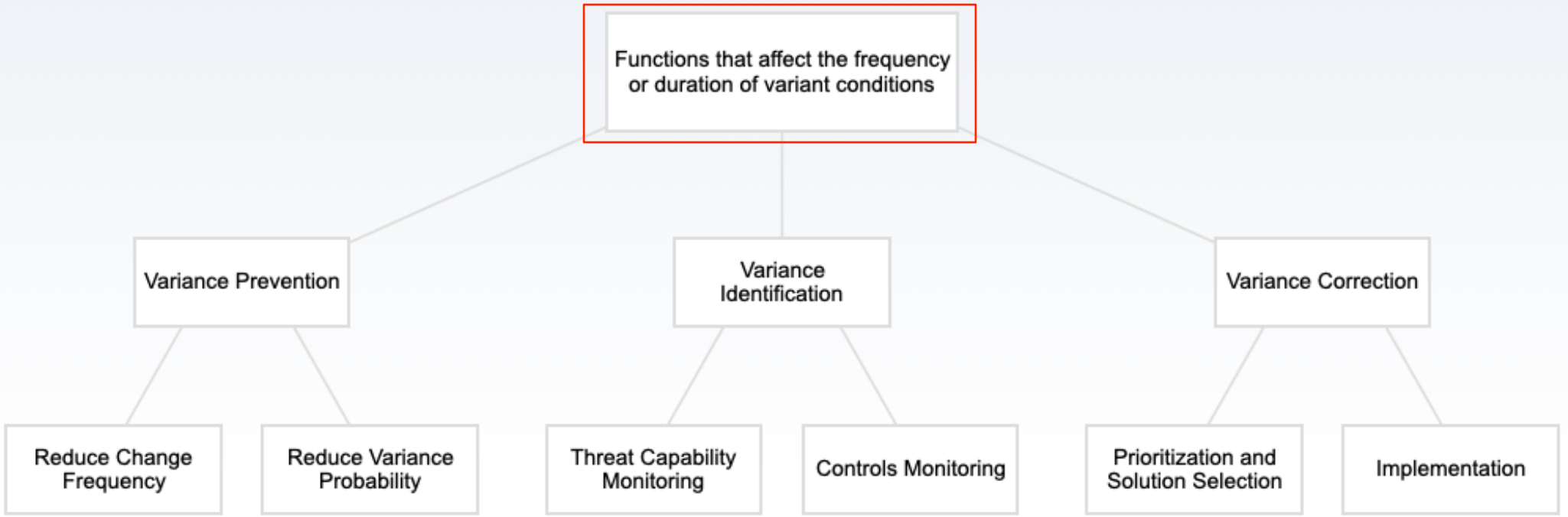
Relationships and dependencies



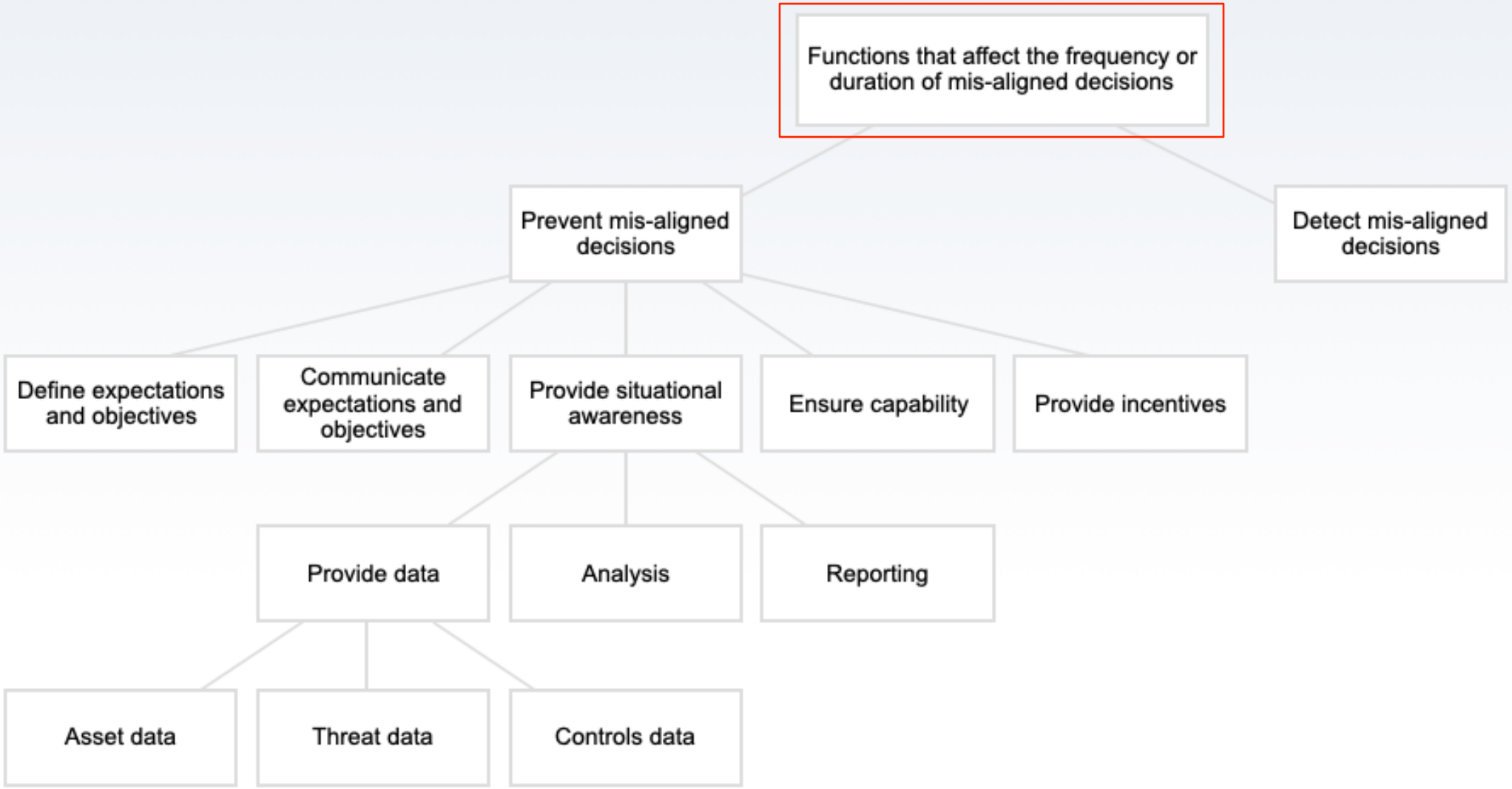
Loss Event Control Functions



Variance Management Control Functions

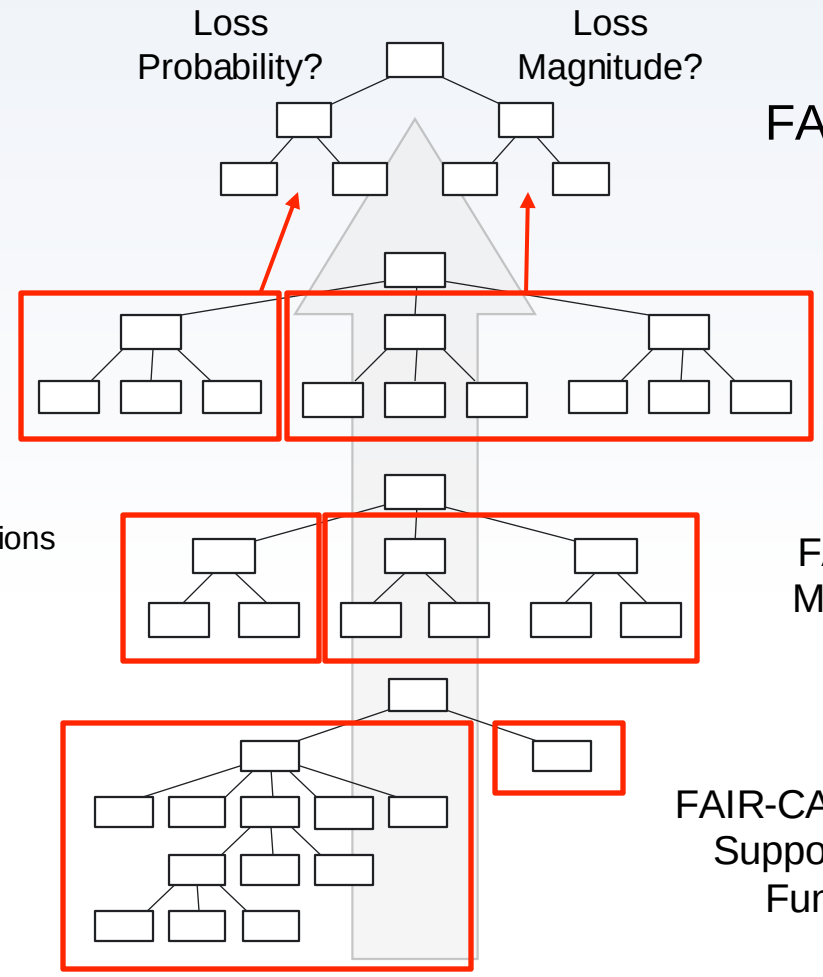


Decision Support Control Functions



FAIR-CAM relationship to FAIR and risk

Some loss event scenario…



FAIR

Controls

* URL filtering
* Authentication
* Access privileges
* Logging
* Monitoring
* Incident response
* Etc…
    * Change management
    * Access privilege restrictions
    * Vulnerability scanning
    * Auditing
    * Patching
    * Etc…
* Policies
* Processes
* Employee awareness training
* Risk analysis
* CMDB
* Root cause analysis
* Etc…

FAIR-CAM Loss Event Control Functions

FAIR-CAM Variance Management Control Functions

FAIR-CAM Decision Support Control Functions

Understanding Efficacy

Understanding Efficacy

Important terms…

Intended efficacy

Variance

Coverage

Operational efficacy

Intended Efficacy

A measure of how effective a control is expected to be when operating and implemented as intended

Variance

A “variant condition” exists when a control is not operating at its intended level of efficacy.

- A system that has not been configured properly
- Vulnerability scanning that does not take place when its supposed to
- A policy that no longer reflects the expectations of leadership

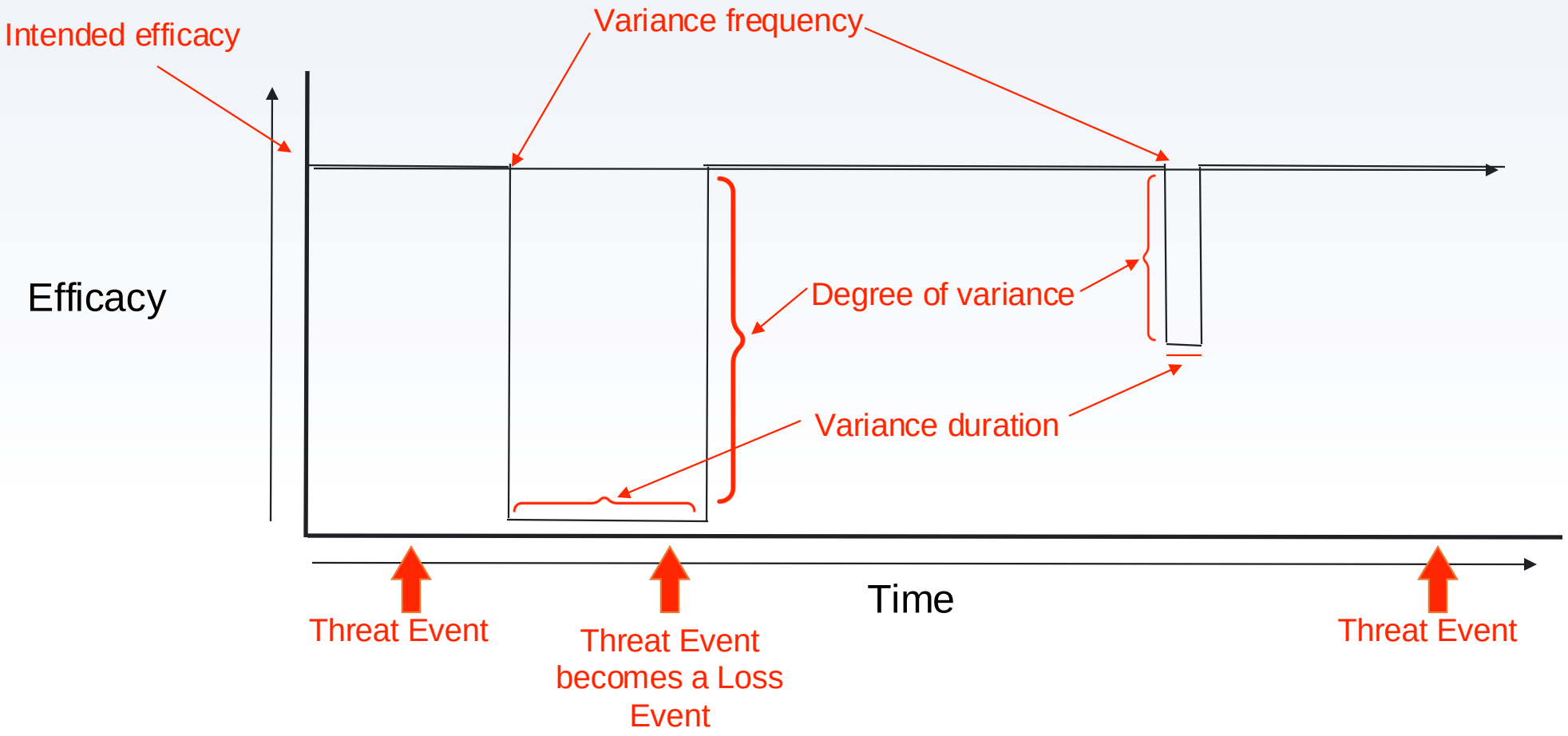
Coverage

The percentage of the environment that a control has been deployed to.

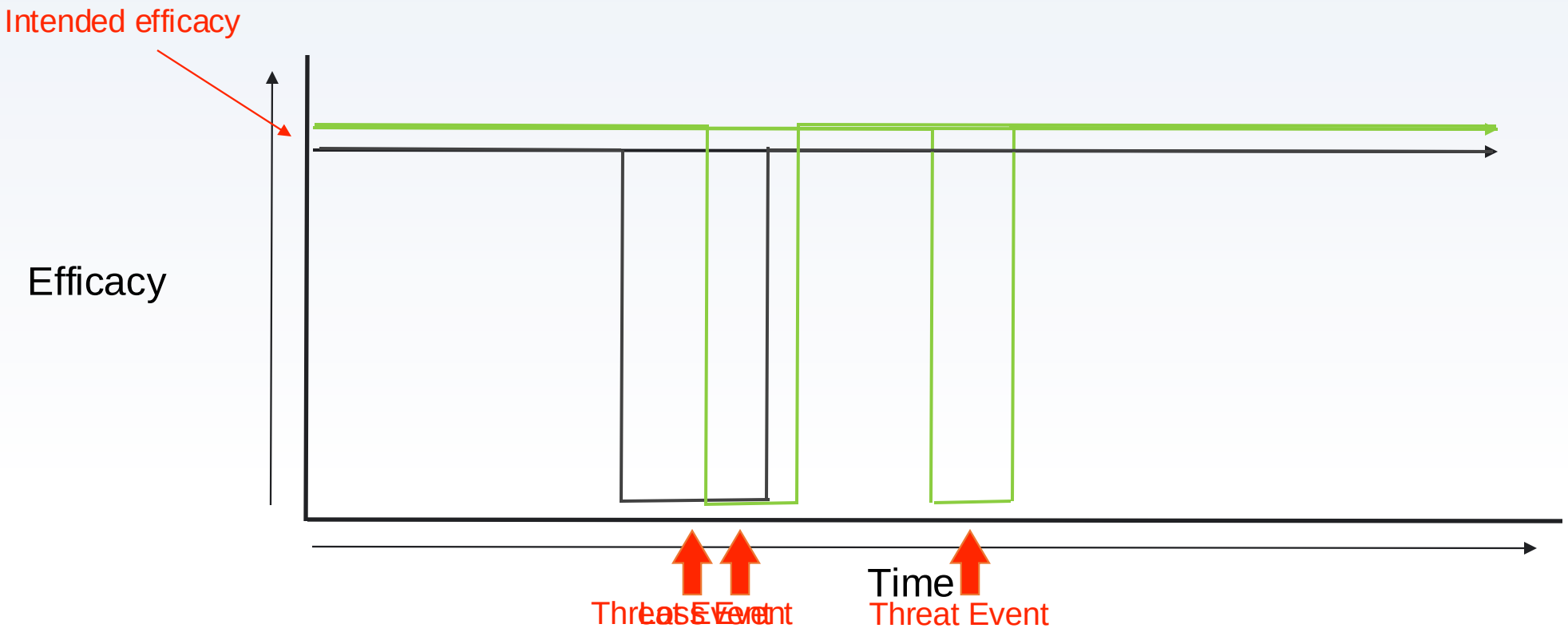
Operational Efficacy

How effective a control is over time given its Intended Efficacy, Variance, and Coverage.

How Variance Affects Operational Efficacy



Functional defense-in-depth



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

We knew what was happening, but we didn’t understand why it was happening.”

A Retired Surgeon

Use Cases

Use Cases for FAIR-CAM

Moving beyond Control Frameworks to modelling how operational control performance impacts risk exposure

- Deep dive on specific concerns and loss event scenarios to understand what controls and risk factors really mater.
- Develop Risk treatment plans for risk scenarios based on the financial risk reduction that *specific control performance improvements* will provide. Use this to articulate the return on investment of different treatment options.
- Perform Root cause analysis on incident and near misses to define the most effective corrective action plans.

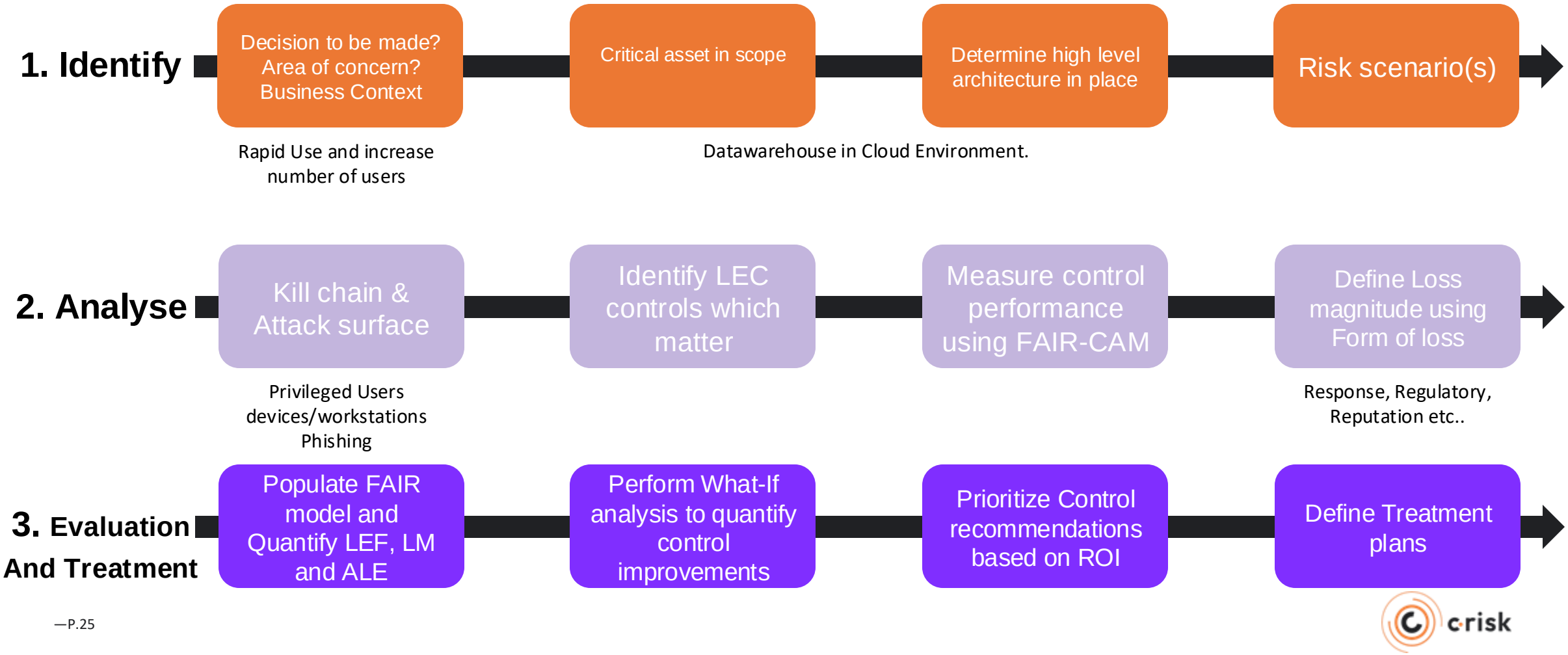
What do I need to perform a FAIR-CAM Analysis

- A decision to make – why perform the analysis
- A precisely scoped risk scenario using OpenFAIR – Asset, Threat Actor, Impact, Vectors/methods using by TA
- Enough knowledge about the Technical Architecture and IT Environment to identify:
  - Attack Surface
  - Context – What Controls are relevant:
    - Probable Attack techniques a threat actor would attempt
    - Controls at each Attack surface which would counteract threat actor
  - Ability to estimate operational control performance via SME input and performance data

c-risk

FAIR-CAM Risk Assessment Process

Organization has deployed a new Datawarehouse system running in a Public Cloud environment. The database contains PII data about entire customer base and supports multiple functions and business units. There are a large number of projects using the system and a high volume of privileged users. The CISO is concerned about the risk of a breach as a result of a privileged account compromise.



Context and Identification

Organization has deployed a new Datawarehouse system running in a Public Cloud environment. The database contains PII data about their entire customer base and supports multiple functions and business units. There are a large number of projects using the system and a high volume of privileged users. The CISO is concerned about the risk of a breach as a result of a privileged account compromise.

Asset	Threat	Vectors	Impact
PII Data in Datawarehouse	Cyber Criminal Targeted	Compromise of Privileged Accounts Phishing	Confidentiality

Risk Statement: Risk of a data breach of customer PII data from a Datawarehouse containing approx. 10M records resulting from a targeted cyber attack using spear phishing of privileged IT users as an attack vector

Attack Path

Context	Threat Actor • **Threat Actor:** Cyber Criminal • **Intent:** Financial Gain • **Frequency:** Targeted and persistent	Initial Attack Surface Accounts and End Points • Advanced phishing of IT employees with privileged access	2nd Attack Surface Cloud Environment in which database is hosted • Customer PII data in Data warehouse • Application and API which have access to PII data • Discovery, Access and Exfiltration	Data Breach Event Financial Impact Volume of records exfiltrated before incident is detected, responded to and contained.
Loss Event Controls		Initial Attack Surface 1. Personnel 2. EDR - End Point Protection 3. Secure Software 4. Logging, Monitoring and Detection	2nd Attack Surface 1. Authentication and Privileged access to PII via database and Application API's 2. Logging, Monitoring and Detection	Data Breach Event Financial Impact 1. Detect Exfiltration and Respond 2. Contain Incident
VMC and DSC Controls to Consider		Initial Attack Surface Threat Intelligence Security Awareness Training Asset Mgmt. Vulnerability mgmt. and patching	2nd Attack Surface Privileged Access Mgmt. and Admin Cloud Configuration Standards	Data Breach Event - Financial Impact Incident Response Planning Alignment of cyber insurance to loss

Analysis

Asset	Threat	Vectors	Impact
PII Data in Datawarehouse	Cyber Criminal Targeted	Compromise of Privileged Accounts Phishing	Confidentiality

Risk Statement: Risk of a data breach of customer PII data from a Datawarehouse containing approx. 10M records resulting from a targeted cyber attack using spear phishing of privileged IT users as an attack vector

Attack Path

Loss Event Controls

Initial Attack Surface

1. Personnel
2. EDR - End Point Protection
3. Secure Software
4. Logging, Monitoring and Detection

2nd Attack Surface

1. Authentication and Privileged access to PII via database and Application API's
2. Logging, Monitoring and Detection

Data Breach Event Financial Impact

1. Detect Exfiltration and Respond
2. Contain Incident

Resistive Control Analysis

					Operational Efficacy			Aggregate Efficacy		
Attack surface	Control	Design Eff	Coverage	Reliability	Min	ML	Max	Min	ML	Max
User Endpoints	Personnel	High	Very High	Very High	19%	68%	97%	19.0%	68.1%	96.7%
	Secure Operating System	Very High	Very High	High	0%	25%	97%	19.4%	76.1%	99.9%
	EDR	High	Very High	High	0%	24%	94%	19.8%	81.9%	100.0%
	N/A	N/A	N/A	N/A	0%	0%	0%	19.8%	81.9%	100.0%
Cloud Environment	Network firewall	High	Very High	Very High	64%	85%	97%	64.4%	85.4%	96.7%
	Access privilege restrictions	Very High	Very High	High	33%	69%	97%	76.1%	95.5%	99.9%
	N/A	N/A	N/A	N/A	0%	0%	0%	76.1%	95.5%	99.9%
PII data in databases	Encryption	N/A	N/A	N/A	0%	0%	0%	0.0%	0.0%	0.0%
	N/A	N/A	N/A	N/A	0%	0%	0%	0.0%	0.0%	0.0%
	N/A	N/A	N/A	N/A	0%	0%	0%	0.0%	0.0%	0.0%

Detection & Response Control Analysis

Control Function	Design Eff	Coverage	Reliability	Op Eff
Visibility	High	Very High	Moderate	76%
Monitoring	High	Very High	Moderate	76%
Recognition	Moderate	Very High	Very High	80%
Containment	High	Very High	Very High	91%
			Agg Efficacy	**42%**

Reduction of the Most Likely loss magnitude value

Measurement of defense in depth Efficacy per attack surface

Capability Translation Scale

Rating	Range	Min	ML	Max
Very High	>97%	0.97	0.985	0.999
High	>90%	0.90	0.935	0.969
Moderate	>75%	0.75	0.825	0.899
Low	>50%	0.50	0.675	0.749
Very Low	<50%	0.00	0.25	0.499
N/A	0%	0	0	0

LEF Analysis

	Min	ML
TEF	4	12
IAS LEF	0.000	2.175
SAS LEF	0.000	0.097
FAS LEF	**0.0000**	**0.097**

IAS = Initial attack surface (e.g., user endpoints)

SAS = Subsequent attack surface

FAS = Final attack surface

Evaluation and Treatment

Asset	Threat	Vectors	Impact
PII Data in Datawarehouse	Cyber Criminal Targeted	Compromise of Privileged Accounts Phishing	Confidentiality

Risk Statement: Risk of a data breach of customer PII data from a Datawarehouse containing approx. 10M records resulting from a targeted cyber attack using spear phishing of privileged IT users as an attack vector

Likelihood of Event

9%
Most Likely

Risk Drivers

Likelihood is driven by frequency of attacks and control performance in the following categories:

Initial Access controls:
- Email Security and Protection
- Security Awareness Training
- Secured End Points
- Access Control

Lateral Movement
- Privileged Access Control
- MFA
- Event logging, detect and Response

Loss Magnitude

$20M
Most Likely

Risk Drivers

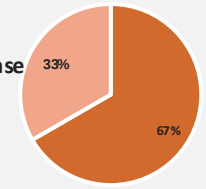
Impact is driven by volume of records exfiltrated before incident is detected and responded to and contained.

Response controls :
- Detect Exfiltration and Respond
- Contain Incident
- Incident Response

Primary Cost Drivers

$10M Incident Mgmt. and Response

$20M Regulatory



Current Residual Risk:

Current	Most Likely
Likelihood	9%
Loss Magnitude	$20M
ALE	$2M

What If Analysis Results:

Target	Most Likely
Likelihood	2%
Loss Magnitude	$15M
ALE	$500K

Risk Treatment Plan

Total cost of treatment plan estimated to be **$500K** with a 6 month time to implement. Annualised risk reduction will be $1.5M with a 3 year **ROI of $4.5M** and per event risk reduction of $5M

Improve End Point OS Secure Configuration
Impact: Reduction in Likelihood by estimated 3%
How: Restrict use ability to install and run unauthorized software

Improve Network Firewall between end user environment and cloud
Impact: Reduction in Likelihood by estimated 2%
How: Reduce users ability to access to IaaS cloud environment without approval and MFA

Improve Privileged Access Management
Impact: Reduction in Likelihood by estimated 2%
How: Reduce users with the ability to extract PII from database

c·risk

Value from use in the field

Operational Experience of using FAIR-CAM

Moving beyond Control Frameworks to modelling how operational control performance impacts risk exposure

- Ability to Engage Security Experts / SME / Security Operations in the risk mgmt. process.
- A model to deal with Complexity
- A model to measure operational performance which compliments control design using Control frameworks.
- CAM provides a model to focus on efficacy In the context of system and scenario in scope. Provides actionable output which engineering teams can use.
- Provides better insight into which controls matter

c-risk

QUESTIONS

INTERTESTED IN LEARNING MORE

https://www.fairinstitute.org/fair-controls-analytics-model

C-RISK – Training on FAIR-CAM coming in Q1 2025

c-risk

c·risk

Questions,
Clarifications,
AOB