A New Lens for Understanding Control Efficacy

March 26, 2025

How much risk reduction did your organization get from its most recent large security investment?

If your security department had its budget cut, how confident would it be in deciding what to cut?

The gap…

The Challenge We All Face

- We know which controls we've implemented (anatomy)
- We don't understand how they function to reduce risk (physiology)
- We can't reliably measure their effectiveness
- We make decisions based on intuition rather than measurement

“In the 1800’s medicine 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.”

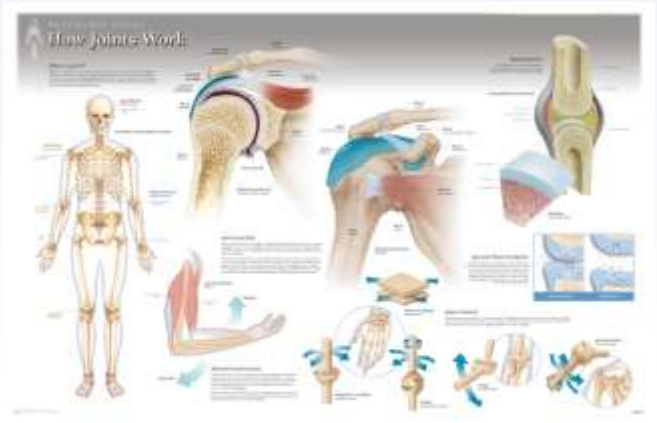
A Retired Surgeon

In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)



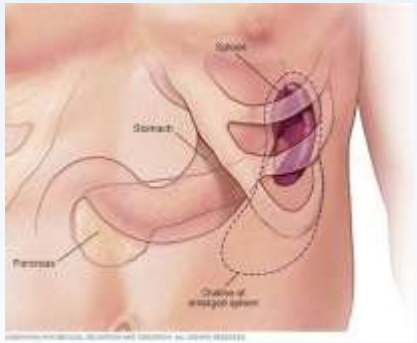
Neither. You need to know both.

Example of cybersecurity “anatomy” (ISO27001)

A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users’ access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Human Anatomy vs. Physiology

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



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

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

Cybersecurity Anatomy vs. Physiology

- **Anatomical component**: Awareness training
  - Content: Passwords, phishing, clean desk, etc.
  - Periodicity: Annual
- **Purpose**: Informs personnel about the organization's expectations and requirements.

- **Physiology (how it functions within the system to reduce risk)**
  - Function: Reduces the frequency of decisions and actions that introduce additional, undesirable levels of risk
  - Depends upon: Policies, risk appetite, risk measurement, etc…
  - Is depended upon by: Authentication, system security, access privileges, physical security, data protection, etc…
  - When deficient, may be partially compensated for by: DLP, password enforcement, Anti-malware, etc.

It's part of a system.

The Missing Piece…

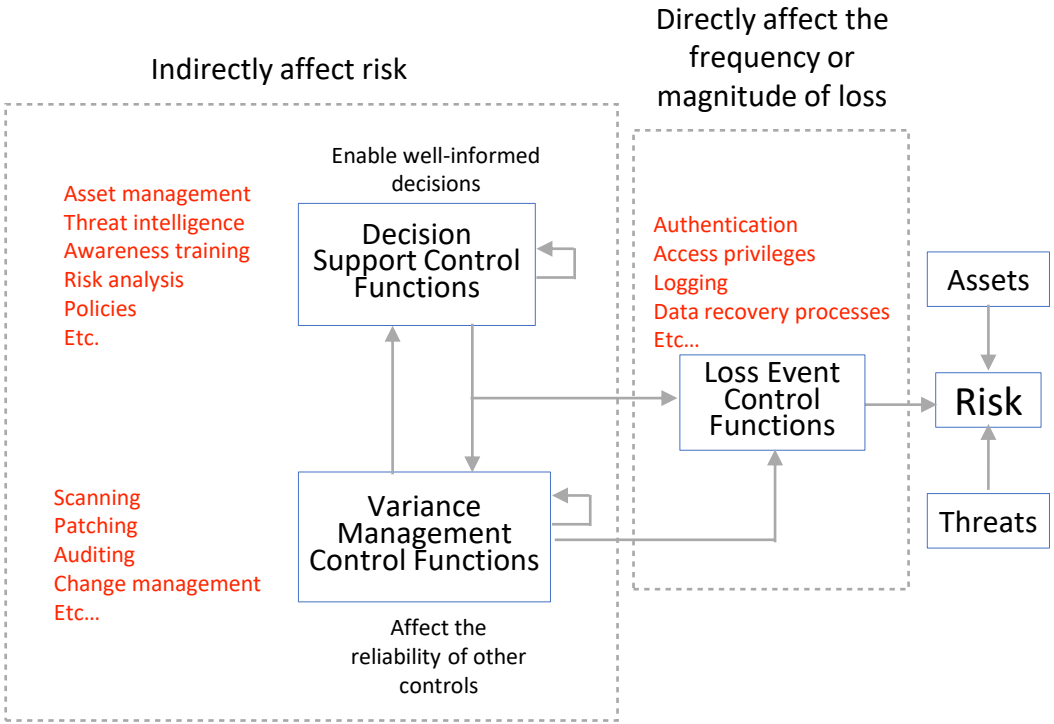
- A model for understanding how controls actually function
- A means to account for how controls work together as a system
- A way to empirically measure control efficacy
- An ability to quantify the value of our investments


Filling the gap…

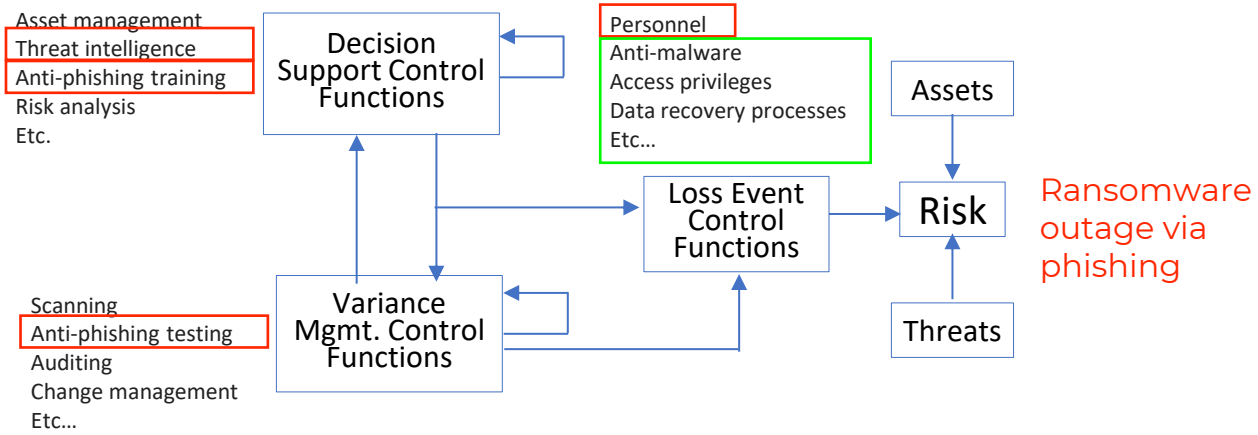
What is FAIR-CAM?

- Factor Analysis of Information Risk - Control Analytics Model
- An extension of FAIR focused on measuring control efficacy
- A model for understanding control “physiology”
- NOT just another control framework

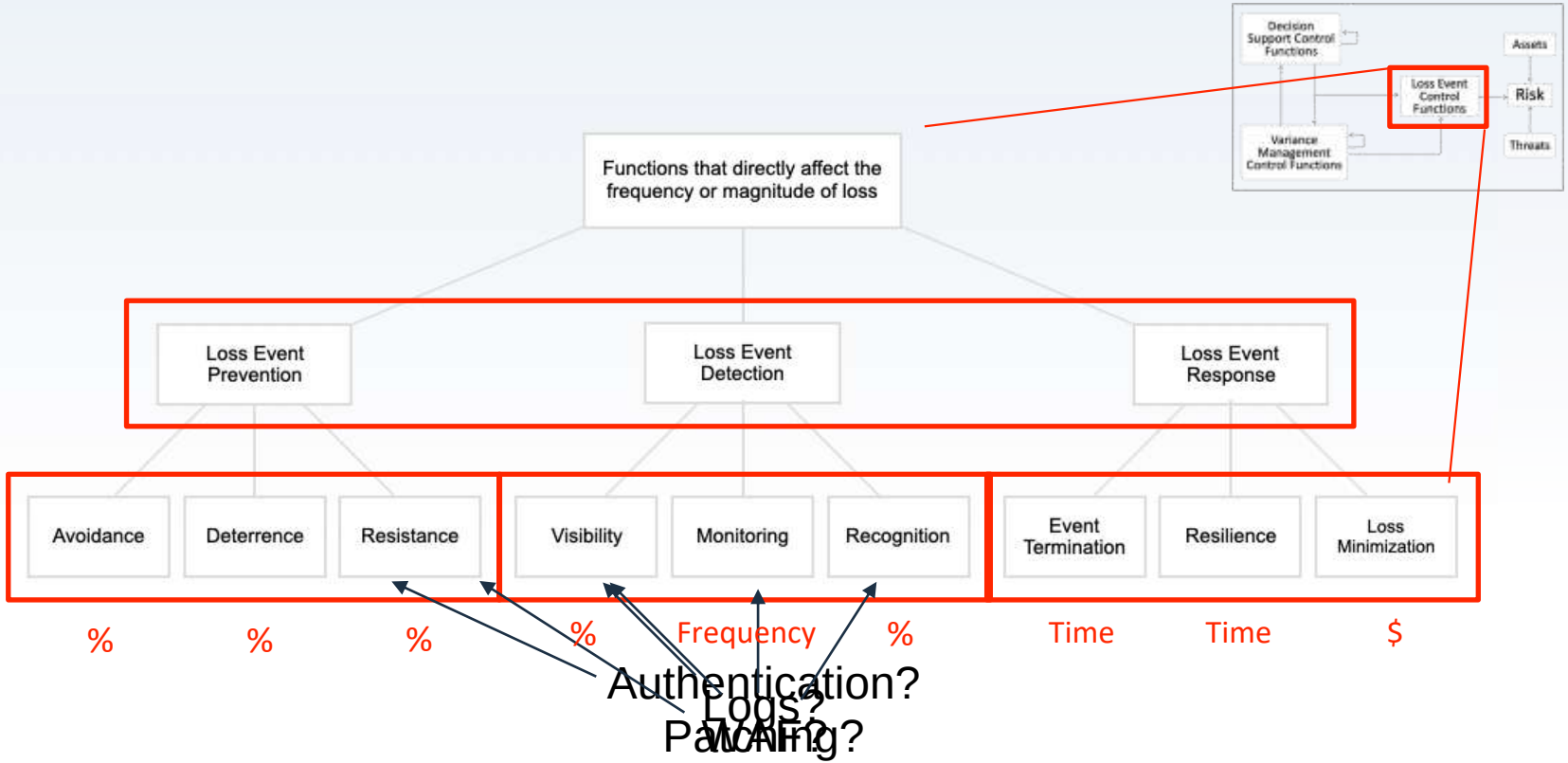
FAIR-CAM's Three Domain Structure



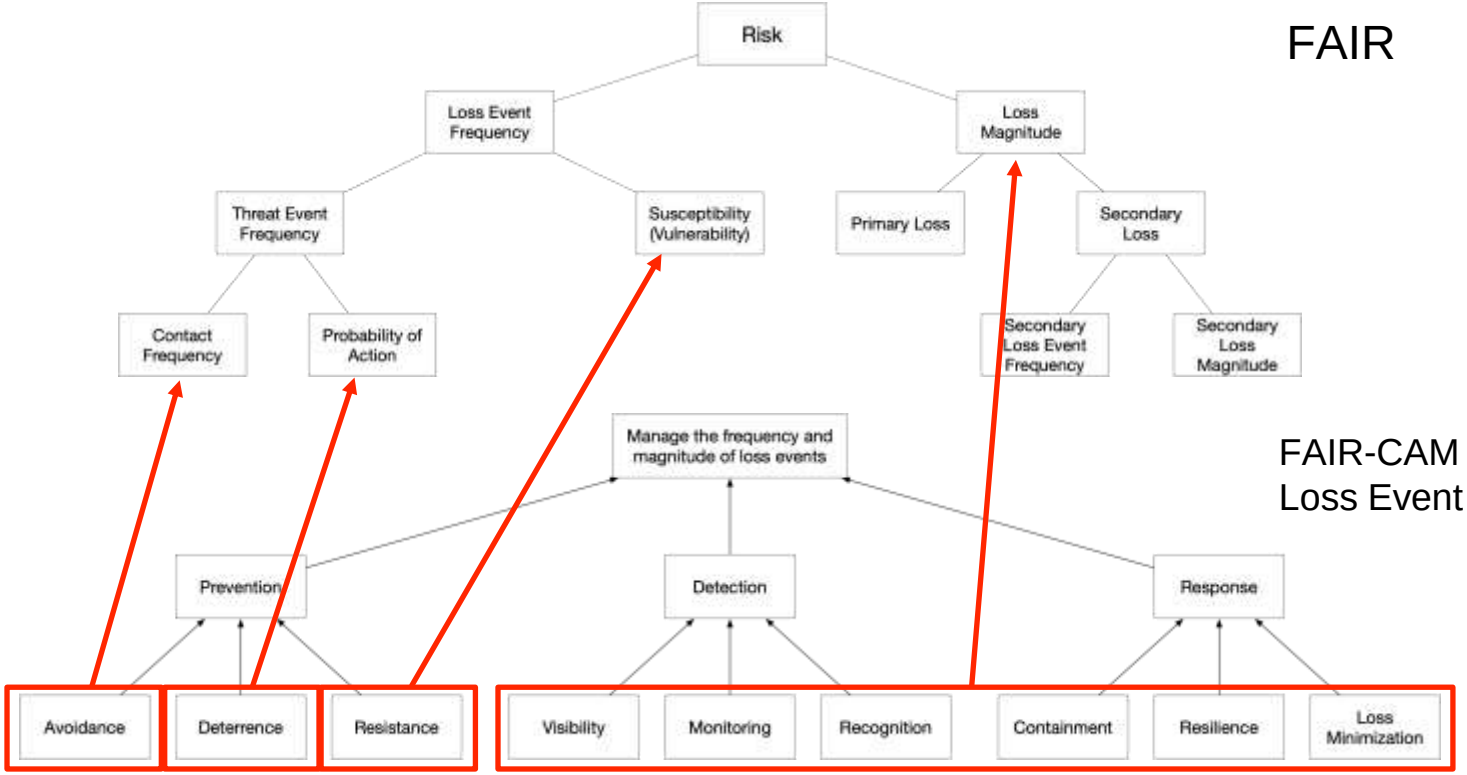
What's the efficacy of personnel as a control against phishing?



Loss Event Control Functions



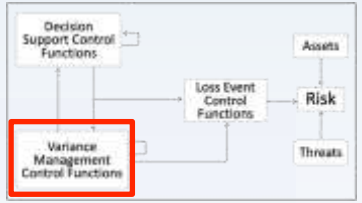
Loss Event Function Mapping to Risk



FAIR

FAIR-CAM
Loss Event Functions

Variance Management Control Functions



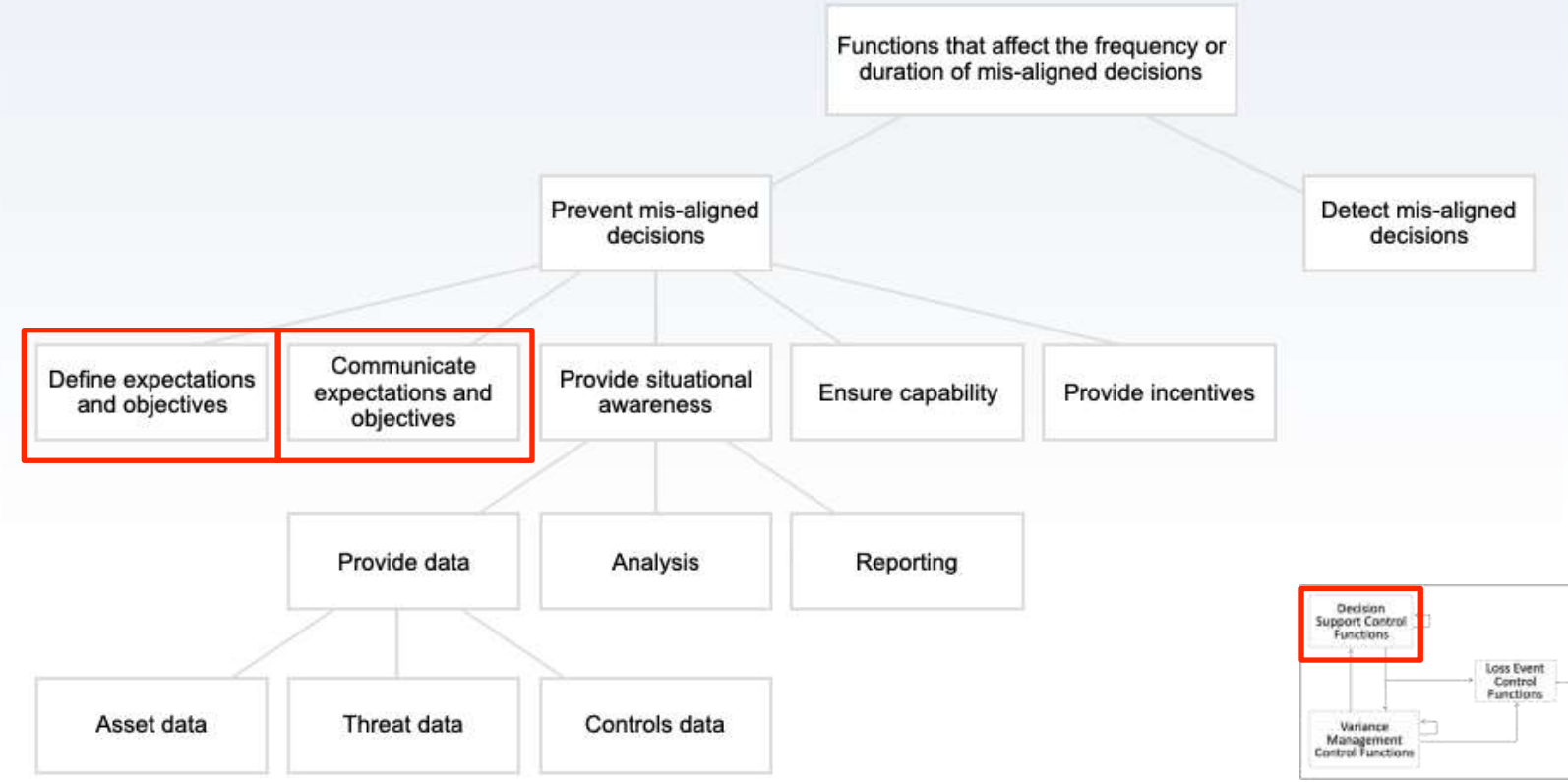
Functions that affect the frequency or duration of variant conditions

- Variance Prevention
  - Reduce Change Frequency
  - Reduce Variance Probability
- Variance Identification
  - Threat Capability Monitoring
  - Controls Monitoring
- Variance Correction
  - Prioritization and Solution Selection
  - Implementation

Restricting Admin Privileges?

Patching?

Decision Support Control Functions



Understanding Efficacy

Example of typical control “measurement”

A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users’ access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

NOT quantitative values!

“3”	“4”
“4”	“1”
“4”	“4”
“4”	“5”
“2”	“3”
“2”	“2”
Avg. 3.17	=? 3.17

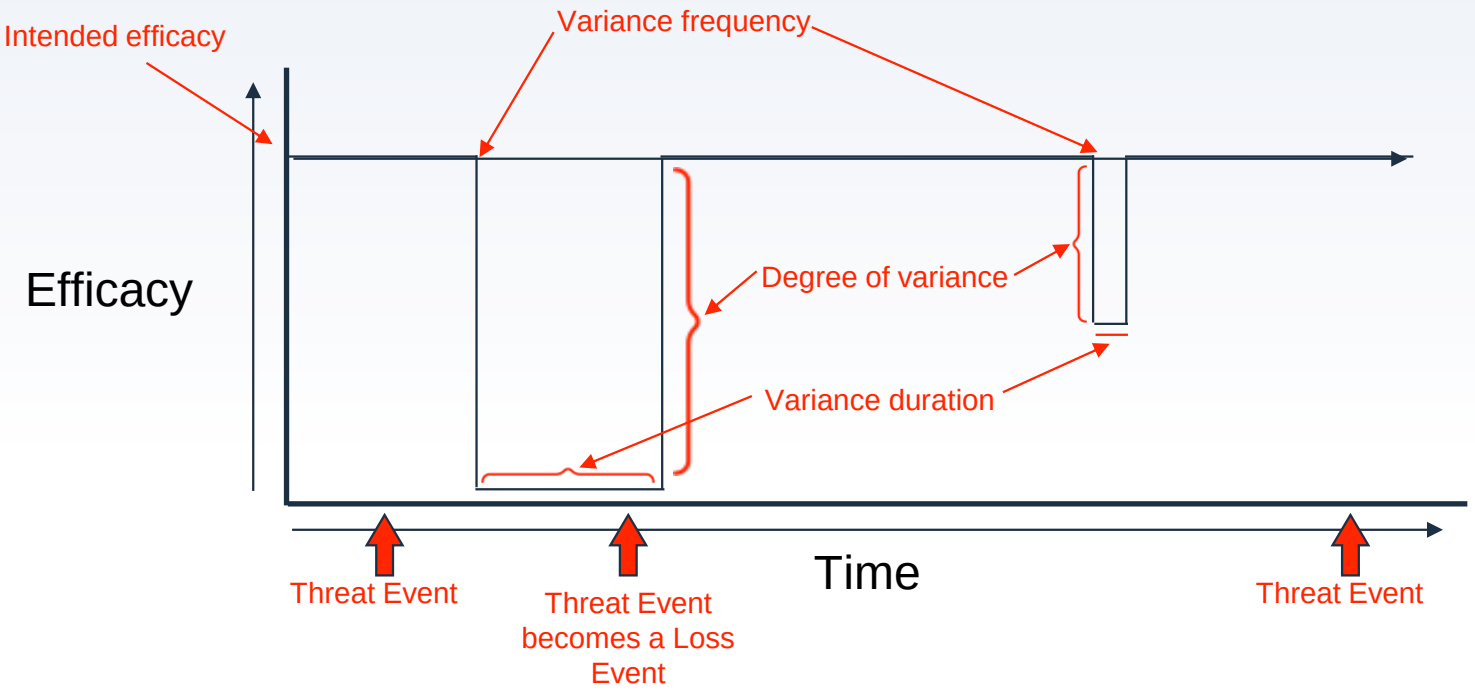
Three states of control efficacy

- Intended efficacy — how well a control works when operating as designed
- Variant efficacy — how well a control works when in a degraded condition
- Operational efficacy — the actual performance over time
  - A function of intended efficacy, variant efficacy, and variance patterns

Understanding “Variance”

- A “variant condition” exists when a control is not operating at its intended level of efficacy. For example:
  - A weak password
  - Logging that is not enabled
  - 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
- Variance has both frequency (VF) and duration (VD)

How Variance Affects Operational Efficacy

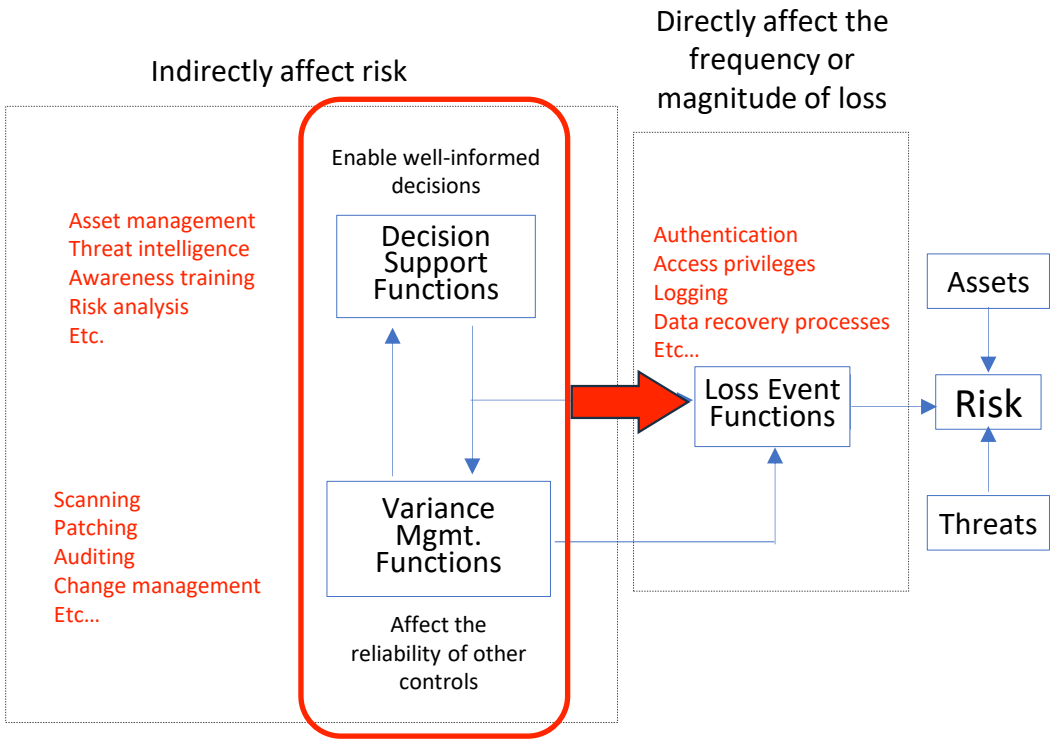


Example Operational Efficacy Analysis

- Control: Access privileges
- Intended Efficacy: 100%
- Variant Efficacy: 0%
- Variance Frequency (VF): 0.5 yr
- Variance Duration (VD): 90 days
- Operational Efficacy: 88%

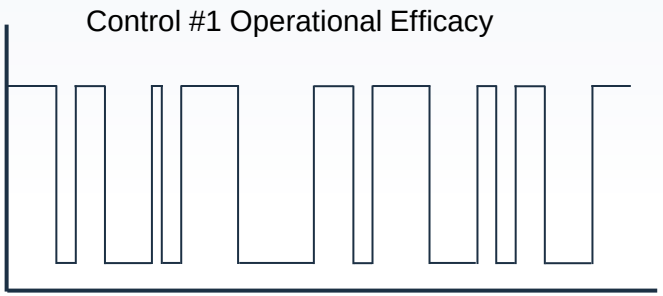
$$(1 - (VF/365))^{VD}$$

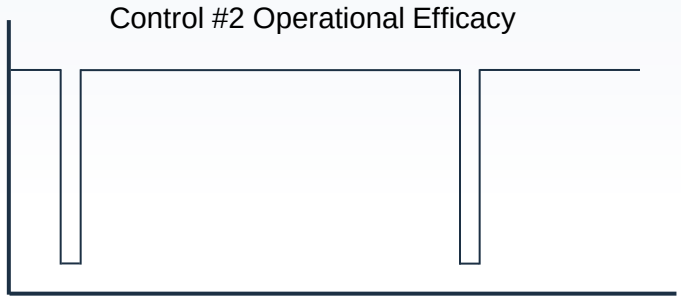
Remember These Relationships?



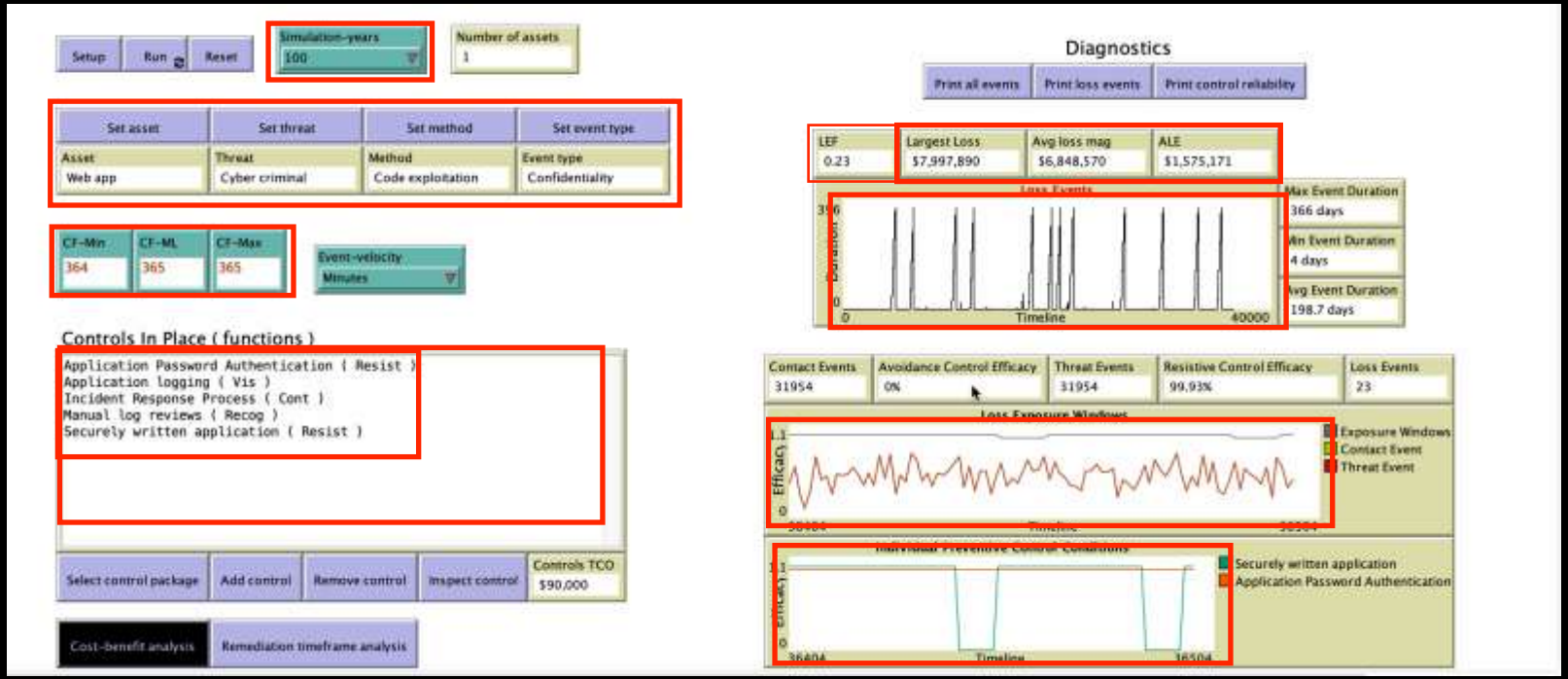
What Drives Variance

- Variance frequency and duration are a function of Variance Management and Decision Support controls (e.g., auditing, policies, training, testing, remediation, risk measurement, etc.)





Cost-benefit analysis simulation

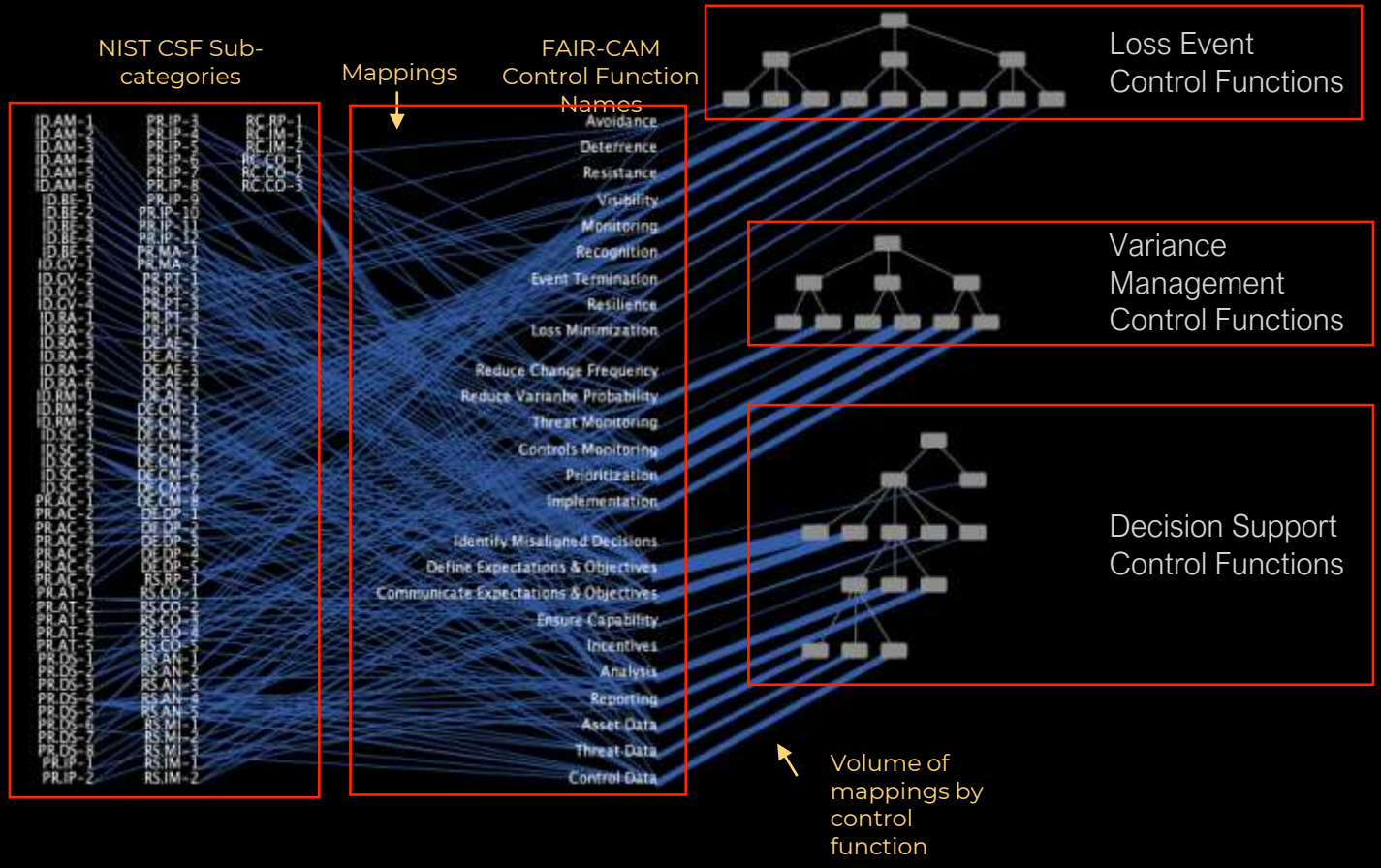


FAIR-CAM & Common Frameworks

FAIR-CAM is NOT a replacement for common control frameworks.

It helps us better understand and apply the controls within those frameworks.

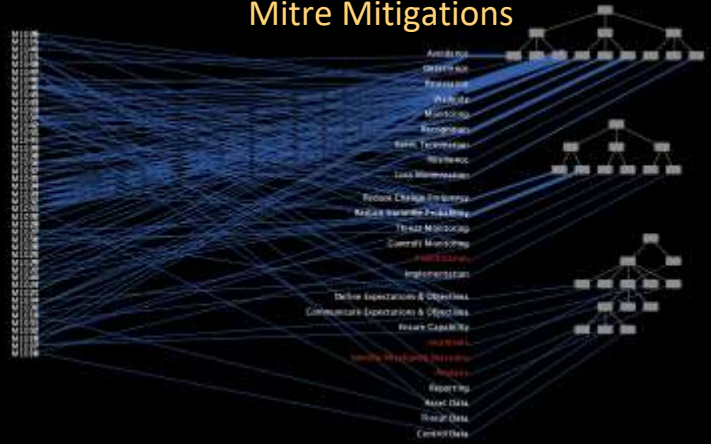
NIST-CSF to FAIR-CAM



NIST CSF

CIS Controls

Mitre Mitigations



Wrapping up

Key take-aways

- Only understanding control “anatomy” doesn’t provide a complete picture of our risk posture
- Overly-simplified approaches to control and risk measurement leads to poor decisions (poor prioritization and wasted resources)
- FAIR-CAM reflects the complexity of our landscape
- Holding our own against the threat actors requires us to understand and reliably measure the efficacy of our controls

QUESTIONS