To Whom It May Concern:

Hello, my name is Luke Bader, Director of Membership and Programs at the FAIR Institute. I am submitting comments to the "Request for Information about Evaluating and Improving Cybersecurity Resources on The Cybersecurity Framework" on behalf of the entire Institute community, Jack Jones, Chairman and author of the FAIR model, our Board of Directors, and our Advisory Board.

The FAIR Institute is an expert, non-profit organization led by cybersecurity and operational risk professionals to develop and promote better risk management practices through the financial quantification of risk. The Institute counts over 12,000 members representing 45% of the Fortune 1,000 Companies and 25 U.S. Federal Government Agencies. The FAIR model was officially listed in the Informative Reference Catalog on the NIST CSF website in 2019.

We believe that even as NIST CSF has seen wonderful adoption as a way to gauge an organization's risk management posture or maturity, even more benefits can be realized. Specifically, there is a great opportunity to increase CSF's value by enabling it to help organizations empirically measure and prioritize their risk remediation efforts.

With the recent release of the new FAIR Controls Analytics Model (FAIR-CAM™), there is now a way to empirically measure control efficacy and risk reduction value. With some modifications, NIST CSF could map cleanly to FAIR-CAM™, which would help organizations understand the efficacy and value of controls in their risk programs.

Our proposed first steps are as follows:

- Modify NIST CSF to provide more granularity at, or below, the subcategory level
- Define measurement scales for each of the elements in the framework to reduce ambiguity and improve quality of benchmarking and measurement

For a more complete look at the ideas underlying this proposal, below and attached are resources from a recent presentation given by Jack Jones, Overcoming the Challenges of Mapping NIST CSF to FAIR CAM™.

Upon your review, we welcome a call to discuss and answer questions. Please connect me with the person best suited to continue this effort.

Thank you,

Luke

Overcoming the Challenges of Mapping NIST CSF to FAIR-CAM

Jack Jones

Chairman FAIR Institute

Perhaps a more accurate title…

Overcoming the Challenges of Measuring the Efficacy and Value of NIST CSF Subcategories

Jack Jones

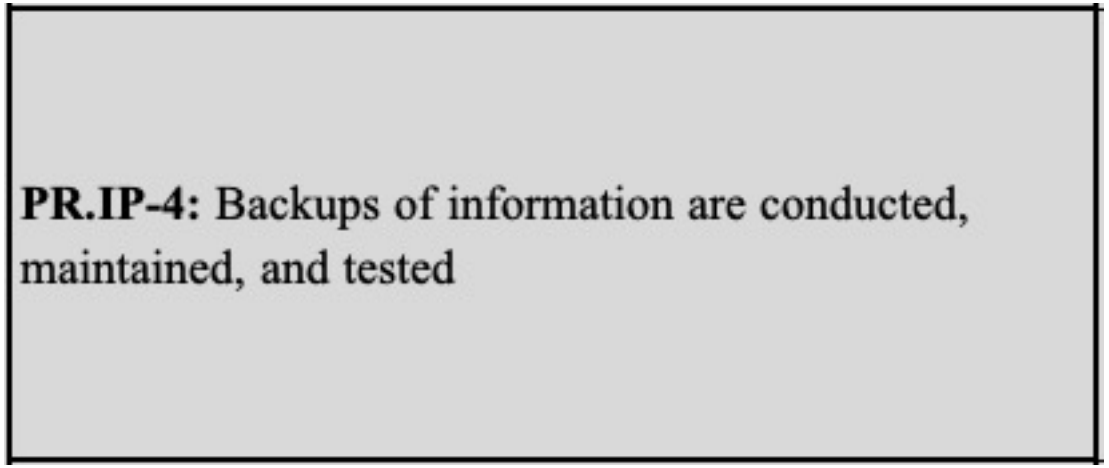
Chairman FAIR Institute

The big question…

Can we take our NIST CSF scores, plug them into FAIR-CAM, and measure their efficacy and risk reduction value?

For example…

How much less risk do we have if we improve our NIST CSF PR.IP-4 score from a “2” to a “3”?



Two things we have to figure out:

1. How does PR.IP-4 affect risk?
2. What do the scores represent?

Quick FAIR-CAM refresher…

Clarifying terms

Controls:

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

Examples:

Policies
Passwords
Patching
Data backups
Auditing
etc…

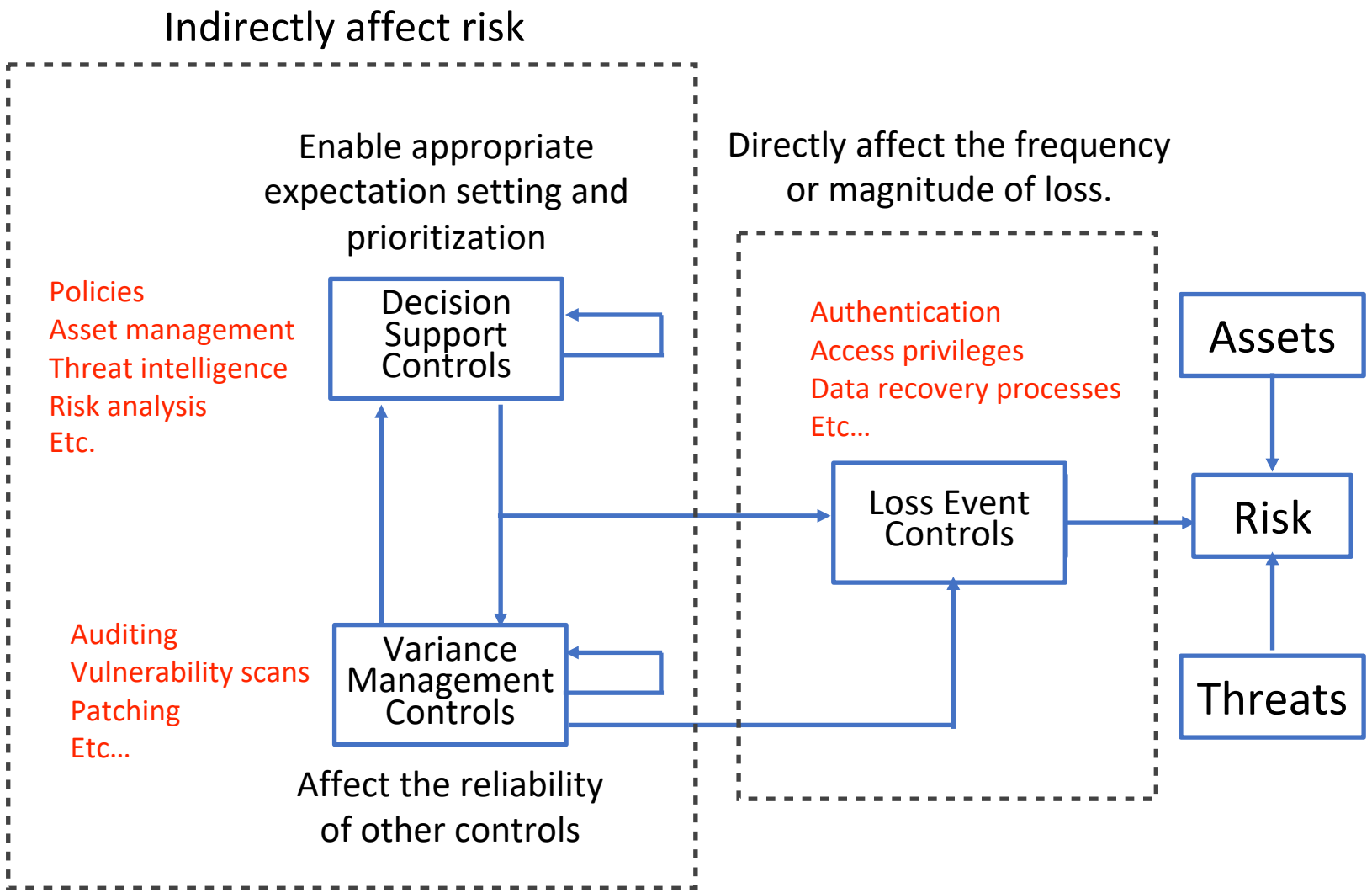
Control Functions:

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

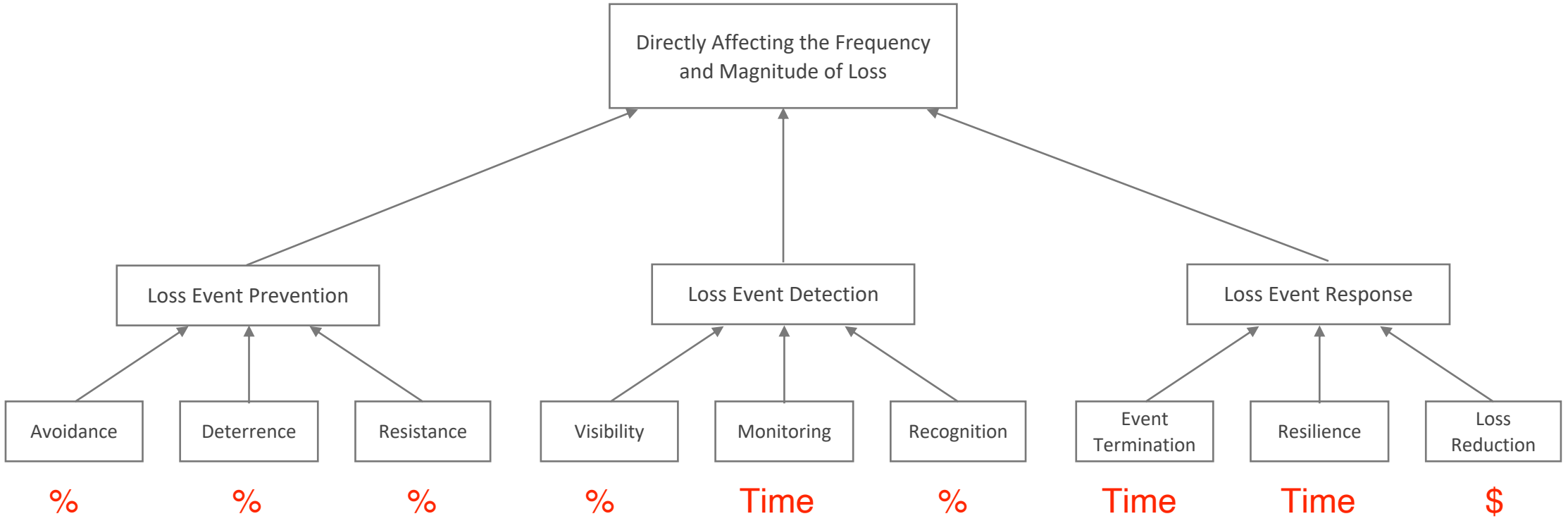
Examples:

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

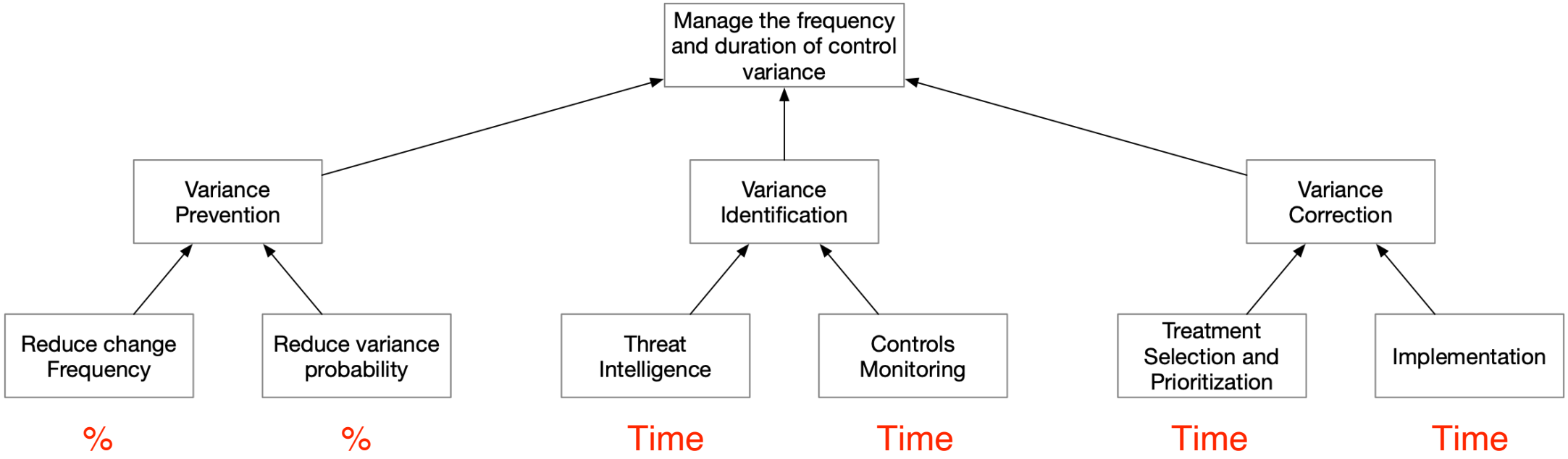
Control Functional Domain Relationships



Loss Event Control Functions

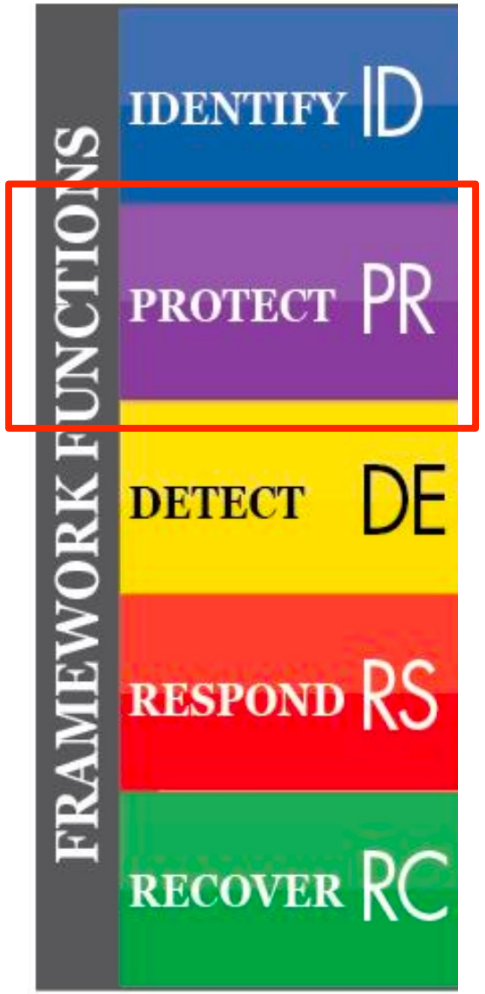


Variance Management Control (VMC) Functions



Challenge #1
How do the NIST CSF subcategories affect risk?

NIST CSF Functions



How do subcategories within NIST's Protect function affect risk? Do they…

- reduce loss event frequency, or
- reduce loss magnitude?

Let's look at a few of them…

PR.IP-4: Backups of information are conducted, maintained, and tested

Reduces loss magnitude

Reduces the duration of control deficiencies

PR.IP-10: Response and recovery plans are tested

PR.AT-2: Privileged users understand their roles and responsibilities

Reduces the probability of poor decisions

Initial mapping completed, and being reviewed

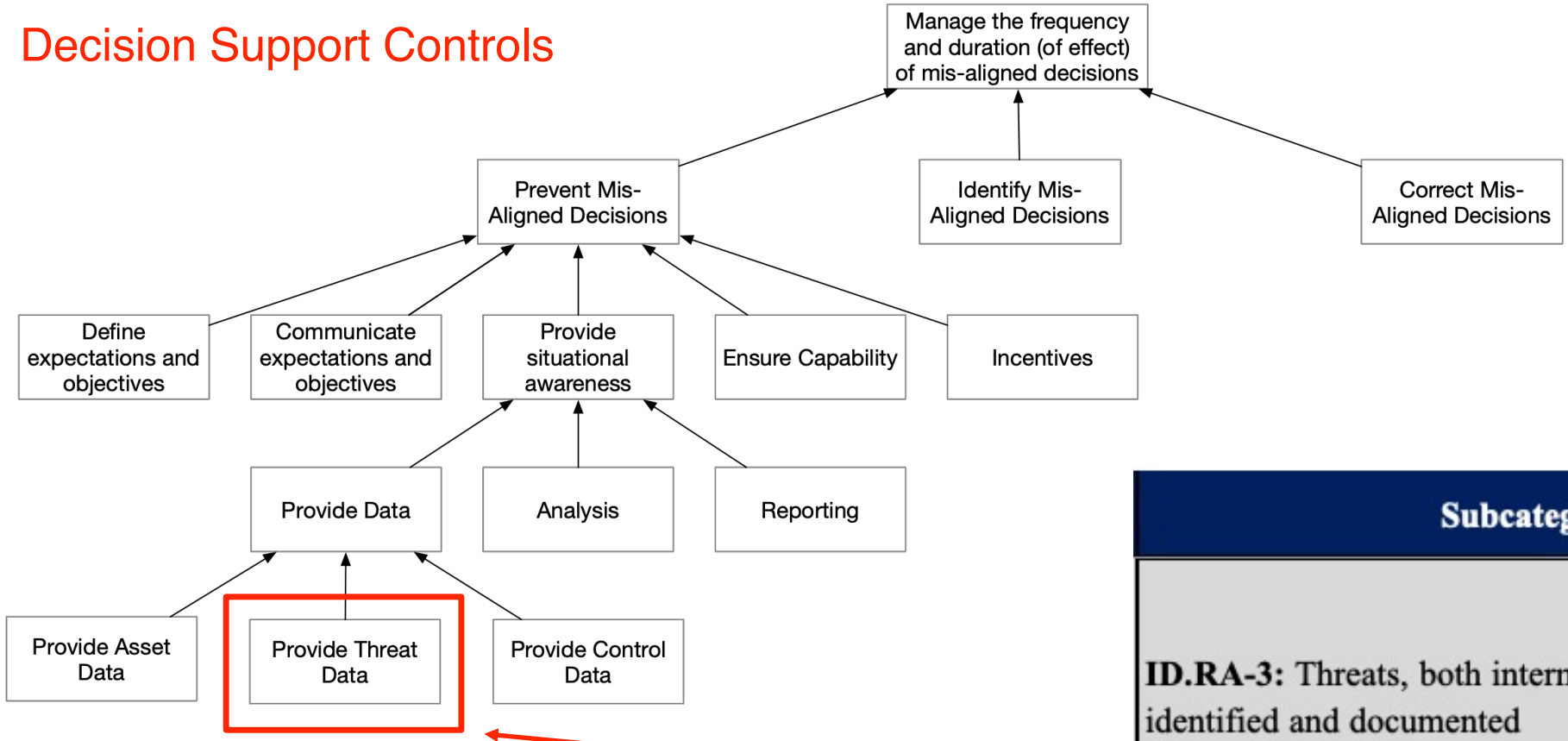
NIST CSF Elements

FAIR-CAM Functions

		Serves Which Functional Domain(s)			Loss Event Control Functions									Variance Management Control Functions						Decision Support Control Functions									
					Prevention			Detection			Response			Prevention		Identification		Correction		Prevention									Identify Misaligned Decisions
																						Provide Situational Awareness						
																						Provide Data						
Category	Subcategory	LEC	VMC	DSC	Avoidance	Deterrence	Resistance	Visibility	Monitoring	Recognition	Event Termintion	Resilience	Loss Reduction	Reduce Chg Freq	Reduce Var Prob	Threat Capability Intel	Controls Monitoring	Treatment Selection & Prioritization	Implementation	Define Exp's & Obj's	Communicate Exp's & Obj's	Asset	Threat	Controls	Analysis	Reporting	Ensure Capability	Incentives	
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)		x	x											x						x								
	PR.IP-2: A System Development Life Cycle to manage systems is implemented		x	x										x							x								
	PR.IP-3: Configuration change control processes are in place		x											x	x														
	PR.IP-4: Backups of information are conducted, maintained, and tested	x	x									x					x												
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met			x																x									
	PR.IP-6: Data is destroyed according to policy	x			x																								
	PR.IP-7: Protection processes are improved		x															x	x										

Some map simply…

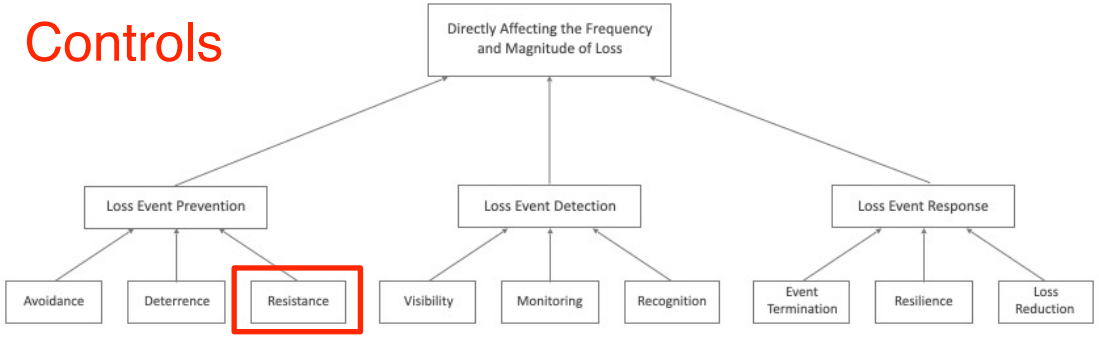
Decision Support Controls



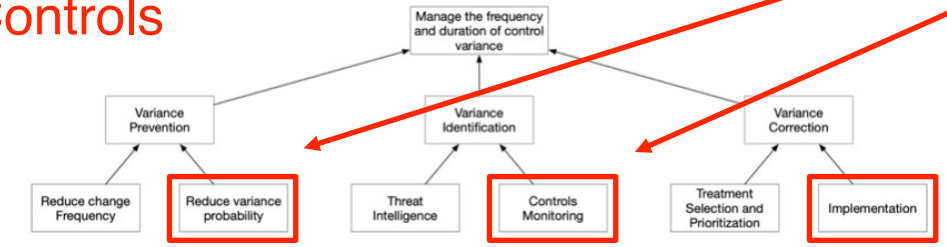
Subcategory
ID.RA-3: Threats, both internal and external, are identified and documented

Many do not…

Loss Event Controls



Variance Management Controls



- Very different ways of affecting risk
- Different units of measurement

Subcategory
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

A score of “2” for this subcategory represents what?

- The average for all of the functions it covers?
- Best case?
- Worst case?

The mapping breakdown (currently)…

FAIR-CAM Functional Domain	Number of Mapped CSF Subcategories
Loss Event Control Functions	24
Variance Management Control Functions	9
Decision Support Control Functions	45
Multiple Functional Domains	29

These affect risk indirectly!

Overcoming the challenge…

The NIST CSF sub-categories have to be redefined to cover no more than a single control function.

Challenge #2
What do NIST CSF scores mean?

What we have to recognize is that…

- There is no standard scoring scale for NIST CSF
  - There are no clear criteria for what constitutes a “2” versus a “3”
  - Therefore, one organization’s “2” doesn’t necessarily equate to another organization’s “2”
- A single scale definition can not be defined to cover all of the control functions
  - E.g., a scale for Loss Event Prevention controls can’t be the same as a scale for Variance Management Identification controls because they have different units of measurement

Translating ordinal values into quantitative ranges

Ordinal Score	Range Minimum	Range Maximum
1	0%	25%
2	26%	50%
3	51%	75%
4	76%	100%

Essentially, translating by quartile

Ordinal Score	Range Minimum	Range Maximum
1	0%	50%
2	51%	75%
3	76%	90%
4	91%	100%

But that doesn't represent reality

…and…

- some are binary
- others have different units of measurement

Overcoming the challenge…

Ordinal scale definitions have to be developed for each control function

Wrapping Up…

What we want to be able to do...

Measure the efficacy and risk reduction value of NIST CSF functions, so that we can prioritize effectively and choose cost-effective solutions

What has to happen first is...

- NIST CSF subcategories that cover multiple functions have to be made more granular and specific
  - The FAIR Institute is reaching out to NISZT to offer assistance if desired
  - Voices from the FAIR community will be important to help make this happen

- Standardized measurement scales have to be defined (these are aalready under development)

Questions?