Mapping NIST CSF & FAIR

Jack Jones
Chairman, FAIR Institute

Why map?

What's the difference?

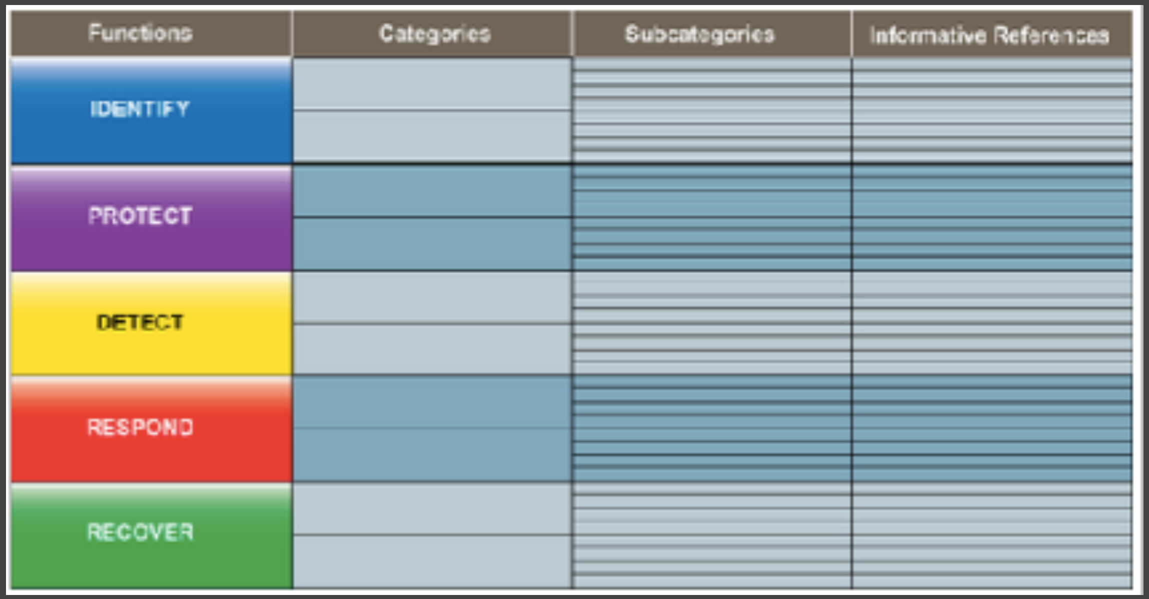
The bottom line…

- There is a critical need to make well-informed business-risk decisions:
    - Effective prioritization
    - Understanding the cost-benefit proposition for risk management efforts
    - Striking the right balance in risk management

Those decisions require…

- An ability to compare elements on some common measurement…

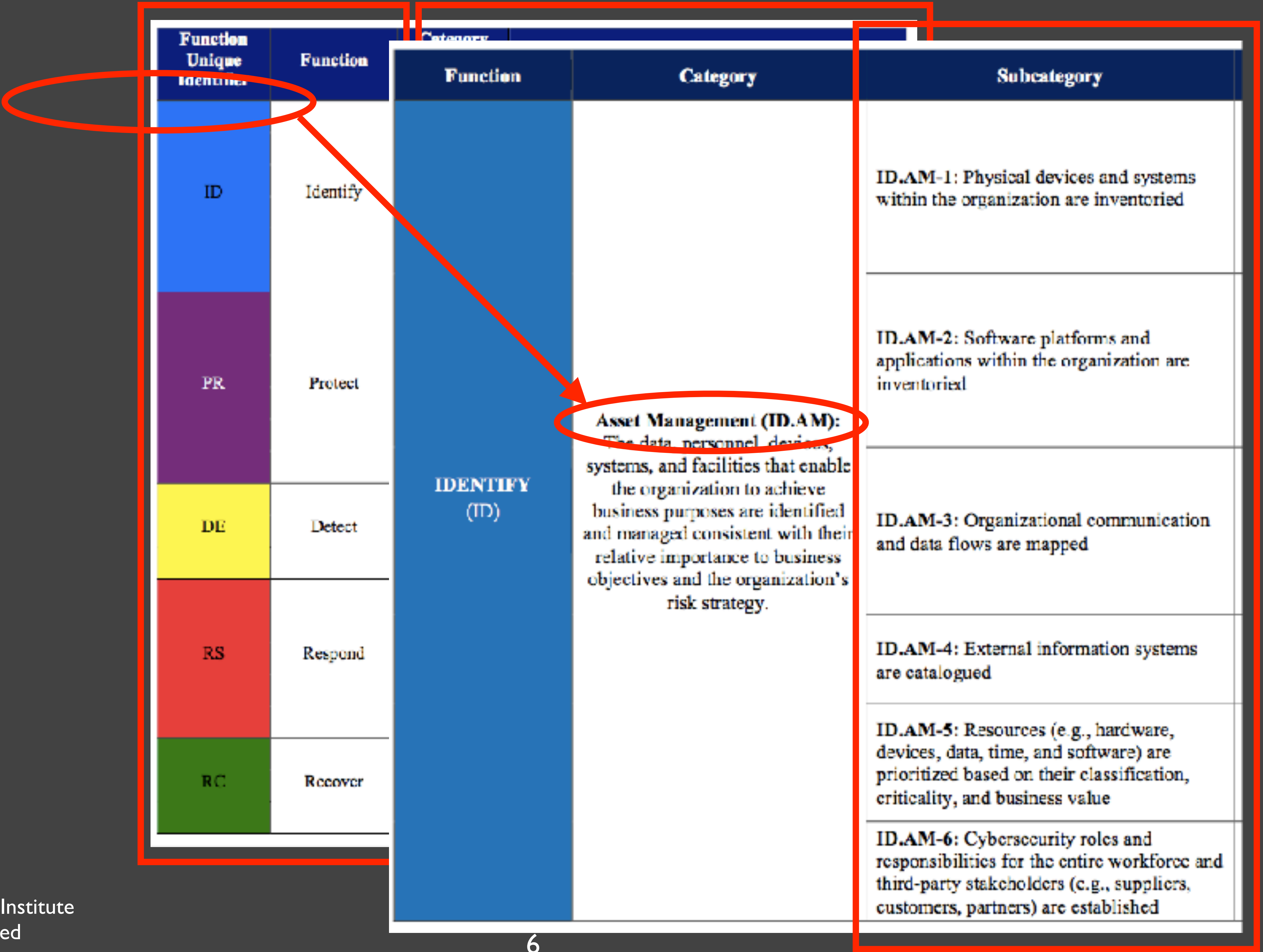
… measurement that is meaningful



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

NIST CSF Overview

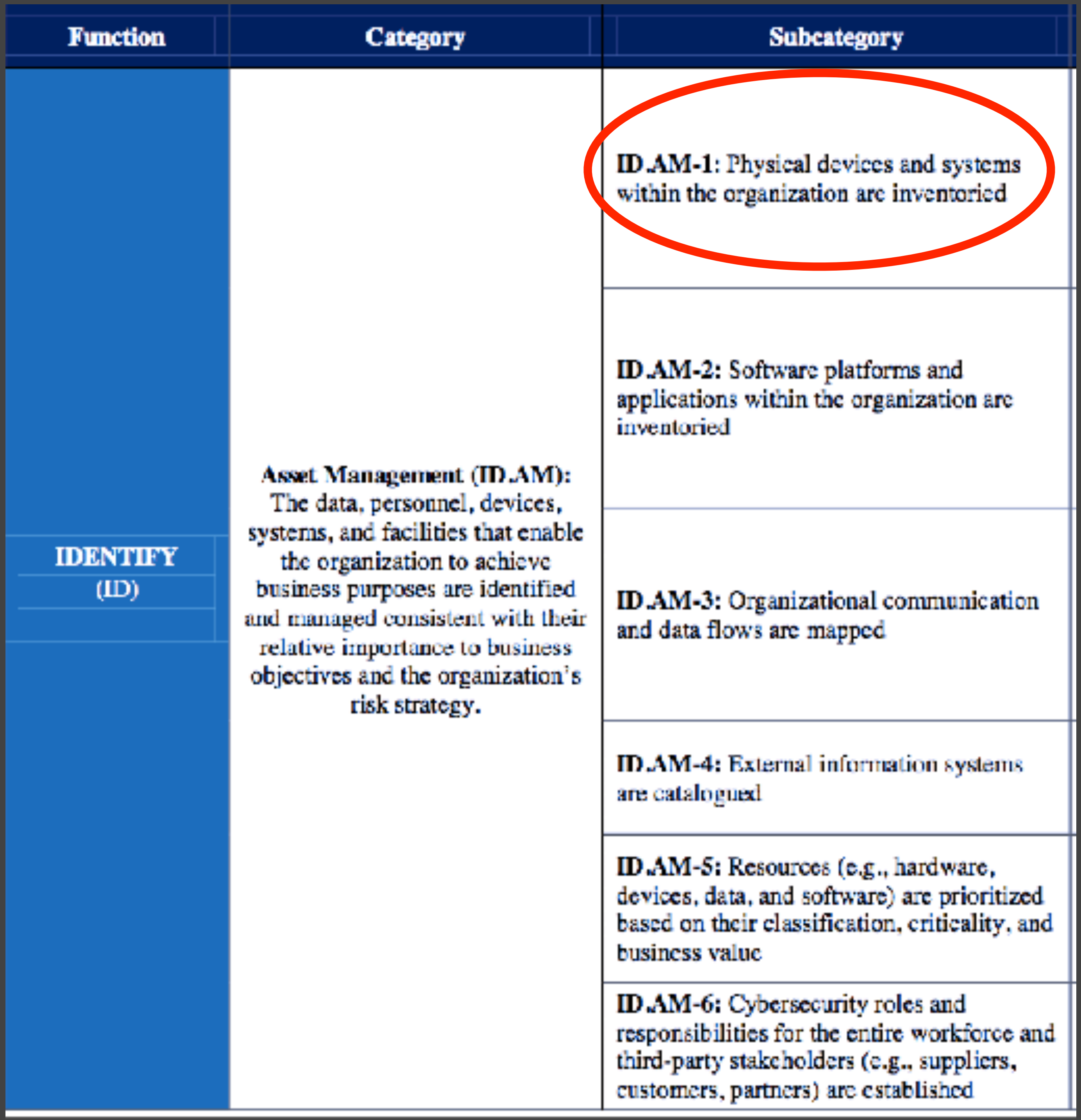
Framework core



Function Unique Identifier	Function
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RC	Recover

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Evaluation and measurement of subcategories



Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Measurement scale definition is up to each organization

1-5

H/M/L

etc…

NOTE: These are measurements of control conditions — not risk

Foundational NIST CSF assumption…

Better risk controls

+ Better risk management

= Less risk

Logical!

But doesn't measure risk.

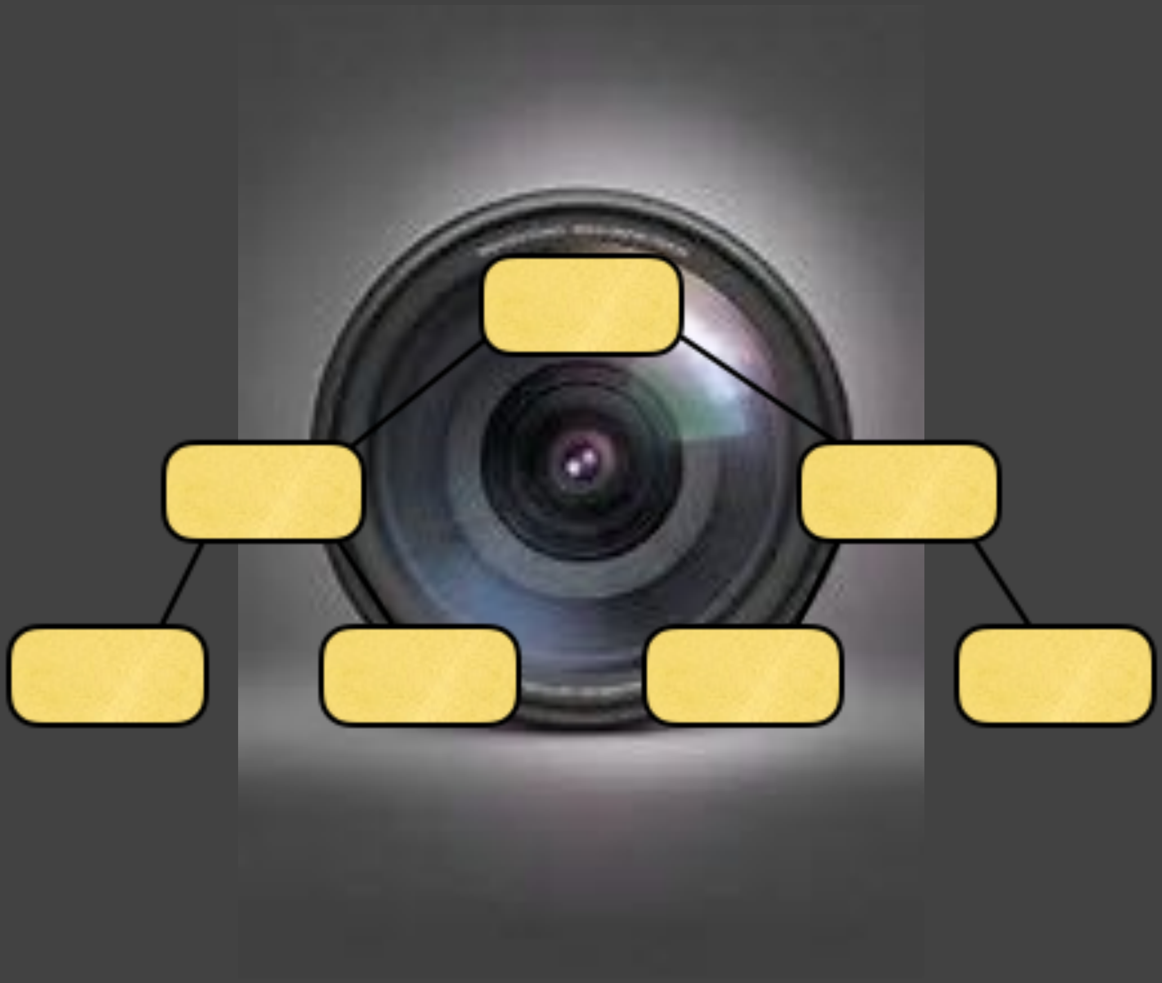
NIST CSF Summary

- Pragmatic size
- Logical structure
- Useful for identifying control gaps
- Is not analytic in nature
- Doesn’t measure risk
- Can’t be used effectively (as is) for prioritization amongst gaps

In order to prioritize…

- Have to understand the risk implications of the control gaps

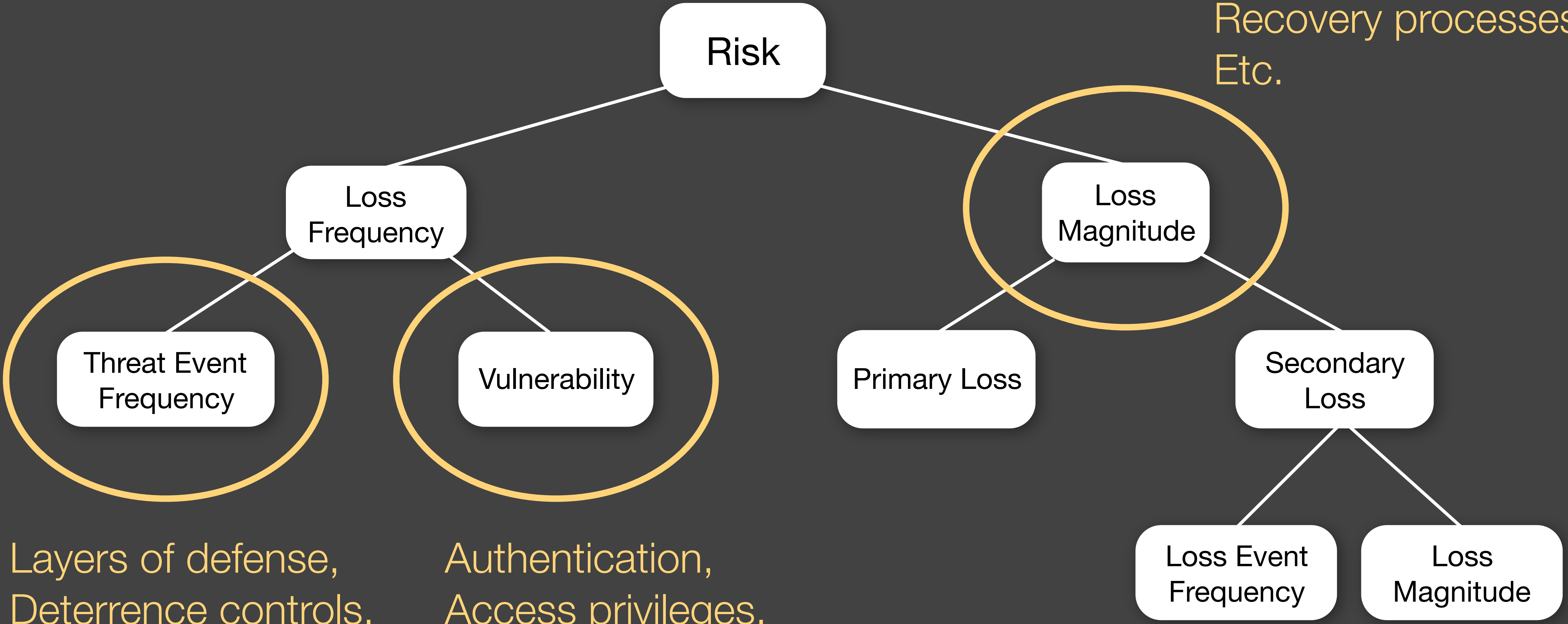
- …which requires an understanding of the role of each control in managing risk
  - Directly
  - Indirectly



A FAIR Lens

Where do controls fit into FAIR?

Incident response,
Recovery processes,
Etc.



Risk

Loss Frequency

Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss

Secondary Loss

Loss Event Frequency

Loss Magnitude

Layers of defense,
Deterrence controls,
Etc.

Authentication,
Access privileges,
Patching/config,
Etc.

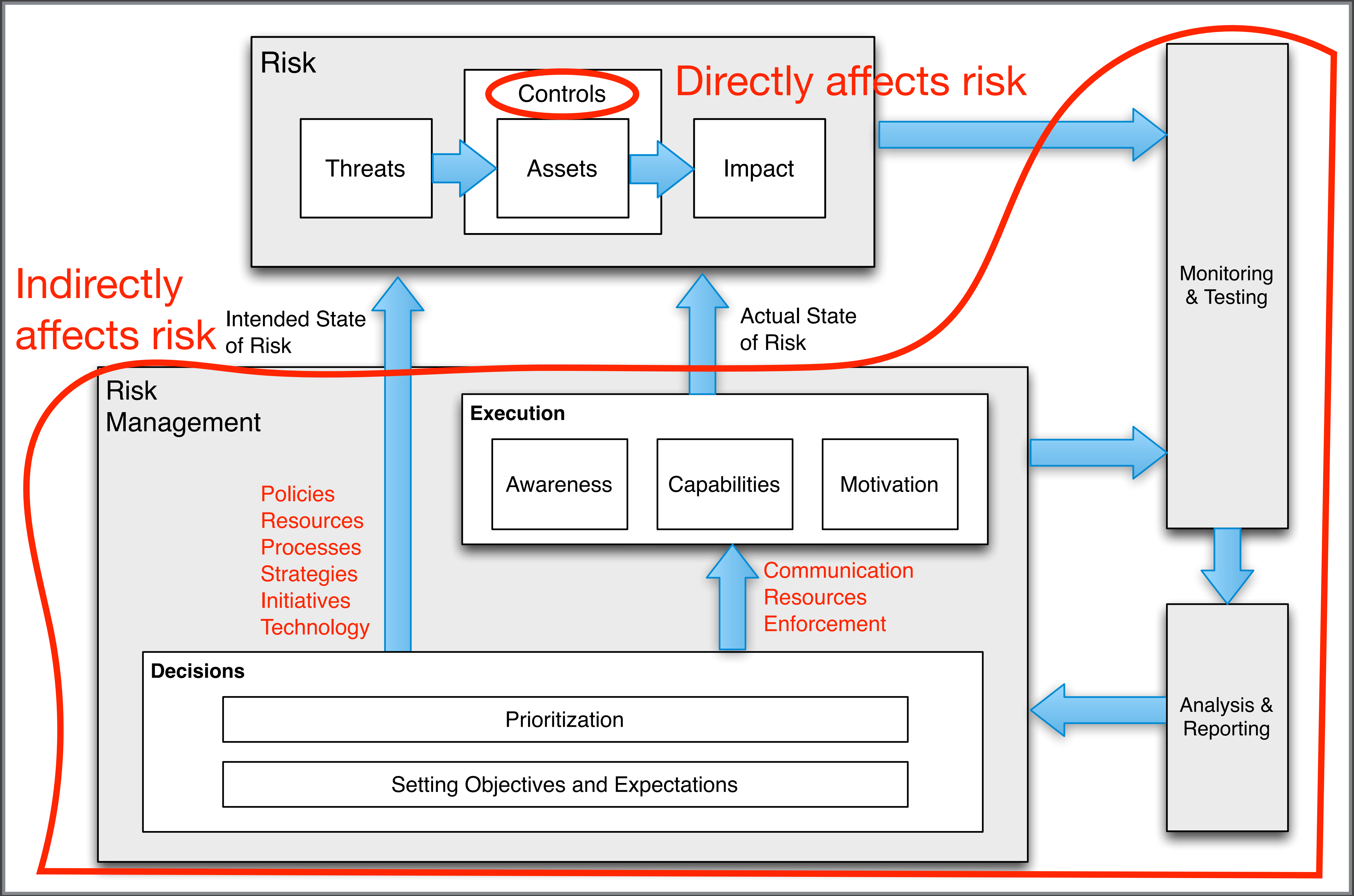
These are Loss Event
(or Asset-Level) controls

But what about…

- Policies & standards?
- Awareness training?
- Auditing & testing?
- Metrics & reporting?

These are risk management controls, which indirectly affect loss

Control categories



Risk

Controls

Threats

Assets

Impact

Directly affects risk

Monitoring & Testing

Indirectly affects risk

Intended State of Risk

Actual State of Risk

Risk Management

Execution

Awareness

Capabilities

Motivation

Policies
Resources
Processes
Strategies
Initiatives
Technology

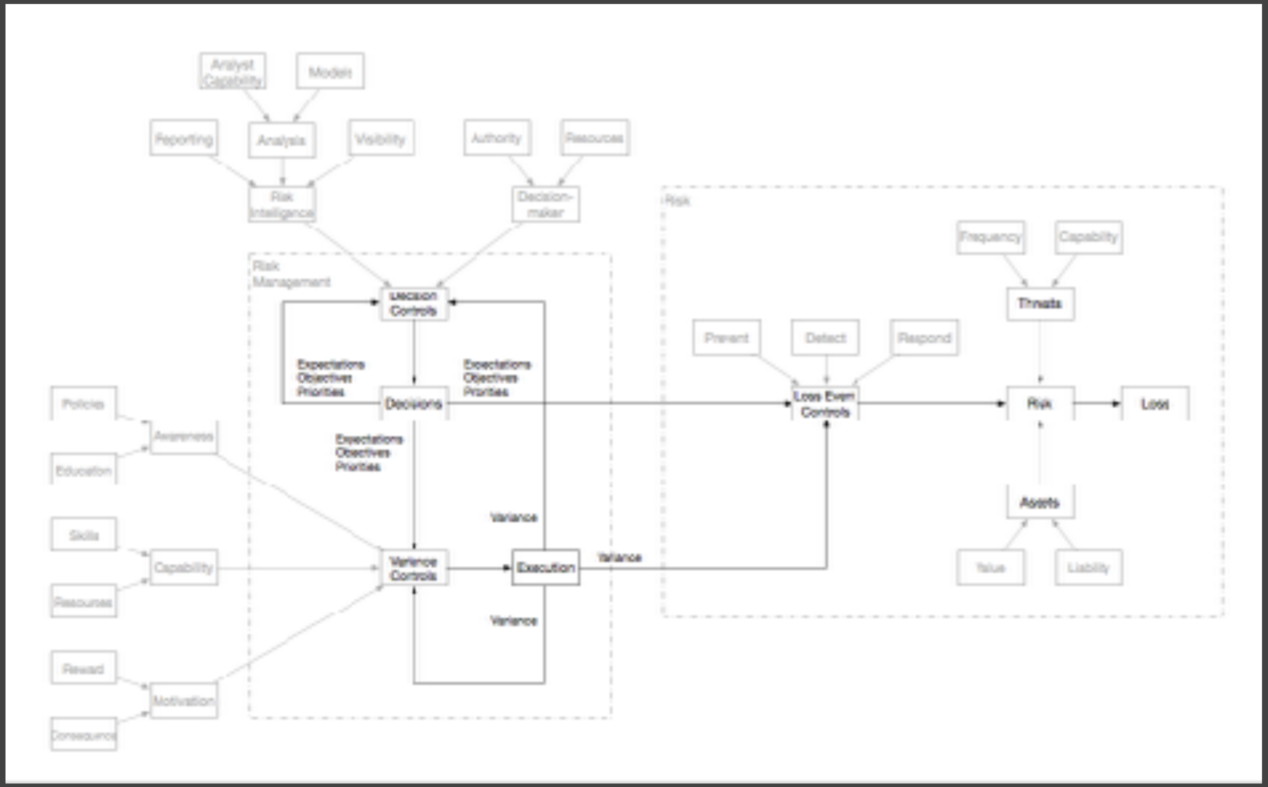
Communication
Resources
Enforcement

Decisions

Prioritization

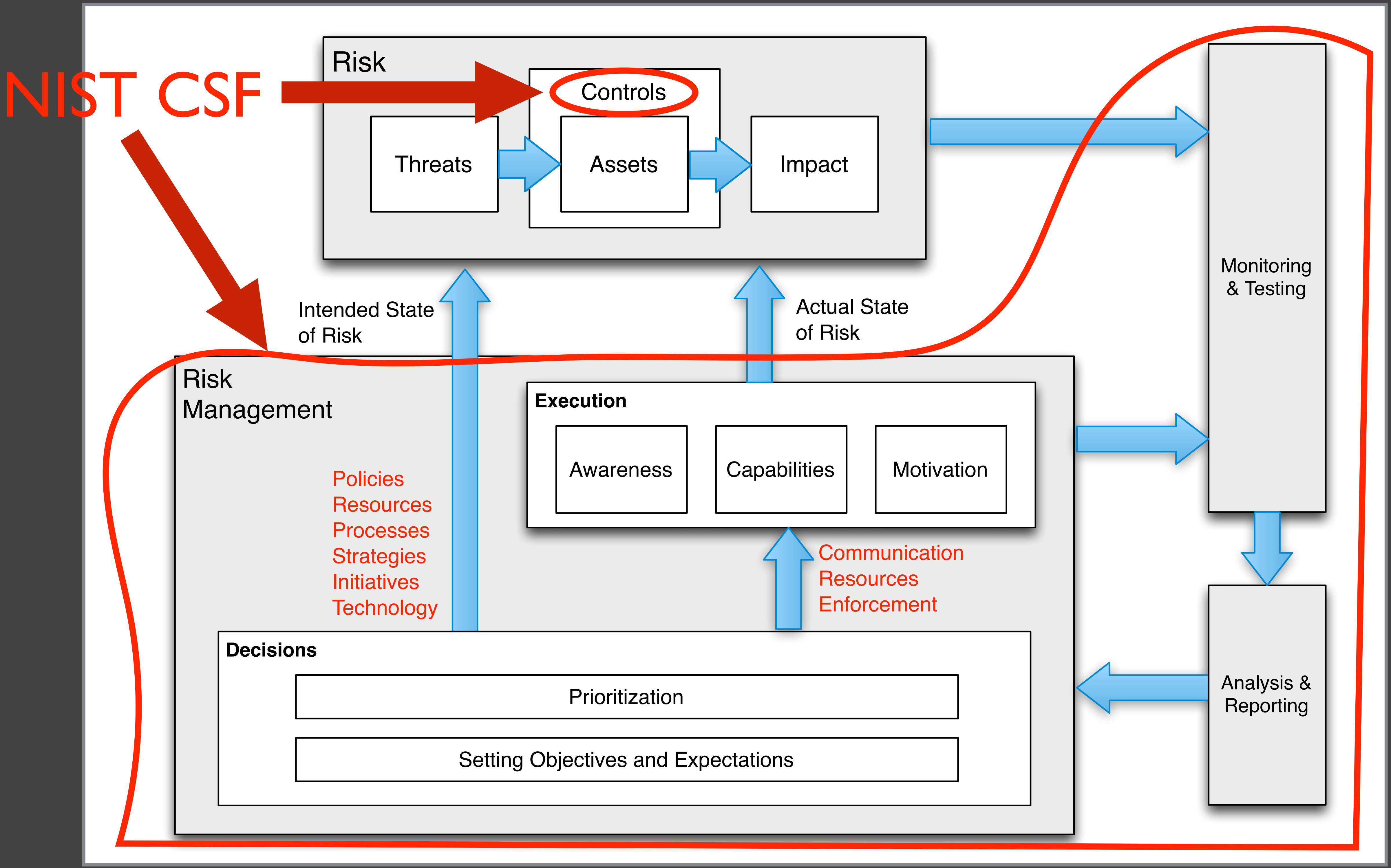
Setting Objectives and Expectations

Analysis & Reporting

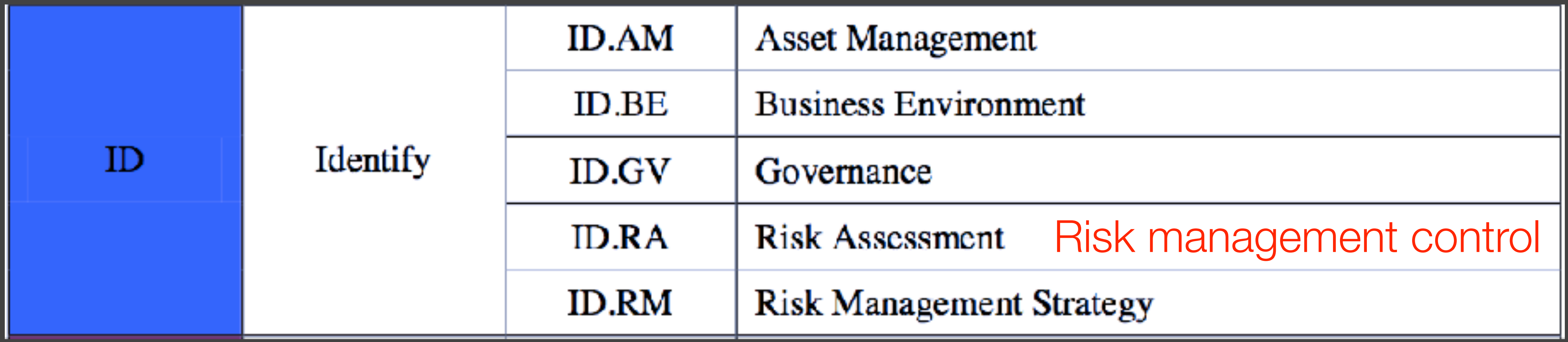


Switch to diagram…

NIST CSF doesn't differentiate

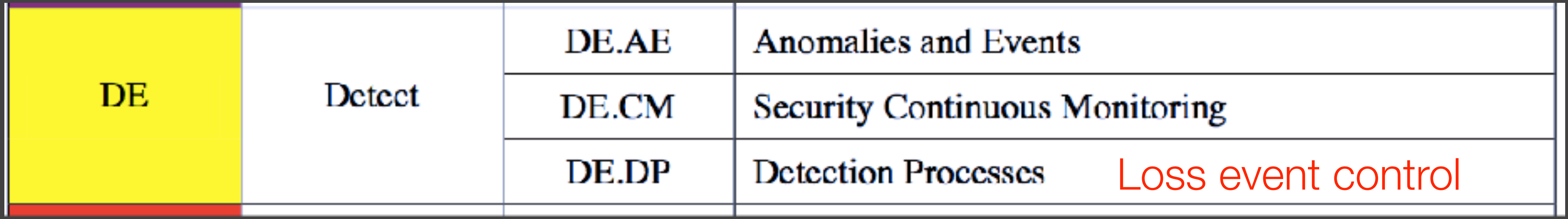


Across Functions…



ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Asscssmcnt
		ID.RM	Risk Management Strategy

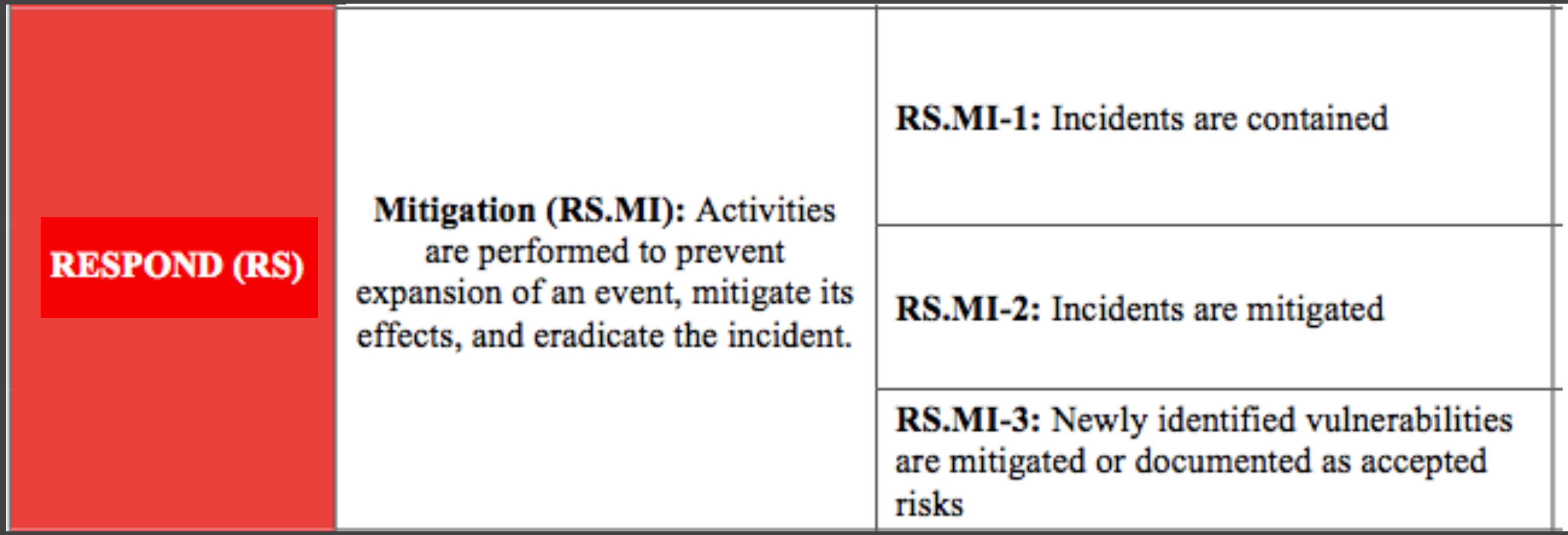
Risk management control



DE	Dctcct	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Dctcction Proccsscs

Loss event control

Or within Functions

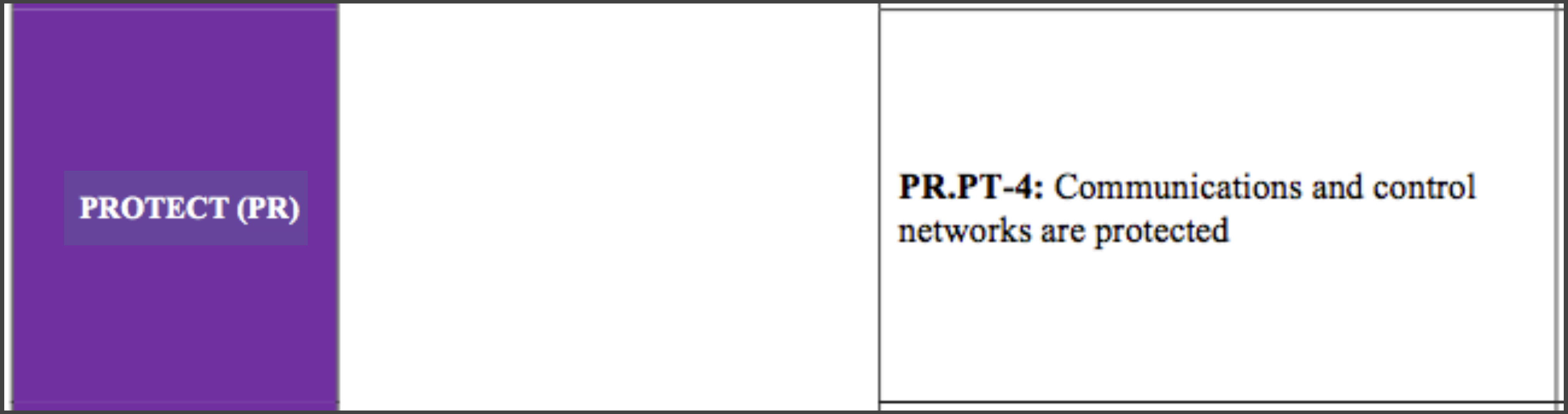


RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	Loss event control
		RS.MI-2: Incidents are mitigated	Loss event control
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Risk management control

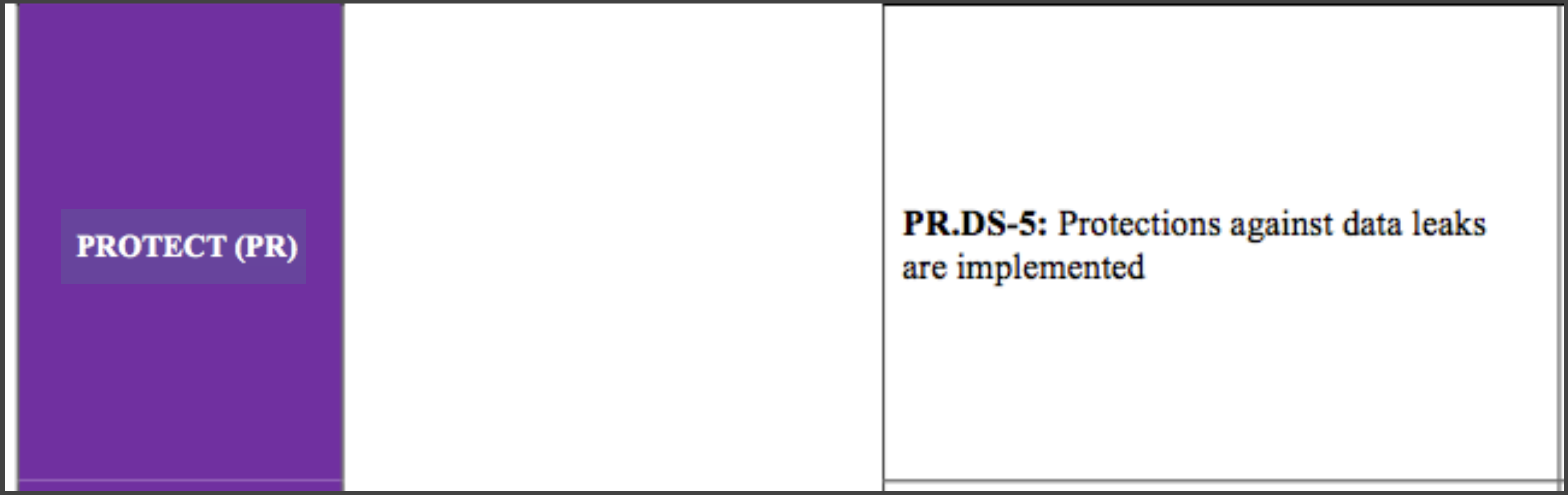
In order to prioritize amongst gaps…

- We first need to understand the role of each control — i.e, how they affect risk
    - Directly or indirectly
- Note that some NIST subcategories aren't even controls…

Outcome of other controls (redundant)

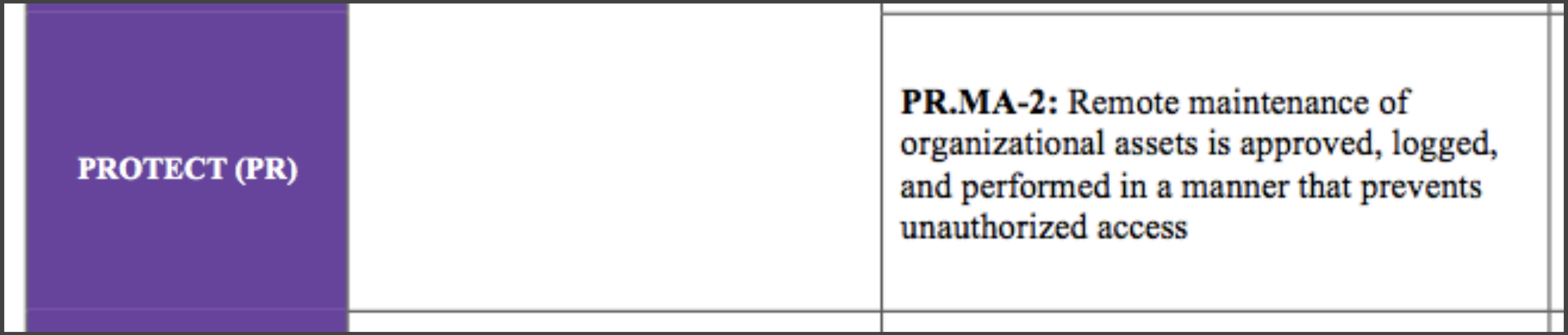


PROTECT (PR)		**PR.PT-4:** Communications and control networks are protected



PROTECT (PR)		**PR.DS-5:** Protections against data leaks are implemented

Some cover multiple roles…



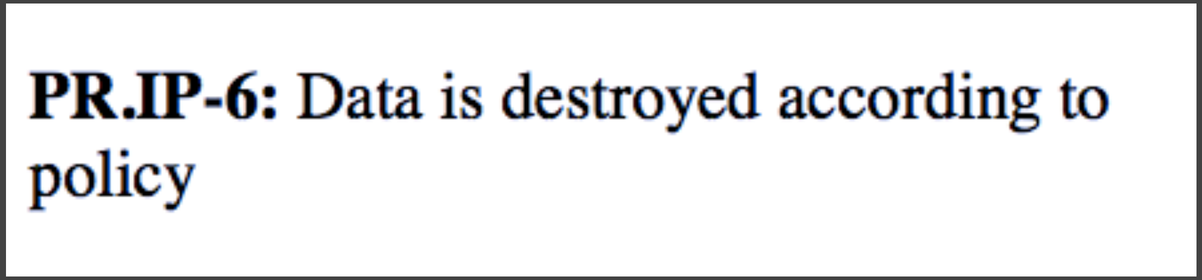
PROTECT (PR)		**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Implication WRT prioritization…

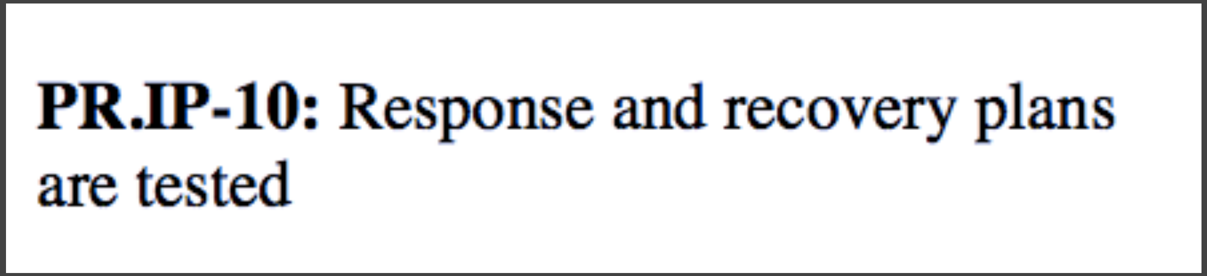
- Makes evaluation/measurement of gap relevance more challenging (and sometimes impossible)
- Some are easier than others

Prioritization

- Let’s say we want to prioritize between two gaps identified using NIST CSF



PR.IP-6: Data is destroyed according to policy

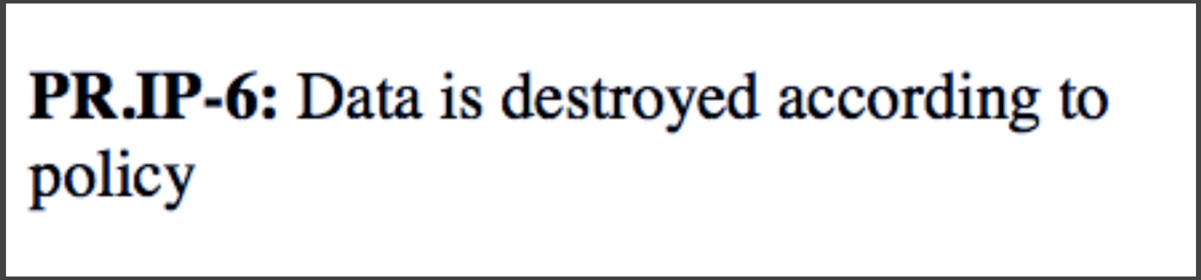


PR.IP-10: Response and recovery plans are tested

These are Loss Event (or Asset-Level) controls

Prioritization - cont.

- Identify and analyze relevant loss event scenarios for each gap



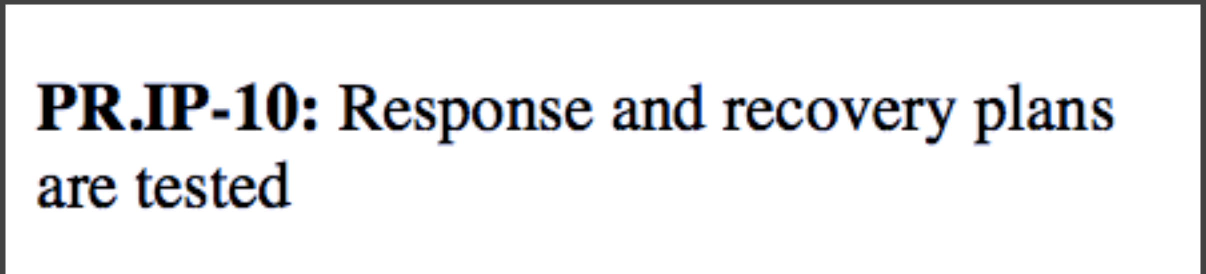
PR.IP-6: Data is destroyed according to policy

1. Compromise by cyber criminal
2. Compromise by insiders
3. etc.…

Prioritization - cont.

- Identify and analyze loss event scenarios for each gap

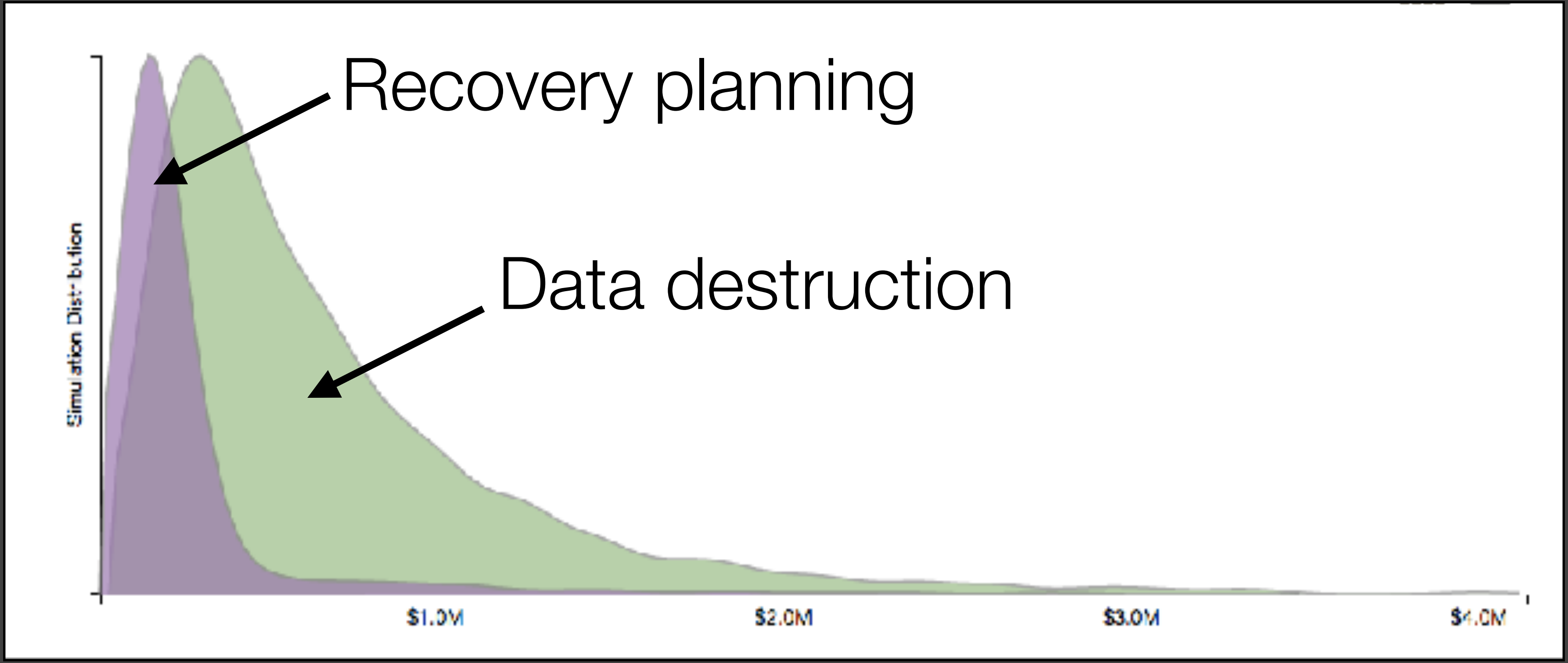
1. Outage due to acts of nature
2. Outage due to technology failure
3. Outage due to human error
4. etc….



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

Prioritization - cont.

- Compare the results



Recovery planning

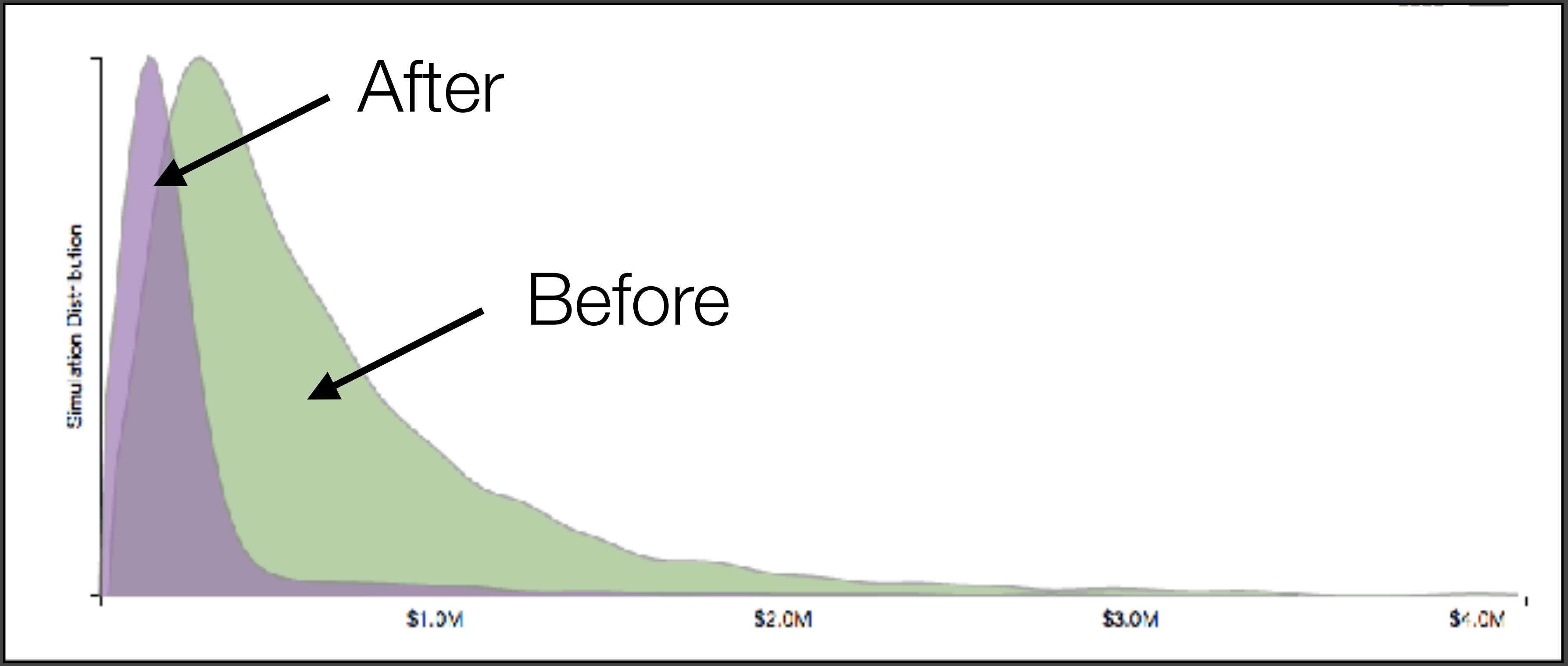
Data destruction

Cost-benefit

- Evaluate the value proposition for improving a NIST CSF sub-category
  - Measure current level of risk
  - Repeat the analysis factoring in the proposed improvement(s)
  - Report the level of risk reduction and the cost

Benefit analysis

- Compare the results

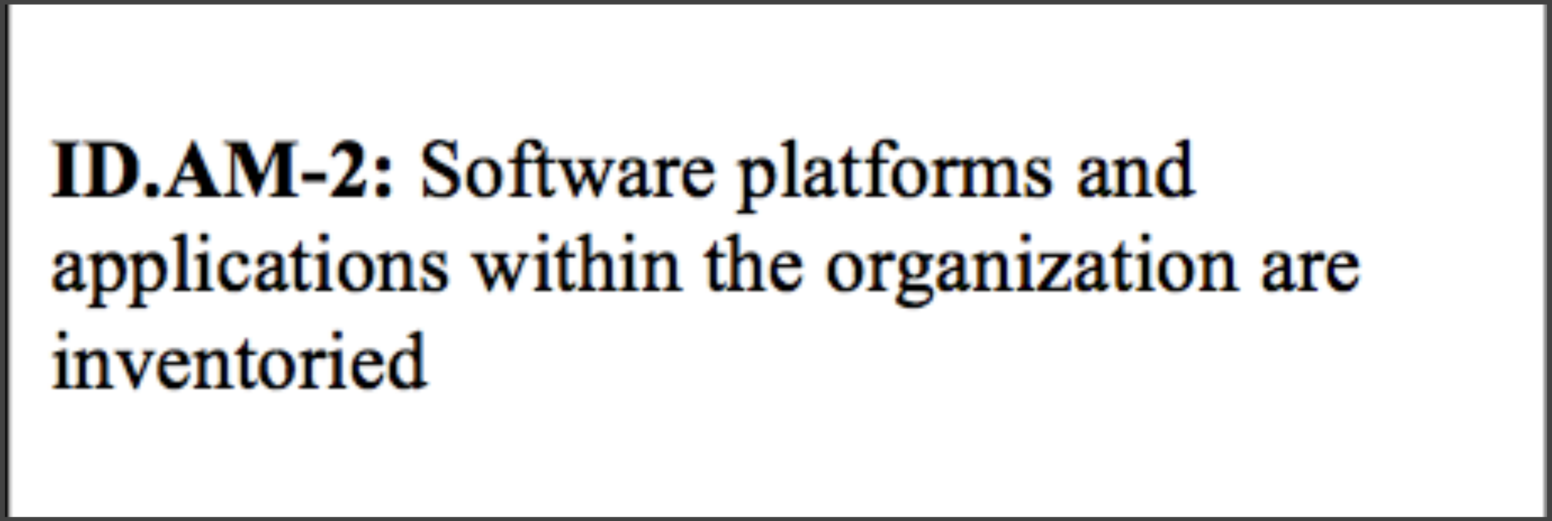


After

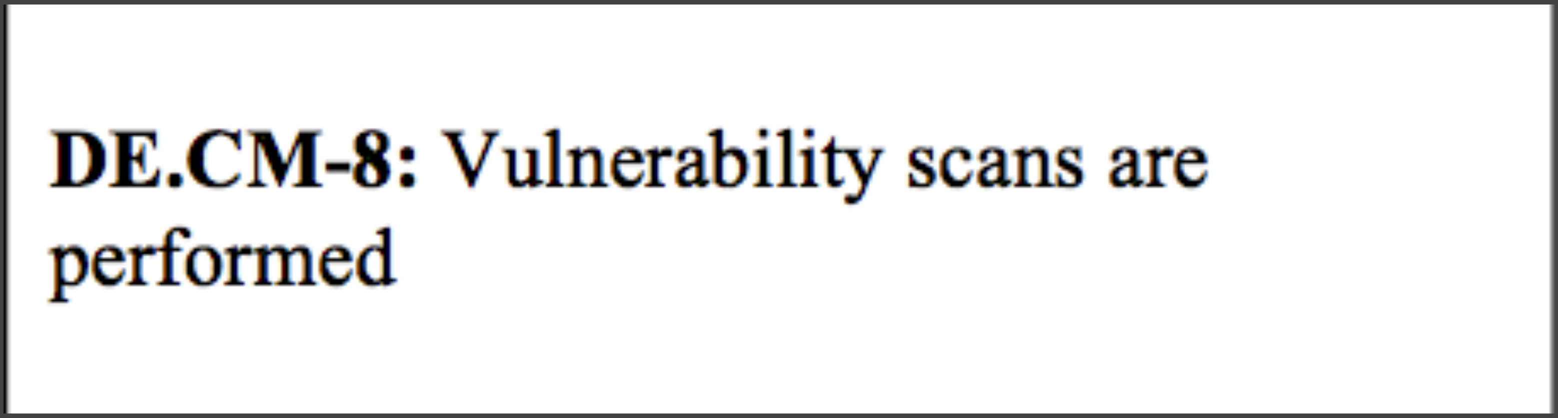
Before

More challenging…

- Prioritizing amongst risk management controls is often more difficult, for example:



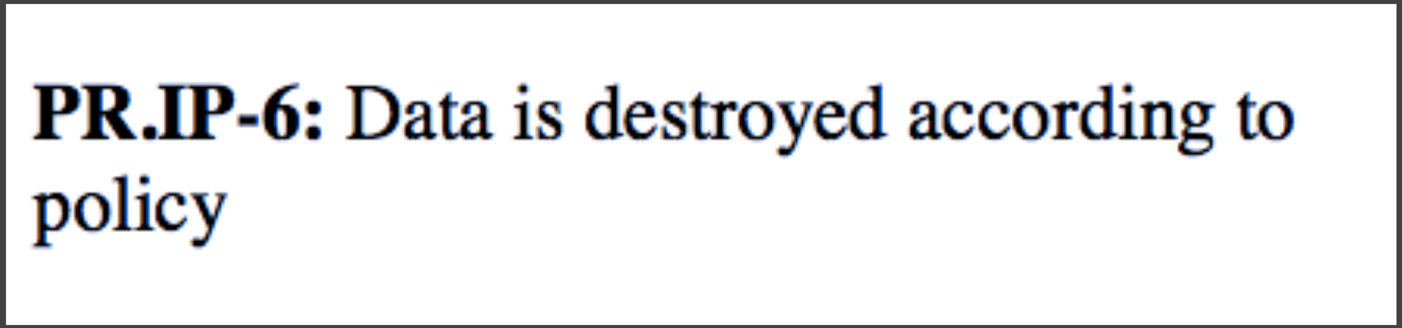
ID.AM-2: Software platforms and applications within the organization are inventoried



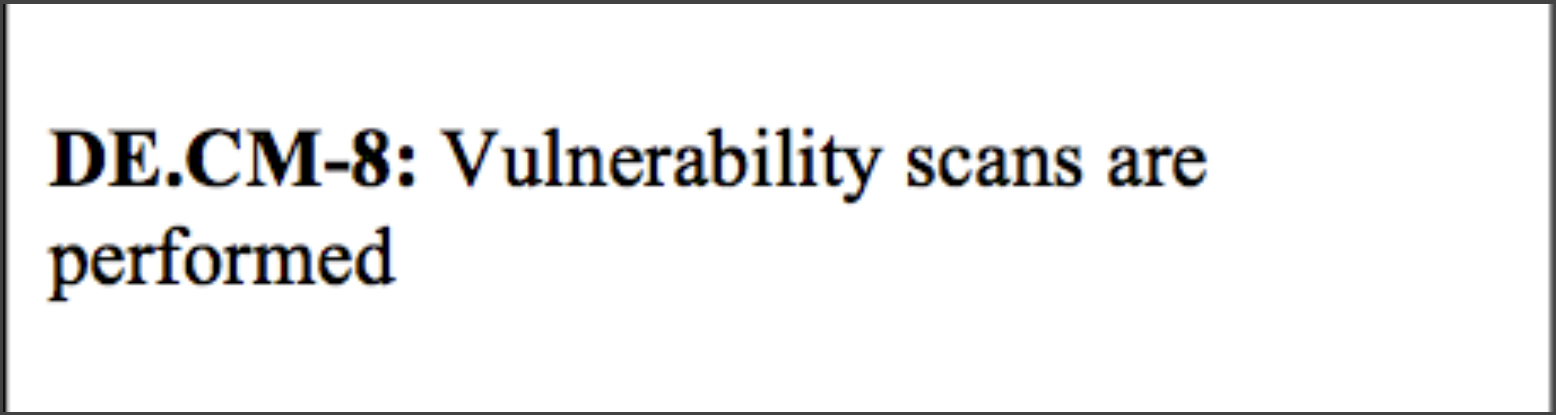
DE.CM-8: Vulnerability scans are performed

More challenging…

- Prioritizing between risk management and loss event controls can also be more difficult, for example:



PR.IP-6: Data is destroyed according to policy



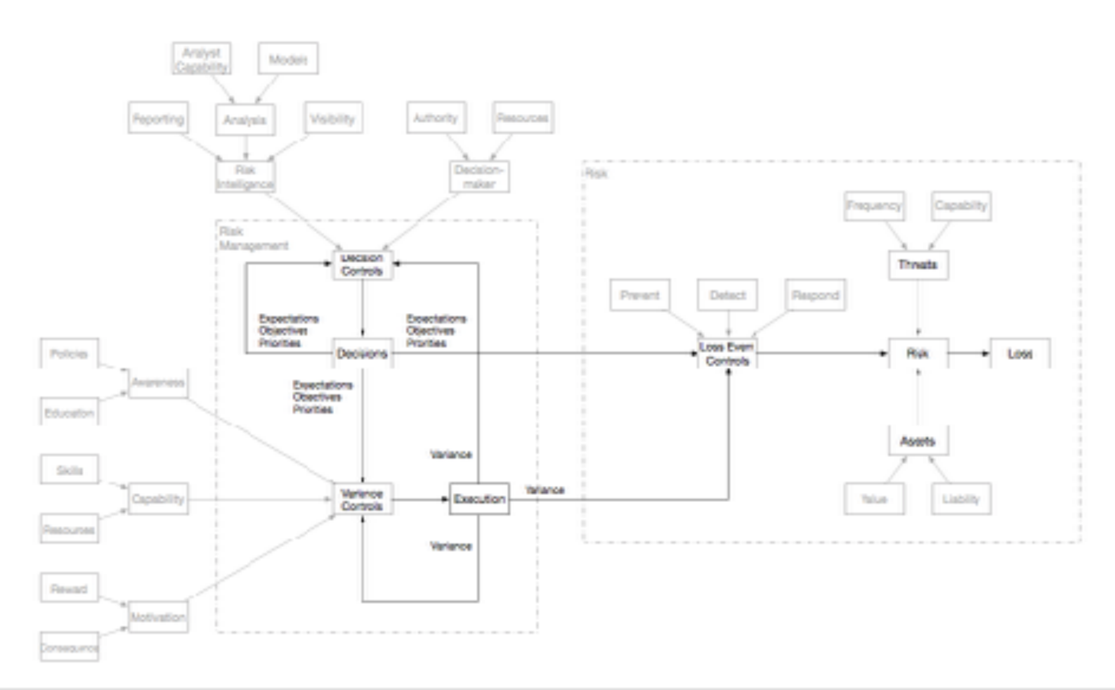
DE.CM-8: Vulnerability scans are performed

Risk Management control analysis…

- Rules of thumb
  - Decision-making controls
    - Improve the likelihood that expectations are appropriate
    - Improve the ability to adjust to changes in the risk landscape
  - Variance controls affect the reliability of Loss Event controls (which helps to reduce risk)

How is this relevant to “data”?

- Security telemetry tools that “automatically” measure risk have to understand the role/relevance of control data
- Metrics regarding controls require context in order to be relevant



Questions?