Aligning NIST CSF and Risk

Jack Jones
Chairman, FAIR Institute
Chief Risk Scientist, RiskLens

Expectations for CISOs Are Changing

Your organization has an overall average NIST CSF score of 2.6.

How much less risk will it have if it improves to an average score of 3?

Your organization has been rated as a “2” on these NIST CSF subcategories:

- DE.AE-3 “Event data are collected and correlated…”
- PR.IP-4 “Backups of information are conducted, maintained…”

If we can only improve one of these, which one should it be?

Understanding context

What are your organization's most significant cybersecurity-related ~~risks~~?

loss event scenarios?

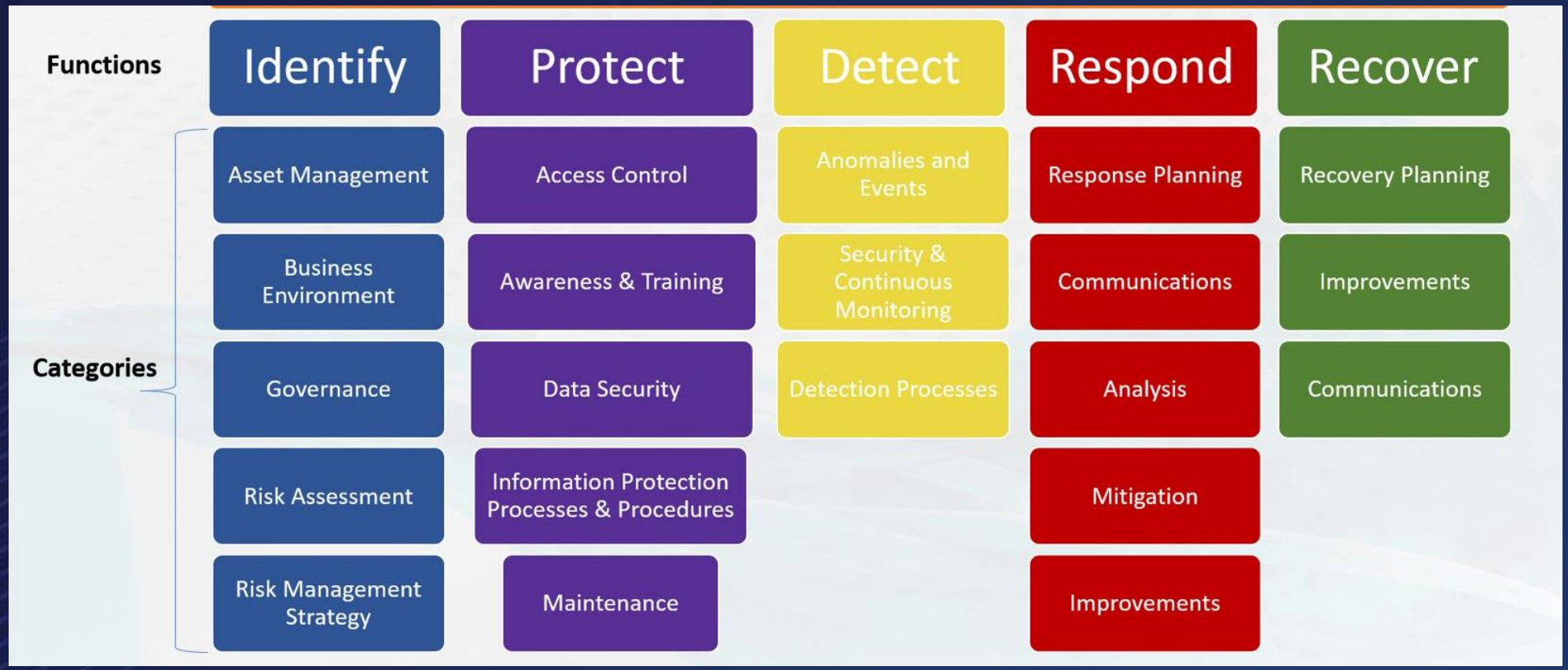
How is risk measured?

Risk = Probability x Impact

Probability and impact of what?

Loss event scenarios

Control capabilities are only relevant within the context of loss event scenarios



Relevance? Pick a scenario…

Loss Event Scenario	DE.AE-3 Event data collected…	PR.IP-4 Backups of information…
Ransomware	✓	✓
Compromise of sensitive information	✓	✗
Insider fraud	✓	✗
Customer account takeover	✓	✗

In a ransomware event, are these equally important?

The bottom line…

Not all NIST CSF subcategories are equally important.

We can only understand their importance within the context of the loss event scenarios they're relevant to.

Account for dependencies

What is a fundamental difference between these two NIST CSF subcategories?

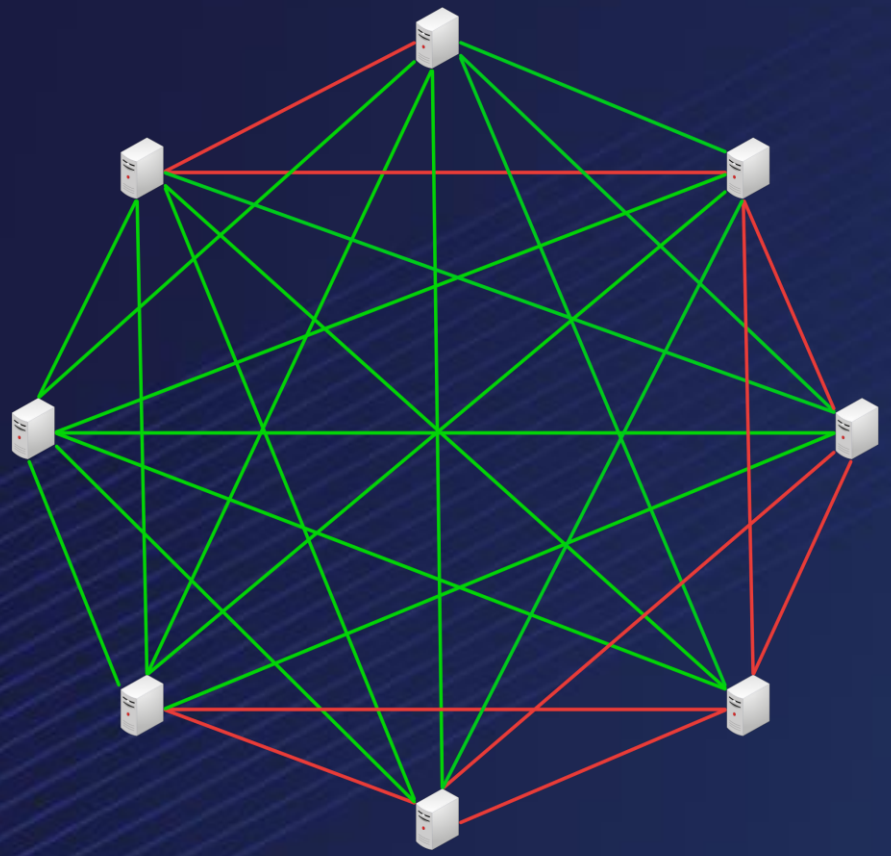
- PR.DS-2 “Data in transit is protected.”
- ID.AM-3 “Organization communication and data flows are mapped.”

Relevance

Loss Event Scenario	PR.DS-2 Data protected in transit	ID.AM-3 Data flow mapping…
Ransomware	✗	✓
Compromise of sensitive information	✓	✓
Insider fraud	✗	✓
Customer account takeover	✓	✓

Are these controls relevant in the same way?

Dependencies matter



"We're great at protecting our assets.

At least the ones we know about…"

Communication Paths

- Known and properly protected
- Unknown and poorly protected

FAIR INSTITUTE

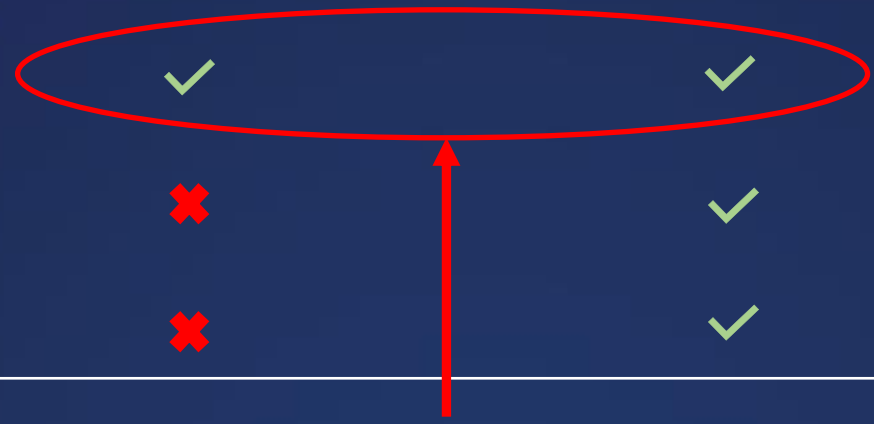
Another dependency example

- DE.CM-1 “The network is monitored…”
- DE.DP-4 “Event detection information is communicated.”

How are these related?

Dependencies

Loss Event Scenario	DE.CM-1 Network is monitored	DE.DP-4 Event detection communicated
Ransomware Event	✓	✓
Compromise of sensitive information	✓	✓
Insider fraud	✗	✓
Customer account takeover	✗	✓



Does a weak score in one of these affect how the other one should be scored?

The bottom line…

Dependencies matter - a lot.

We have to recognize and account for these dependencies if we want to focus on the things that matter most.

Measuring Risk

What is the most commonly-used risk measurement model in cyber security today?

What assumptions?

Mental models

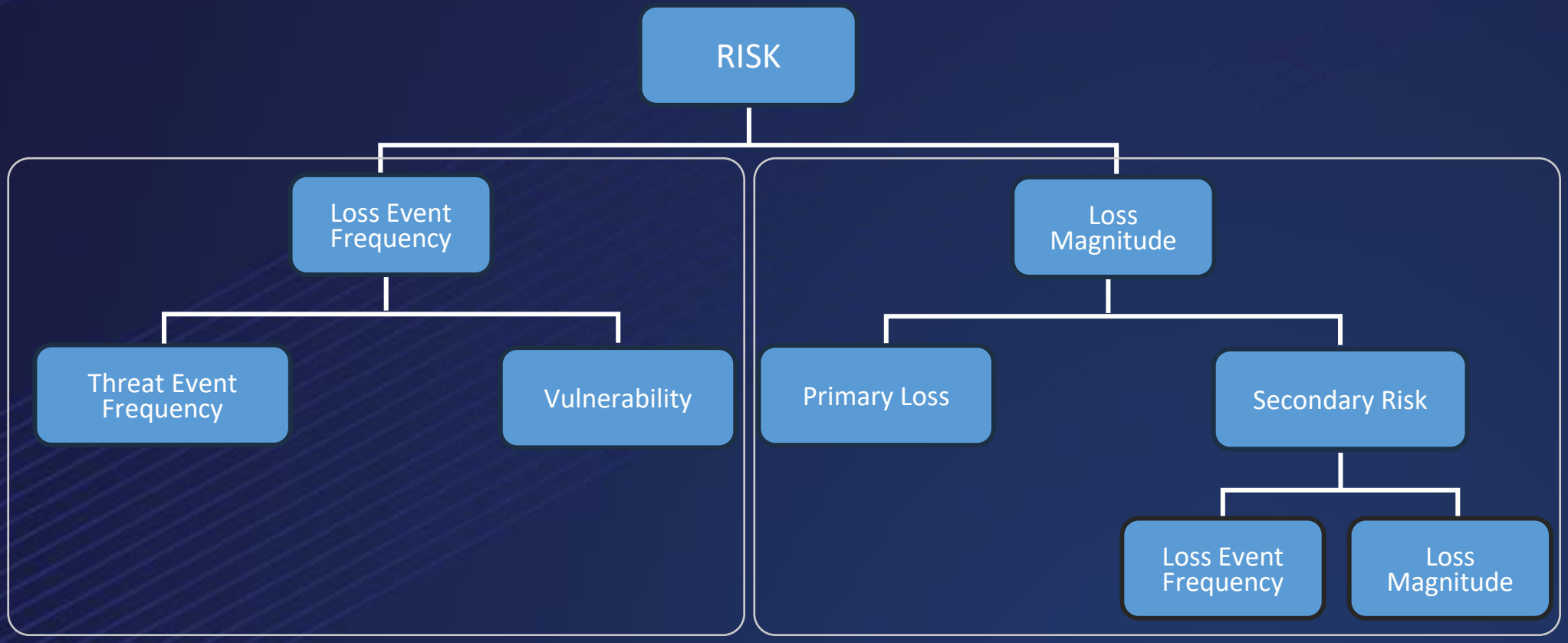
What formula?

What data?

The combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure.

Source: "Measuring and Managing Information Risk: A FAIR Approach"

Factor Analysis of Information Risk (FAIR) Model

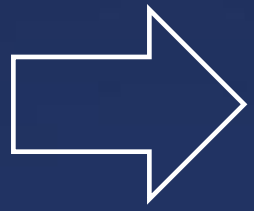


Another Key Dependency…

- ID.RA-4 “Potential business impacts and likelihoods are identified”
- DE.RM (all) “The organization’s priorities… are established…”

Relevance?

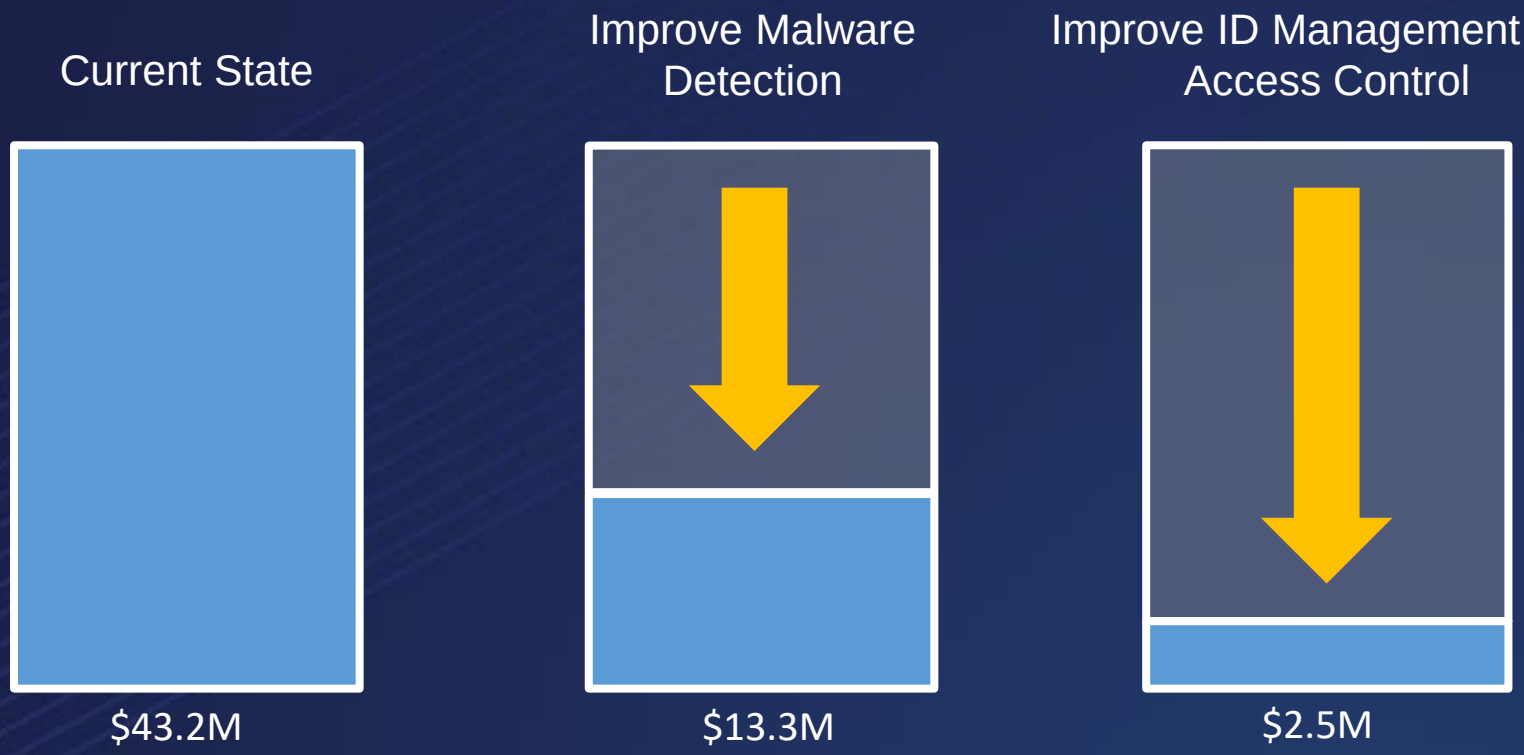
Loss Event Scenario	ID.RA-4 … impacts and likelihoods	DE.RM (all) … priorities established
Ransomware	✓	✓
Compromise of sensitive information	✓	✓
Insider fraud	✓	✓
Customer account takeover	✓	✓



Relevance?

Loss Event Scenario	Impact	Probability
Ransomware	> $10M	15% -> 30%
Compromise of sensitive information	> $10M	10% -> 15%
Insider fraud	> $10M	< 5%
Customer account takeover	> $10M	< 5%

Real World Analysis – Risk Reduction Comparisons



The bottom line…

Better risk measurements lead to better decisions

This is where we can provide the most direct and meaningful linkage between NIST CSF and risk.

FAIR Resources

- The FAIR Institute (www.fairinstitute.org)
- The Open Group (www.opengroup.org/certifications/openfair)
- RiskLens (www.risklens.com/resources)
- Measuring and Managing Information Risk: A FAIR Approach (www.amazon.com)

Wrapping Up

Applying what we've covered…

- Identify your organization's most significant loss event scenarios
- Determine which NIST CSF subcategories are directly relevant to each significant loss event scenario
- Identify and account for the dependencies between relevant NIST CSF subcategories
- Begin the journey to better risk measurement — familiarize yourself with FAIR

Questions?

