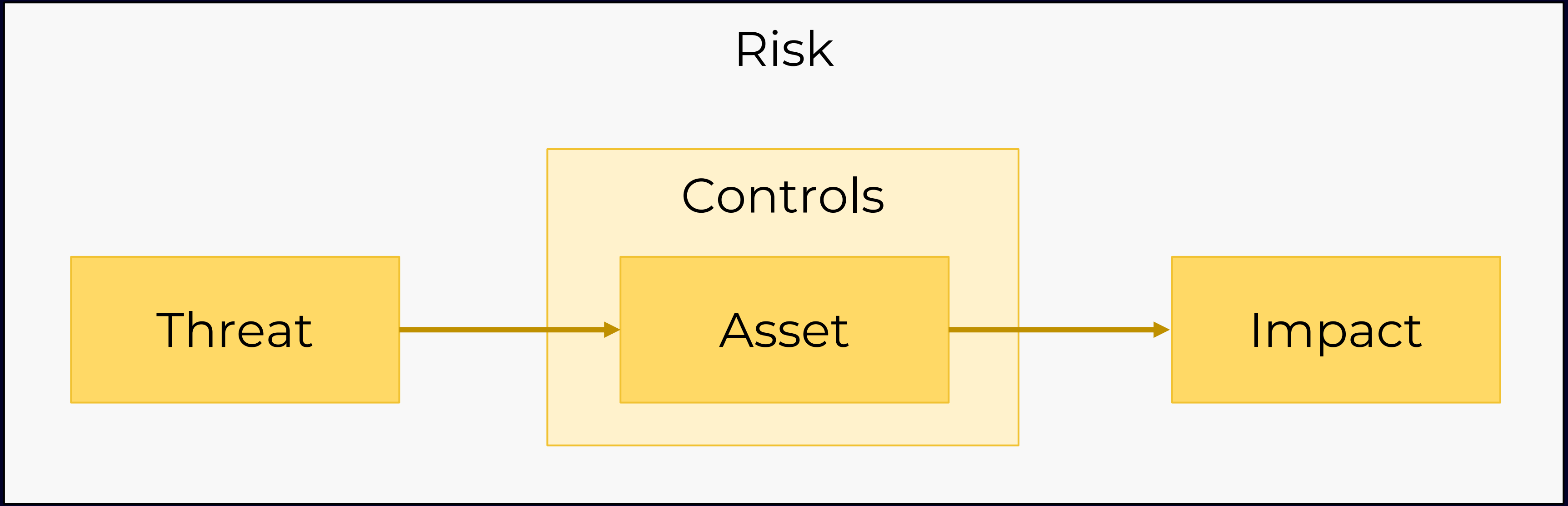
Getting Your Money's Worth: Putting Your Controls Inventory to Work

Marta Palanques, Director of Risk Methodologies,
Technology Risk Management, Capital One

FAIR22 CONFERENCE

Why do we inventory controls?



Source: Measuring and Managing Information Risk: A FAIR Approach

But also...

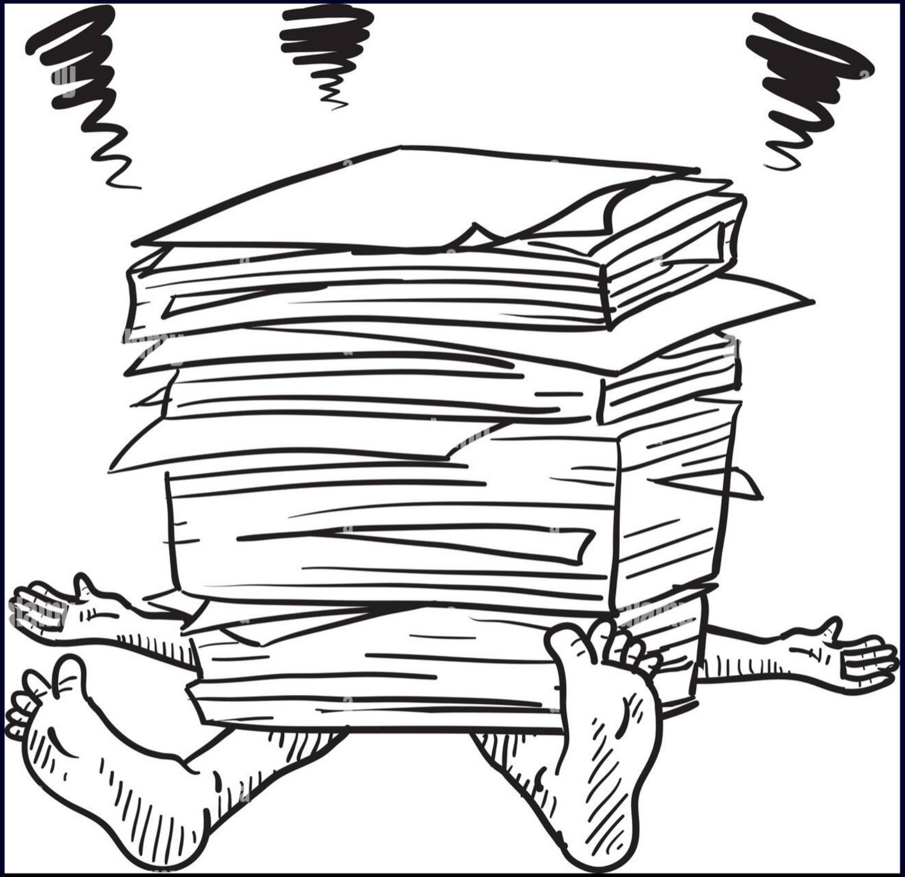
1. Controls are more deterministic and easier to articulate

1. There's an abundance of reference frameworks

1. In some cases it's required by law

The controls inventory turns into a check the box exercise

Why am I here?



How do we perform against NIST CSF?

Do we meet all GDPR requirements?

What's security's portfolio of services? How mature is it?

What are we spending our money on?

FAIR22 CONFERENCE

In this talk, we will...

Identify
use cases for a
controls inventory

Understand factors contributing to the cost of the controls inventory

Discuss strategies to align scale of the inventory to the value it provides

FAIR22 CONFERENCE

What is in the controls inventory

- FAIR-CAM defines control as “Anything that can be used to reduce the frequency or magnitude of loss.”

- During this talk, I will assume that inventory includes a list of activities performed regularly with the intent of mitigating risk.

How many controls should my inventory have?

Size of the inventory determines cost of maintenance

- Records to periodically review/update
- Volume to test
- Difficulty to retrieve/identify what we’re looking for

How many controls should my inventory have?

Uneven granularity results in

- Methodology and framework complications
- Difficulty applying to risk management
- Unfair comparisons between controls
- Frustrated stakeholders

Establishing and following a criteria is foundational

Framework

Straightforward implementation

Uneven sizing
Produces duplicates
Little control over structure

Ownership

Aligned to drive change/action

Unclear control objective
Evaluating design and effectiveness may be challenging

Value delivery

Aligns to risk analysis
Enables value measurement

Complex definition

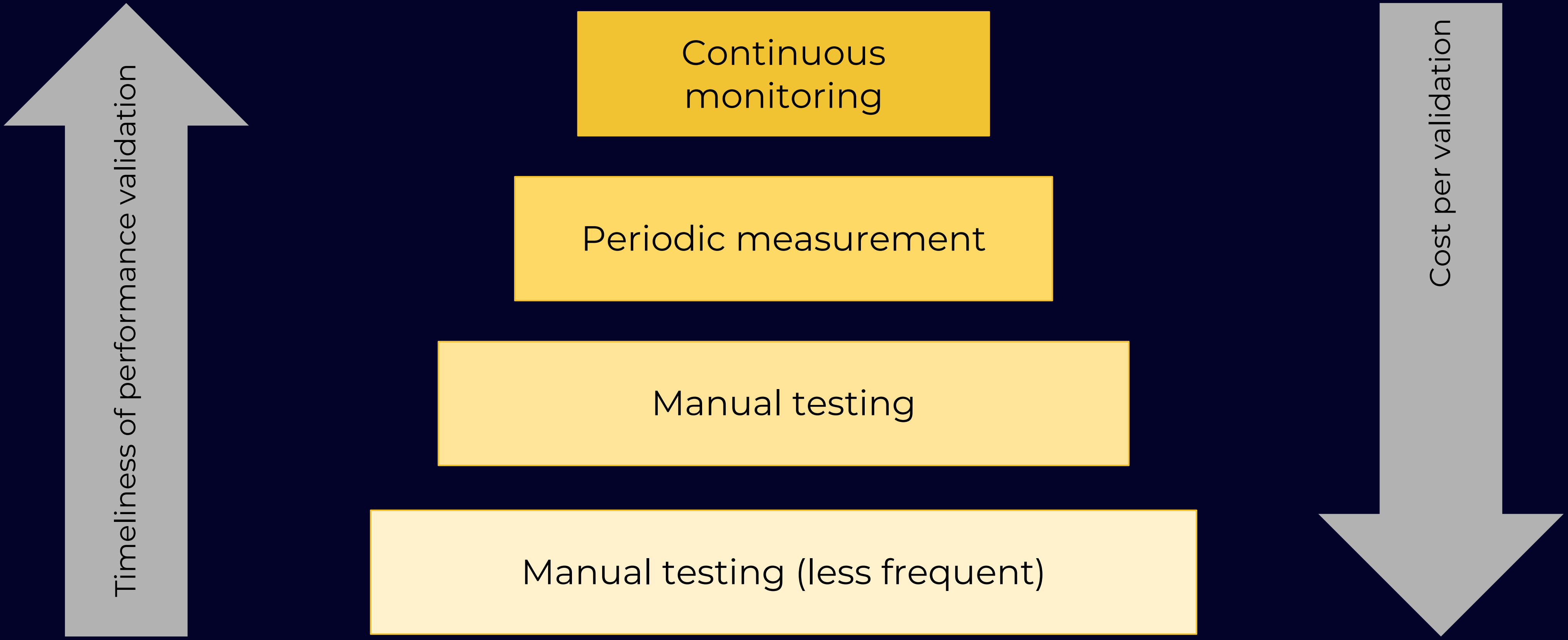
Value-centric definition of control

- “**A process** that can be used to reduce the frequency or magnitude of loss.”
    - *Process: “a series of actions or events performed to make something or **achieve a particular result**”*
- Rule of thumb for granularity: can you assign a measurable goal for the control?
- “If you want to measure controls you can't munge them together. “

Control testing

	Unit cost	Frequency	Total cost	Value
Attestation: confirmation that the activity is being performed	↓	↓	↓	↓
Design testing: the design is adequate, based on some criteria	↑	↓	↑	↑/→
Operational effectiveness testing: validates that activities are performed as designed	→	↑	↑	→

Choose the right approach to validate operational effectiveness



Timeliness of performance validation

Continuous monitoring

Periodic measurement

Manual testing

Manual testing (less frequent)

Cost per validation

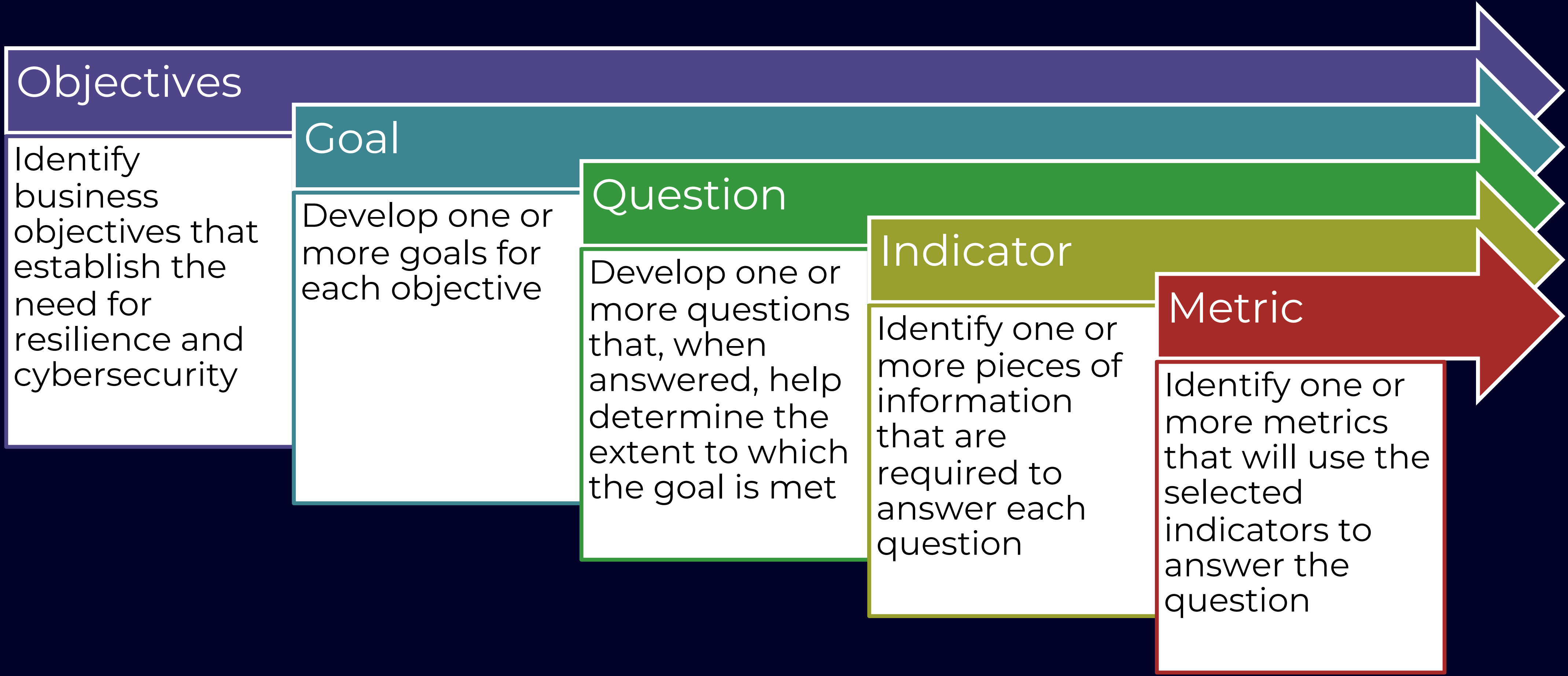
Why not do continuous monitoring of all?

- It’s expensive

- Value of continuous monitoring decreases with control execution frequency.

- Value of continuous monitoring increases with relevance of the control you’re monitoring.

What are the right metrics and indicators for continuous monitoring?



Objectives

Identify business objectives that establish the need for resilience and cybersecurity

Goal

Develop one or more goals for each objective

Question

Develop one or more questions that, when answered, help determine the extent to which the goal is met

Indicator

Identify one or more pieces of information that are required to answer each question

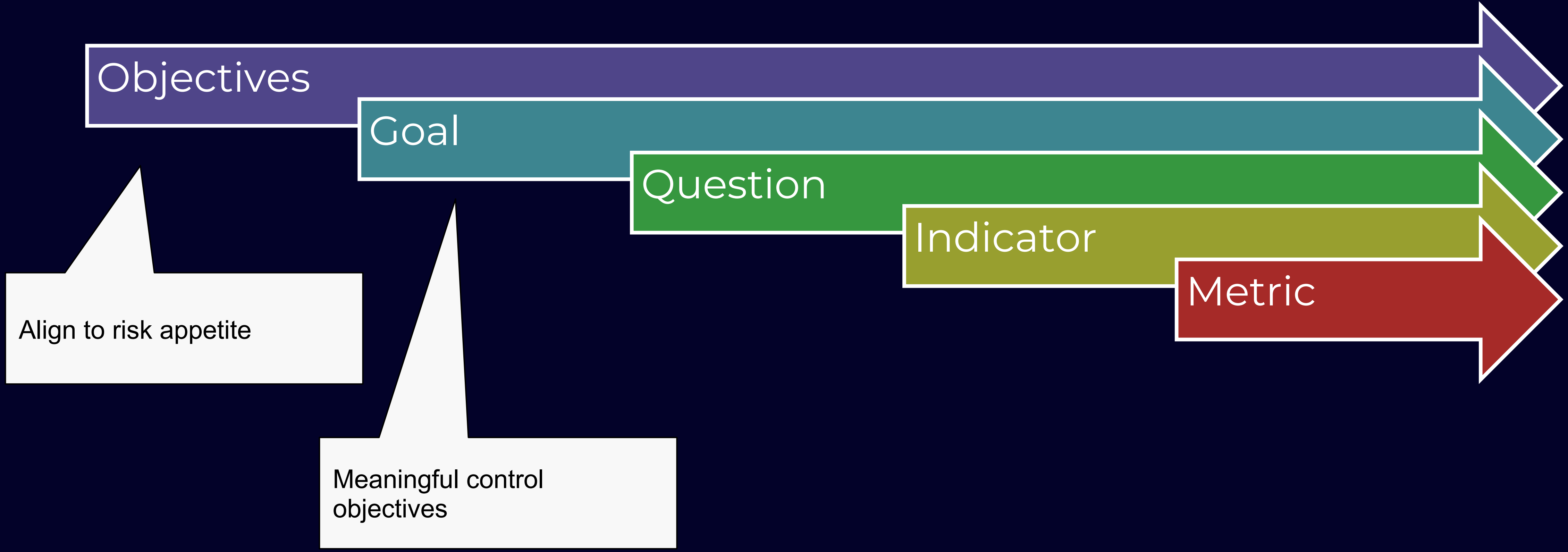
Metric

Identify one or more metrics that will use the selected indicators to answer the question

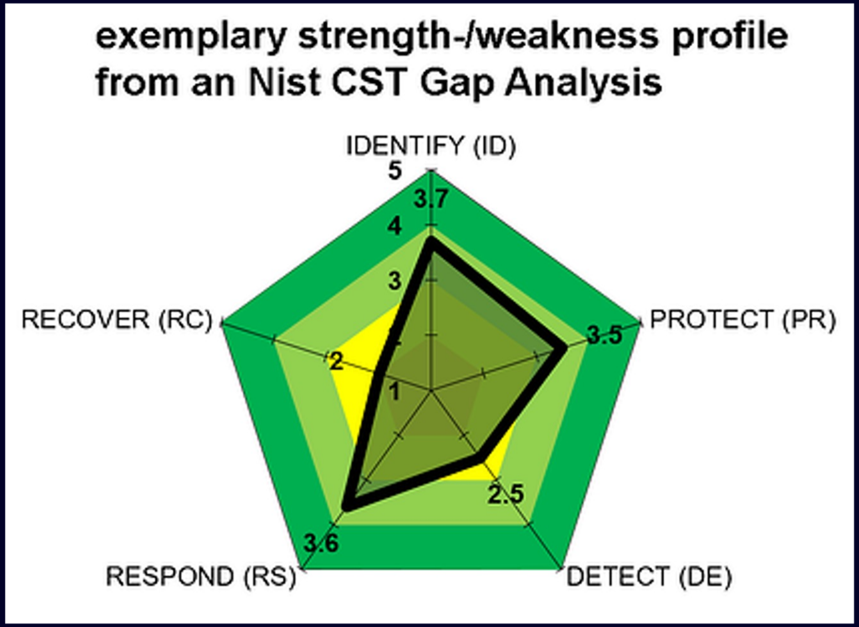
Source: Lisa Young, Measuring What Matters

FAIR22 CONFERENCE

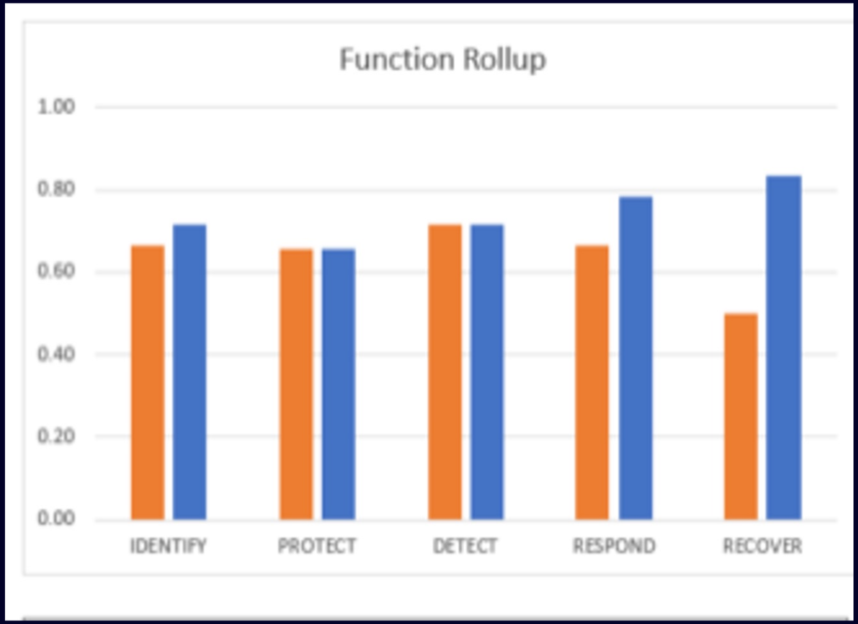
What are the right parameters for measurement and monitoring?



Framing your cyber capabilities



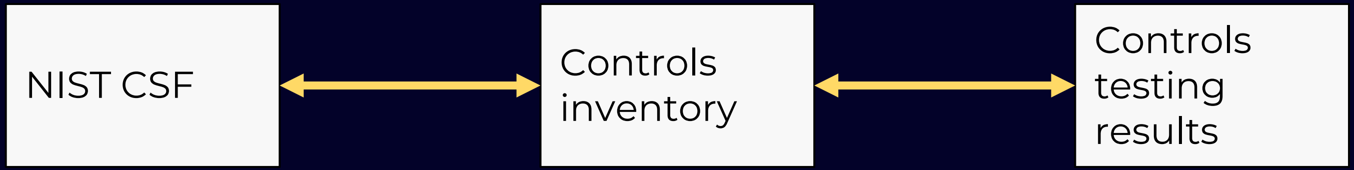
Source: InfoGuard https://www.infoguard.ch/en/nist-csf-gap-analysis-0



https://watkinsconsulting.com/our-projects/nist-csf-comparison-excel-workbook/

You already have most of this information

- Controls inventory: activities you perform to mitigate risk → *akin to security portfolio*
- Testing results: information on how well defined and operated they are → *akin to maturity*



- … just add a framework mapping

FAIR22 CONFERENCE

Example maturity based on test results

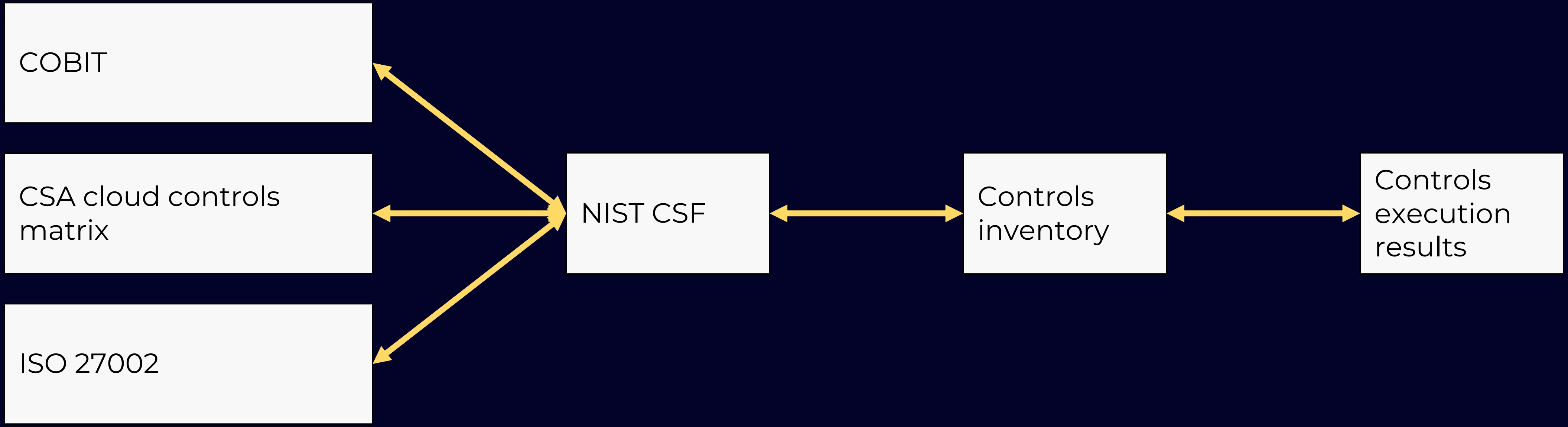
5	Continuous monitoring	- Control is designed appropriately AND - Continuous monitoring/periodic measurement results are within expectation
4	Appropriate design and operation	- Control is designed appropriately AND - Passed the latest manual operational check
3	Operational gaps	- Control is designed appropriately (according to latest test) BUT - Failed operational effectiveness test (incl. continuous monitoring
2	Design gaps	- Control was found to not be designed appropriately in the most recent tests
1	Non-existent / maturity unknown	- No reference in the controls inventory OR - Has not been tested recently enough

Stakeholders may have a preference for a particular framework

This preference may be based on:

- Regulatory expectations
- Industry context
- Strategic plans
- Cultural background
- Familiarity

Integrating with more external frameworks



- Include framework references in the inventory so they can be reused
- Rely on industry mappings to “translate” between frameworks

Large control inventories are difficult to navigate

- Difficulty to find what is applicable in a specifically risk scenario

- Controls may seem to do similar things based on the description

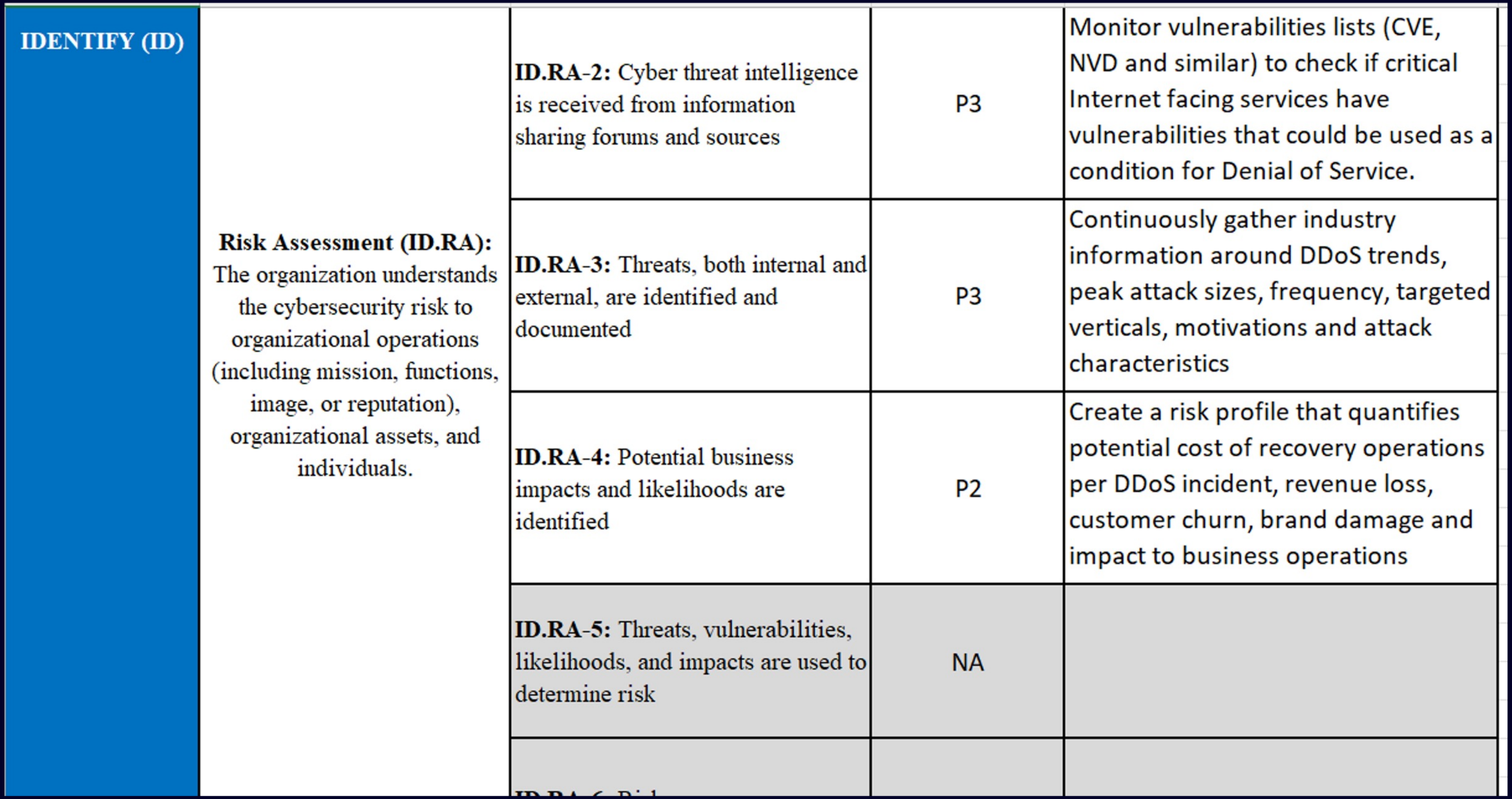
- Perception that more controls is better risk reduction

Packaging your controls inventory for a purpose

Create template risk profiles for generic threats or scenarios:

- Narrow down which controls may be applicable
- Establish some basic priority based on prerequisites: Loss Event Controls should be prioritized over Variance Controls

DDoS profile example

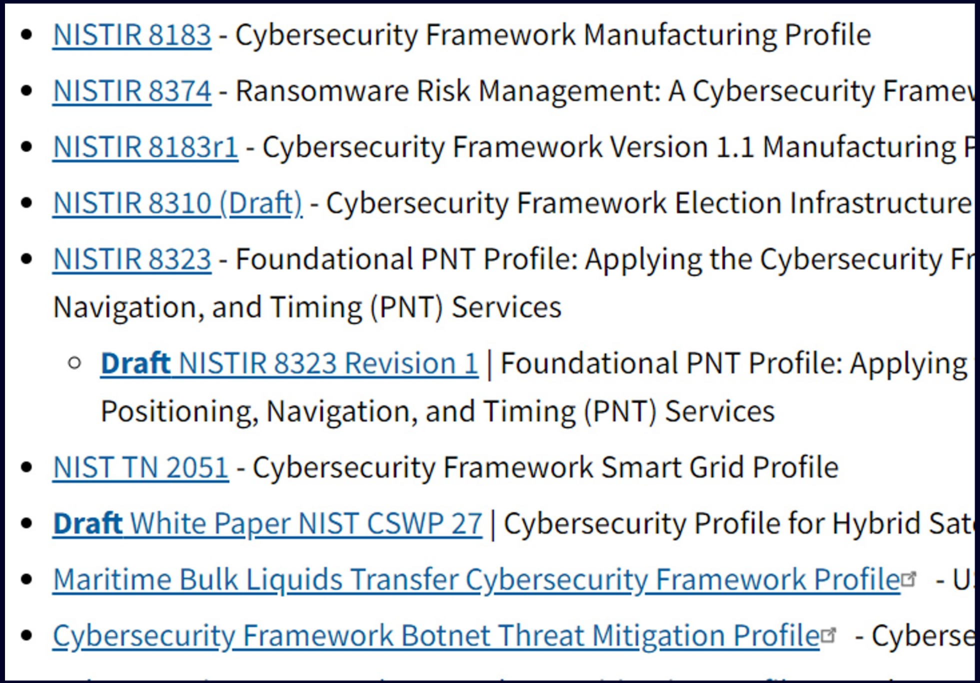


IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources	P3	Monitor vulnerabilities lists (CVE, NVD and similar) to check if critical Internet facing services have vulnerabilities that could be used as a condition for Denial of Service.
		ID.RA-3: Threats, both internal and external, are identified and documented	P3	Continuously gather industry information around DDoS trends, peak attack sizes, frequency, targeted verticals, motivations and attack characteristics
		ID.RA-4: Potential business impacts and likelihoods are identified	P2	Create a risk profile that quantifies potential cost of recovery operations per DDoS incident, revenue loss, customer churn, brand damage and impact to business operations
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	NA	
		ID.RA-6: Risk		

Source: CyberSecurity Coalition

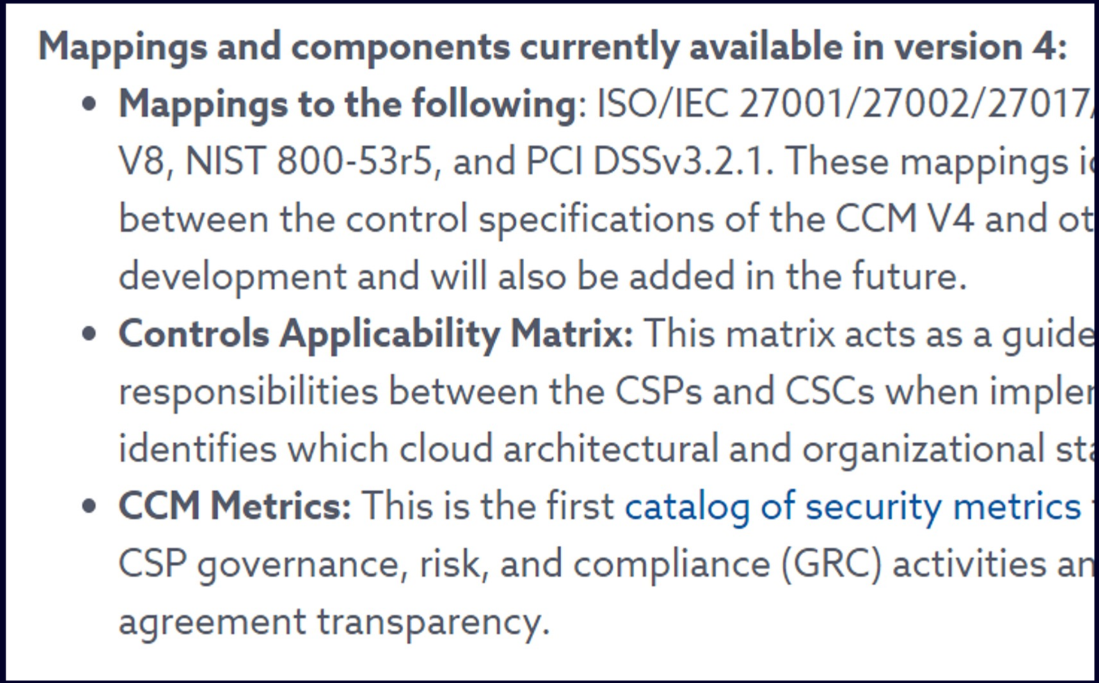
Framework bonus points: risk profiles (and other benchmarking)

From the NIST website:



- NISTIR 8183 - Cybersecurity Framework Manufacturing Profile
- NISTIR 8374 - Ransomware Risk Management: A Cybersecurity Framew
- NISTIR 8183r1 - Cybersecurity Framework Version 1.1 Manufacturing P
- NISTIR 8310 (Draft) - Cybersecurity Framework Election Infrastructure
- NISTIR 8323 - Foundational PNT Profile: Applying the Cybersecurity Fr Navigation, and Timing (PNT) Services
  - ○ **Draft** NISTIR 8323 Revision 1 | Foundational PNT Profile: Applying Positioning, Navigation, and Timing (PNT) Services
- NIST TN 2051 - Cybersecurity Framework Smart Grid Profile
- **Draft** White Paper NIST CSWP 27 | Cybersecurity Profile for Hybrid Sat
- Maritime Bulk Liquids Transfer Cybersecurity Framework Profile - U
- Cybersecurity Framework Botnet Threat Mitigation Profile - Cyberse

From the CSA website:



Mappings and components currently available in version 4:

- **Mappings to the following**: ISO/IEC 27001/27002/27017/ V8, NIST 800-53r5, and PCI DSSv3.2.1. These mappings i between the control specifications of the CCM V4 and ot development and will also be added in the future.
- **Controls Applicability Matrix:** This matrix acts as a guide responsibilities between the CSPs and CSCs when imple identifies which cloud architectural and organizational st
- **CCM Metrics:** This is the first catalog of security metrics CSP governance, risk, and compliance (GRC) activities an agreement transparency.

FAIR22 CONFERENCE

Do you really need that much detail?

- The amount of detail captured for each control also needs to be maintained
- Unclear requirements are a resource sinkhole
- Unclear requirements and unnecessary detail influence the granularity of your inventory

- Remove attributes you don’t use
- Write strong definitions and promote them
- Get rid of unclear details

Examples of unclear / unnecessary fields

Key/non-key

Try instead...

- FAIR-CAM Control Functions
- Framework references
- Relationships/mapping to specific scenarios

Control Owner

Try instead...

- Control operator
- Control objective owner or Policy/Standard owner
- Control tester

In a nutshell

Use it as much as you can…

1. As a reference point during risk analysis
2. To frame cyber capabilities
3. To measure adherence to external frameworks and benchmark

…while keeping it as simple as possible

1. Get the granularity right
2. Remove attributes that are not used or helpful
3. Replace testing with continuous monitoring

Timing matters

Iterate over the inventory once you are ready for new use cases.

Be opportunistic to make sure you can deliver value.

Apply it

- Spot 3-5 attributes that can be removed from your controls inventory
- Identify 5-10 controls that are already being continuously monitored and start discussions around reducing testing requirements and replacing with formal KPIs
- Scout for pre-existing framework mapping exercises and look to centralize them

Questions?

Reach out!

marta.palanquesvilallonga@capitalone.com