

From Assessment to Action:

Turning Risk Assessments into Actionable Security Insights

Teresa E. Banks, CISM

Eric Samboy, MS



Risk Management Benefits



Information Security



Old thinking – technical controls are the only ones that count!

Information Security

Balance!

- **Administrative:** Governance documentation, awareness and training
- **Technical:** Technology safeguards protecting systems, data, networks
- **Physical:** Facility security, access control, environmental protections



Information Security



Information Security Risk Management Program (RMaP)

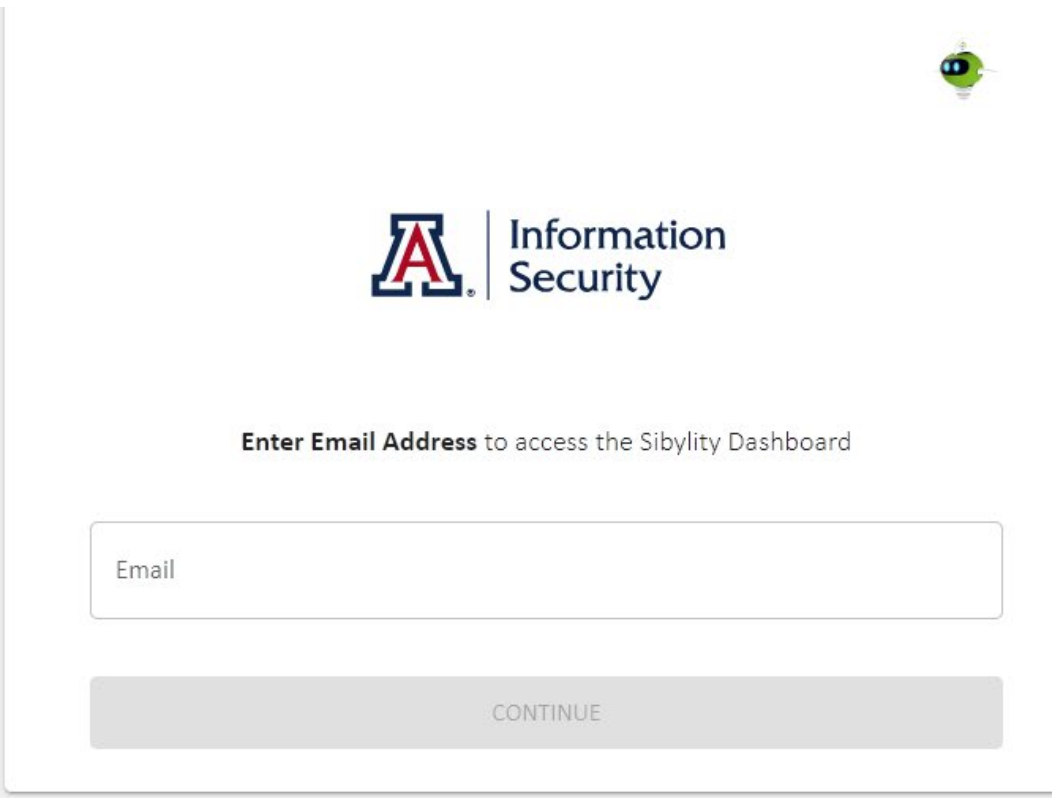
- **Collaboration:** Shared Responsibility
- **Awareness:** Understanding risk enables informed decision-making
- **Continuous Improvement:** Assess/Mitigate/Reassess leads to risk reduction over time

Information Security

UASecure

- RMaP is possible because of UASecure





Information
Security

In the beginning. . . QuickPlans!

Identify the security and privacy controls

[1]

Are the in-scope Information Resource(s) subject to University information security policy and process requirements? Yes

Hide help

For additional information, see the ISO policies and other governance documentation which can be found at https://emailarizona.sharepoint.com/sites/ISO-Communications/SitePages/ISO-Governance.aspx

Notes to share with authorized users (not included in security plans).

Information Security



Success with repetition!

- Of **70** required security plans, **18** had no identified risks in FY2026 using the QuickPlan

Information Security

FY2027

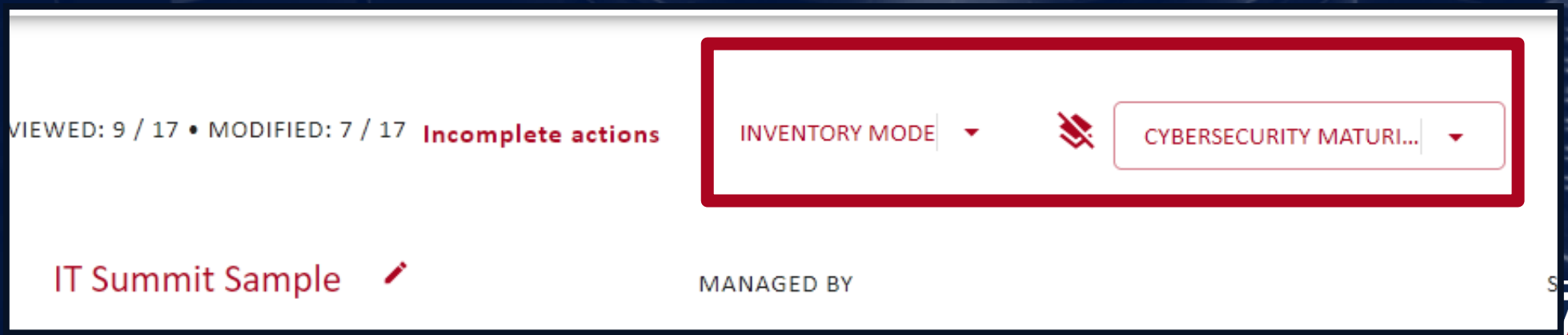
- QuickPlans still available if these are the right fit (self-service)
- Inventory Mode (mature your security posture!)
- Onboarding more “Common Controls”



Information Security

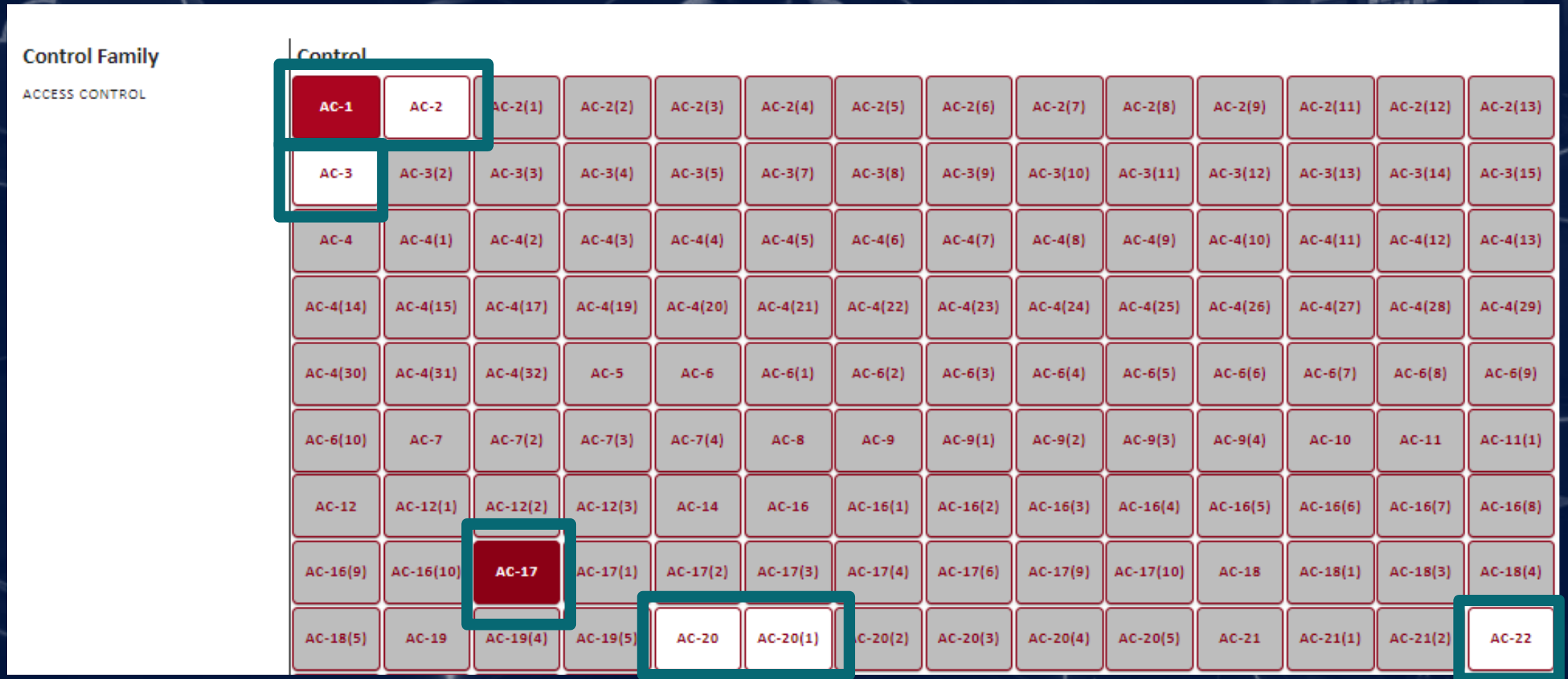
Ready for a deeper security assessment?

- Broader control coverage
- Better risk identification (especially when QuickPlan no longer reveals vulnerabilities)
- Most likely selection is CMMC Level 1 (15 security controls)



Information Security

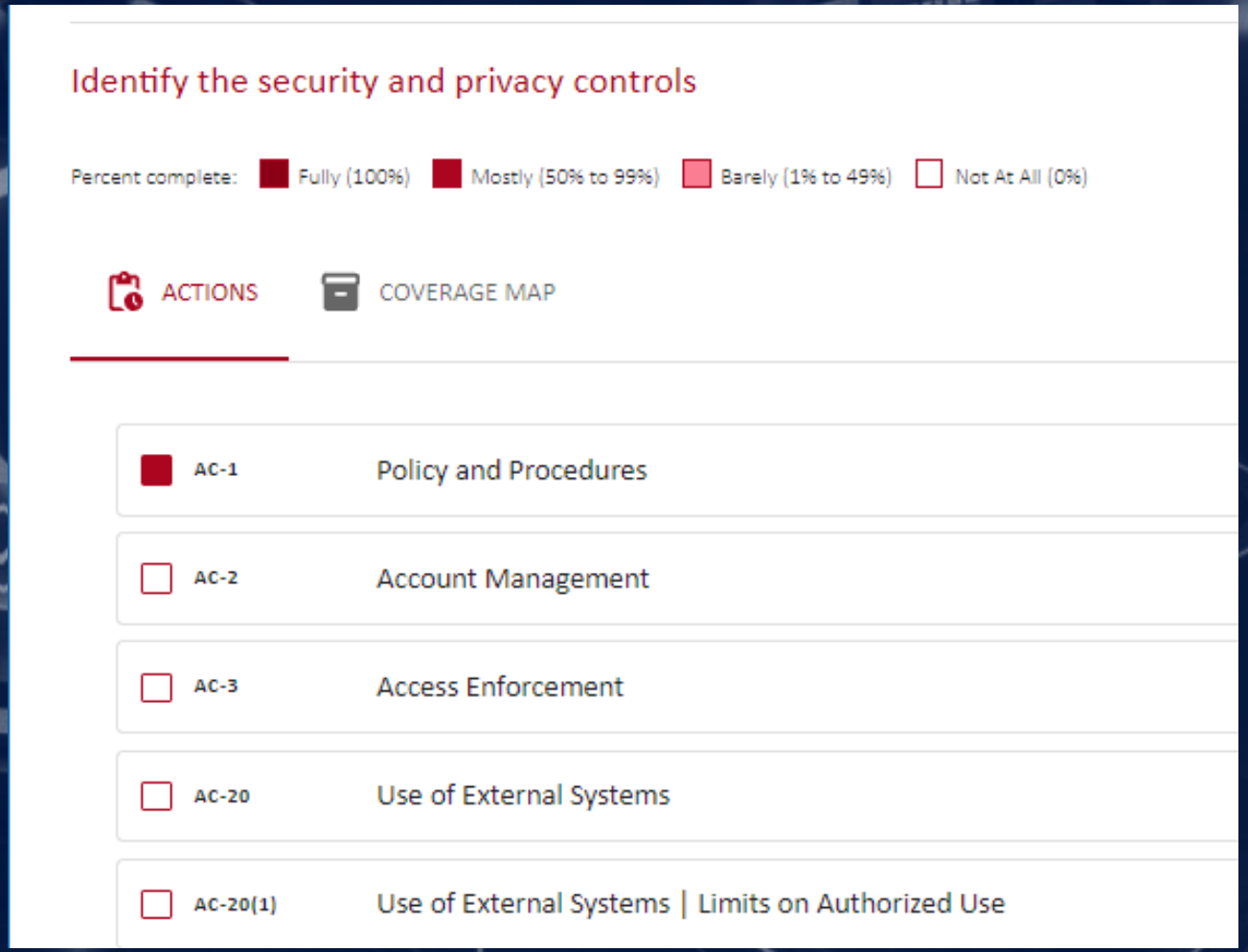
Baseline eliminates MANY NIST Controls



Information Security

User-Friendly View for Completion

- Use **Actions** view so you only focus on the security controls in scope



Information Security

Common Control Services Program

- **Common Control:**
  - A security control implemented, managed, and monitored centrally and inherited.
  - Examples: NetID, Sophos, VPN, ISO Governance
  - Onboarding based on FY2027 70 critical services

Information Security

Help is available!

- Request a Consultation!
- Visit our RMaP and Common Controls Services Page
- All content is linked at https://security.arizona.edu/links

Information Security

ASSESS THE TECHNOLOGY. UNDERSTAND THE RISK. MAKE BETTER DECISIONS.

Are we assessing the technology, or just completing an assessment?



OR

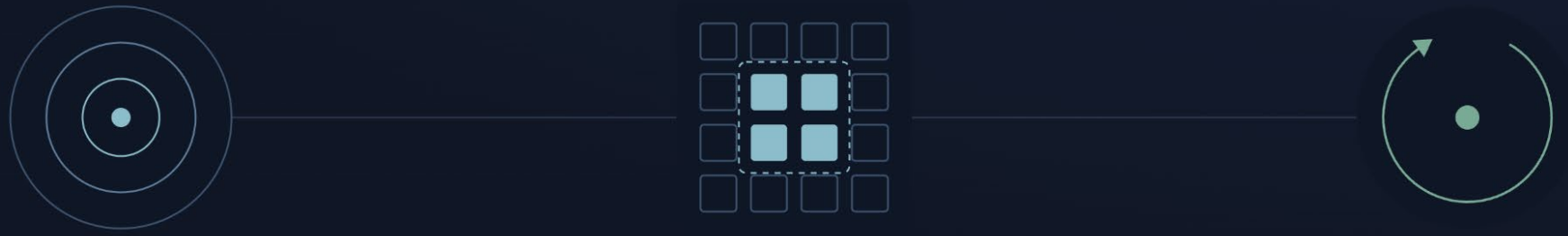


COMPLETING A PROCESS

UNDERSTANDING A SYSTEM

THE APPROACH

Meaningful assessments start with understanding.



01

Understand the technology

02

Tailor the assessment

03

Turn insight into action

RISK ASSESSMENT

Identify · Analyze · Evaluate

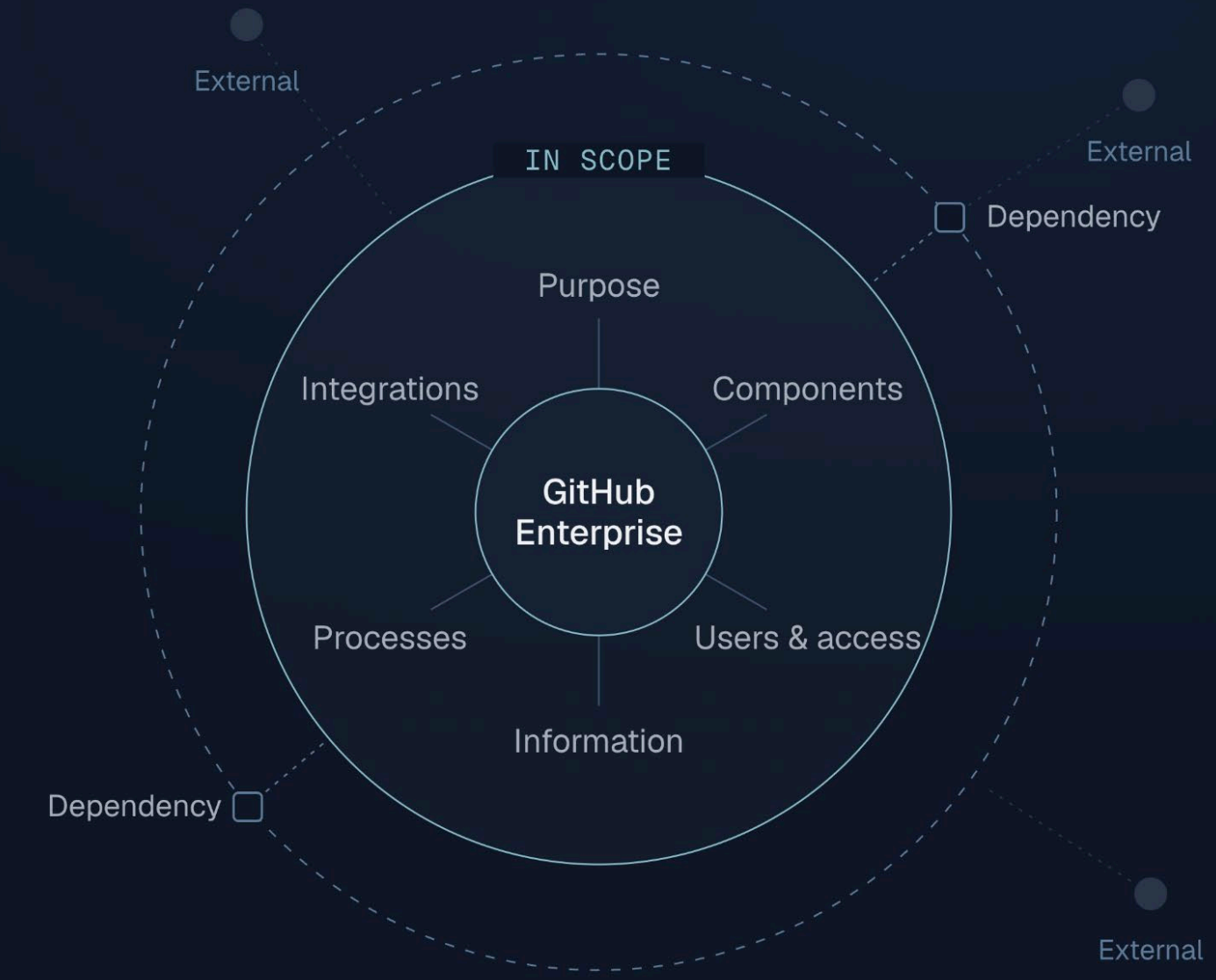
RISK MANAGEMENT

Decide · Treat · Monitor — continuously

STEP 1 — DEFINE THE SCOPE

Before assessing risk, understand what you're assessing.

- Assessed resource
- Relevant dependencies
- External systems

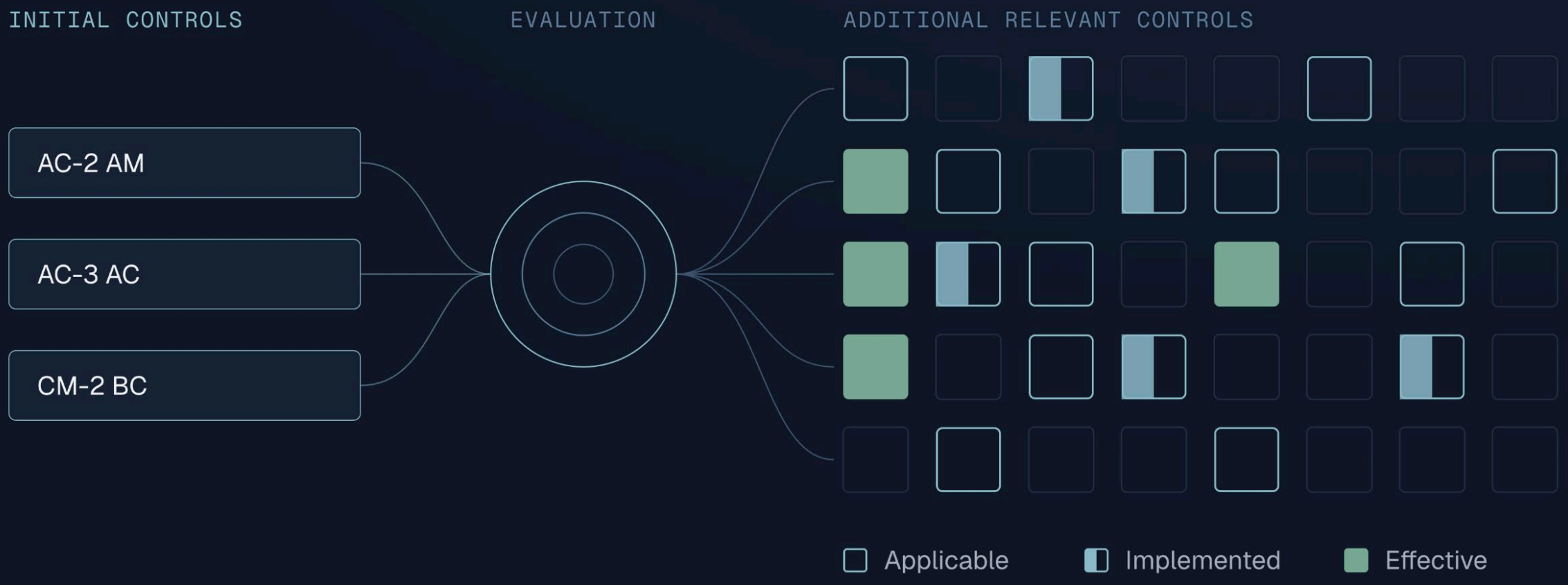


STEP 2 — INVENTORY WHAT MATTERS

Understand the information before evaluating the risk.



Start focused. Expand with understanding.



STEP 4 — MEASURE WHAT MATTERS

Risk must be evaluated, not simply identified.

WHAT COULD BE AFFECTED

C Confidentiality

I Integrity

A Availability



Documented reasoning

STEP 5 — PRIORITIZE AND DETERMINE TREATMENT

Understanding risk leads to better decisions.



Mitigate
Reduce likelihood or impact

Accept
Within tolerance, documented

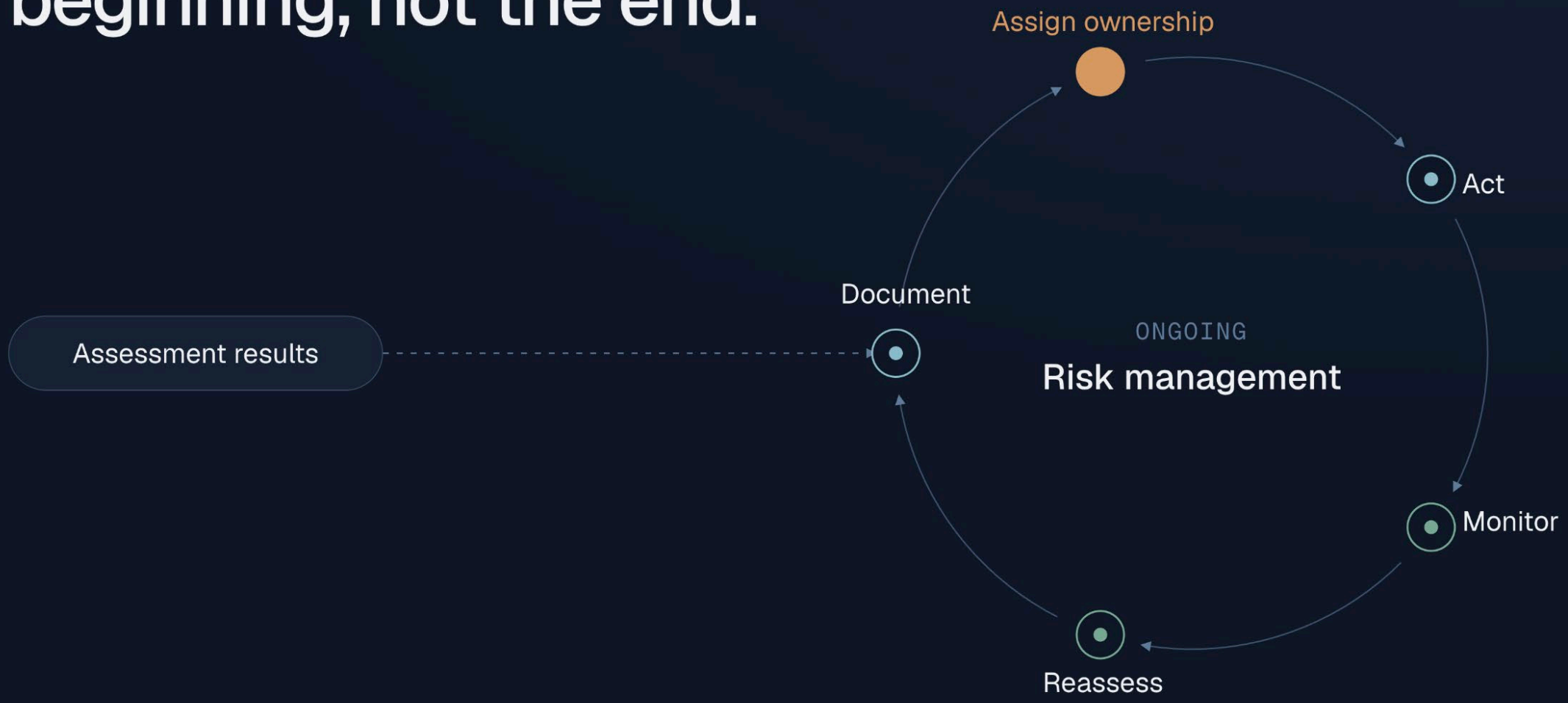
Transfer
Share with another party

Avoid
Stop or change the activity

WEIGHED AGAINST Safeguards · Impact · Exposure · Tolerance

STEP 6 — TURN ASSESSMENT INTO RISK MANAGEMENT

The assessment is the beginning, not the end.



WHAT WE LEARNED

A focused strategy creates better visibility.

CHALLENGES

Scope definition

Data selection

Control mapping

Risk evaluation



OUTCOMES

- Clearer understanding of the technology
- Better-defined scope
- More relevant control evaluation
- Structured risk visibility
- More informed decisions

THE TAKEAWAY

Make the assessment about the technology, not the checklist.



“Meaningful risk assessments begin with understanding the technology, the information it supports, and the way people actually work.”

Thank you QUESTIONS?