RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-R05**

Leveraging Issues Management as a Force Multiplier in Cybersecurity

Jamie Sanderson Reid
Director, Cyber GRC
The AES Corporation

Ryan Boulais
VP and CISO
The AES Corporation

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

The Challenge & Vision

The Problem - Anecdotally

Strategic

"Where are we taking cyber risk?"

"Do you have a thoughtful approach to understanding cyber risk?"

"I don't understand the quantification of cyber risk"

Operational

"How much cyber risk is associated with this?"

"I don't know what my Cyber requirements are..."

Tactical

"Just tell me what I have to do"

"Can you just approve my exception?"

"Employee A said it was ok"

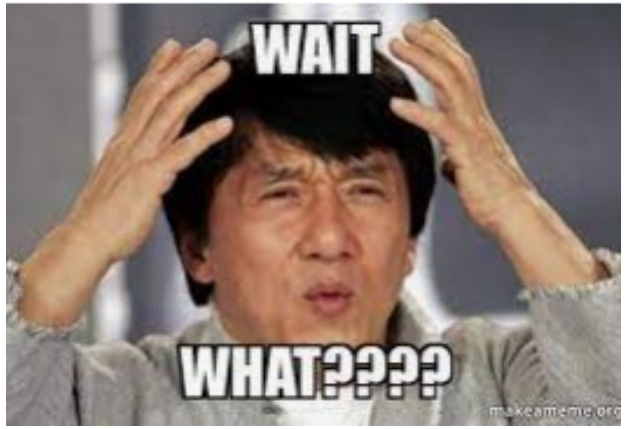
Building GRC Ground Up

Greenfield for Corporate function

- Culture of Accountability
- Purpose built – right sized
- Low overhead
- Risk based approach
- Aligned goals and objectives

Culture Challenge

No formal Cyber Security Policy + Disparate Request/ Approval Process + Limited understanding of Issues/Risks + Disconnected Accountability Model + Limited Oversight = "Cyber said I'm good"



Culture Change - Vision

1. Enable teams to follow a consistent process
2. Empower team members to escalate risks/issues
3. Engage with business leaders so they understand the risk
4. Enhance the decision-making process to align with business accountability

Cyber becomes both custodians of the process and an *input* to decisions

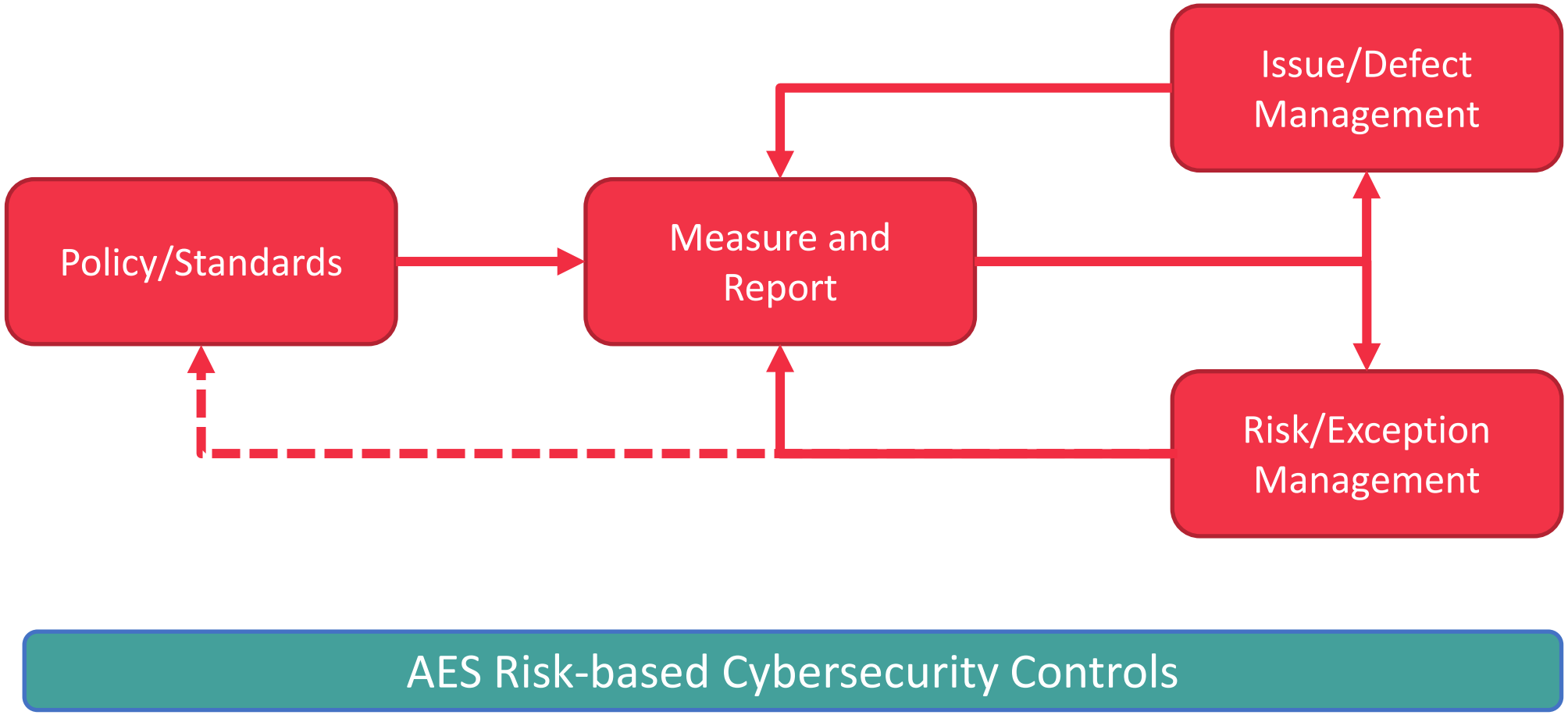
RSAConference2022

Issues Management – Nexus for Change

Issues Management

Issues management is integrated with every aspect of cybersecurity

Cyber GRC Operating Model



Key Program Elements for Issues Management

- Policies, standards, and controls
- Asset Management
- Risk/Issue identification process
- Decision making process/forum
- Analytics capability
- Metrics/Governance reporting
- Enabling technology
- Team to support the overall model

Policy/Standards

Cyber Security Standard

- Everything and the kitchen sink!
- 19 Pages
- Limited enforcement

Cyber Security Policy

- Aligned with company Cyber Program
- 3 Pages

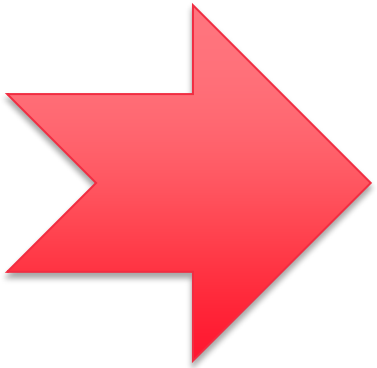
Purpose built:

- Scope
- Implementation guidance
- Exceptions process

Policies/Standards are operational, not aspirational

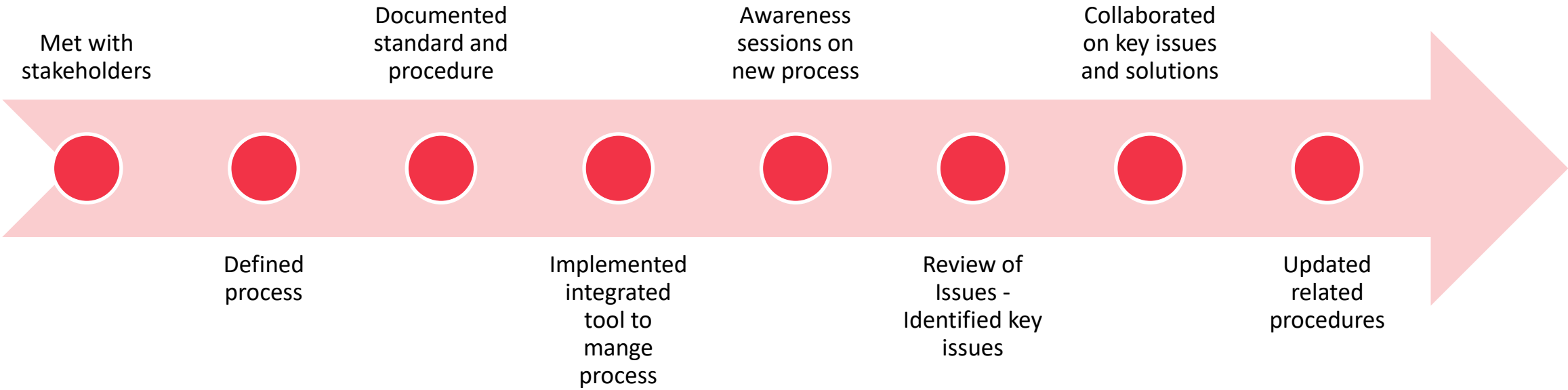
Asset Management

- Infrastructure
  - Server
  - Laptop/Desktop
  - Cloud
  - Mobile
  - Network
- Applications
  - SaaS
  - Internal development
- OT

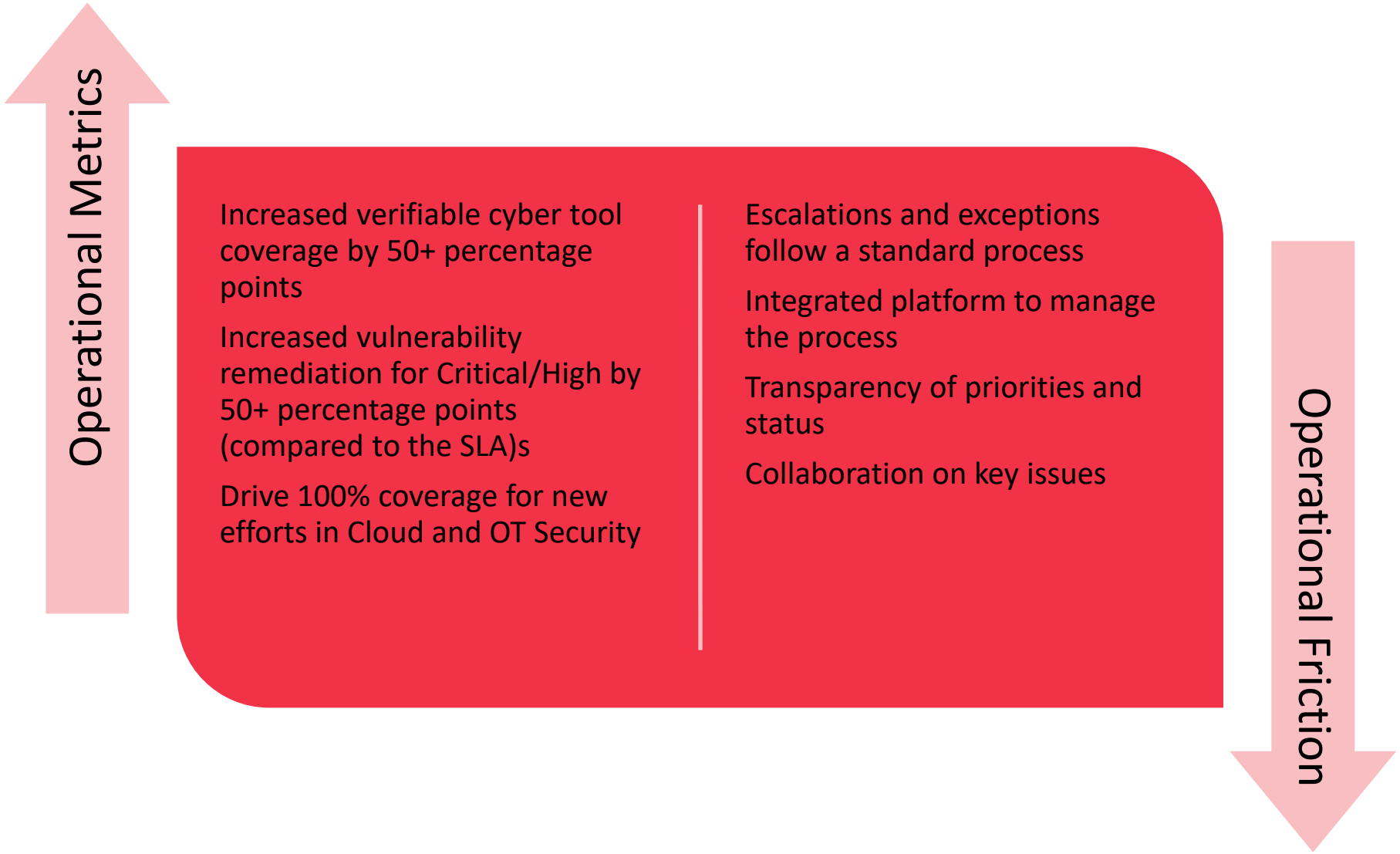


Drove our Digital partners to implement a Lifecycle Asset Management Program

What We Did – Risk/Decision Processes

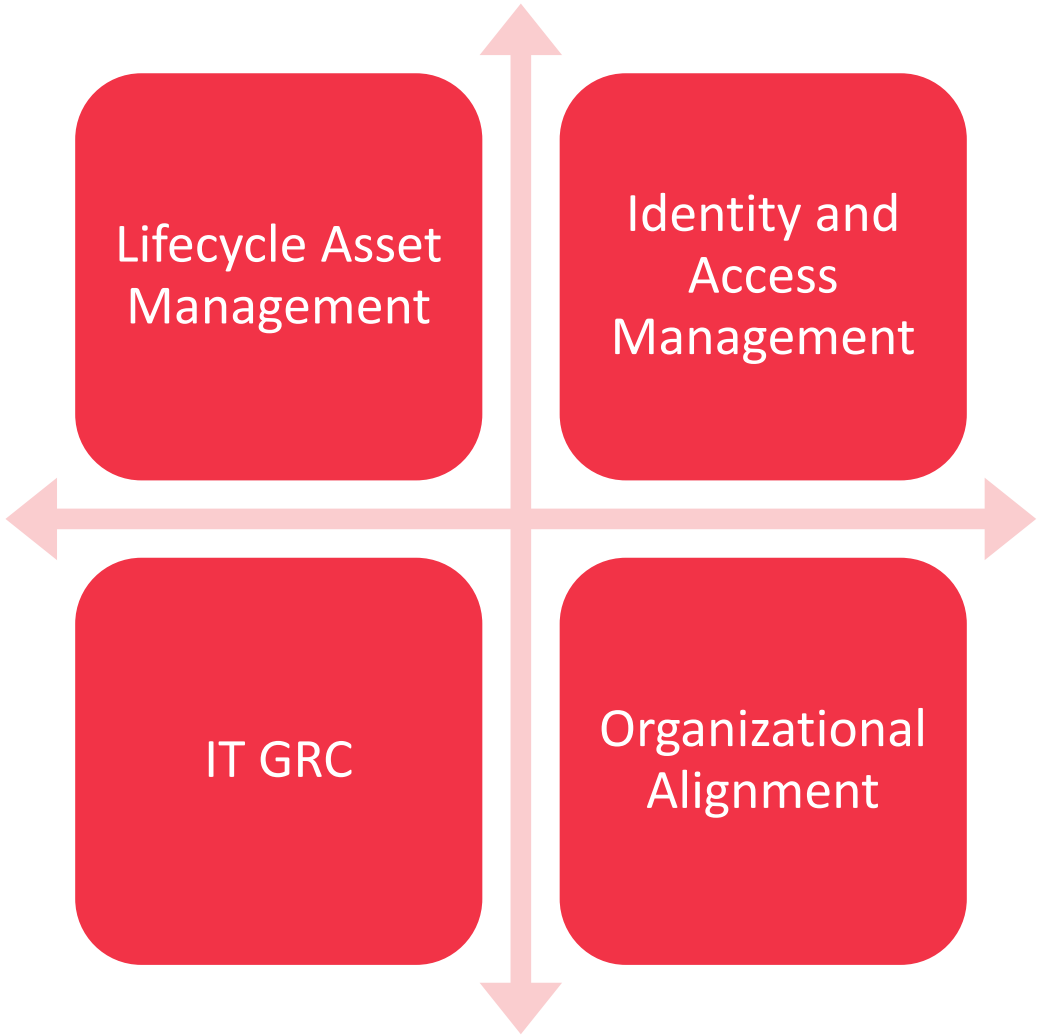


Results – Analytics and Metrics



Results – Transformative Initiatives

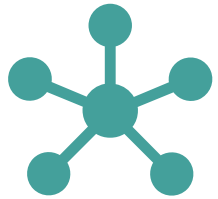
Influenced the business case for several IT/Digital initiatives



So, what's changed?

- Faster escalation of risks
- Fewer Exceptions requested
- Board/Executive level conversations about Cyber Risk

Escalation and awareness of cyber risks



Centralization of data with increased alignment

Visibility of various levels of risks

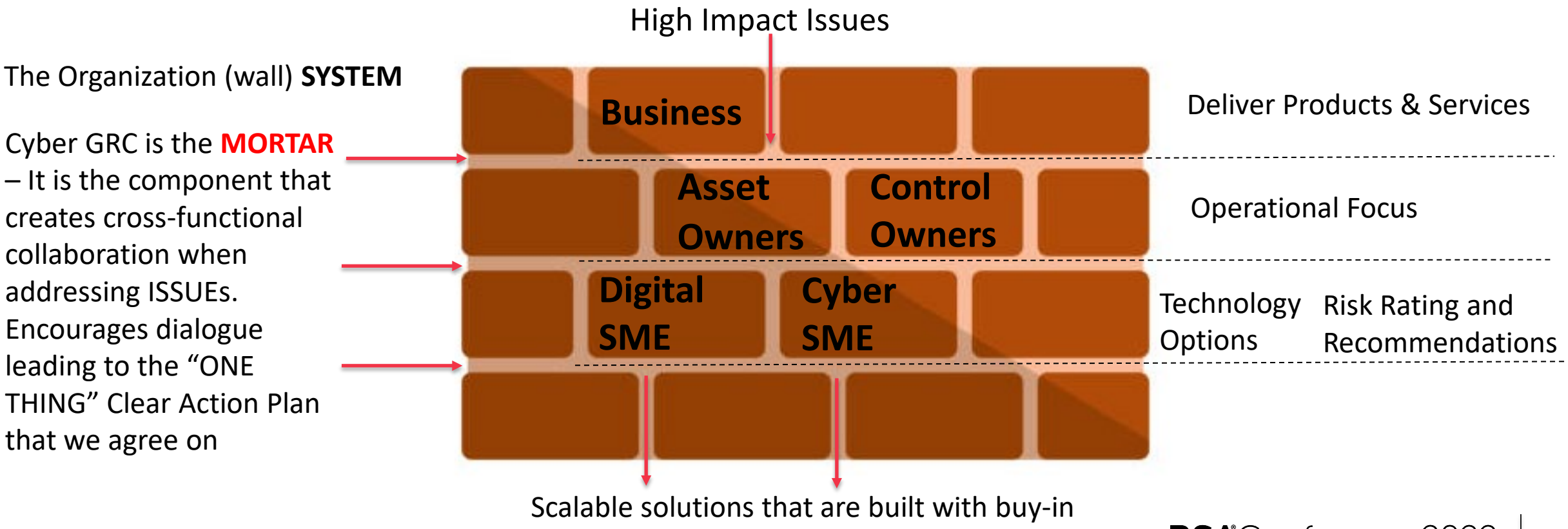
RSAConference2022

Issues Management – Force Multiplier

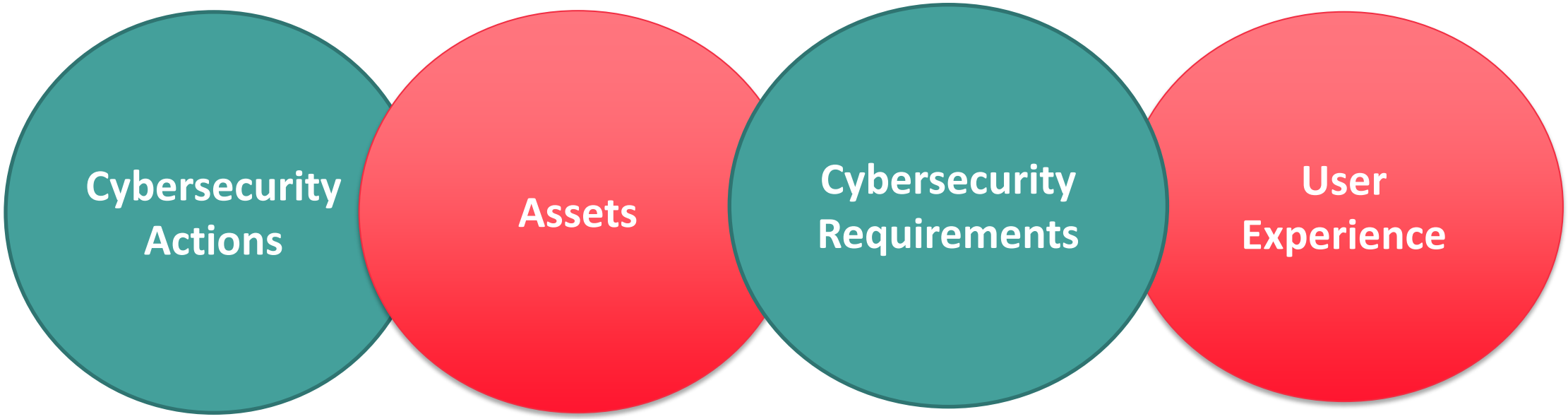
Keys to implementation

Collaboration

- Requires open mindset and commitment to collaboration
- Shift to strategic enabler – mortar for the business



Visibility



Issues are cross cutting: providing visibility of *real-actual* indicators of our security posture and process improvement opportunities

Focus

1. Strategic Enablement of Digital Transformation
2. Risk Management
3. Communication & Reporting
4. Partnership Between Cybersecurity & Digital

Lessons Learned

- Increased collaboration and interactions amongst teams = better issues management
- Discussions increase understanding of business needs and risks
- Ideas for program and process improvement
- Partnership on asset management and project management
- Tackle a problem – opportunity to collaborate and co-create great outcomes

Apply – Action Plan

Next Week	Within 3 Months	Within 6 Months
○ Identify a high impact issue that requires cross functional collaboration to resolve.	○ Schedule workshops with stakeholders from business, technology and cybersecurity to work on the identified issue	○ Update standards/controls ○ Update processes and procedures ○ Report on success to organization