



LET'S KILL TPRM

Managing Third-Party Cyber Risk at the Speed of the Business

Next-Gen Third-Party Risk Management (TPRM)
with FAIR, MITRE ATT&CK, AI Automation



Vince Dasta


Senior Partner - Risk Strategy
Safe Security



Ram Vemula

Product Management - Head of Partnerships
Safe Security

Agenda for TPRA

- Why is TPRM broken
 - Siloed tools and processes
 - Assessment Types vs Risk Outcomes
 - Fundamental Change Needed
 - FAIR-TAM
 - Risk Led decision making
- 

Current TPRM approaches are not working



60%

Of all data breaches are initiated via
third-parties

45%

Of organizations worldwide would have
experienced a software supply chain
attack by 2025 according to Gartner

>50% attacks happened through supply chain!

CISOs and Practitioners are not feeling confident



CISOs' lack confidence in Third Party Risk Programs

"I am running blind on my third party risk." - CISO of a Fortune 100

Healthcare Provider

"I don't know how to manage my third parties." - CISO of a Fortune 500

Technology Company

TPRM Practitioners are overwhelmed

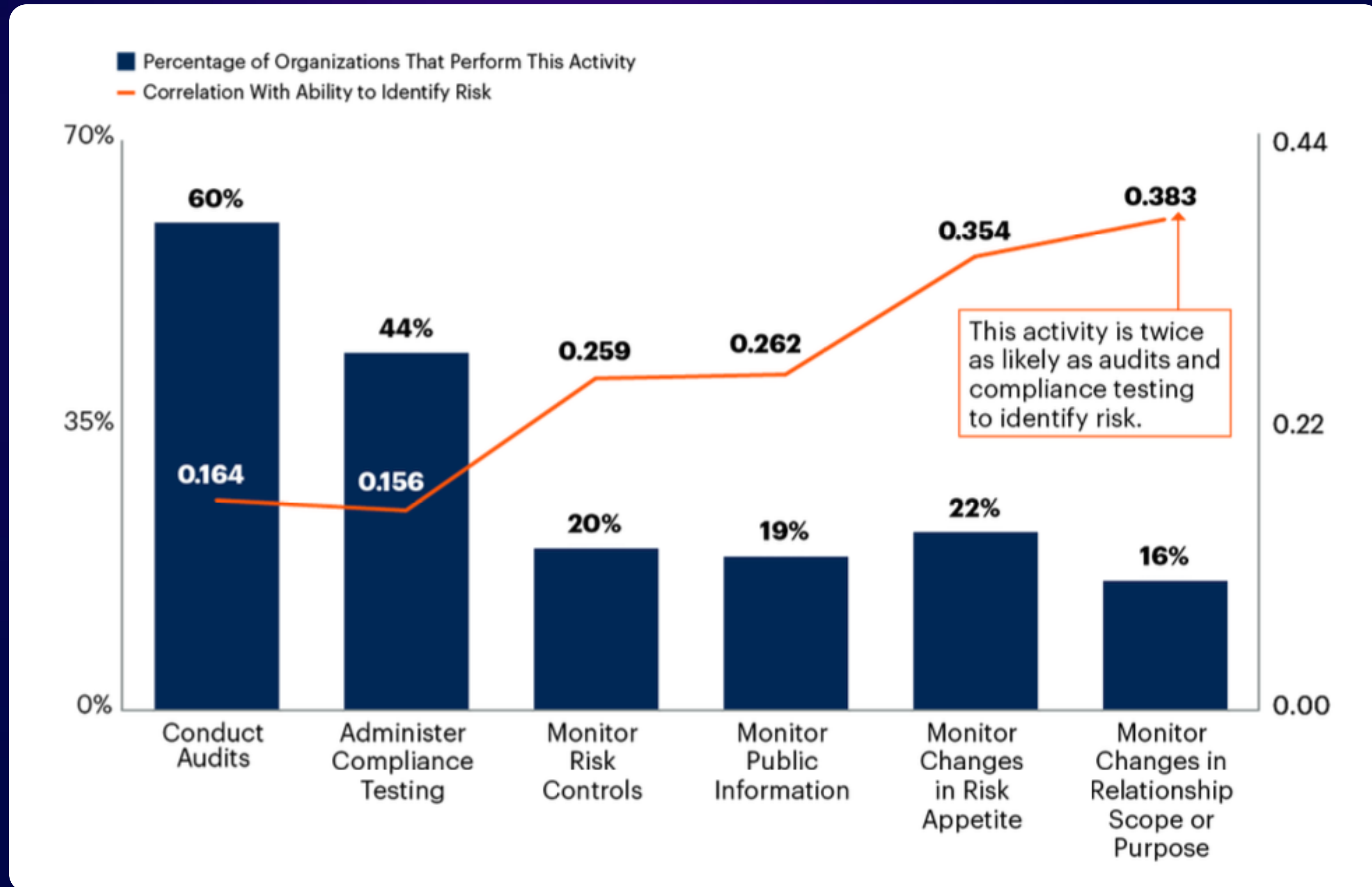
"I am overwhelmed - 1000s of third parties with a small team!"

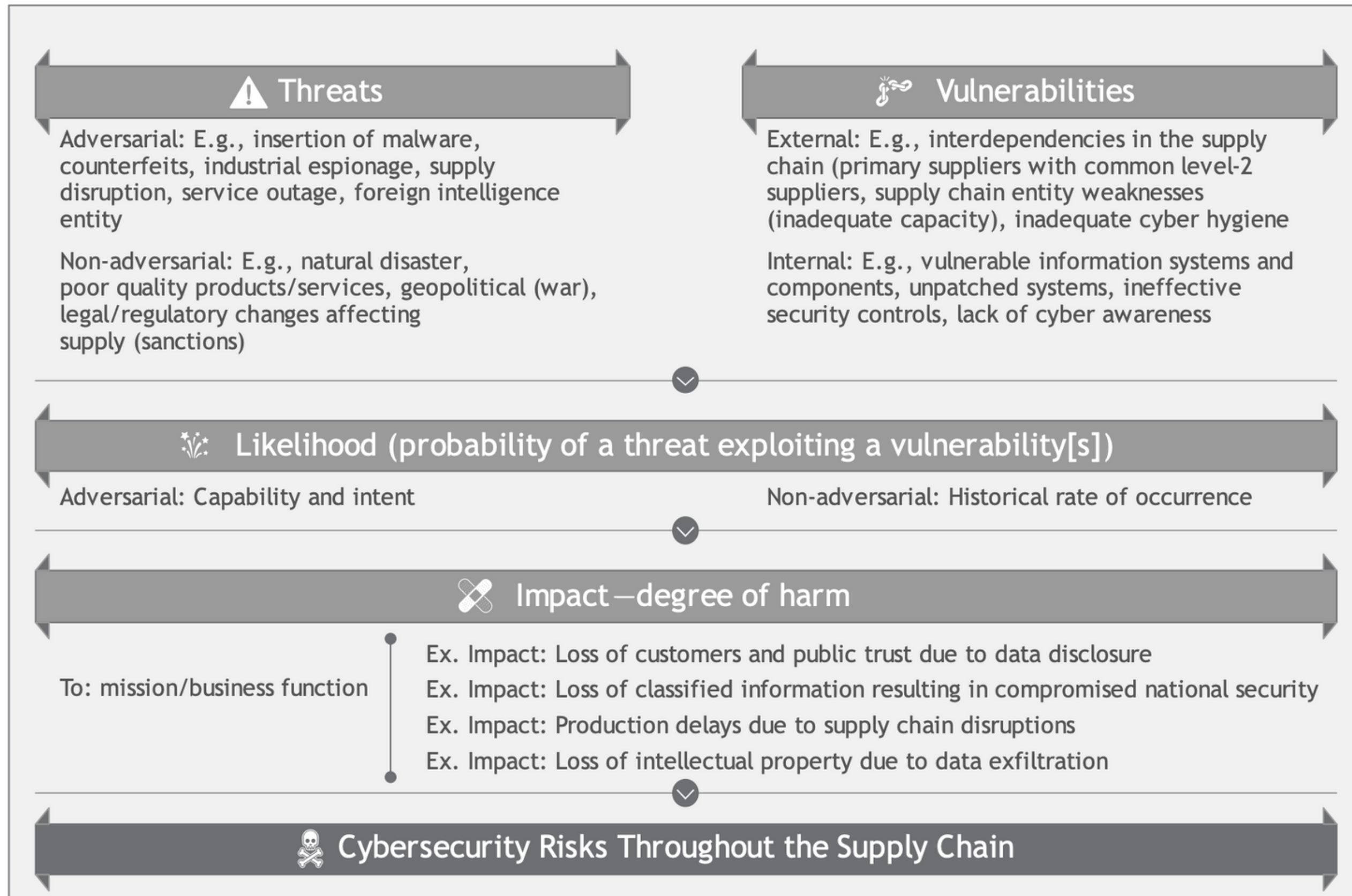
"I am a process person - I keep chasing my internal folks, my vendors..."

"I don't know where to focus on"

"My vendors hate me, my business owners don't understand me"

Relationship between assessment types and risk outcomes



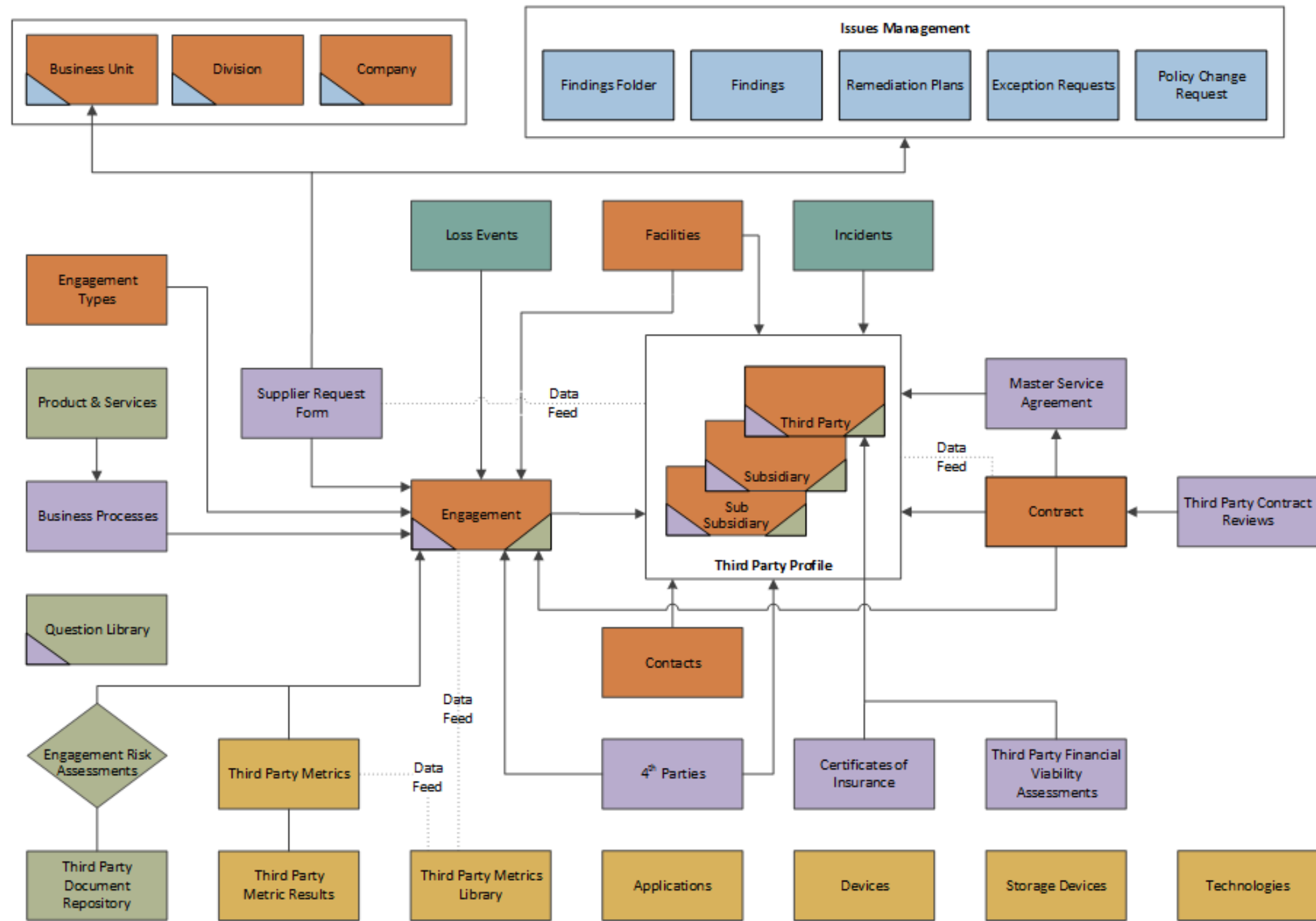


NIST 800-161 frames Supply Chain Risk in this way...

Why do companies fail to achieve their goals



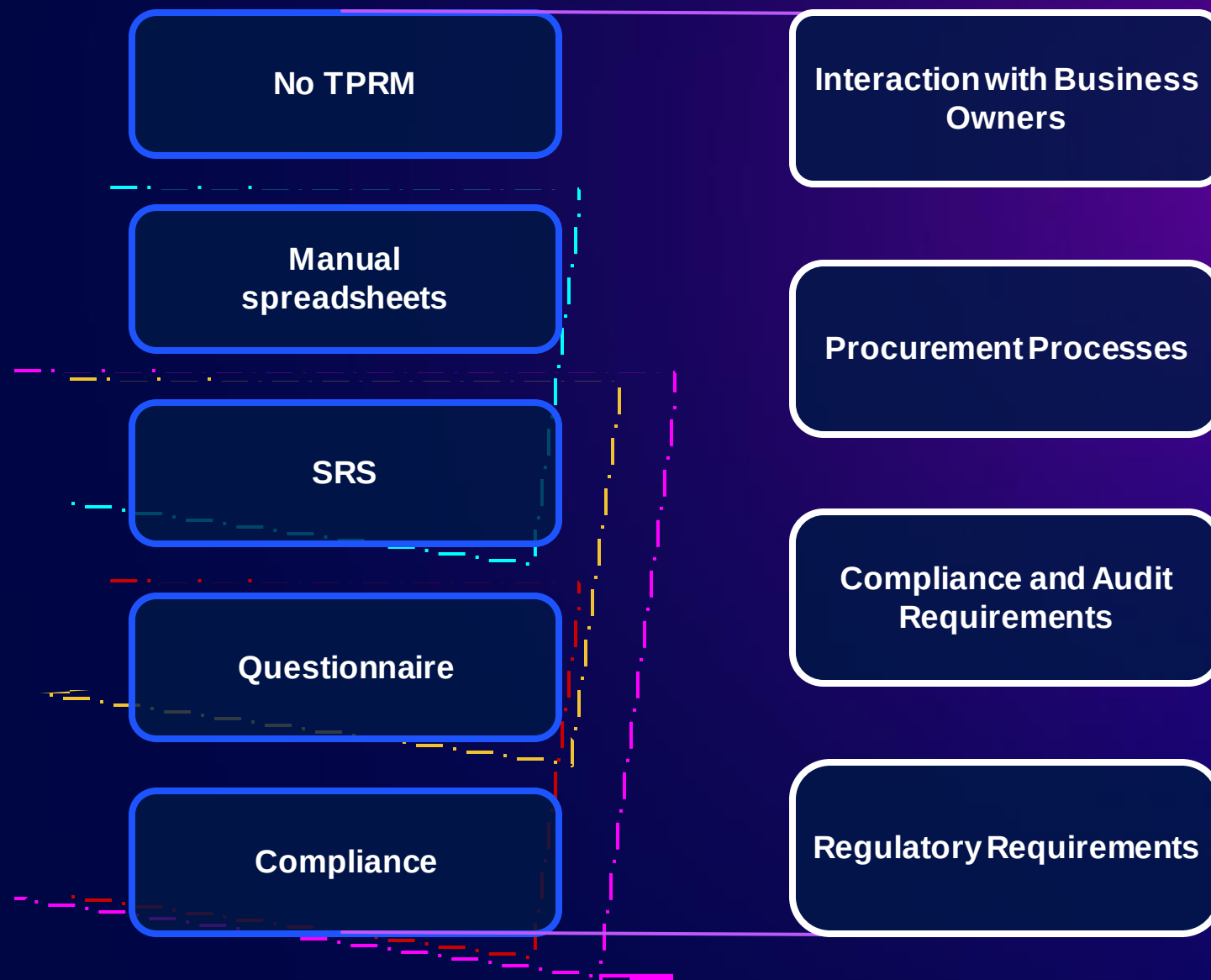
A real world example



Customers are struggling to operationalize and scale TPRM



Siloed Tools to Complex Stack



Siloed processes and functions

- Different tools providing different risk view
- Risk reporting is inconsistent
- No real science behind TPRM
- Questionnaire based
- Time consuming (avg 2-4 weeks)
- Point in time
- Not 100% reliable
- Tools that scan the external presence
- Too many false positives
- No actionable insights based on risks
- Don't want to become vendor's security department
- No strong partnership with vendors



Fundamental Change

What if

you could start making risk based,
proactive TPRM decisions

instead of audits and compliance
based, reactive fire-fighting?

What is Factor Analysis of Information Risk (FAIR)?



The **FAIR standard** enables risk to be quantitatively defined, measured, managed and communicated

FAIR-CAM, FAIR-MAM, FAIR-TAM are all extensions of FAIR

Accredited as an Industry Standard by



Complementary to Risk Frameworks



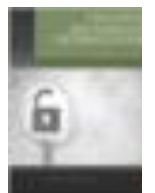
Supported by a Community of 15,000+



Wide Industry Adoption
50% Fortune 1000



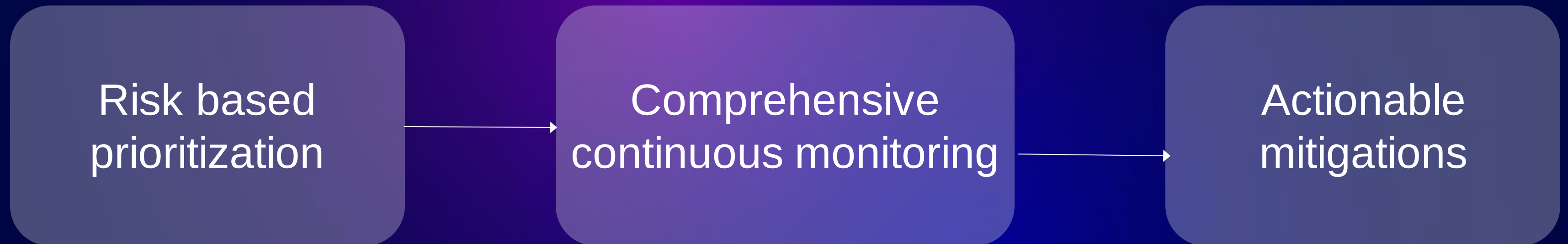
FAIR Book Inducted in Cybersecurity Canon



FAIR Approach for TPRM



FAIR-TAM



FAIR-TAM



Risk based
prioritization

Prioritization based on contract value, size
of the vendor...



Prioritization based on risk to YOUR
business – data, network, revenue access
– using FAIR-MAM



FAIR-TAM



Comprehensive
continuous monitoring

- Just outside-in
- One-time manual questionnaires

Not
enough

- Inside-out telemetry from first and third parties
- Likelihood using FAIR-CAM





Actionable
mitigations

- *'You have more control than you think'* – actively fix and build your controls
- Active collaboration with vendors
- Open dialogue and sharing of data

Moving from a Compliance to Risk Based Program



Questions

- Do I know the risk this third-party poses?
- Can I enter into a business relationship?

- How do I think about TPRM frameworks?
- How do I respond to compliance and regulatory requirements?

- Who are my risky third-parties?
- Do third-parties have access to my network and data?

- How do I implement zero trust controls
- What kind of automation can be implemented to scale third-party risk program

Capabilities Leveraged

- SOC2, ISO 27001 certifications of third-parties
- Leverage existing resources from procurement, GRC and security teams

- Outside-In assessment
- Procurement tools

- Questionnaire assessment to understand third-party controls
- Risk Exchanges

- First-Party Zero Trust Controls
- Automating Questionnaire Responses to Assess First Party and Third Party Controls
- Inside-Out Assessment of critical third-parties



Foundational

Risk-led

What Does an Effective TPRM Program Look Like?



SAFE: The industry's first and leading Unified Risk Management Platform



Persona-Based Dashboards SAFEGPT SAFE Mobile App

AI-Driven UX

Cyber Risk Quantification Materiality Risk Reporting Control Prioritization & ROI Emerging Risks Cyber Insurance Planning **Third Party Risk Management**

Integrated Cyber Risk Management

MITRE | ATT&CK® **FAIR** **FAIR-CAM** **FAIR-MAM**

Open Analytics Engine

 First-Party Business Context	 Business Relationship Business Resources Third-Party Business Context	 SecurityTrail SPAMHAL MITRE ATT&CK SHODA SpyClou SHARED ASSESSMENT Malwar Patrol Threat Intel	 aws Qualy salesforce Google App Google Cloud Platfor tenable network security Azur Adobe Experience Manager RAPIDT KnowBe4 Human error. Conquered nessu Professional CROWDSTRIK Exchange proofpoint acuneti Enterprise Security Data	 NIST NIST CSF AICPA SOC 2 Compliance and Questionnaire Data
----------------------------------	---	--	---	--

Cyber Risk Cloud

Learn more about SAFE and the FAIR Institute



www.safe.security



www.fairinstitute.org

Stop by the SAFE table for a demo or
schedule your SAFE Demo:

<https://www.safe.security/safe/request-demo/>

