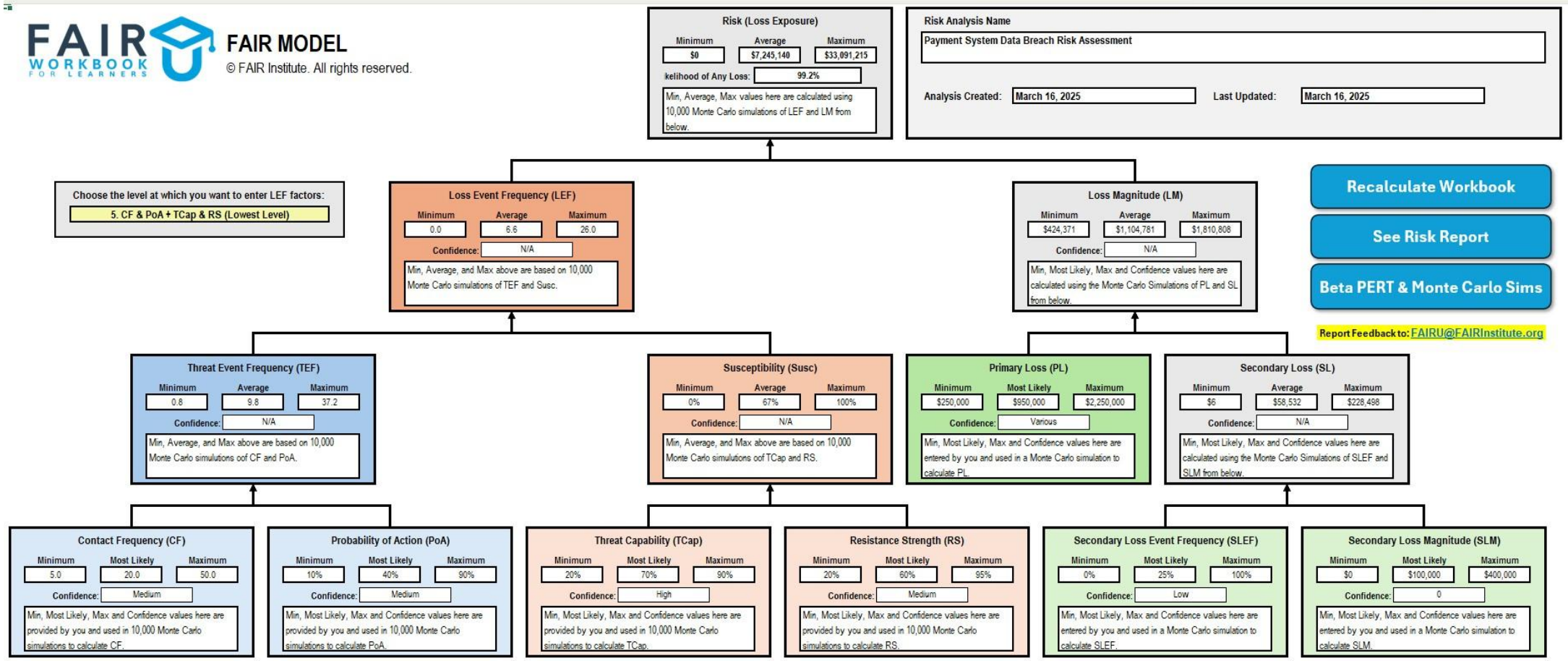
Measuring KRI using the FAIR-U Workbook



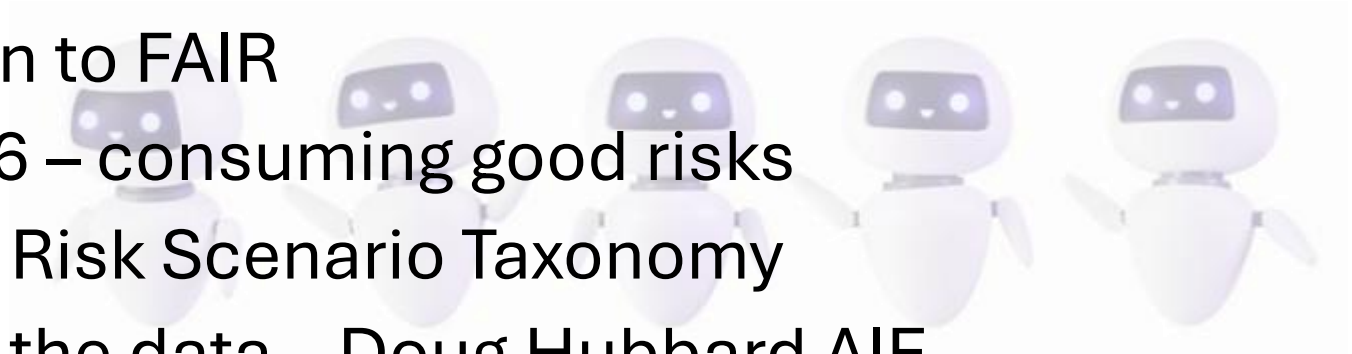
- Instructor: Denny Wan
- Date: Thu 22nd May 2025

Acknowledgement of Country

I would like to acknowledge the Gadigal of the Eora Nation, the traditional custodians of the City of Sydney and pay my respects to the Elders, both past and present.

Agenda

- Measure what needs to be managed
- Using the FAIR-U Workbook
- Understanding KRI
- Introduction to FAIR
- NISTIR 8286 – consuming good risks
- FAIR Cyber Risk Scenario Taxonomy
- Calibrating the data – Doug Hubbard AIE
- Modelling Agentic AI risk with FAIR-CAM
- Simulation exercise



Denny Wan

- Founder of Reasonable Security Institute
- AISA FELLOW
- FAIR Ambassador (APEC) 2024
- 2024 "Cyber Security Professional of the Year - Professional and Financial Services“
- CI-ISAC Australia Ambassador
- FAIR Institute Standards Committee member
- Chair – FAIR-CAM Workgroup

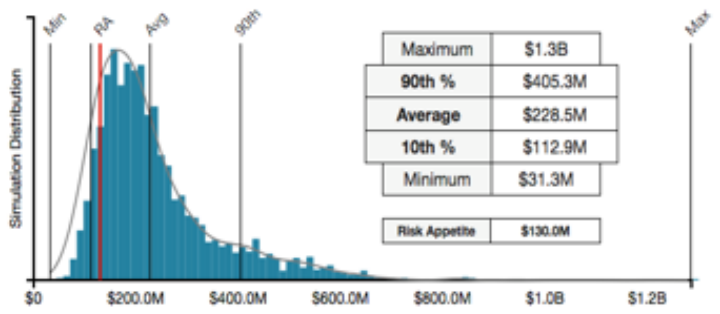
Email: dwan@reasonablesecurity.org.au
LinkedIn: https://www.linkedin.com/in/wandenny/
Twitter: @denny_wan

Measure what needs to be managed

Source: The FAIR Institute

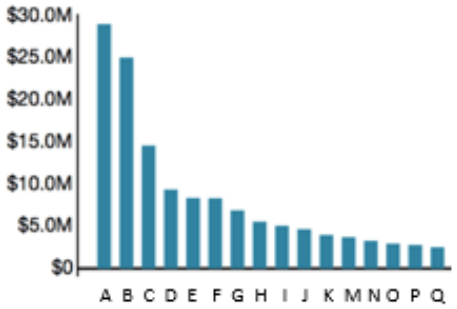
Communicating Cyber Risk in dollar value

"HOW MUCH RISK DO WE HAVE?"

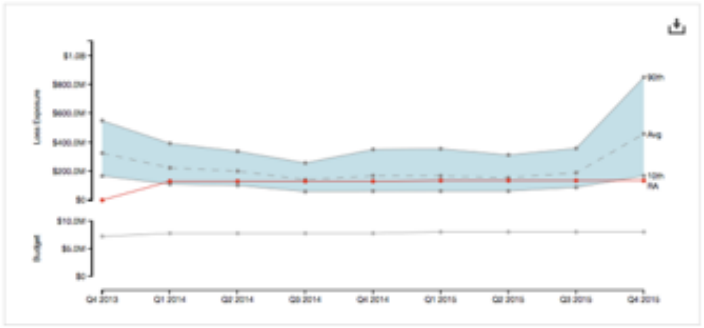


Maximum	$1.3B
90th %	$405.3M
Average	$228.5M
10th %	$112.9M
Minimum	$31.3M
Risk Appetite	$130.0M

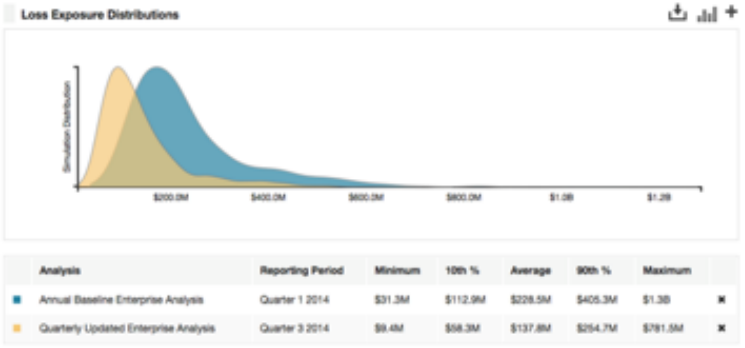
"WHAT ARE OUR TOP RISKS?"



"HOW IS OUR RISK TRENDING VS. APPETITE?"

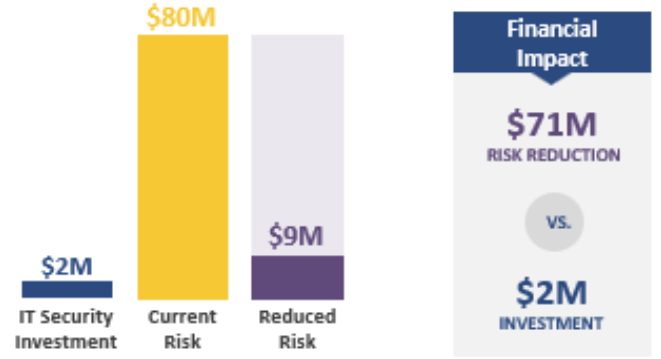


"HAVE WE REDUCED RISK?"



"WHAT TYPE OF LOSS CAN WE EXPECT?"

"WHAT IS THE COST/BENEFIT OF THIS PROJECT?"



Source: The FAIR Institute

Using the FAIR-U Workbook

Hands-On Experience with the FAIR Cyber Risk Management Framework

We collaborated with our founder and technical advisor, Safe Security, to provide a free tool for learners called **FAIR-U for Cyber (beta release)**. Powered by Safe ONE, FAIR-U for Cyber shows how the FAIR Model, FAIR-CAM, and FAIR-MAM work together in a cyber risk management system (CRMS) to manage risk.

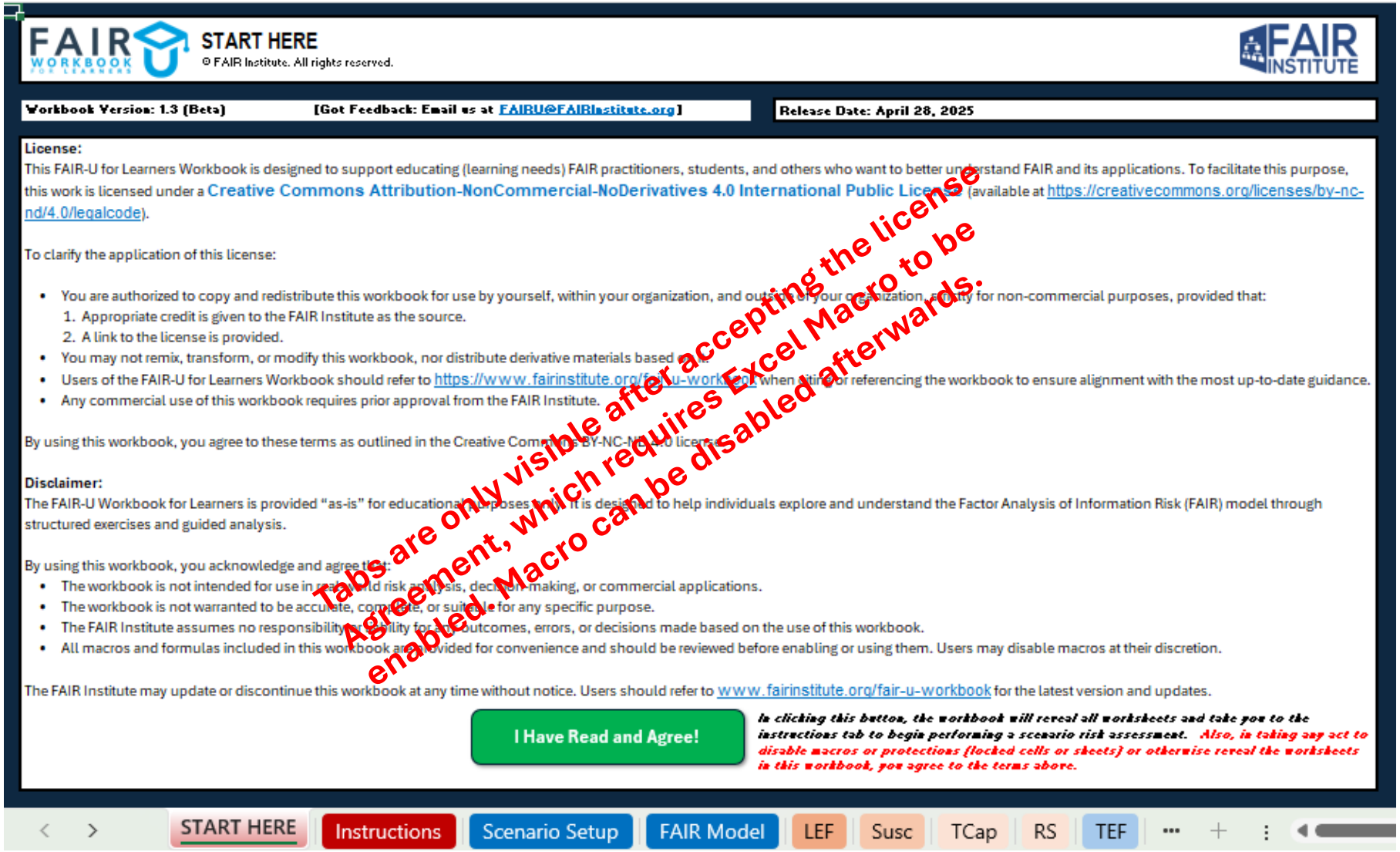
Learners should read this white paper to see how the three FAIR standards are integrated as part of the FAIR Cyber Risk Management Framework.

FAIR U FOR CYBER

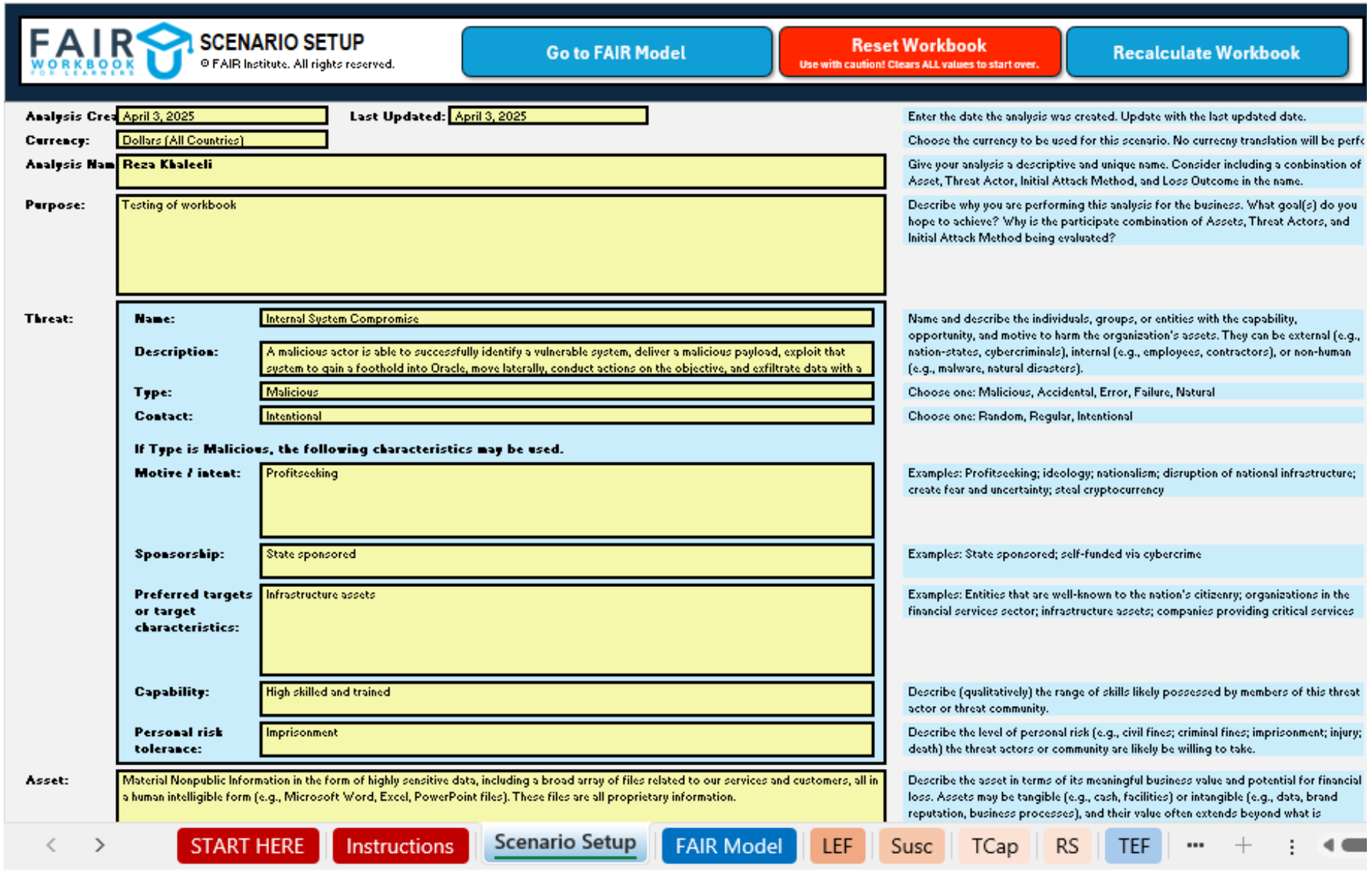
Source: https://www.fairinstitute.org/fair-u-workbook

REASONABLE SECURITY

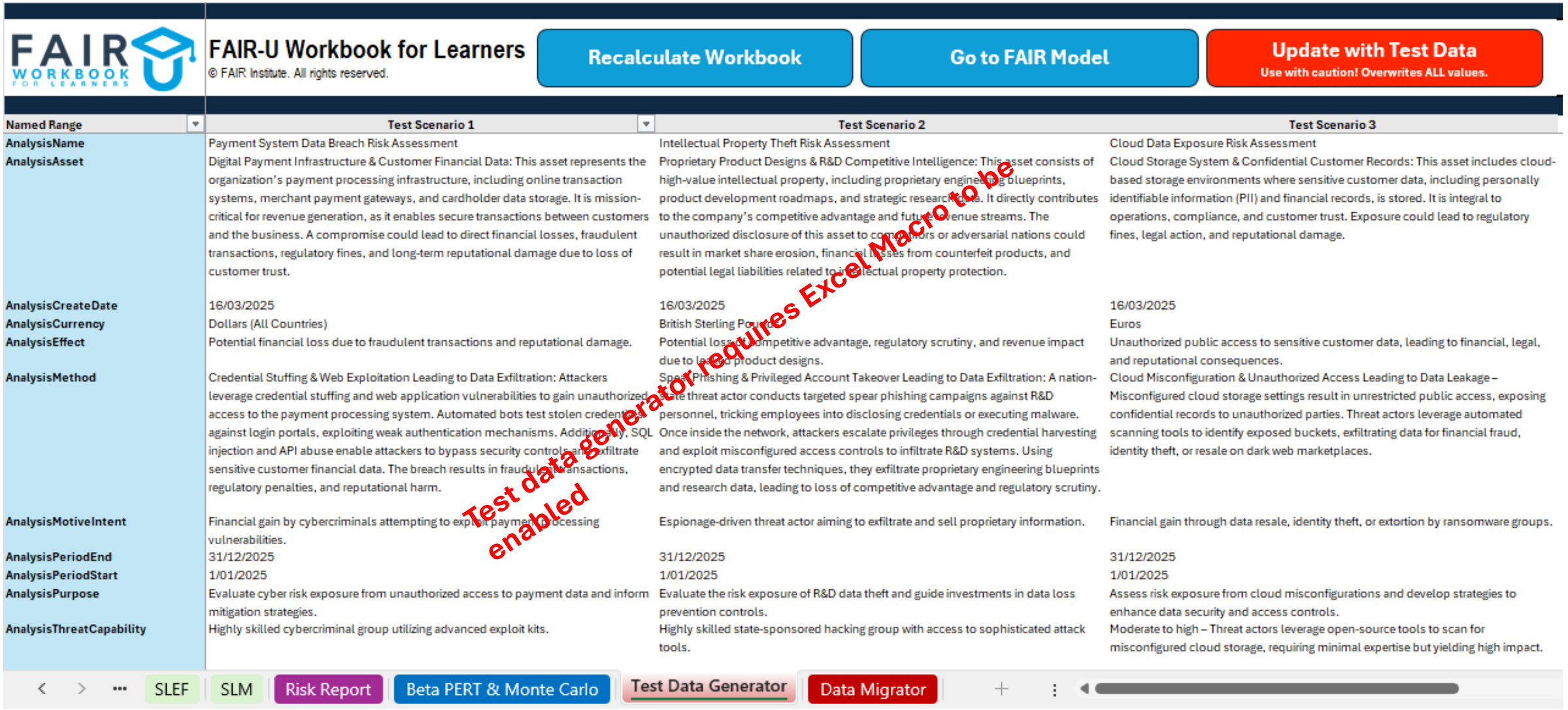
Using the FAIR-U Workbook



Using the FAIR-U Workbook



Using the FAIR-U Workbook



FAIR WORKBOOK FOR LEARNERS

FAIR-U Workbook for Learners

Recalculate Workbook | Go to FAIR Model | Update with Test Data (Use with caution! Overwrites ALL values.)

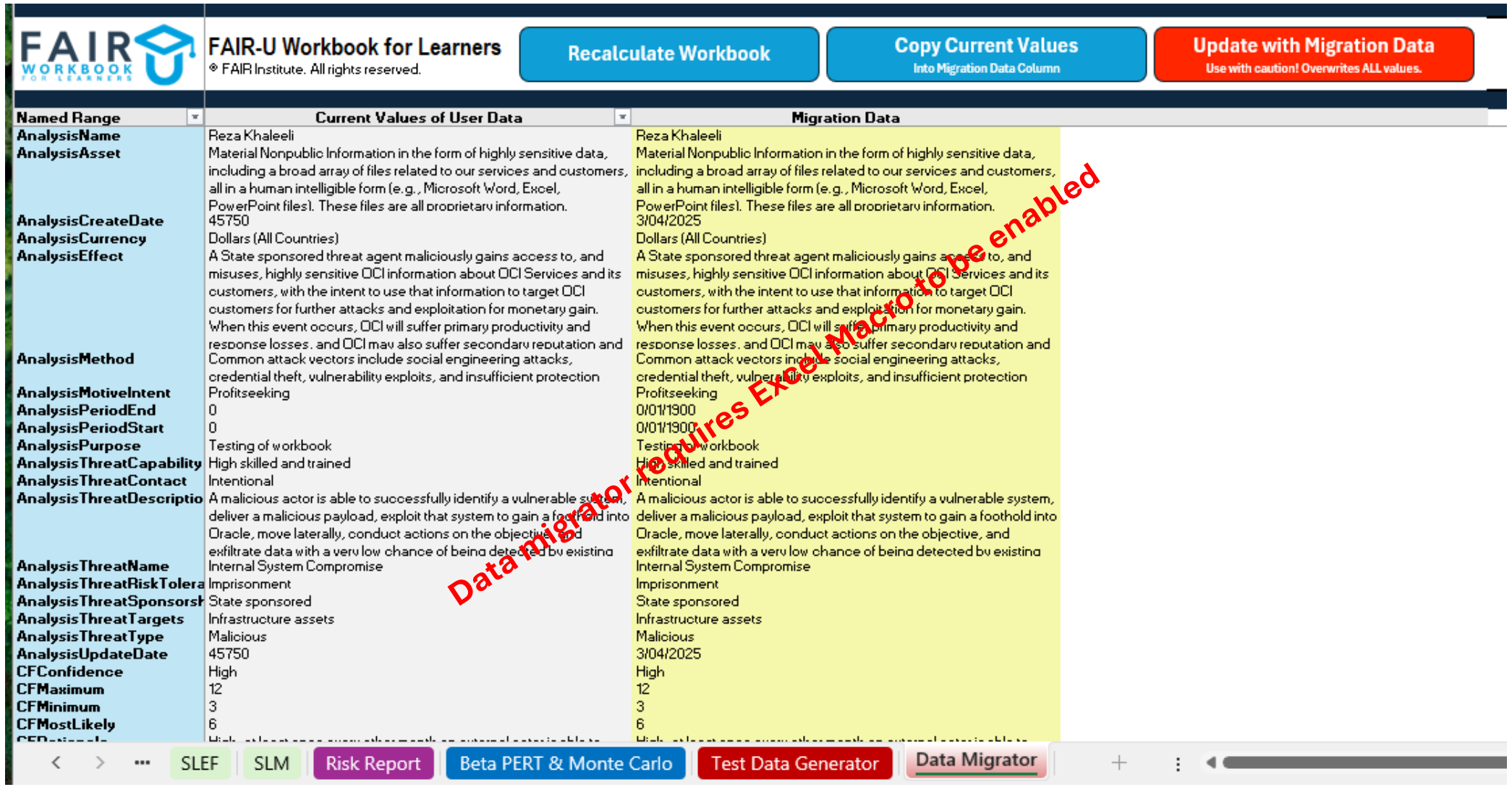
Named Range	Test Scenario 1	Test Scenario 2	Test Scenario 3
AnalysisName	Payment System Data Breach Risk Assessment	Intellectual Property Theft Risk Assessment	Cloud Data Exposure Risk Assessment
AnalysisAsset	Digital Payment Infrastructure & Customer Financial Data: This asset represents the organization's payment processing infrastructure, including online transaction systems, merchant payment gateways, and cardholder data storage. It is mission-critical for revenue generation, as it enables secure transactions between customers and the business. A compromise could lead to direct financial losses, fraudulent transactions, regulatory fines, and long-term reputational damage due to loss of customer trust.	Proprietary Product Designs & R&D Competitive Intelligence: This asset consists of high-value intellectual property, including proprietary engineering blueprints, product development roadmaps, and strategic research data. It directly contributes to the company's competitive advantage and future revenue streams. The unauthorized disclosure of this asset to competitors or adversarial nations could result in market share erosion, financial losses from counterfeit products, and potential legal liabilities related to intellectual property protection.	Cloud Storage System & Confidential Customer Records: This asset includes cloud-based storage environments where sensitive customer data, including personally identifiable information (PII) and financial records, is stored. It is integral to operations, compliance, and customer trust. Exposure could lead to regulatory fines, legal action, and reputational damage.
AnalysisCreateDate	16/03/2025	16/03/2025	16/03/2025
AnalysisCurrency	Dollars (All Countries)	British Sterling Pounds	Euros
AnalysisEffect	Potential financial loss due to fraudulent transactions and reputational damage.	Potential loss of competitive advantage, regulatory scrutiny, and revenue impact due to leaked product designs.	Unauthorized public access to sensitive customer data, leading to financial, legal, and reputational consequences.
AnalysisMethod	Credential Stuffing & Web Exploitation Leading to Data Exfiltration: Attackers leverage credential stuffing and web application vulnerabilities to gain unauthorized access to the payment processing system. Automated bots test stolen credentials against login portals, exploiting weak authentication mechanisms. Additionally, SQL injection and API abuse enable attackers to bypass security controls and exfiltrate sensitive customer financial data. The breach results in fraudulent transactions, regulatory penalties, and reputational harm.	Spear Phishing & Privileged Account Takeover Leading to Data Exfiltration: A nation-state threat actor conducts targeted spear phishing campaigns against R&D personnel, tricking employees into disclosing credentials or executing malware. Once inside the network, attackers escalate privileges through credential harvesting and exploit misconfigured access controls to infiltrate R&D systems. Using encrypted data transfer techniques, they exfiltrate proprietary engineering blueprints and research data, leading to loss of competitive advantage and regulatory scrutiny.	Cloud Misconfiguration & Unauthorized Access Leading to Data Leakage – Misconfigured cloud storage settings result in unrestricted public access, exposing confidential records to unauthorized parties. Threat actors leverage automated scanning tools to identify exposed buckets, exfiltrating data for financial fraud, identity theft, or resale on dark web marketplaces.
AnalysisMotiveIntent	Financial gain by cybercriminals attempting to exploit payment processing vulnerabilities.	Espionage-driven threat actor aiming to exfiltrate and sell proprietary information.	Financial gain through data resale, identity theft, or extortion by ransomware groups.
AnalysisPeriodEnd	31/12/2025	31/12/2025	31/12/2025
AnalysisPeriodStart	1/01/2025	1/01/2025	1/01/2025
AnalysisPurpose	Evaluate cyber risk exposure from unauthorized access to payment data and inform mitigation strategies.	Evaluate the risk exposure of R&D data theft and guide investments in data loss prevention controls.	Assess risk exposure from cloud misconfigurations and develop strategies to enhance data security and access controls.
AnalysisThreatCapability	Highly skilled cybercriminal group utilizing advanced exploit kits.	Highly skilled state-sponsored hacking group with access to sophisticated attack tools.	Moderate to high – Threat actors leverage open-source tools to scan for misconfigured cloud storage, requiring minimal expertise but yielding high impact.

Test data generator requires Excel Macro to be enabled

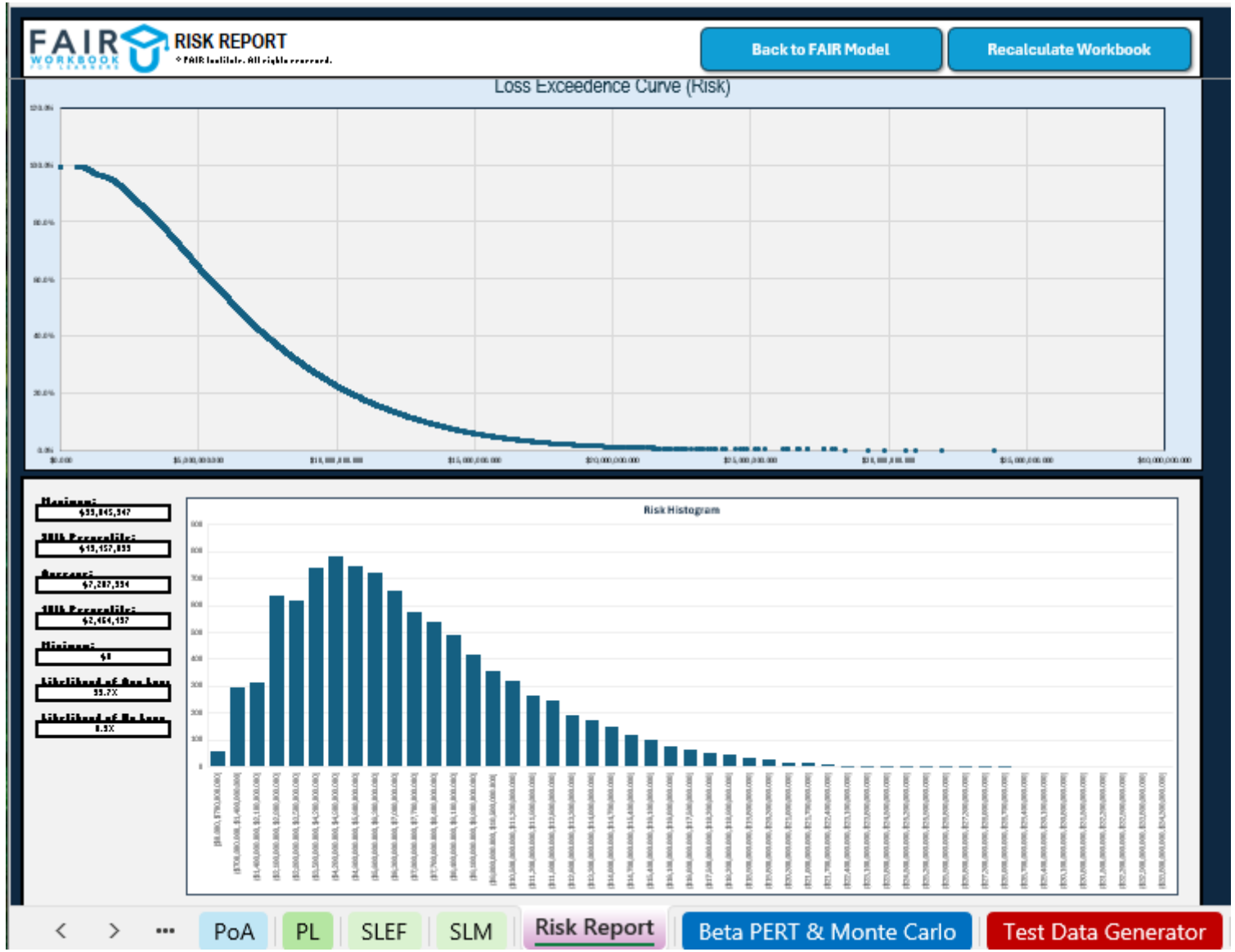
SLEF | SLM | Risk Report | Beta PERT & Monte Carlo | Test Data Generator | Data Migrator

REASONABLE SECURITY

Using the FAIR-U Workbook



Using the FAIR-U Workbook



Understanding KRI

- A measurable metric used to signal potential risks
- Risk = effect of uncertainty on objectives (ISO Guide 73)
- Risk = Lost Event Frequency * Loss Magnitude
- Identify emerging threats before they escalate into major issues

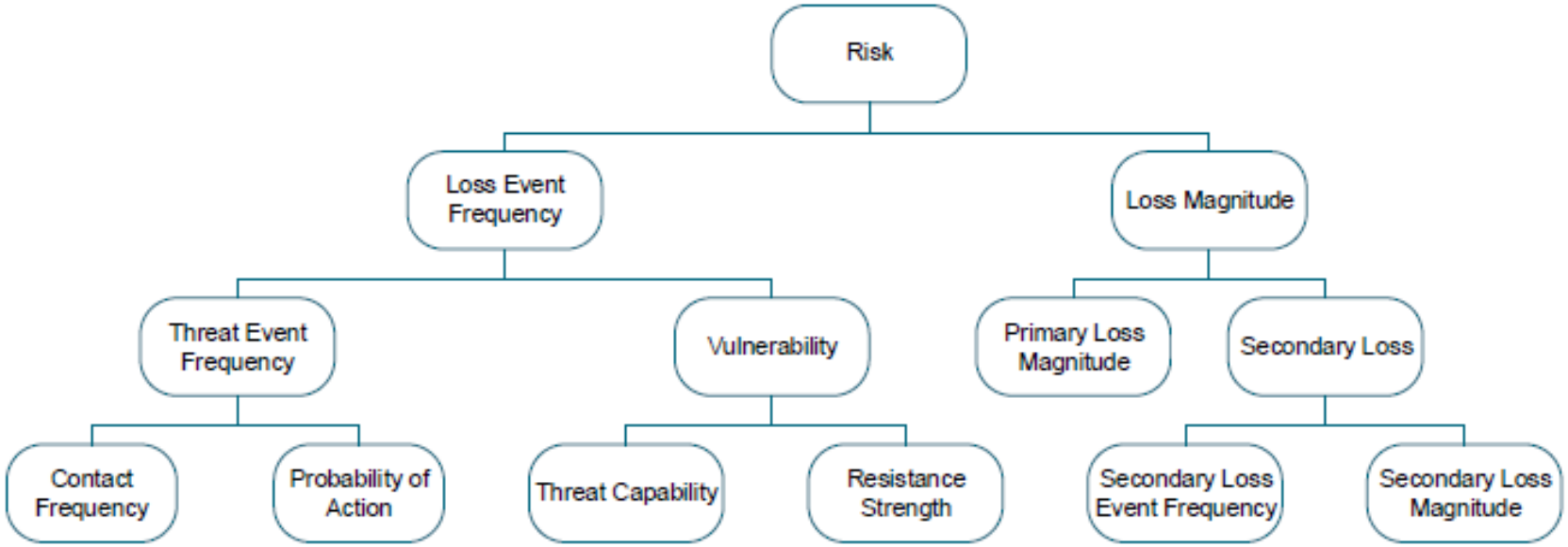
Measuring KRI

- Define Risk Categories – Identify the specific risks relevant to the organization
- Select Measurable Indicators –financial ratios, incident rates, etc
- Set Thresholds & Benchmarks – Establish acceptable risk levels and trigger points for action
- Monitor Trends Over Time – Track KRIs regularly to detect patterns and emerging risks

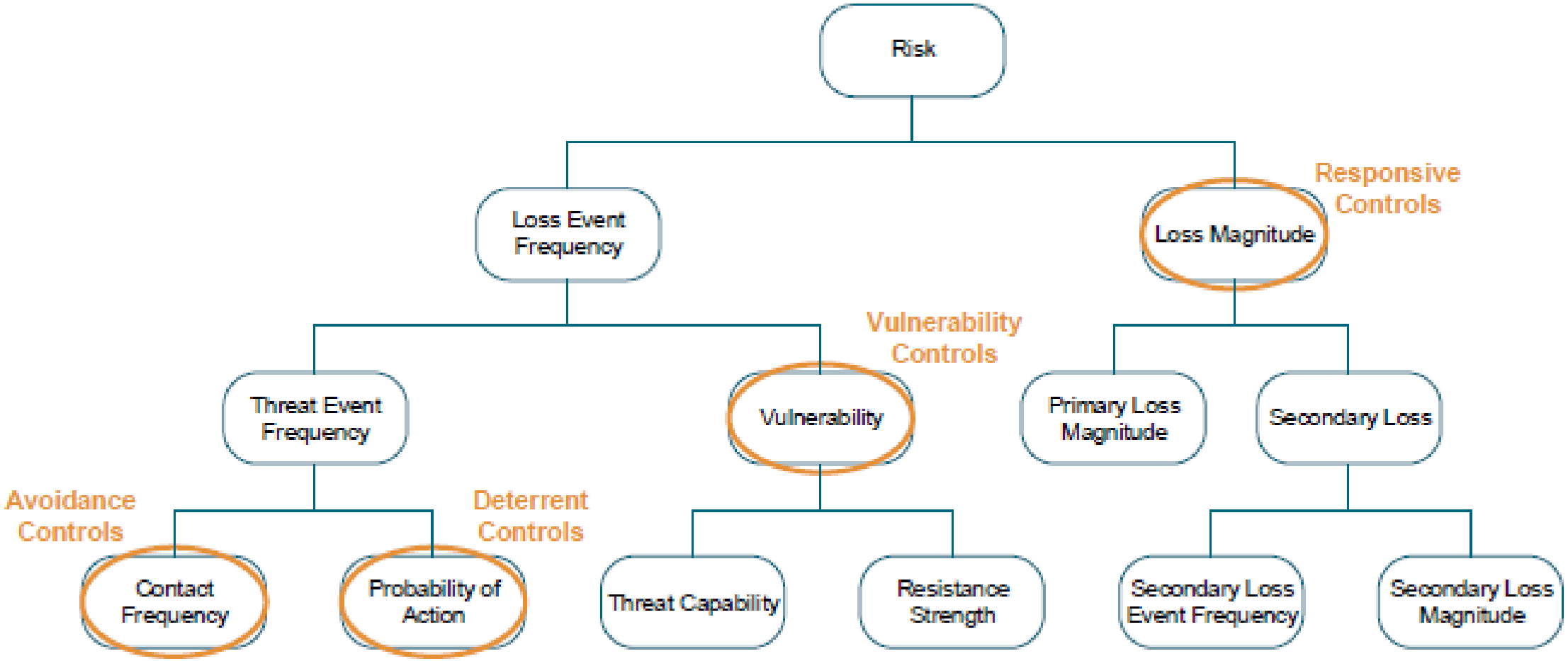
Introduction to FAIR

Open FAIR standard

The Open Group FAIR Risk Analysis (O-RA), Version 2.0 (https://pubs.opengroup.org/security/o-ra/)
The Open Group FAIR Risk Taxonomy (O-RT), Version 3.0 (https://pubs.opengroup.org/security/o-rt/)

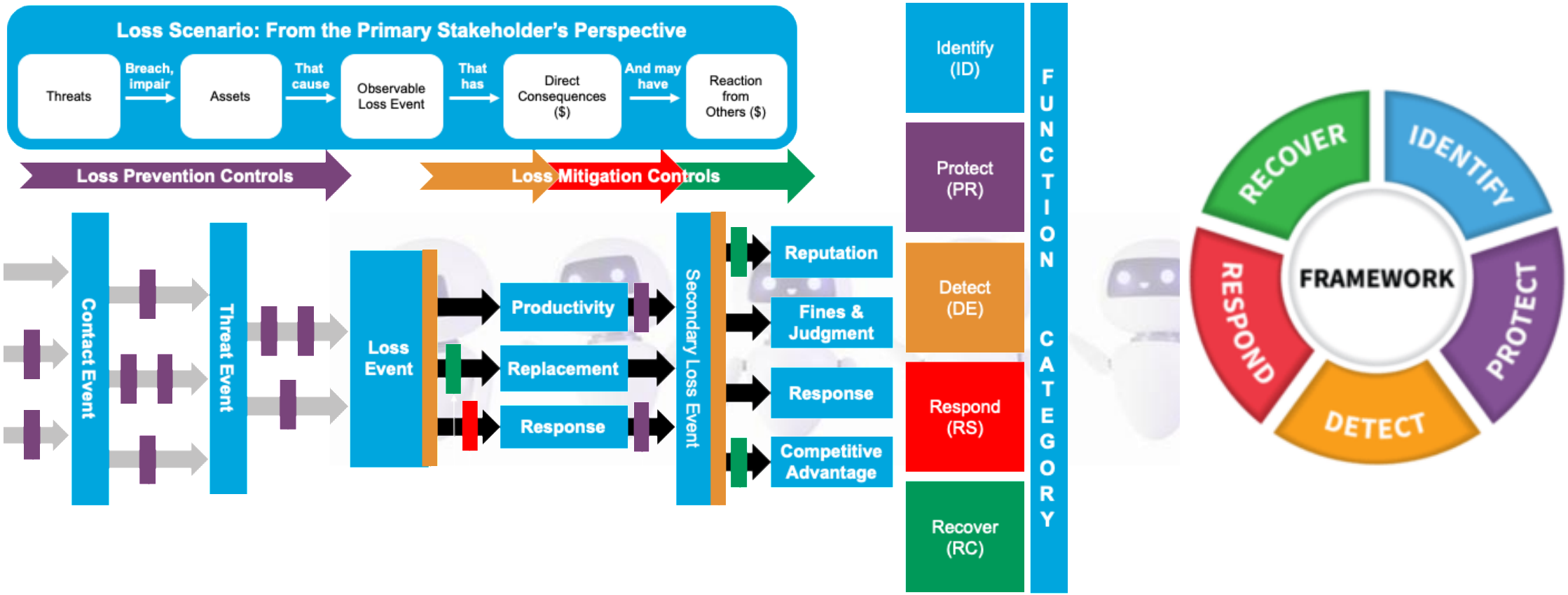


FAIR Control Categories



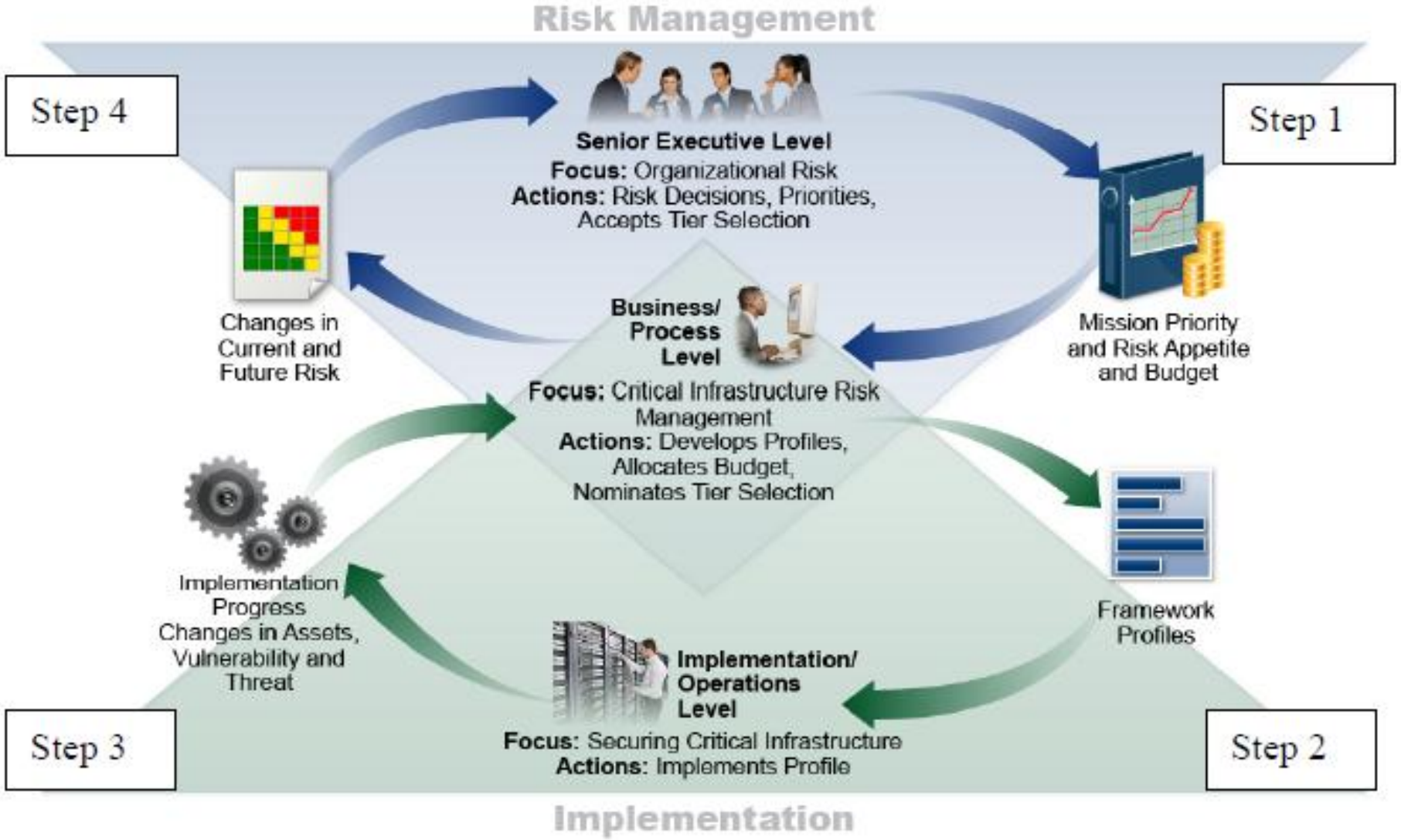
Risk Analysis (O-RA), Version 2.0.1
https://pubs.opengroup.org/security/o-ra/
https://publications.opengroup.org/c20a

Mapping to NIST CSF



Source: The Open Group FAIR Risk Analysis (O-RA), Version 2.0 (https://pubs.opengroup.org/security/o-ra/)

NISTIR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM)



Source: https://csrc.nist.gov/pubs/ir/8286/final

Consuming good risks

risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks."

Assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications—and to use readily understandable and agreed upon terms and categories such as strategic objectives, organizational priorities, decision-making processes, and risk reporting or tracking methodologies (e.g., regular risk management committee discussions and meetings).

An effective ERM program defines and communicates enterprise risk appetite so that meaningful risk tolerance statements can be created, used and monitored. Risk appetite also serves as a guidepost and reflects strategic risk direction from leadership. As adopted from COSO, OMB Circular A-123 defines risk appetite as "the broad-based amount of risk an enterprise is willing to accept in pursuit of its mission/vision." With strategic risk direction communicated to the organizational and system levels of the enterprise, cybersecurity officers can apply the guideline when establishing risk expectations at organization and system levels. Risk management strategy should also include direction regarding the risk register, such as how entries should be categorized. The use of common risk categories supports the aggregation of various types of risk across the enterprise.

What is good risk?

3.7 Considerations of Positive Risks as an Input to ERM

Planning for success is equally as important as avoiding disasters. As mentioned in Section 3.2.2, OMB states in Circular A-123 that regarding the inclusion of opportunities (positive risks) as a function of the ERM profile, "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)."

In the CSRM discipline, a significant portion of risk information is collected and reported with regard to weaknesses and threats that could result in negative consequences. However, positive risks (opportunities) also inform decisions by senior leaders for setting the risk appetite and tolerance of the enterprise. For example, conducting a SWOT analysis that considers strengths *and* weaknesses as well as threats *and* opportunities may be a useful exercise.

Risk appetite and tolerance

This document draws on ERM principles regarding integration with culture, strategy, and performance. One such principle is that an "organization must manage risk to strategy and business objectives in relation to its *risk appetite*—that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value" [8]. OMB adapted this language for government use in Circular A-123 by similarly stating risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision." Risk appetite is established by the organization's most senior-level leadership (enterprise) and serves as the guidepost for decisions such as setting strategy and selecting objectives.

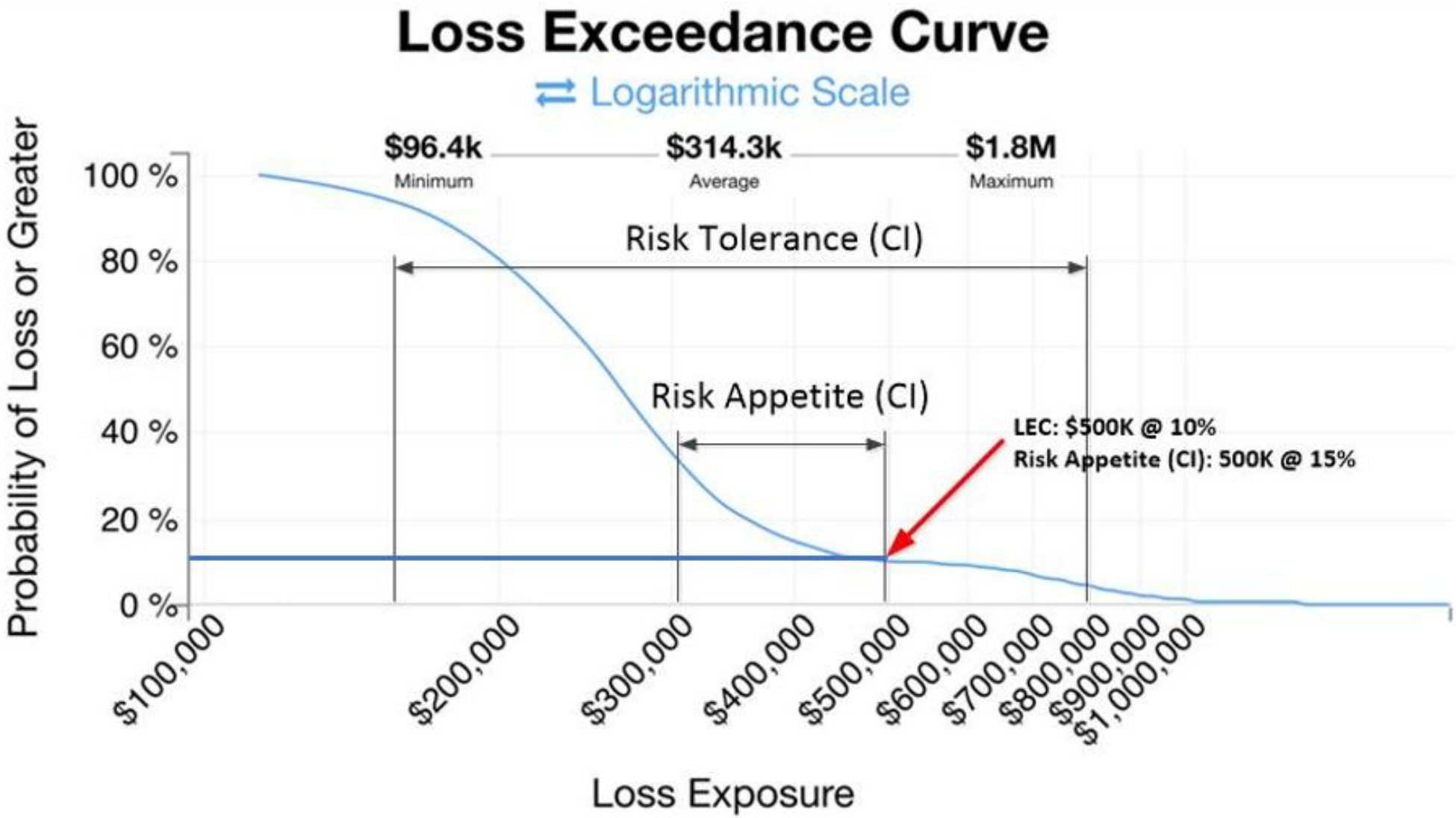
Another important ERM concept is *risk tolerance*—the organization or stakeholders' readiness to bear the remaining risk *after responding to or considering the risk* in order to achieve its objectives (while recognizing that such tolerance can be influenced by legal or regulatory requirements) [6].[10] OMB again adapted the COSO language by stating that risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives."

Risk appetite and tolerance

appetite is narrower, stating: "Email services shall not be interrupted more than five minutes during core hours."

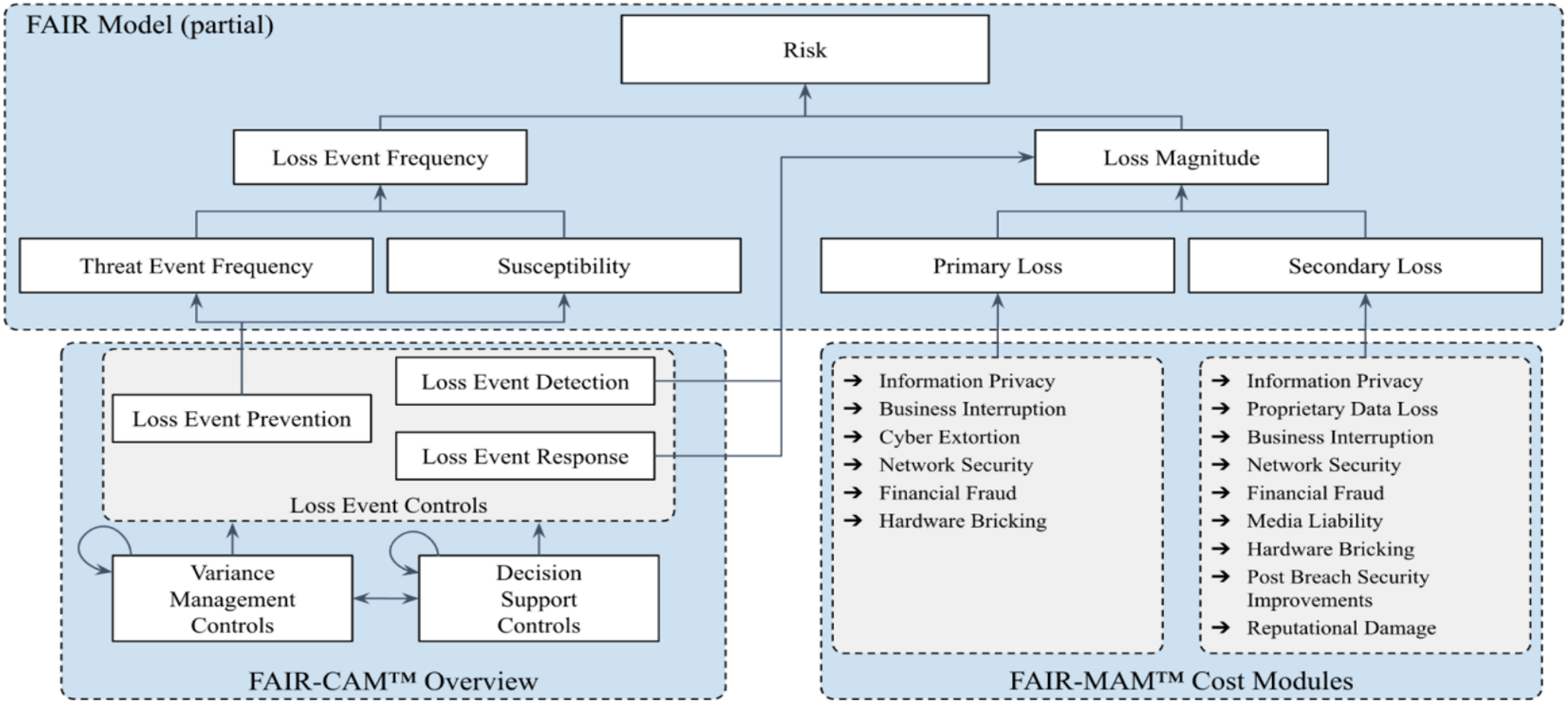
Senior enterprise executives provide risk guidance (including advice regarding mission priority, risk appetite and tolerance guidance, and capital and operating budgets to manage known risks) to the organizations within their purview. Risk appetite and risk tolerance statements are the usual means for communicating this guidance. Organizations then manage and monitor processes that properly balance the risks and resource allocation with the value created by information and technology. Measurements (e.g., from key risk indicators, or KRIs) demonstrate where risk tolerances have been exceeded or validate that the enterprise is operating within the defined appetite. A subsequent report in this series (NISTIR 8286A) will provide detailed examples of risk appetite and risk tolerance statements and how they are interrupted and applied with the associated risk defined, managed, and communicated back to executive management via the risk register.

Risk Appetite



Source: https://www.linkedin.com/pulse/building-apra-cps-234-compliance-template-denny-wan/

Framework for Effective Cyber Risk Management



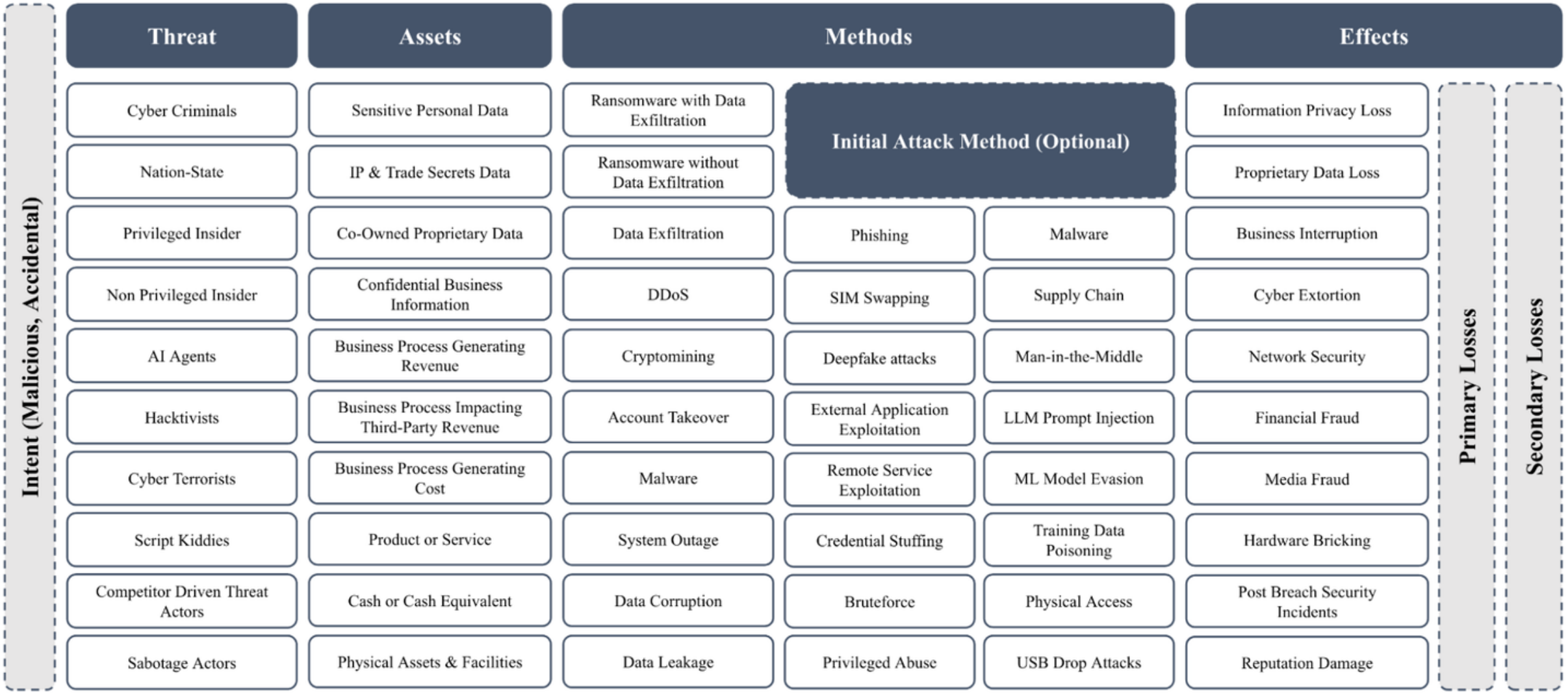
Source: https://www.fairinstitute.org/blog/integrating-fair-models-a-unified-framework-for-cyber-risk-management

FAIR Cyber Risk Scenario Taxonomy (An Analyst's Guide)

- **Incorrectly Defined Risk Scenarios**: These scenarios lack specificity and fail to reflect real-world situations, hindering their applicability to actual risk assessments.
- **Irrelevant Risk Scenarios**: These scenarios focus on hypothetical or low-impact risks, diverting attention from more critical threats and potential losses.
- **Excessive Number of Risk Scenarios**: Overloading the risk register with too many scenarios creates unnecessary complexity and impedes actionable insights.
- **Poorly Measured Risk Scenarios**: These scenarios lack effective quantification of potential impact and likelihood, making it difficult to prioritize risks and allocate resources appropriately.

Source: https://www.fairinstitute.org/resources/fair-cyber-risk-scenario-taxonomy

FAIR Cyber Risk Scenario Taxonomy



Source: https://www.fairinstitute.org/blog/announcing-a-fair-taxonomy-for-cyber-risk-scenarios

Calibrating the data – Doug Hubbard AIE

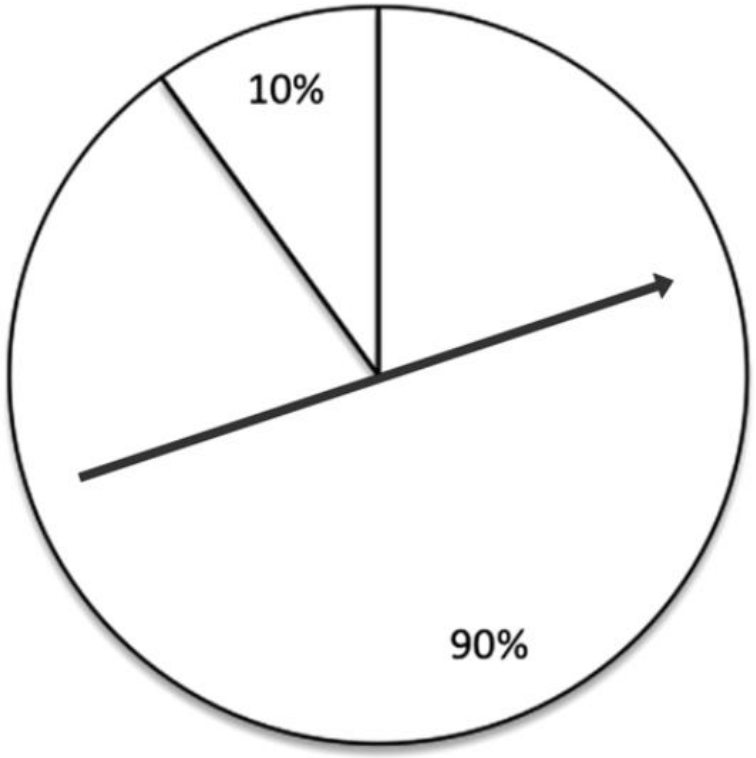
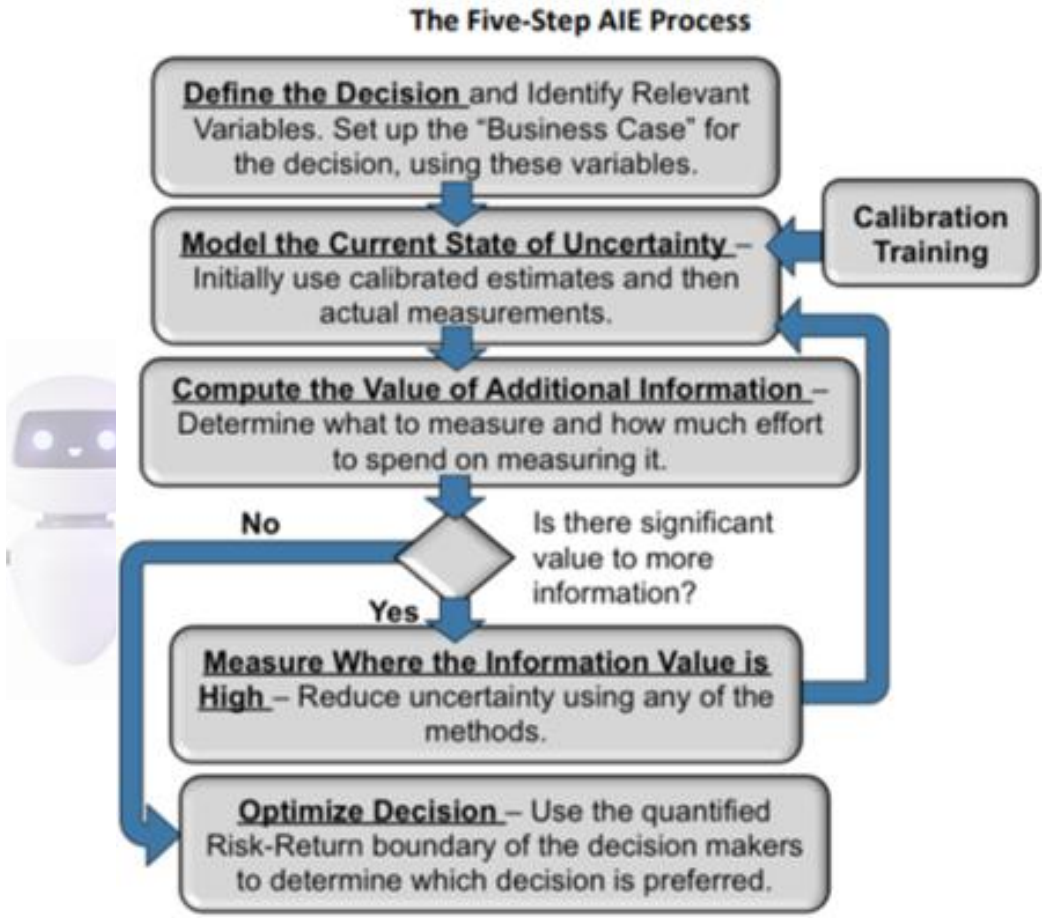
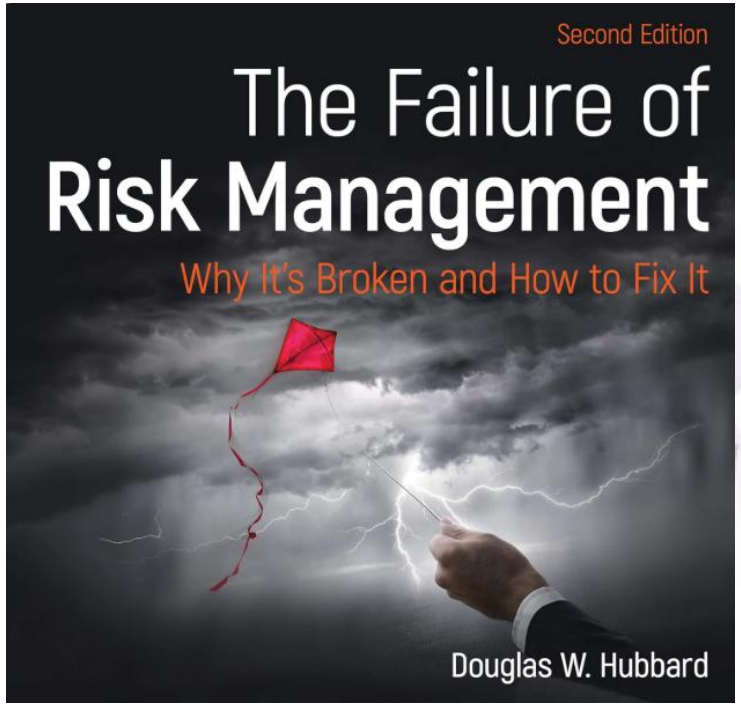


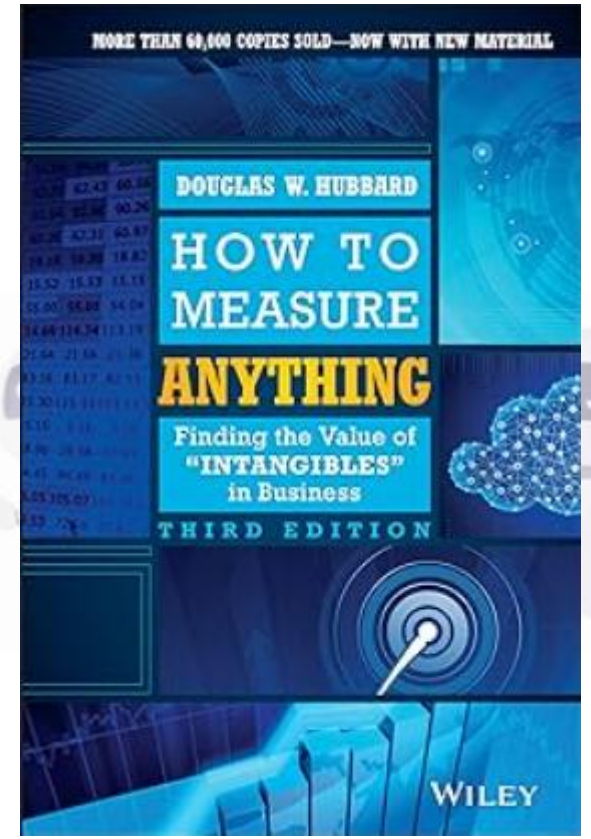
FIGURE 5.5 An equivalent bet test wheel.

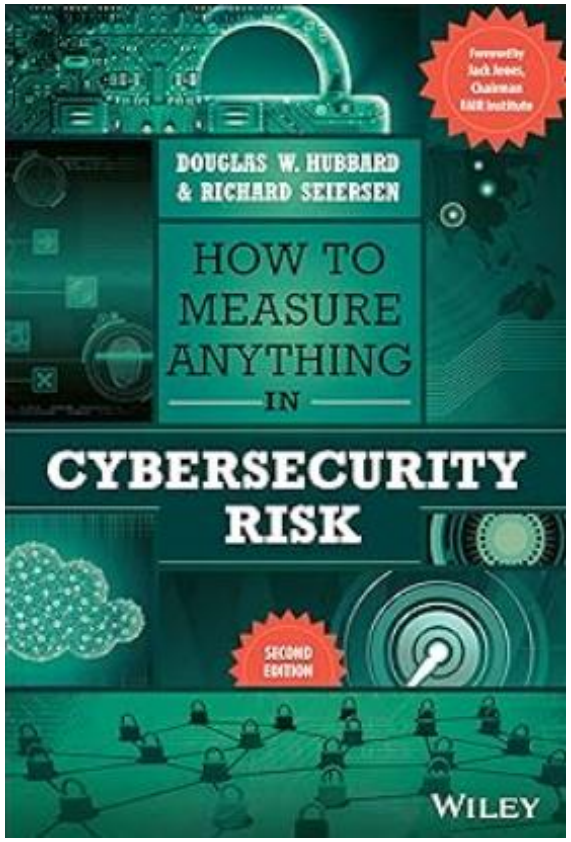


Source: https://hubbardresearch.com/about/applied-information-economics/

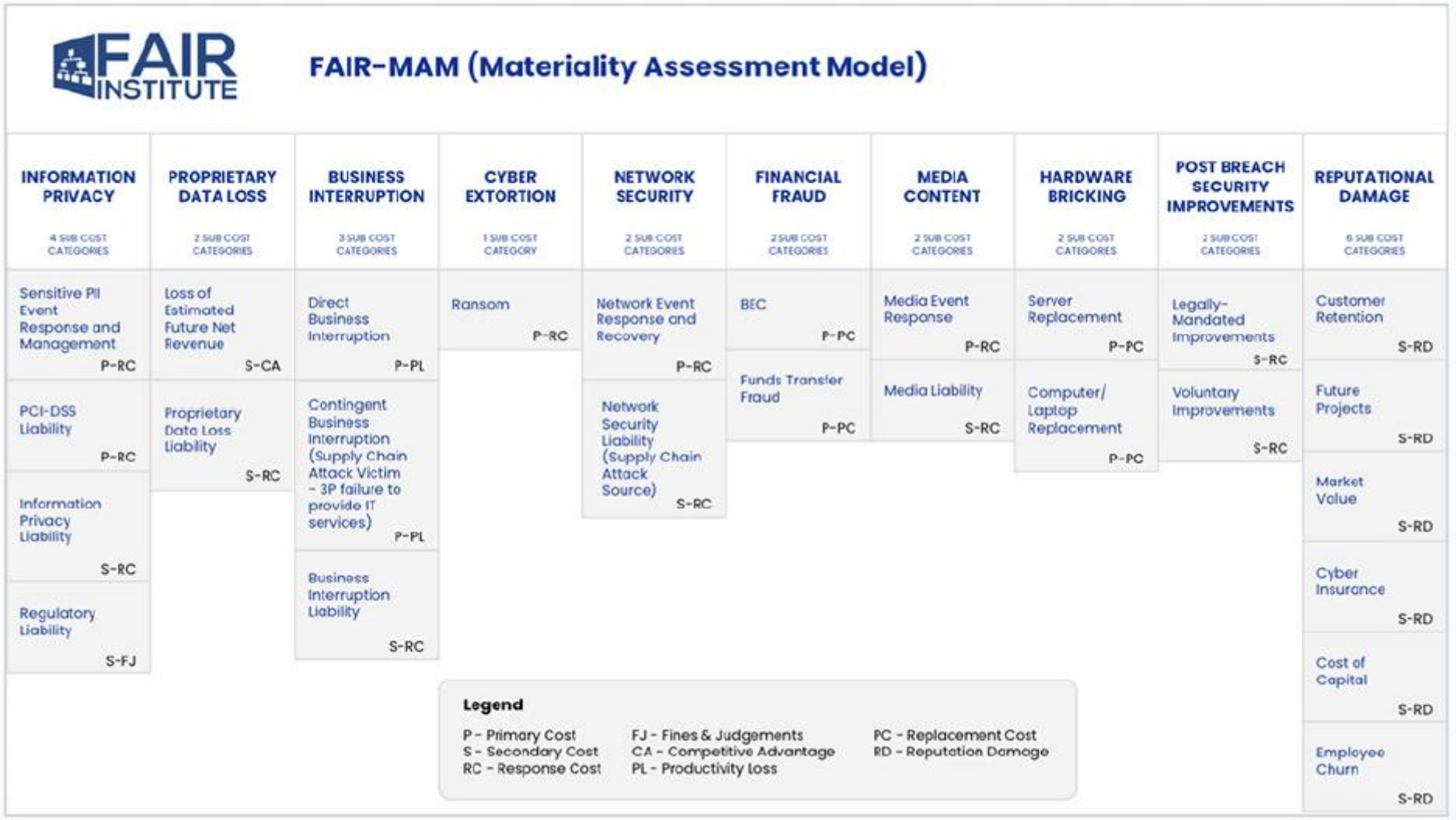
How to Measure Anything in Cybersecurity Risk







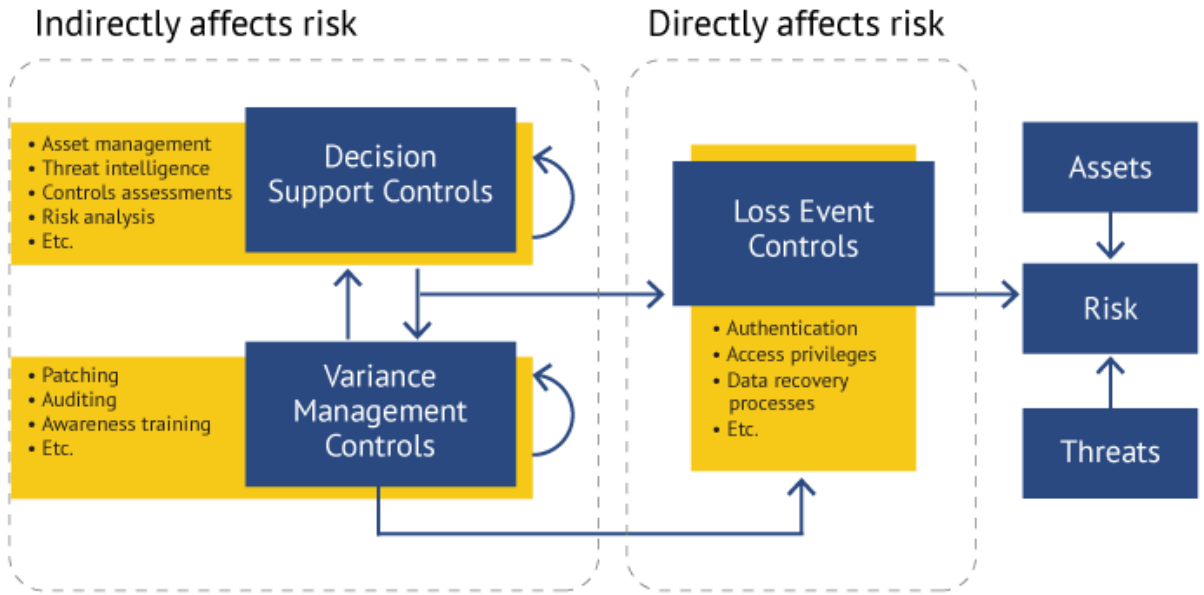
Materiality, Materiality, Materiality



https://www.fairinstitute.org/resources/fair-mam

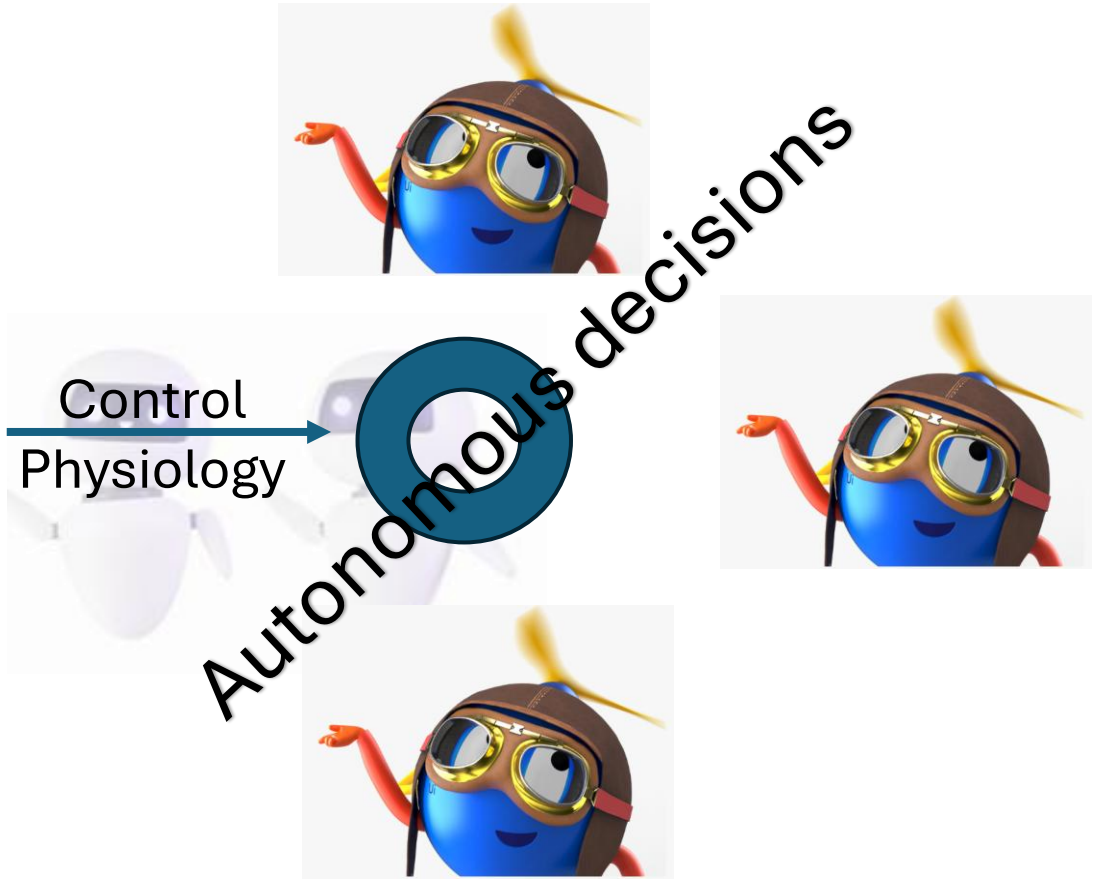
REASONABLE SECURITY

Modelling Agentic AI risk with FAIR-CAM

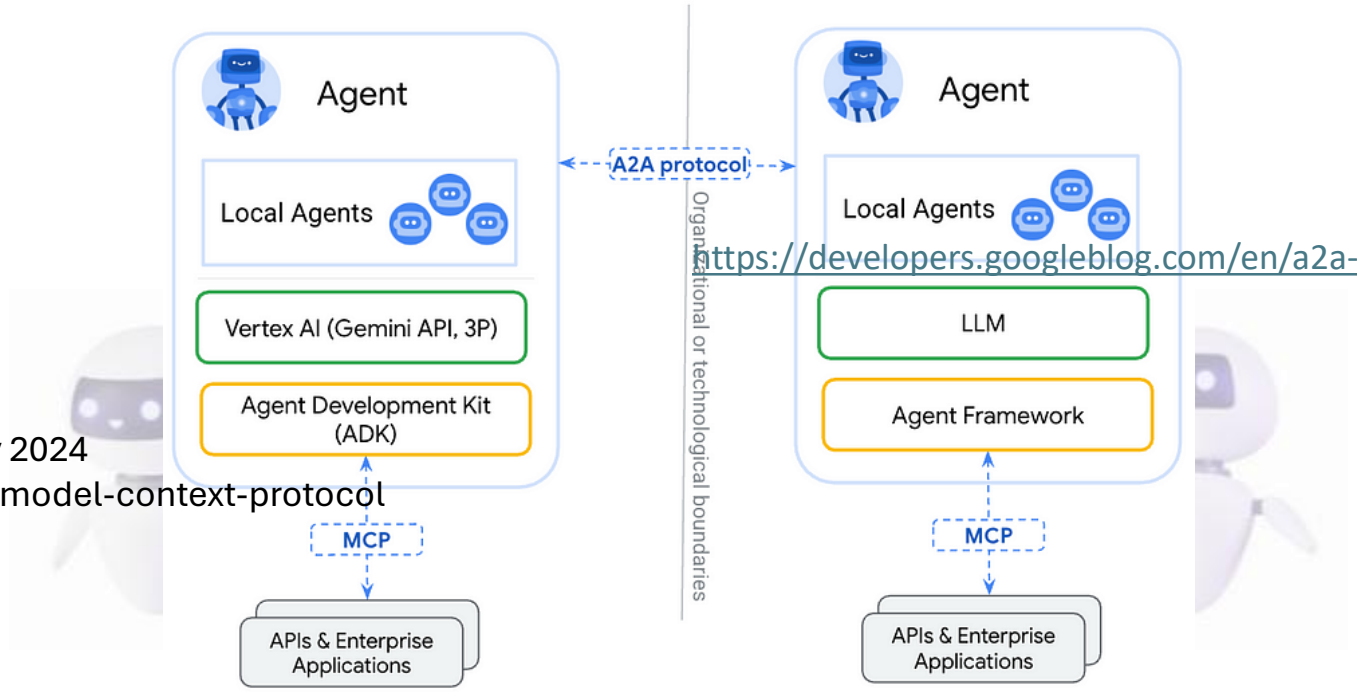


FAIR Controls Analytics Model™ (FAIR-CAM™)

https://www.fairinstitute.org/fair-controls-analytics-model



Model Context



Model Context Protocol (MCP) Nov 2024
https://www.anthropic.com/news/model-context-protocol

Google Agent2Agent Protocol (A2A)
https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/

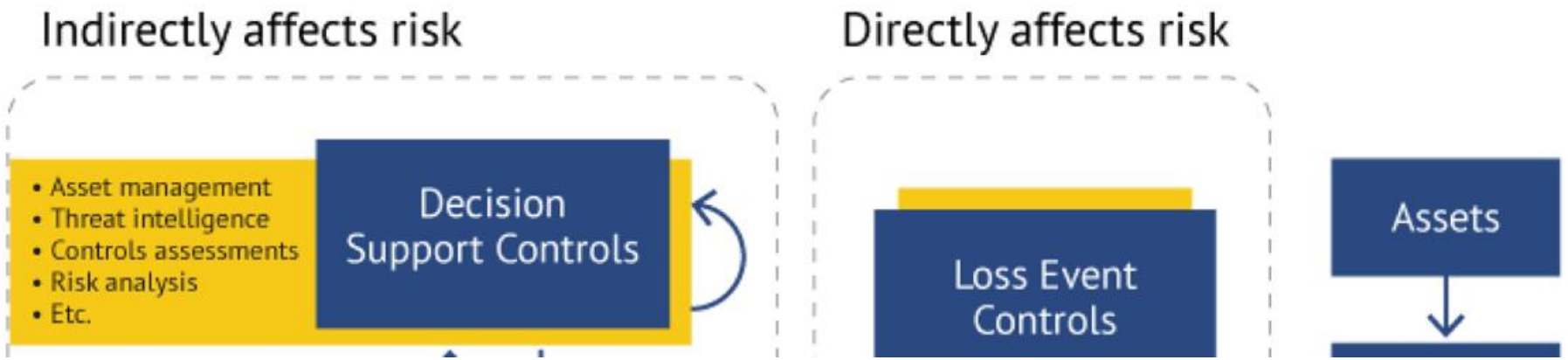
Source: Unlock Collaborative, agent-to-agent scenarios with a new open protocol
https://google.github.io/A2A/#/

Taming Agentic AI risks with FAIR-CAM

ARTIFICIAL INTELLIGENCE (AI), FAIR FRAMEWORK

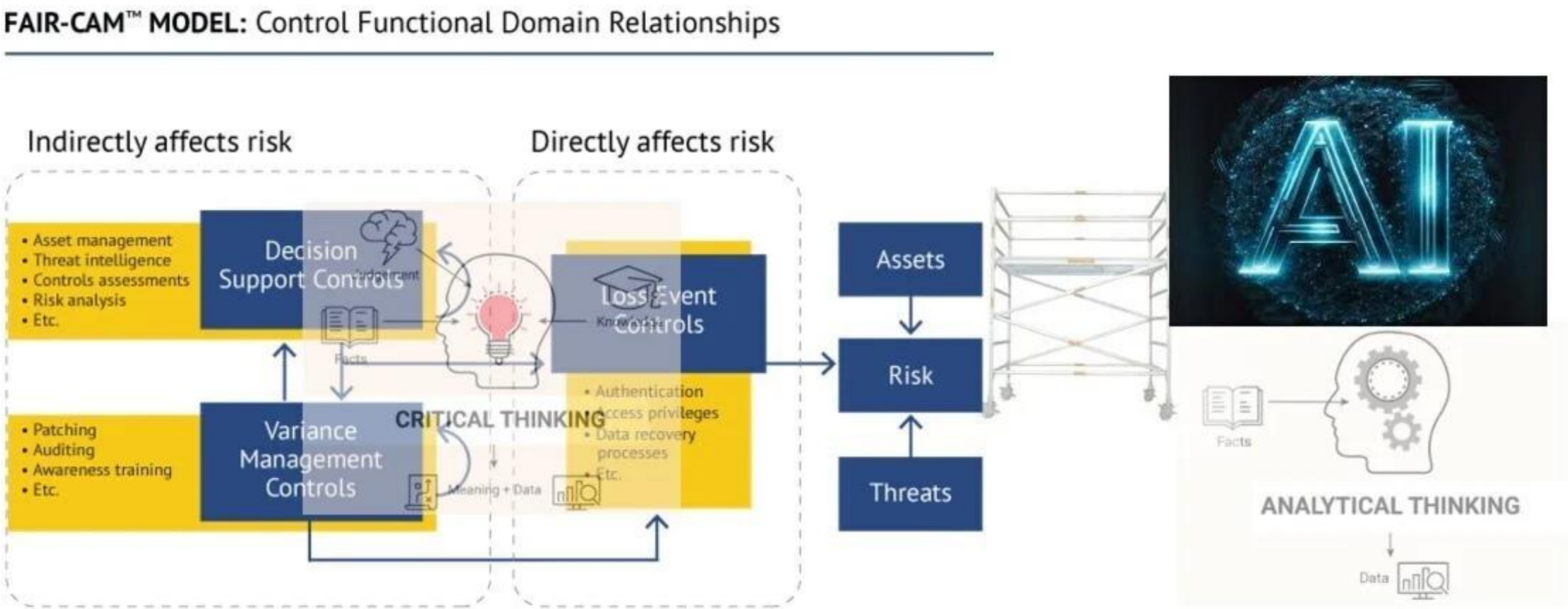
Taming Agentic AI risks with FAIR-CAM

MAR 11, 2025 10:02:49 AM / DENNY WAN



Reference: https://www.fairinstitute.org/blog/taming-agentic-ai-risks-with-fair-cam

Scaffolding for Critical Thinking



Source: https://www.fairinstitute.org/blog/fair-cam-scaffolding-for-critical-thinking

Simulation exercise