

# Measuring KRI using the FAIR-U Workbook



**Risk (Loss Exposure)**

Minimum	Average	Maximum
\$0	\$7,245,140	\$33,091,215

likelihood of Any Loss: 99.2%

Min, Average, Max values here are calculated using 10,000 Monte Carlo simulations of LEF and LM from below.

**Risk Analysis Name**

Payment System Data Breach Risk Assessment

Analysis Created: March 16, 2025      Last Updated: March 16, 2025

Choose the level at which you want to enter LEF factors:

5. CF & PoA + TCap & RS (Lowest Level)

**Loss Event Frequency (LEF)**

Minimum	Average	Maximum
0.0	6.6	26.0

Confidence: N/A

Min, Average, and Max above are based on 10,000 Monte Carlo simulations of TEF and Susc.

**Loss Magnitude (LM)**

Minimum	Average	Maximum
\$424,371	\$1,104,781	\$1,810,808

Confidence: N/A

Min, Most Likely, Max and Confidence values here are calculated using the Monte Carlo Simulations of PL and SL from below.

**Recalculate Workbook**

**See Risk Report**

**Beta PERT & Monte Carlo Sims**

Report Feedback to: [FAIRU@FAIRInstitute.org](mailto:FAIRU@FAIRInstitute.org)

**Threat Event Frequency (TEF)**

Minimum	Average	Maximum
0.8	9.8	37.2

Confidence: N/A

Min, Average, and Max above are based on 10,000 Monte Carlo simulations of CF and PoA.

**Susceptibility (Susc)**

Minimum	Average	Maximum
0%	67%	100%

Confidence: N/A

Min, Average, and Max above are based on 10,000 Monte Carlo simulations of TCap and RS.

**Primary Loss (PL)**

Minimum	Most Likely	Maximum
\$250,000	\$950,000	\$2,250,000

Confidence: Various

Min, Most Likely, Max and Confidence values here are entered by you and used in a Monte Carlo simulation to calculate PL.

**Secondary Loss (SL)**

Minimum	Average	Maximum
\$6	\$58,532	\$228,498

Confidence: N/A

Min, Most Likely, Max and Confidence values here are calculated using the Monte Carlo Simulations of SLEF and SLM from below.

**Contact Frequency (CF)**

Minimum	Most Likely	Maximum
5.0	20.0	50.0

Confidence: Medium

Min, Most Likely, Max and Confidence values here are provided by you and used in 10,000 Monte Carlo simulations to calculate CF.

**Probability of Action (PoA)**

Minimum	Most Likely	Maximum
10%	40%	90%

Confidence: Medium

Min, Most Likely, Max and Confidence values here are provided by you and used in 10,000 Monte Carlo simulations to calculate PoA.

**Threat Capability (TCap)**

Minimum	Most Likely	Maximum
20%	70%	90%

Confidence: High

Min, Most Likely, Max and Confidence values here are provided by you and used in 10,000 Monte Carlo simulations to calculate TCap.

**Resistance Strength (RS)**

Minimum	Most Likely	Maximum
20%	60%	95%

Confidence: Medium

Min, Most Likely, Max and Confidence values here are provided by you and used in 10,000 Monte Carlo simulations to calculate RS.

**Secondary Loss Event Frequency (SLEF)**

Minimum	Most Likely	Maximum
0%	25%	100%

Confidence: Low

Min, Most Likely, Max and Confidence values here are entered by you and used in a Monte Carlo simulation to calculate SLEF.

**Secondary Loss Magnitude (SLM)**

Minimum	Most Likely	Maximum
\$0	\$100,000	\$400,000

Confidence: 0

Min, Most Likely, Max and Confidence values here are entered by you and used in a Monte Carlo simulation to calculate SLM.

- Instructor: Denny Wan
- Date: Thu 22<sup>nd</sup> 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](mailto:dwan@reasonablesecurity.org.au)

LinkedIn: <https://www.linkedin.com/in/wandenny/>

Twitter: @denny\_wan

# Measure what needs to be managed

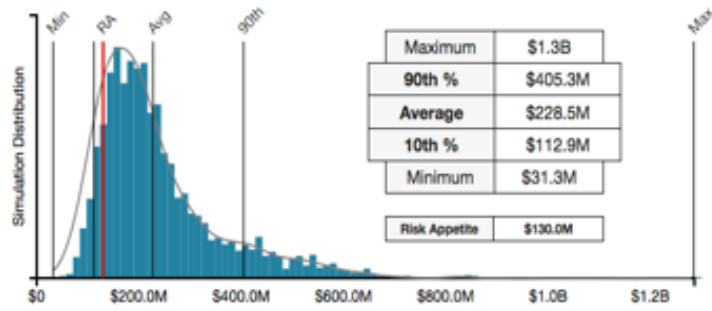
## THE COMMUNICATION CHALLENGE



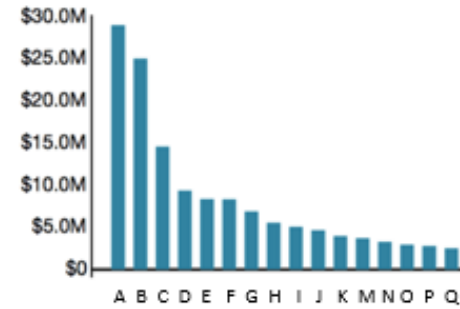
Source: The FAIR Institute

# Communicating Cyber Risk in dollar value

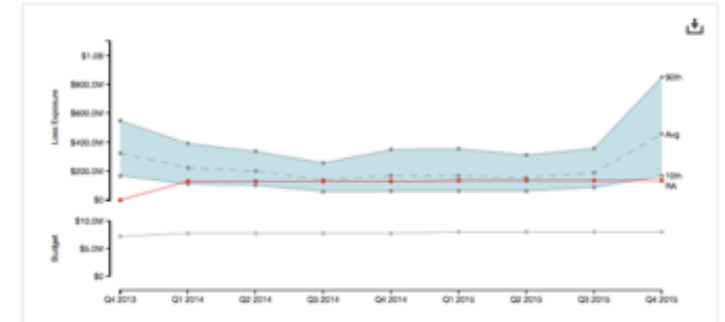
## "HOW MUCH RISK DO WE HAVE?"



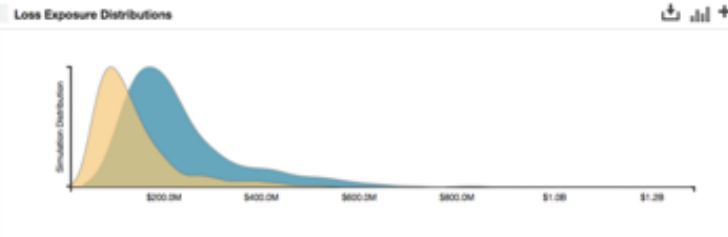
## "WHAT ARE OUR TOP RISKS?"



## "HOW IS OUR RISK TRENDING VS. APPETITE?"

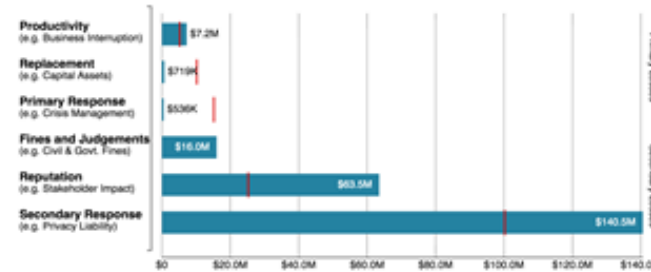


## "HAVE WE REDUCED RISK?"

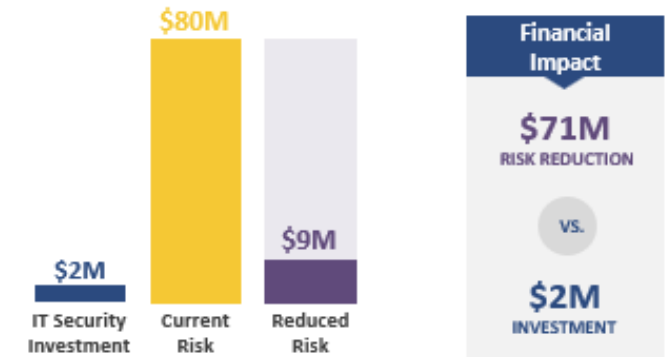


Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum
Annual Baseline Enterprise Analysis	Quarter 1 2014	\$31.3M	\$112.9M	\$228.5M	\$405.3M	\$1.3B
Quarterly Updated Enterprise Analysis	Quarter 3 2014	\$9.4M	\$58.3M	\$137.8M	\$254.7M	\$781.5M

## "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.




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

# Using the FAIR-U Workbook



© FAIR Institute. All rights reserved.



**Workbook Version: 1.3 (Beta)**      **[Got Feedback: Email us at [FAIRU@FAIRInstitute.org](mailto:FAIRU@FAIRInstitute.org)]**      **Release Date: April 28, 2025**

**License:**  
This FAIR-U for Learners Workbook is designed to support educating (learning needs) FAIR practitioners, students, and others who want to better understand FAIR and its applications. To facilitate this purpose, this work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License](https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode) (available at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To clarify the application of this license:

- You are authorized to copy and redistribute this workbook for use by yourself, within your organization, and outside of your organization, solely for non-commercial purposes, provided that:
  - Appropriate credit is given to the FAIR Institute as the source.
  - A link to the license is provided.
- You may not remix, transform, or modify this workbook, nor distribute derivative materials based on this workbook.
- Users of the FAIR-U for Learners Workbook should refer to <https://www.fairinstitute.org/fair-u-workbook> when citing or referencing the workbook to ensure alignment with the most up-to-date guidance.
- Any commercial use of this workbook requires prior approval from the FAIR Institute.

By using this workbook, you agree to these terms as outlined in the Creative Commons BY-NC-ND 4.0 license.

**Disclaimer:**  
The FAIR-U Workbook for Learners is provided "as-is" for educational purposes. It is designed to help individuals explore and understand the Factor Analysis of Information Risk (FAIR) model through structured exercises and guided analysis.

By using this workbook, you acknowledge and agree that:


- The workbook is not intended for use in real-world risk analysis, decision-making, or commercial applications.
- The workbook is not warranted to be accurate, complete, or suitable for any specific purpose.
- The FAIR Institute assumes no responsibility or liability for any outcomes, errors, or decisions made based on the use of this workbook.
- All macros and formulas included in this workbook are provided for convenience and should be reviewed before enabling or using them. Users may disable macros at their discretion.

The FAIR Institute may update or discontinue this workbook at any time without notice. Users should refer to [www.fairinstitute.org/fair-u-workbook](http://www.fairinstitute.org/fair-u-workbook) for the latest version and updates.

**I Have Read and Agree!**      *In clicking this button, the workbook will reveal all worksheets and take you to the instructions tab to begin performing a scenario risk assessment. Also, in taking any act to disable macros or protections (locked cells or sheets) or otherwise reveal the worksheets in this workbook, you agree to the terms above.*

< >    **START HERE**    Instructions    Scenario Setup    FAIR Model    LEF    Susc    TCap    RS    TEF    ...    +    :

# Using the FAIR-U Workbook

**SCENARIO SETUP**  
© FAIR Institute. All rights reserved.

[Go to FAIR Model](#) [Reset Workbook](#) [Recalculate Workbook](#)

**Analysis Created:**  **Last Updated:**

**Currency:**

**Analysis Name:**

**Purpose:**

**Threat:**

<b>Name:</b>	<input type="text" value="Internal System Compromise"/>
<b>Description:</b>	<input type="text" value="A malicious actor is able to successfully identify a vulnerable system, deliver a malicious payload, exploit that system to gain a foothold into Oracle, move laterally, conduct actions on the objective, and exfiltrate data with a"/>
<b>Type:</b>	<input type="text" value="Malicious"/>
<b>Contact:</b>	<input type="text" value="Intentional"/>
<b>If Type is Malicious, the following characteristics may be used.</b>	
<b>Motive / intent:</b>	<input type="text" value="Profitseeking"/>
<b>Sponsorship:</b>	<input type="text" value="State sponsored"/>
<b>Preferred targets or target characteristics:</b>	<input type="text" value="Infrastructure assets"/>
<b>Capability:</b>	<input type="text" value="High skilled and trained"/>
<b>Personal risk tolerance:</b>	<input type="text" value="Imprisonment"/>

**Asset:**

Enter the date the analysis was created. Update with the last updated date.

Choose the currency to be used for this scenario. No currency translation will be performed.

Give your analysis a descriptive and unique name. Consider including a combination of Asset, Threat Actor, Initial Attack Method, and Loss Outcome in the name.

Describe why you are performing this analysis for the business. What goal(s) do you hope to achieve? Why is the participate combination of Assets, Threat Actors, and Initial Attack Method being evaluated?

Name and describe the individuals, groups, or entities with the capability, opportunity, and motive to harm the organization's assets. They can be external (e.g., nation-states, cybercriminals), internal (e.g., employees, contractors), or non-human (e.g., malware, natural disasters).

Choose one: Malicious, Accidental, Error, Failure, Natural

Choose one: Random, Regular, Intentional

Examples: Profitseeking; ideology; nationalism; disruption of national infrastructure; create fear and uncertainty; steal cryptocurrency

Examples: State sponsored; self-funded via cybercrime


Examples: Entities that are well-known to the nation's citizenry; organizations in the financial services sector; infrastructure assets; companies providing critical services

Describe (qualitatively) the range of skills likely possessed by members of this threat actor or threat community.


Describe the level of personal risk (e.g., civil fines; criminal fines; imprisonment; injury; death) the threat actors or community are likely be willing to take.

Describe the asset in terms of its meaningful business value and potential for financial loss. Assets may be tangible (e.g., cash, facilities) or intangible (e.g., data, brand reputation, business processes), and their value often extends beyond what is

[START HERE](#) [Instructions](#) [Scenario Setup](#) [FAIR Model](#) [LEF](#) [Susc](#) [TCap](#) [RS](#) [TEF](#) ... +



# Using the FAIR-U Workbook



**FAIR-U Workbook for Learners**  
© FAIR Institute. All rights reserved.

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
<b>AnalysisName</b>	Payment System Data Breach Risk Assessment	Intellectual Property Theft Risk Assessment	Cloud Data Exposure Risk Assessment
<b>AnalysisAsset</b>	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.
<b>AnalysisCreateDate</b>	16/03/2025	16/03/2025	16/03/2025
<b>AnalysisCurrency</b>	Dollars (All Countries)	British Sterling Pounds	Euros
<b>AnalysisEffect</b>	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.
<b>AnalysisMethod</b>	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.
<b>AnalysisMotiveIntent</b>	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.
<b>AnalysisPeriodEnd</b>	31/12/2025	31/12/2025	31/12/2025
<b>AnalysisPeriodStart</b>	1/01/2025	1/01/2025	1/01/2025
<b>AnalysisPurpose</b>	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.
<b>AnalysisThreatCapability</b>	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.

< > ...

SLEF

SLM

Risk Report

Beta PERT & Monte Carlo


Test Data Generator

Data Migrator

+ : ◀

Test data generator requires Excel Macro to be enabled

# Using the FAIR-U Workbook



**FAIR-U Workbook for Learners**  
© FAIR Institute. All rights reserved.

Recalculate Workbook

Copy Current Values  
Into Migration Data Column

Update with Migration Data  
Use with caution! Overwrites ALL values.

Named Range	Current Values of User Data	Migration Data
<b>AnalysisName</b>	Reza Khaleeli	Reza Khaleeli
<b>AnalysisAsset</b>	Material Nonpublic Information in the form of highly sensitive data, including a broad array of files related to our services and customers, all in a human intelligible form (e.g., Microsoft Word, Excel, PowerPoint files). These files are all proprietary information.	Material Nonpublic Information in the form of highly sensitive data, including a broad array of files related to our services and customers, all in a human intelligible form (e.g., Microsoft Word, Excel, PowerPoint files). These files are all proprietary information.
<b>AnalysisCreateDate</b>	45750	3/04/2025
<b>AnalysisCurrency</b>	Dollars (All Countries)	Dollars (All Countries)
<b>AnalysisEffect</b>	A State sponsored threat agent maliciously gains access to, and misuses, highly sensitive OCI information about OCI Services and its customers, with the intent to use that information to target OCI customers for further attacks and exploitation for monetary gain. When this event occurs, OCI will suffer primary productivity and response losses, and OCI may also suffer secondary reputation and	A State sponsored threat agent maliciously gains access to, and misuses, highly sensitive OCI information about OCI Services and its customers, with the intent to use that information to target OCI customers for further attacks and exploitation for monetary gain. When this event occurs, OCI will suffer primary productivity and response losses, and OCI may also suffer secondary reputation and
<b>AnalysisMethod</b>	Common attack vectors include social engineering attacks, credential theft, vulnerability exploits, and insufficient protection	Common attack vectors include social engineering attacks, credential theft, vulnerability exploits, and insufficient protection
<b>AnalysisMotiveIntent</b>	Profitseeking	Profitseeking
<b>AnalysisPeriodEnd</b>	0	0/01/1900
<b>AnalysisPeriodStart</b>	0	0/01/1900
<b>AnalysisPurpose</b>	Testing of workbook	Testing of workbook
<b>AnalysisThreatCapability</b>	High skilled and trained	High skilled and trained
<b>AnalysisThreatContact</b>	Intentional	Intentional
<b>AnalysisThreatDescription</b>	A malicious actor is able to successfully identify a vulnerable system, deliver a malicious payload, exploit that system to gain a foothold into Oracle, move laterally, conduct actions on the objective, and exfiltrate data with a very low chance of being detected by existing	A malicious actor is able to successfully identify a vulnerable system, deliver a malicious payload, exploit that system to gain a foothold into Oracle, move laterally, conduct actions on the objective, and exfiltrate data with a very low chance of being detected by existing
<b>AnalysisThreatName</b>	Internal System Compromise	Internal System Compromise
<b>AnalysisThreatRiskTolerance</b>	Imprisonment	Imprisonment
<b>AnalysisThreatSponsor</b>	State sponsored	State sponsored
<b>AnalysisThreatTargets</b>	Infrastructure assets	Infrastructure assets
<b>AnalysisThreatType</b>	Malicious	Malicious
<b>AnalysisUpdateDate</b>	45750	3/04/2025
<b>CFConfidence</b>	High	High
<b>CFMaximum</b>	12	12
<b>CFMinimum</b>	3	3
<b>CFMostLikely</b>	6	6

Data Migrator requires Excel Macro to be enabled

< > ...

SLEF

SLM

Risk Report

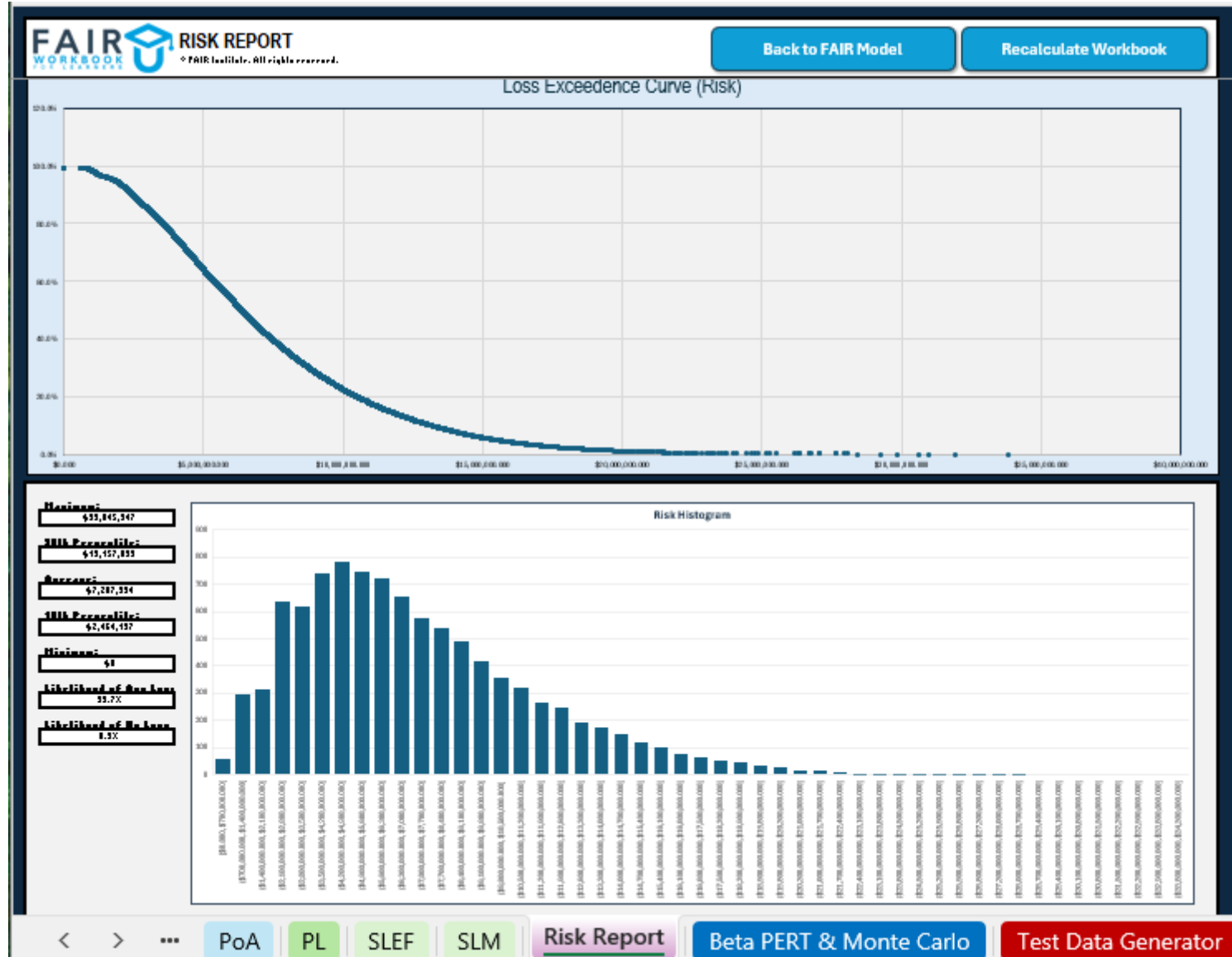
Beta PERT & Monte Carlo

Test Data Generator

Data Migrator

+ ⋮ ◀

# 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

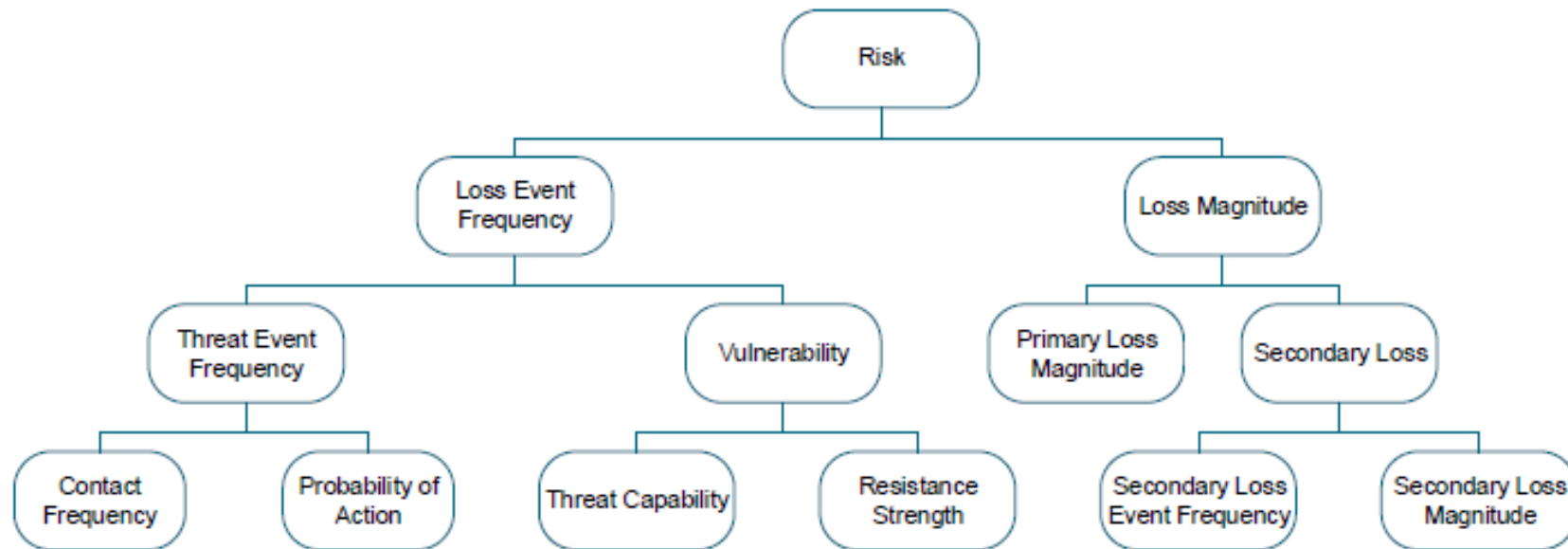
- Define Risk Categories – Identify the specific risks relevant to the organization
- Select Measurable Indicators – financial ratios, incident rates, etc
- Set Thresholds & Benchmarks – Establish acceptable risk levels and trigger points for action
- Monitor Trends Over Time – Track KRIs regularly to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

# Introduction to FAIR

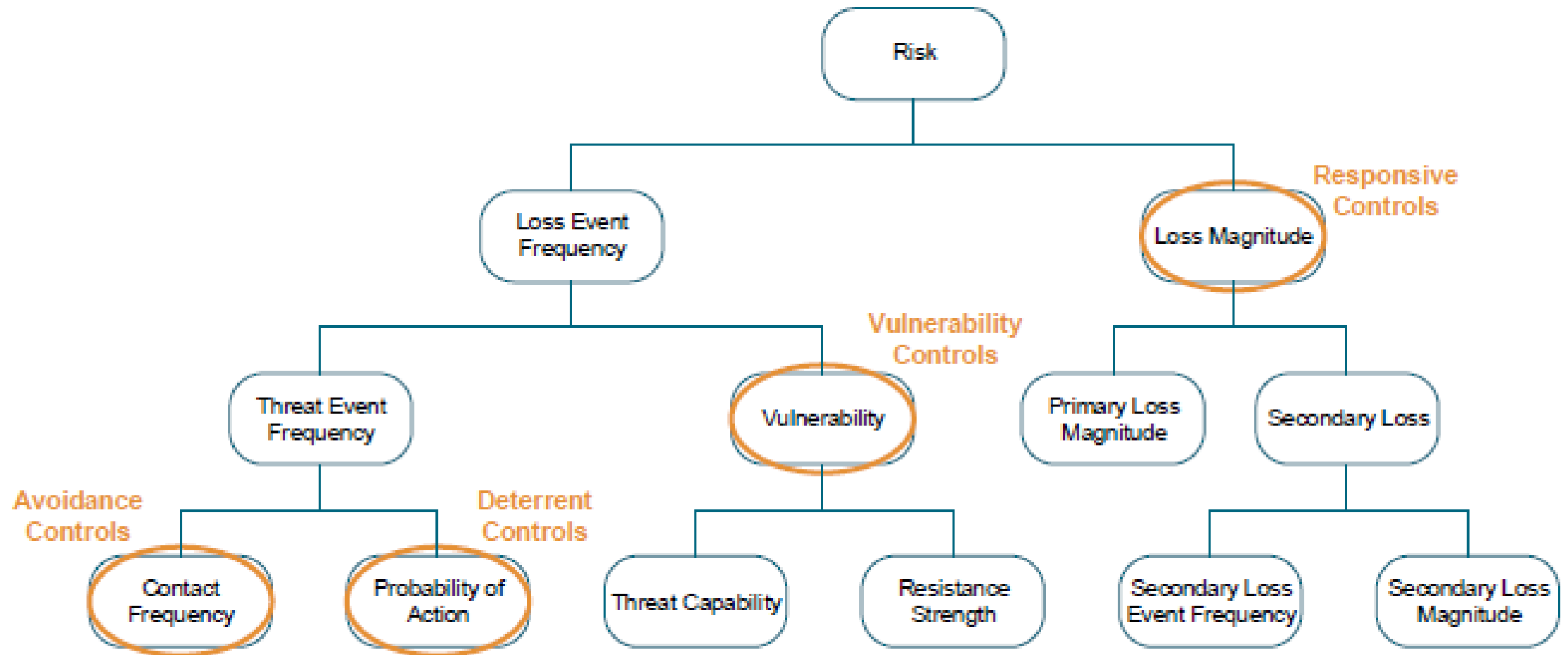
## Open FAIR standard

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

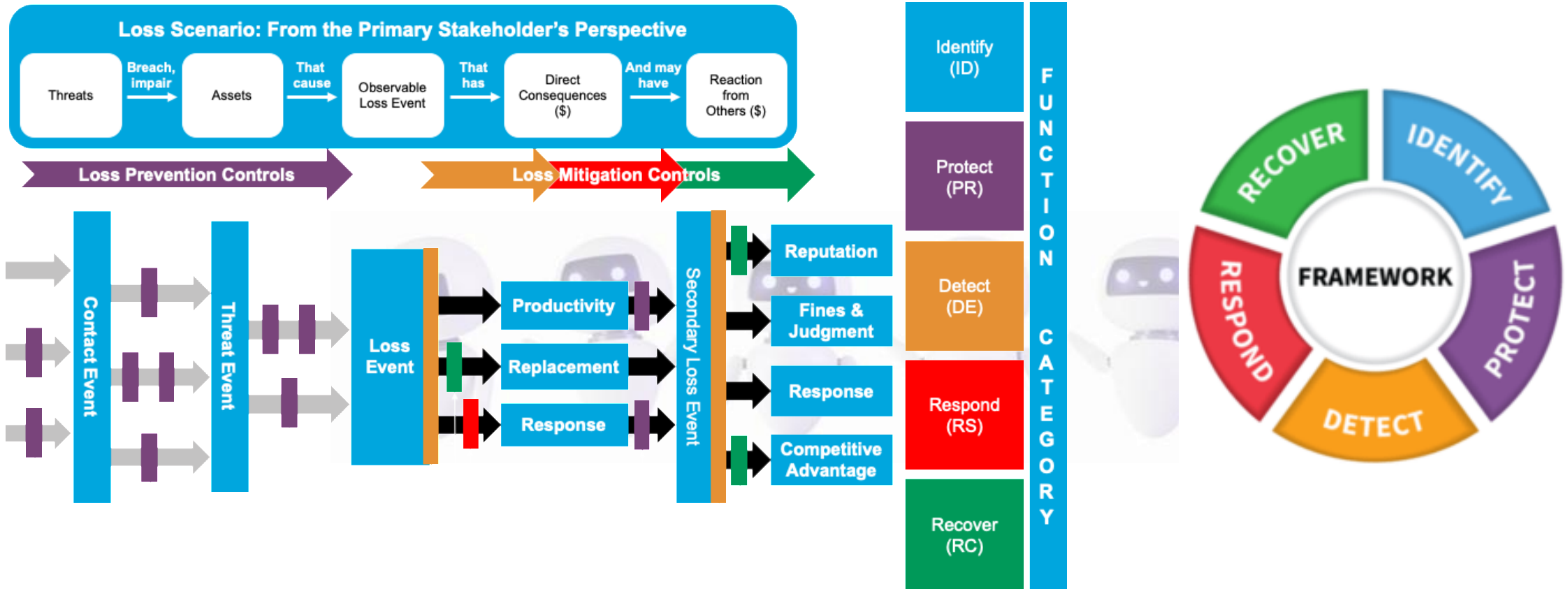


Risk Analysis (O-RA), Version 2.0.1

<https://pubs.opengroup.org/security/o-ra/>

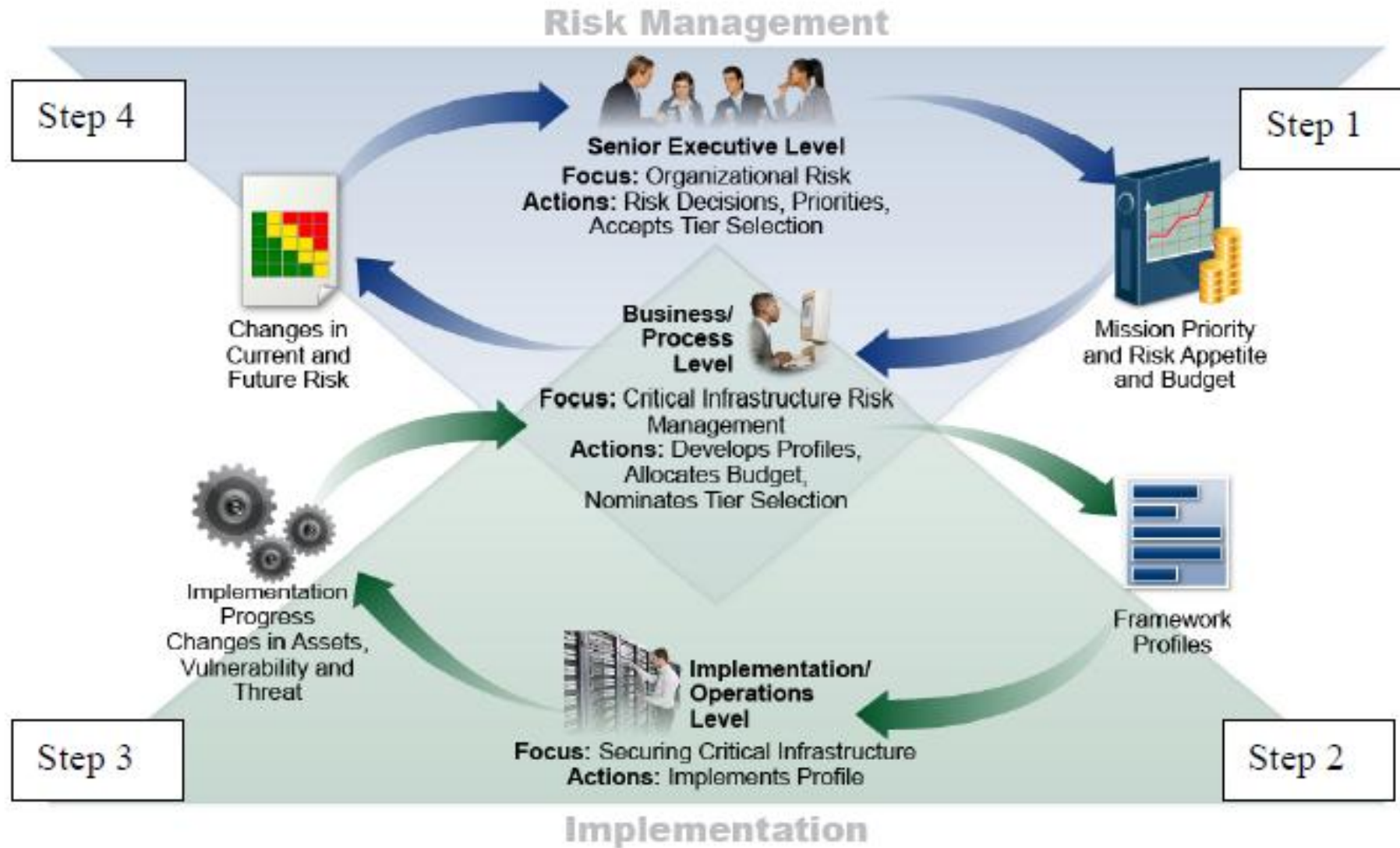
<https://publications.opengroup.org/c20a>

# 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

NISTIR 8286

INTEGRATING CYBERSECURITY AND ERM

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].<sup>10</sup> 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

NISTIR 8286

INTEGRATING CYBERSECURITY AND ERM

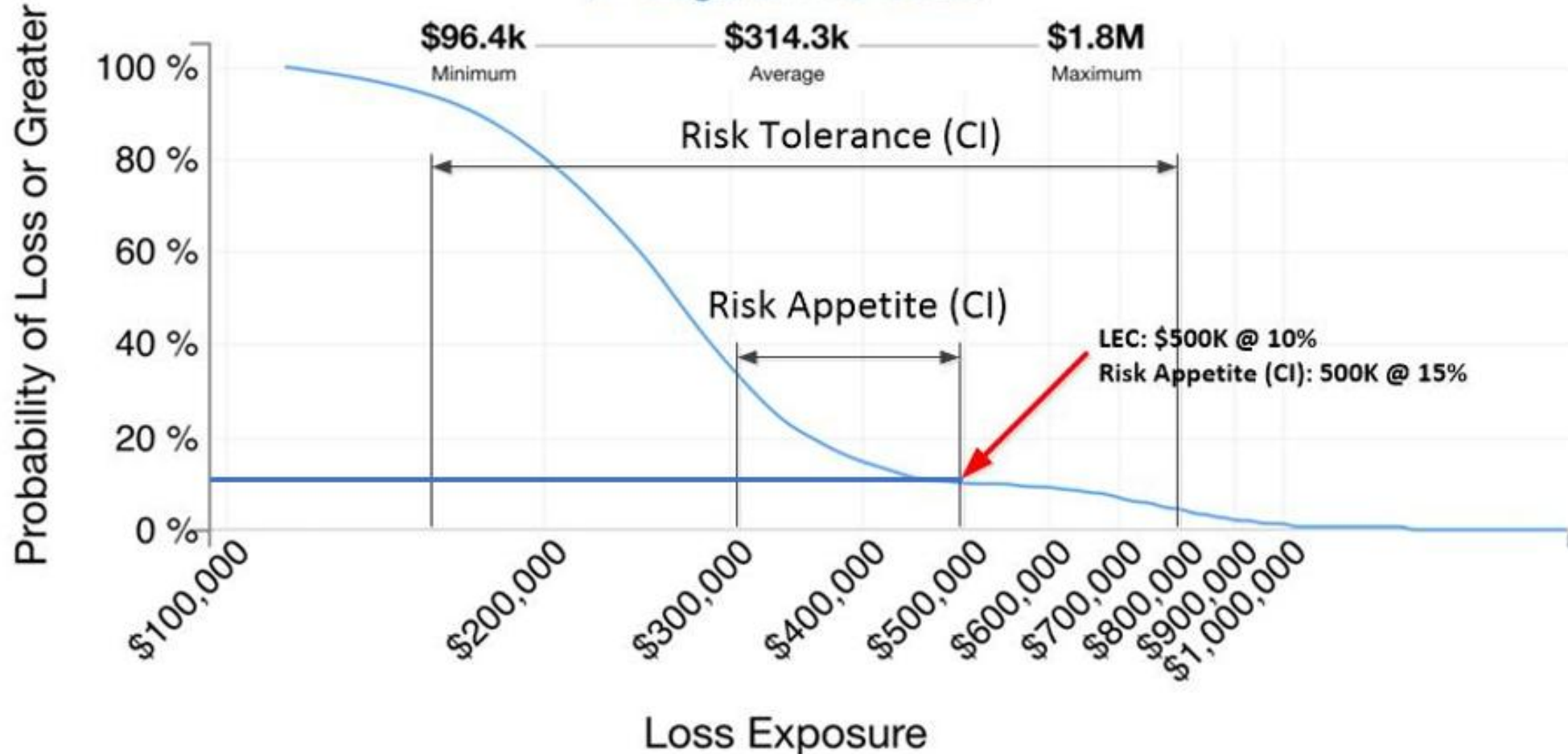
appetite is narrower, stating: “Email services shall not be interrupted more than five minutes during core hours.”

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

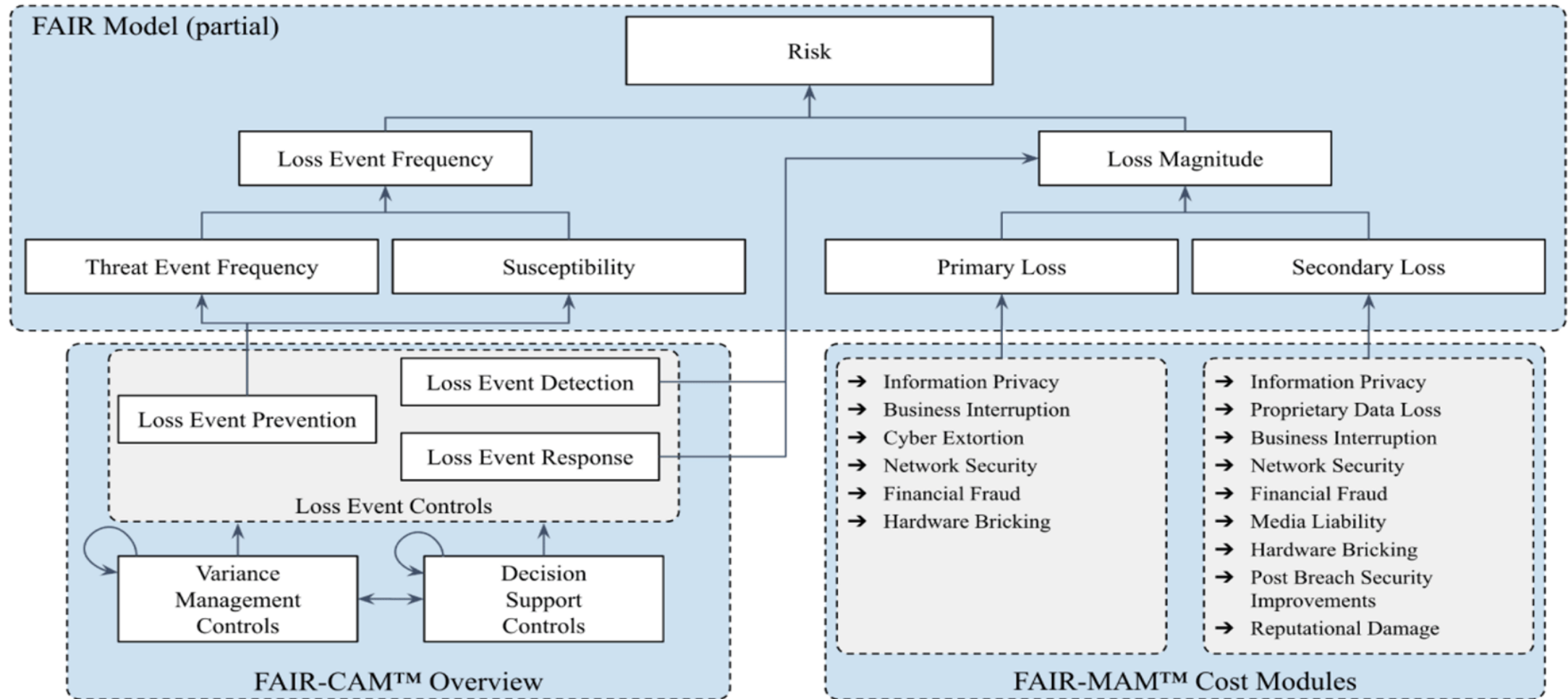
## Loss Exceedance Curve

⇔ Logarithmic Scale



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

	Threat	Assets	Methods		Effects			
Intent (Malicious, Accidental)	Cyber Criminals	Sensitive Personal Data	Ransomware with Data Exfiltration	Initial Attack Method (Optional)		Information Privacy Loss	Primary Losses	Secondary Losses
	Nation-State	IP & Trade Secrets Data	Ransomware without Data Exfiltration			Proprietary Data Loss		
	Privileged Insider	Co-Owned Proprietary Data	Data Exfiltration	Phishing	Malware	Business Interruption		
	Non Privileged Insider	Confidential Business Information	DDoS	SIM Swapping	Supply Chain	Cyber Extortion		
	AI Agents	Business Process Generating Revenue	Cryptomining	Deepfake attacks	Man-in-the-Middle	Network Security		
	Hacktivists	Business Process Impacting Third-Party Revenue	Account Takeover	External Application Exploitation	LLM Prompt Injection	Financial Fraud		
	Cyber Terrorists	Business Process Generating Cost	Malware	Remote Service Exploitation	ML Model Evasion	Media Fraud		
	Script Kiddies	Product or Service	System Outage	Credential Stuffing	Training Data Poisoning	Hardware Bricking		
	Competitor Driven Threat Actors	Cash or Cash Equivalent	Data Corruption	Bruteforce	Physical Access	Post Breach Security Incidents		
	Sabotage Actors	Physical Assets & Facilities	Data Leakage	Privileged Abuse	USB Drop Attacks	Reputation Damage		

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

# Calibrating the data – Doug Hubbard AIE

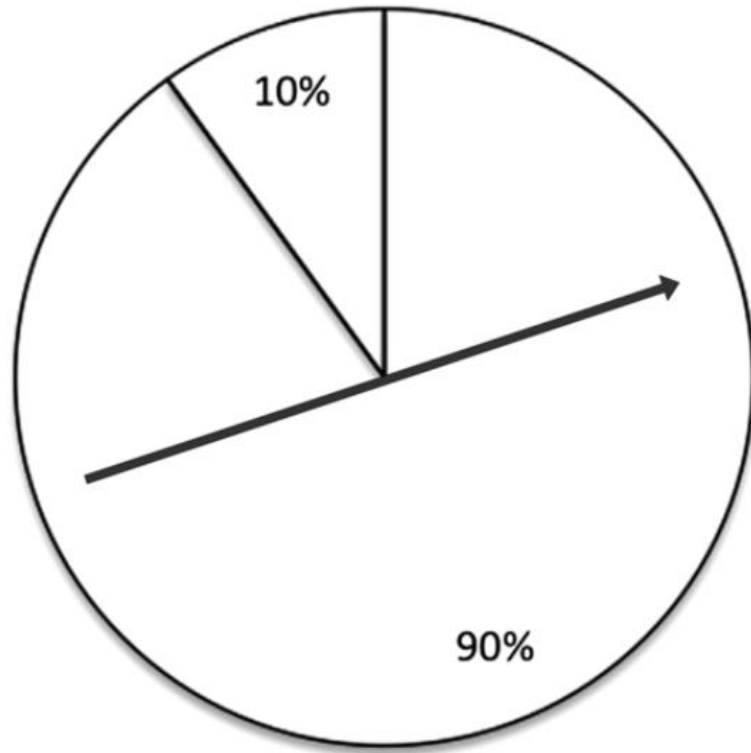
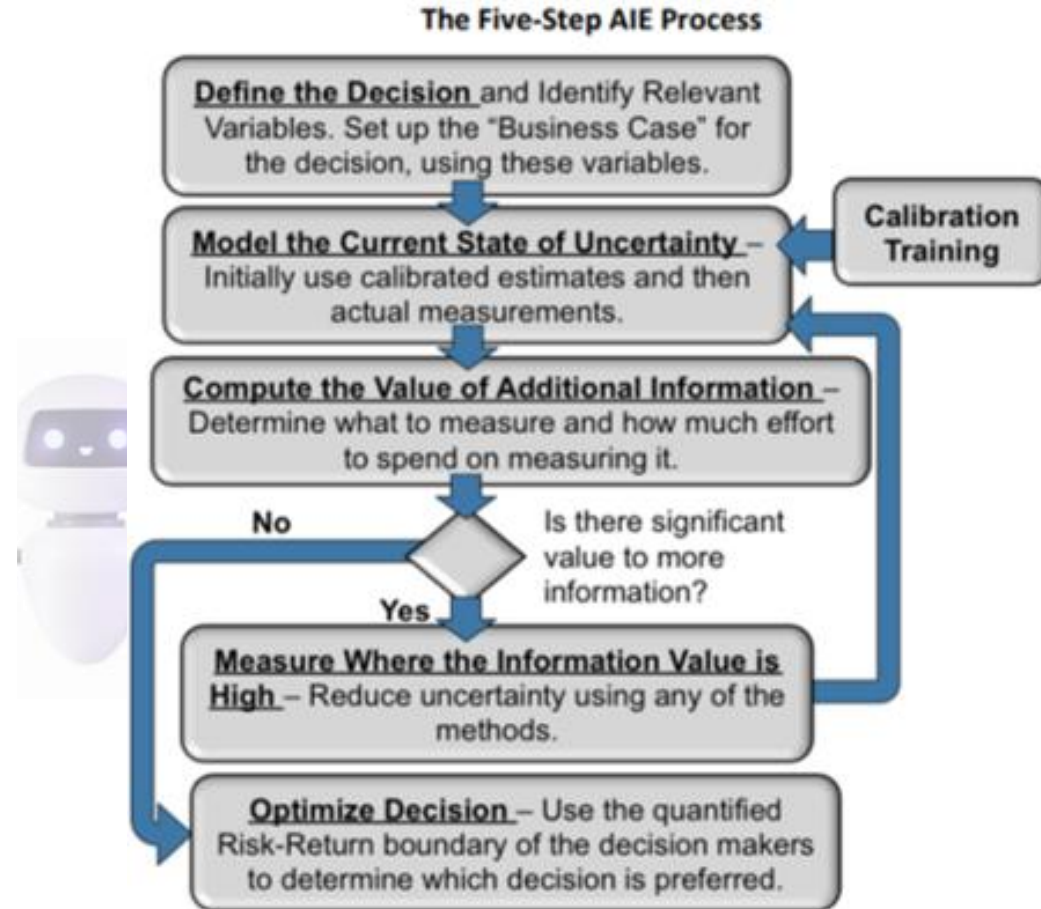
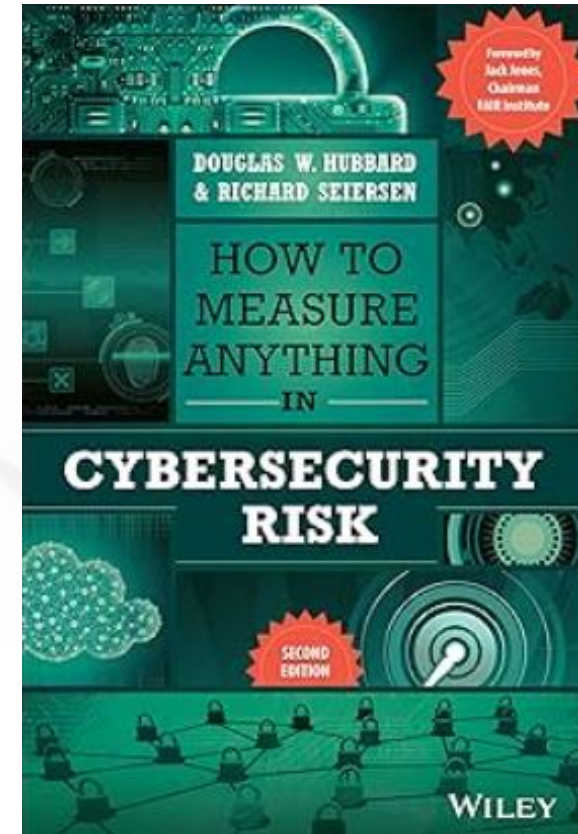
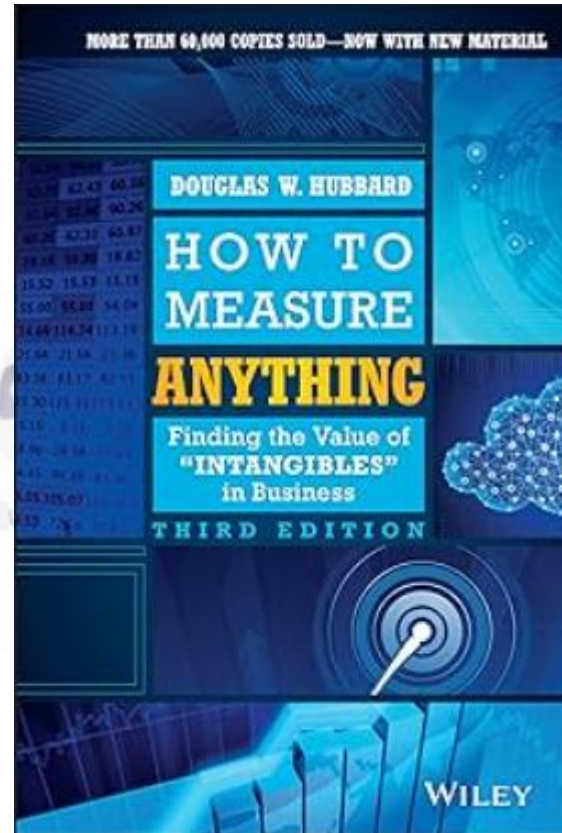
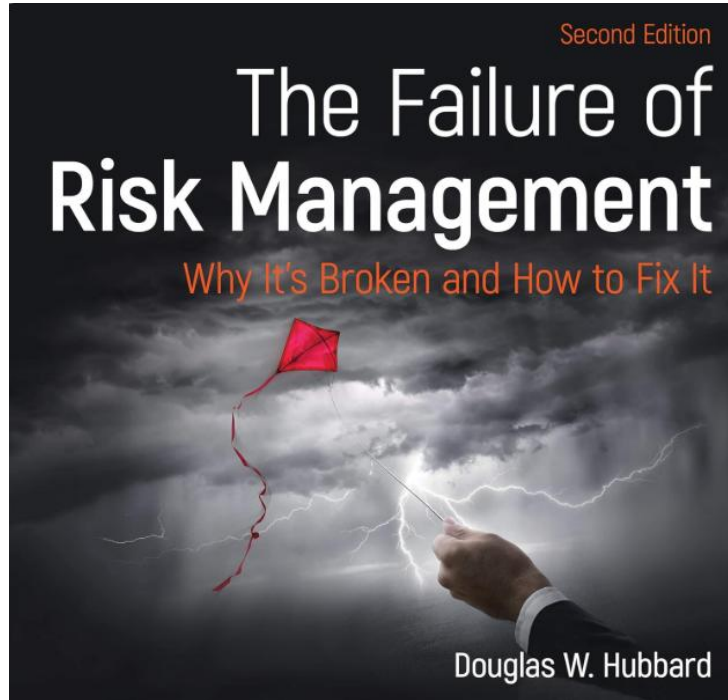


FIGURE 5.5 An equivalent bet test wheel.




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

# How to Measure Anything in Cybersecurity Risk



# Materiality, Materiality, Materiality

 <b>FAIR-MAM (Materiality Assessment Model)</b>									
INFORMATION PRIVACY	PROPRIETARY DATA LOSS	BUSINESS INTERRUPTION	CYBER EXTORTION	NETWORK SECURITY	FINANCIAL FRAUD	MEDIA CONTENT	HARDWARE BRICKING	POST BREACH SECURITY IMPROVEMENTS	REPUTATIONAL DAMAGE
4 SUB-COST CATEGORIES	2 SUB-COST CATEGORIES	3 SUB-COST CATEGORIES	1 SUB-COST CATEGORY	2 SUB-COST CATEGORIES	2 SUB-COST CATEGORIES	2 SUB-COST CATEGORIES	2 SUB-COST CATEGORIES	2 SUB-COST CATEGORIES	6 SUB-COST CATEGORIES
Sensitive PII Event Response and Management P-RC	Loss of Estimated Future Net Revenue S-CA	Direct Business Interruption P-PL	Ransom P-RC	Network Event Response and Recovery P-RC	BEC P-PC	Media Event Response P-RC	Server Replacement P-PC	Legally-Mandated Improvements S-RC	Customer Retention S-RD
PCI-DSS Liability P-RC	Proprietary Data Loss Liability S-RC	Contingent Business Interruption (Supply Chain Attack Victim - 3P failure to provide IT services) P-PL		Network Security Liability (Supply Chain Attack Source) S-RC	Funds Transfer Fraud P-PC	Media Liability S-RC	Computer/Laptop Replacement P-PC	Voluntary Improvements S-RC	Future Projects S-RD
Information Privacy Liability S-RC									
Regulatory Liability S-FJ		Business Interruption Liability S-RC							Cyber Insurance S-RD
									Cost of Capital S-RD
									Employee Churn S-RD

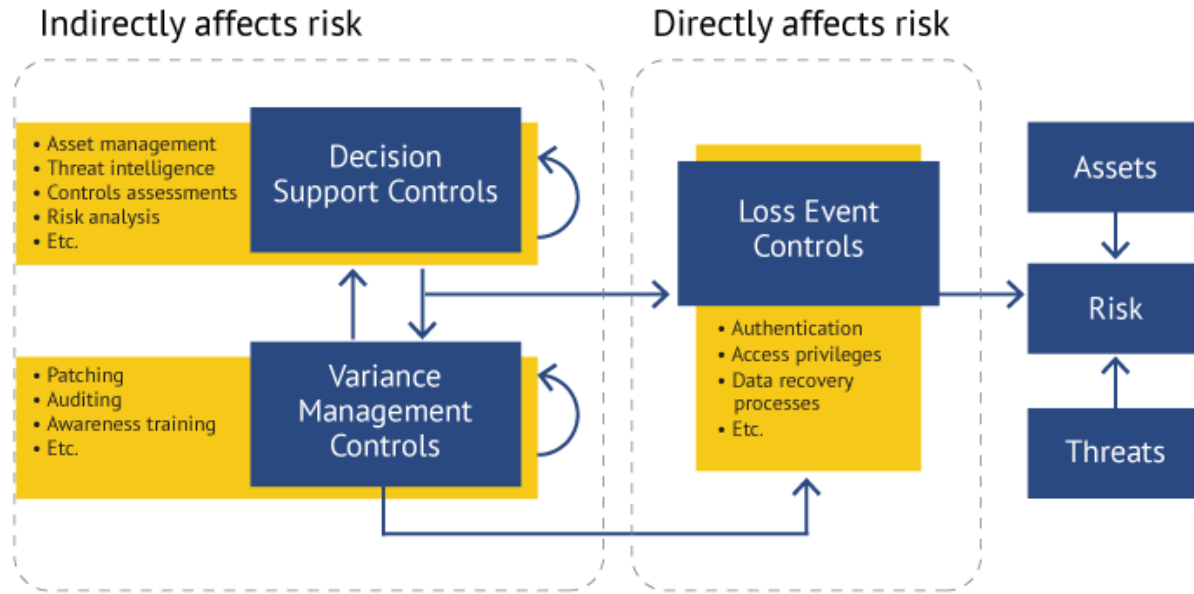
**Legend**

P - Primary Cost      FJ - Fines & Judgements      PC - Replacement Cost  
 S - Secondary Cost      CA - Competitive Advantage      RD - Reputation Damage  
 RC - Response Cost      PL - Productivity Loss

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

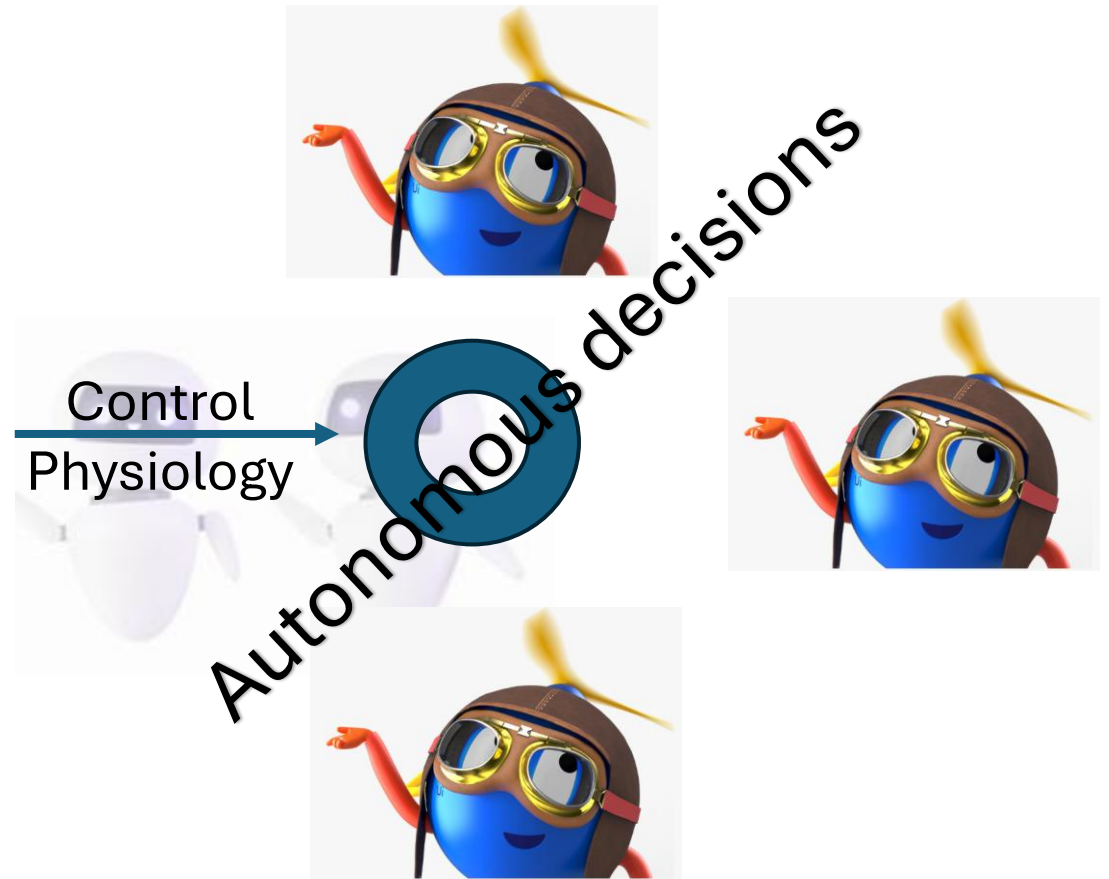


# Modelling Agentic AI risk with FAIR-CAM

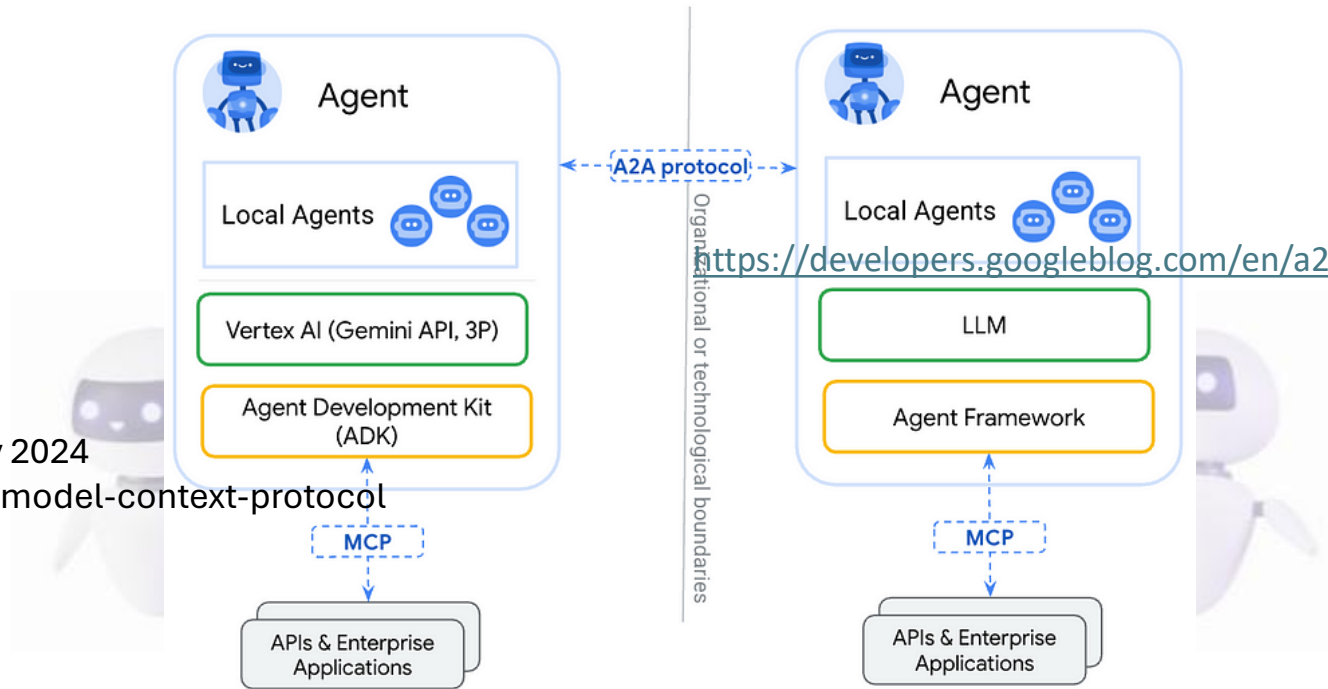


FAIR Controls Analytics Model™ (FAIR-CAM™)

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



# Model Context



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

<https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/>

Model Context Protocol (MCP) Nov 2024

<https://www.anthropic.com/news/model-context-protocol>

Source: Unlock Collaborative, agent-to-agent scenarios with a new open protocol

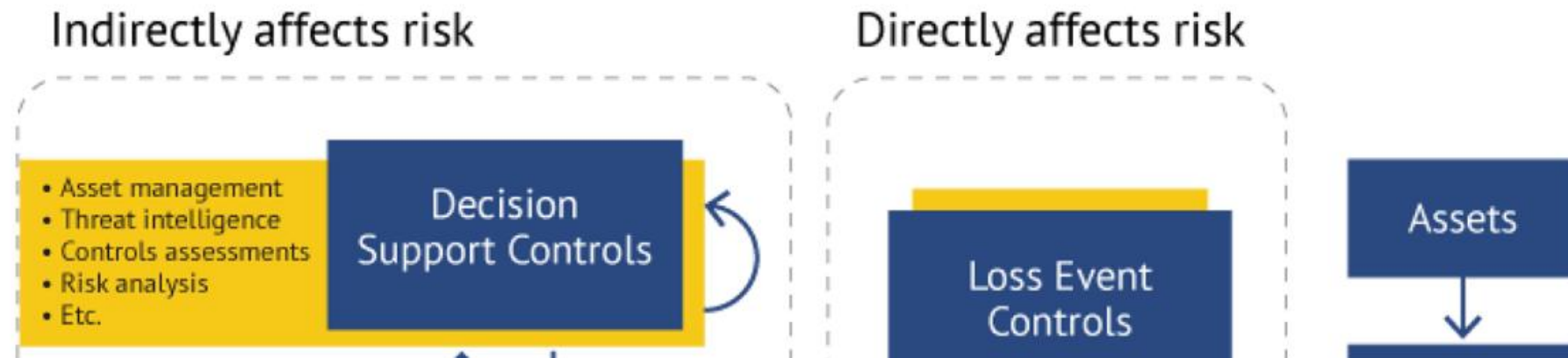
<https://google.github.io/A2A/#/>

# Taming Agentic AI risks with FAIR-CAM

ARTIFICIAL INTELLIGENCE (AI), FAIR FRAMEWORK

## Taming Agentic AI risks with FAIR-CAM

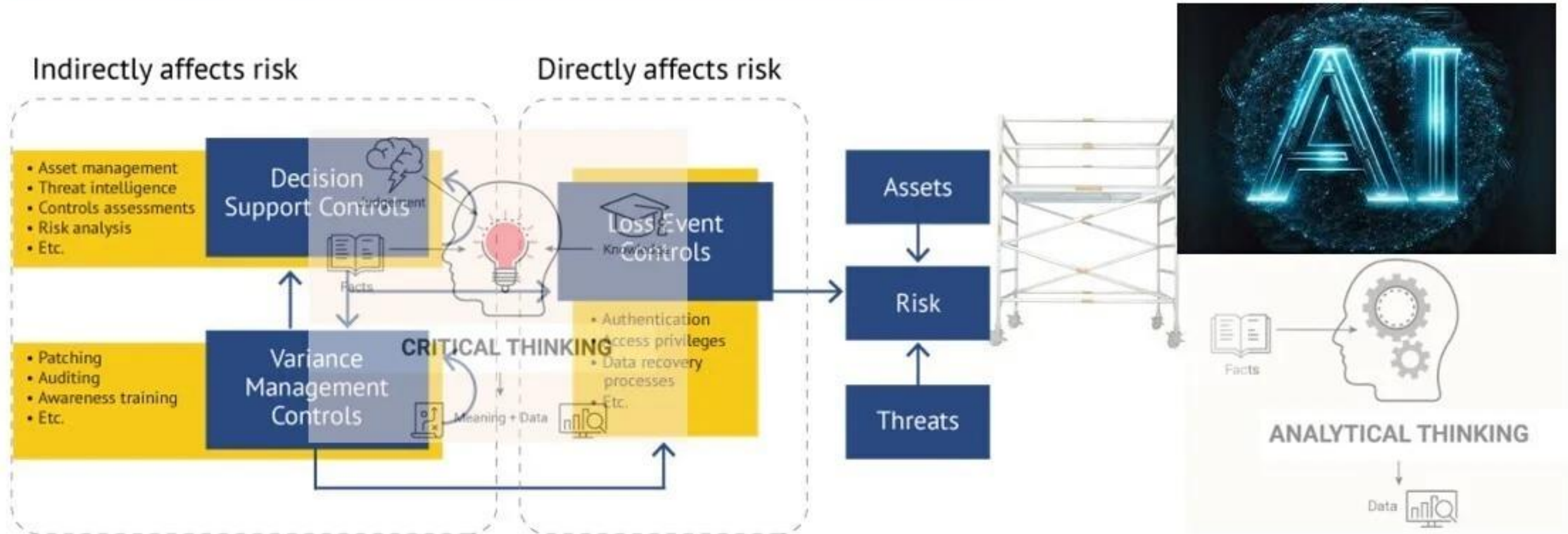
MAR 11, 2025 10:02:49 AM / DENNY WAN



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

# Scaffolding for Critical Thinking

FAIR-CAM™ MODEL: Control Functional Domain Relationships



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

# Simulation exercise

