FAIR INSTITUTE

FAIR™ Standards

Enabling a Risk-based Approach
to Cybersecurity and AI

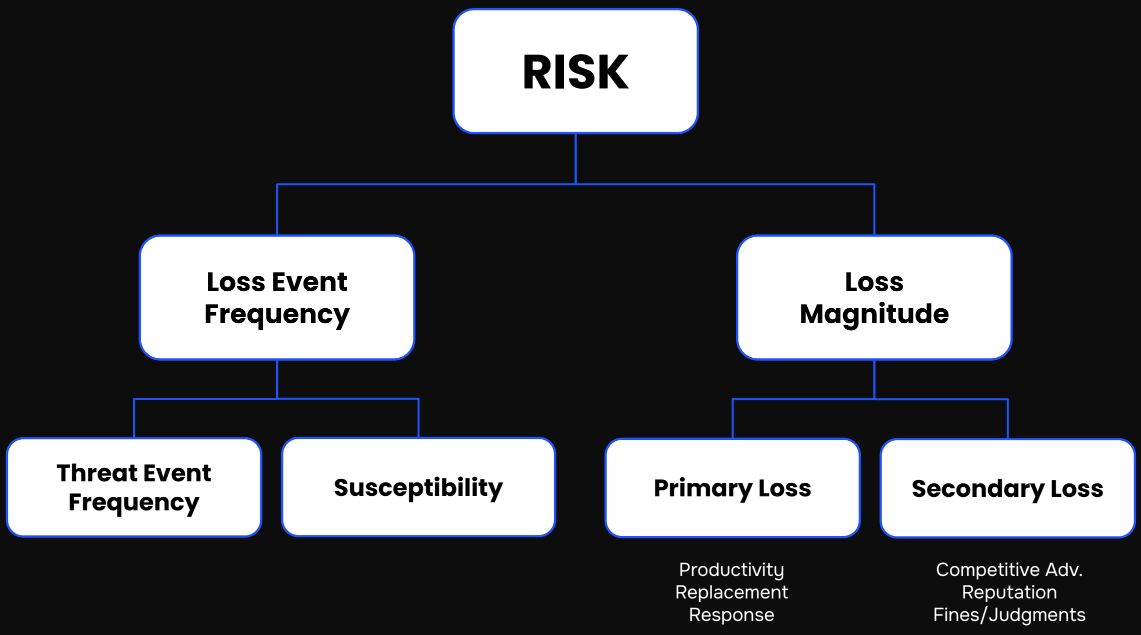
FAIR™: A Methodology for Quantifying and Managing Risk in Any Organization

Factor Analysis of Information Risk (FAIR™) is the only international standard quantitative model for information security and operational risk.

- FAIR ™provides a model for understanding, analyzing and quantifying cyber risk and operational risk in financial terms.
- It is unlike risk assessment frameworks that focus their output on qualitative color charts or numerical weighted scales.
- It builds a foundation for developing a robust approach to information risk management.

THE FAIR™ MODEL

Factor Analysis of Information Risk (FAIR™) is the only international standard quantitative model for information security and operational and operational risk



With FAIR™, you can:

- Speak in one language concerning your risk;
- Take a portfolio view to organizational risk;
- Challenge and defend risk decisions using an advanced risk model; and
- Understand how time and money will impact your security profile.

FAIR's risk model components are specifically designed to support risk quantification:

- A standard taxonomy and ontology for information and operational risk.
- A framework for establishing data collection criteria.
- Measurement scales for risk factors.
- A modeling construct for analyzing complex risk scenarios.
- Integration into computational engines such as Safe Security for calculating risk.

FAIR’s risk analysis capabilities complement the existing risk management frameworks:

- Risk frameworks from organizations such as NIST, ISO, OCTAVE, ISACA, etc. are useful for defining and assessing risk management programs.
- They all prescribe the need to quantify risk, but for the most part, they leave it up to the practitioners to figure it out.
- Some are silent on the subject of how to compute risk, while others are open in the allowance of 3rd party methods.
- Frameworks such as NIST 800-30 attempt to measure risk, but fall short as they rely on qualitative scales and flawed definitions.
- FAIR™ helps fill that gap by providing a proven and standard risk quantification methodology that can be leveraged on top of those frameworks.

Measure The Value of Controls with the FAIR Controls Analytics Model™

Can you say which is the most valuable control in your cybersecurity program? The least valuable? Why are those questions for the cybersecurity and risk management professions difficult to answer? We have frameworks that list recommended controls but provide no insight into the effectiveness of those controls for risk reduction, either on their own or as a system. It's like practicing medicine based on anatomy – an inventory of body parts – without physiology, the knowledge of how they work together.

What is FAIR-CAM™

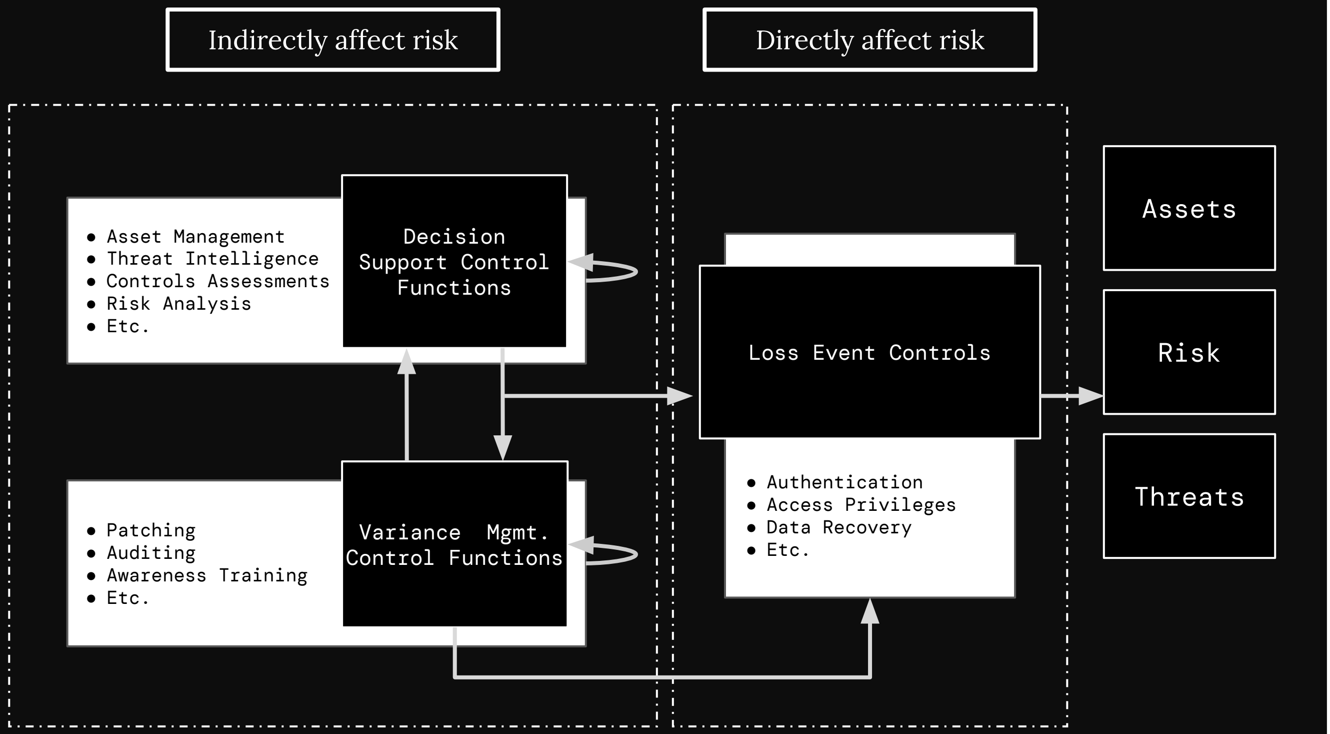
FAIR-CAM™ is an extension of the FAIR standard that documents how controls physiology functions by describing how controls affect the frequency and magnitude of loss events. The FAIR-CAM™ model accounts for controls both with direct and indirect effects on risk, yielding a complete system view.

With FAIR-CAM™, the effect of each control on risk can be measured based on a specific unit (for instance frequency, probability, or time) as opposed to subjective ordinal values like "1-through-5" or "red/yellow/green." The result is an understanding of controls and control systems based on empirical measurements.

This controls physiology for FAIR™ enables you to:

- Use empirical measurement of control efficacy and value
- Account for individual control functionality as well as systemic effects
- More effectively leverage cybersecurity telemetry

THE FAIR-CAM^{TM} MODEL - Control Functional Domain Relationships



Indirectly affect risk

Directly affect risk

- Asset Management
- Threat Intelligence
- Controls Assessments
- Risk Analysis
- Etc.

Decision Support Control Functions

- Patching
- Auditing
- Awareness Training
- Etc.

Variance Mgmt. Control Functions

Loss Event Controls

- Authentication
- Access Privileges
- Data Recovery
- Etc.

Assets

Risk

Threats

FAIR-CAM™ Complements Popular Control Framework

The FAIR-CAM™ model can readily be leveraged to make better use of existing control frameworks. Expert workgroups convened by the FAIR Institute have mapped, or are in the process of mapping the FAIR-CAM™ model to:

- NIST 800-53
- CIS Controls
- ISO 2700
- HITRUST

Work is being scheduled to map other common frameworks to the FAIR-CAM™ model. When combined with a well-defined control “anatomy-like” framework and solid risk measurement using FAIR™, the FAIR-CAM™ model will improve an organization’s ability to focus on the controls that matter most, significantly reducing the odds of cybersecurity loss events and wasted resources.

The FAIR Materiality Assessment Model™

Measure the Materiality of Cyber Events with the FAIR Materiality Assessment Model™ (FAIR-MAM™)

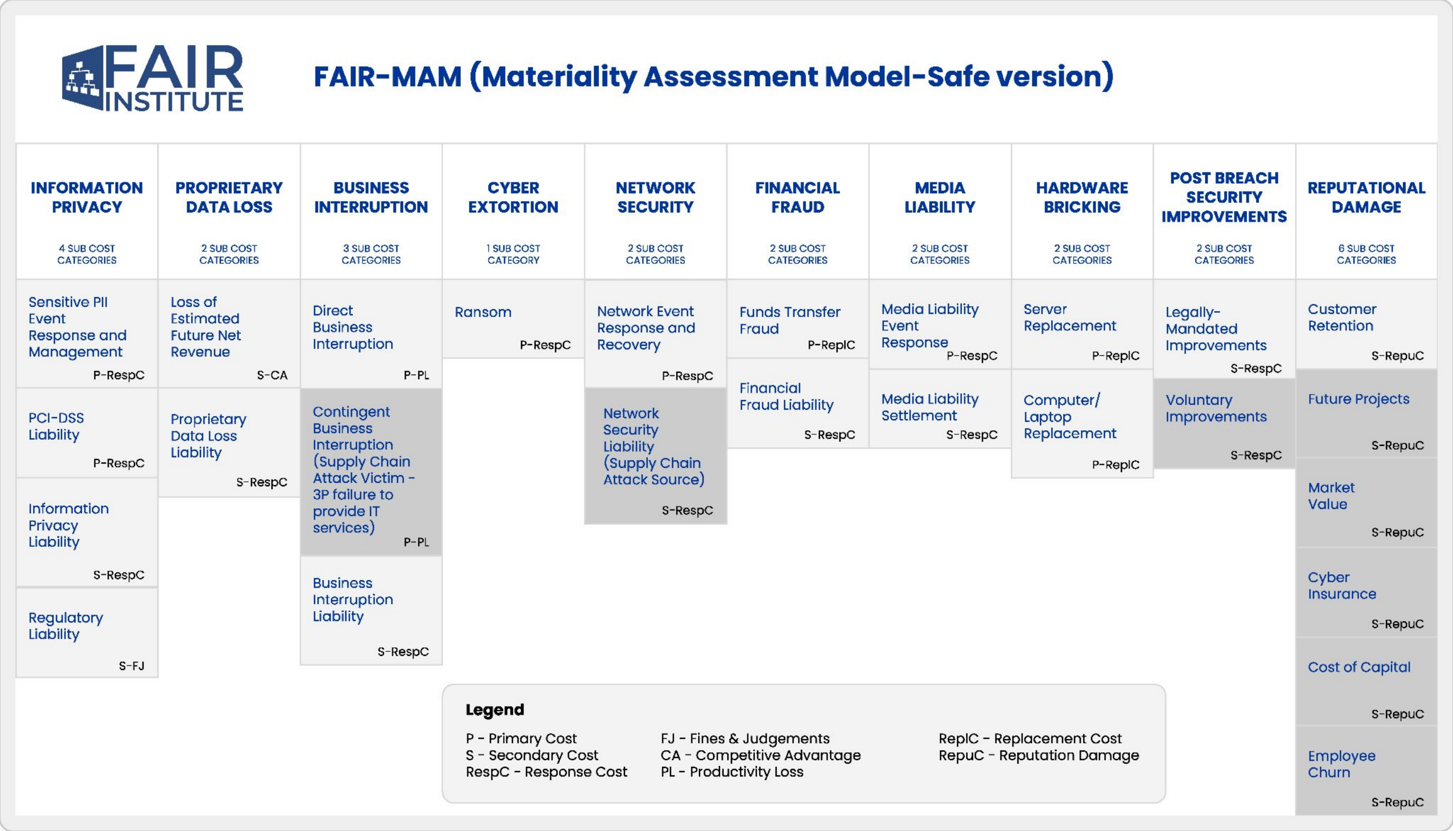
The new Securities and Exchange Commission Rule on Cybersecurity exposed the problem that many companies are not equipped to assess and disclose material risks from cybersecurity incidents in a timely, accurate and comparable way to their stakeholders. The rule requires regulated companies to report a cyber loss event within four business days of determining that its impact would likely be material, and to report when past events cumulatively reach the level of materiality.

What is FAIR-MAM™?

The FAIR Materiality Assessment Model (FAIR-MAM™) is a standard that helps organizations assess the materiality of cybersecurity risk and incidents. FAIR-MAM™ expands the loss magnitude factor of the FAIR™ model, and provides a more detailed taxonomy and breakdown of loss categories driven by cybersecurity incidents.

FAIR-MAM™ is an open, financial loss model that enables organizations to:

- Quantify the impact of cyber incidents so they can quickly and reliably disclose legally defensible material risk on SEC Form 8-K.
- Report financial risk internally to inform cybersecurity investment and management decisions for a full range of custom cyber risk scenarios.
- Create a timeline of the multi-year life cycle of the total cost of an incident.
- The FAIR-MAM™ standard also allows companies to report 'comparable' material financial costs related to cybersecurity incidents, a critical requirement for institutional investors.



FAIR INSTITUTE

FAIR-MAM (Materiality Assessment Model-Safe version)

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

Legend

P - Primary Cost
S - Secondary Cost
RespC - Response Cost
FJ - Fines & Judgements
CA - Competitive Advantage
PL - Productivity Loss
ReplC - Replacement Cost
RepuC - Reputation Damage

How Material is that Hack?

Interested in learning how cyber incident losses can be broken down and estimated using the FAIR-MAM™ standard?

Researchers from the FAIR Institute's Technical Advisor Safe Security have utilized FAIR-MAM™ as an analytical basis to estimate the cyber losses incurred by the victims of recent cyber attacks.

Learn more here: https://howmaterialisthathack.org/

Measure and Manage Third Party Risk with FAIR-TAM™

A 2023 RSA Conference survey of Fortune 1000 CISO's found that 87% of the companies were affected by a significant cyber incident at a third party in the previous 12 months. Call it third party risk, vendor risk or supply chain risk, it is the major blind spot of cybersecurity defense.

The solutions for third party risk management (TPRM) badly need a rethink. Vendors mainly offer one or the other or a mix of :

- Questionnaires for the third-party to answer – quickly out of date even if accurately filled out
- Outside-in scans of controls that are more noise than signal

These solutions can't identify the riskiest vendors and don't give quantitative insights into how to prioritize mitigations to achieve a return on investment. They are also manual processes that can't be automated to respond to changing threats. With an unreliable toolkit, CISOs fall back on compliance to frameworks, lists of recommended controls disconnected from measurable risk reduction. Or they prioritize among vendors based on size of contract, not size of loss exposure.

Despite having a fleet of tools at their disposal, CISOs and TPRM practitioners are unable to answer the basic questions: "What is the most critical third-party risk, and how efficient is your program in managing that risk?"

What is the FAIR Thirds Party Assessment Model (FAIR-TAM™)?

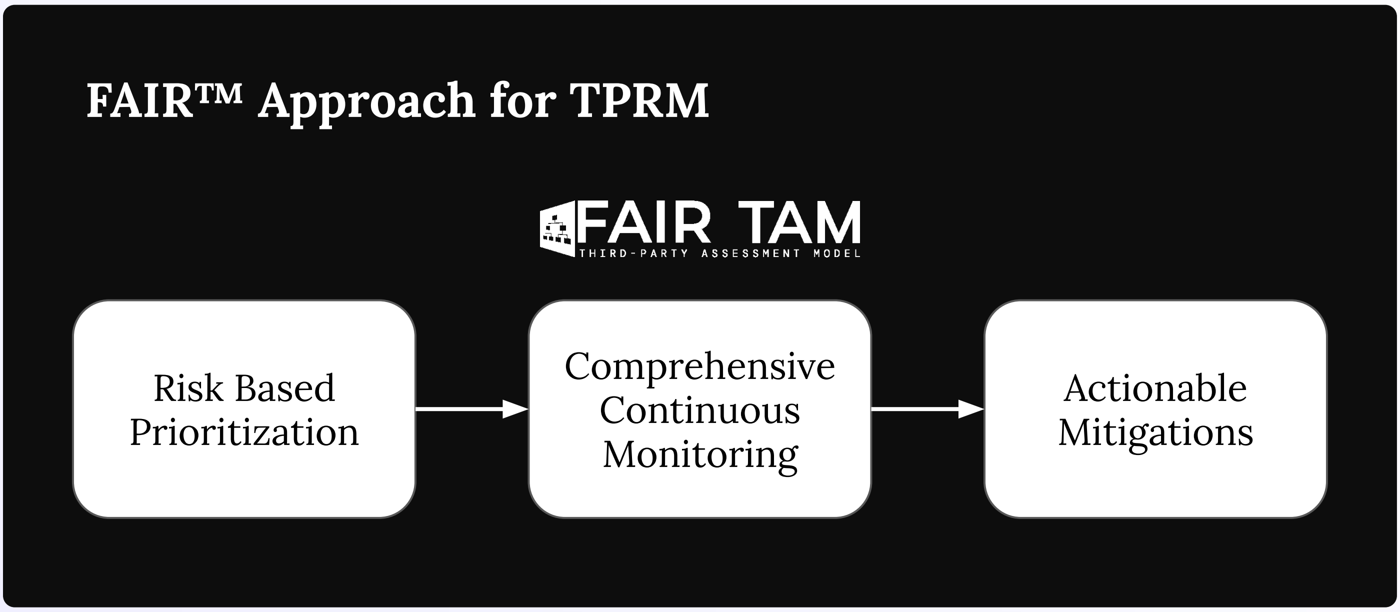
The FAIR Institute (through our Supply Chain Risk Workgroup) is developing a solution to the challenge of third-party risk with an extension to the FAIR™ model: FAIR-TAM™, a third-party risk assessment model. Foundational concepts include:

1. **Risk-based prioritization**: Run a FAIR assessment of the risk the vendor poses to your organization as a first party. That risk can be analyzed using the FAIR Materiality Assessment Model (FAIR-MAM) based on data access, server access or revenue access. Tier your supply chain partners accordingly.

2. **Comprehensive, continuous monitoring**: Instead of questionnaires or outside-in scans, use inside-out telemetry from first and third parties as they access your network, reporting on a continuous basis through automation. With the FAIR Controls Analytics Model (FAIR-CAM™), you can gauge the breach likelihood for these actors.
3. **Actionable Mitigations**: Treat third parties as your attack surface. Apply Zero Trust Principles to TPRM. How are you managing data access, network access and revenue dependency towards your third parties?

How to Use FAIR-TAM™

1. **Tier Your Third Parties.** Base it on a scientific, risk-driven method instead of arbitrary numbers. You can't focus on 5,000 third parties, you can focus on 50. How can you do that? Understand your data, network, and revenue exposure to a third party, quantify it.
2. **Treat third parties as your attack surface**. Apply Zero Trust Principles to TPRM. How are you managing data access, network access and revenue dependency towards your third parties? In a bad neighborhood, you protect your house first, and then try to fix the neighborhood.
3. **Get inside-out, real-time telemetry.** Use the environments of your most critical vendors and do it i n a non-intrusive way. This real time telemetry will help you to truly understand the risk posture of your third parties in different risk scenarios. Outside-in scans are insufficient.
4. **Run Active Risk Management,** not Passive Risk Management. Fix your native controls first, then work with your vendors to mutually improve controls.
5. **Automate, automate, automate**. There are many ways to reduce redundant and manual work in the TPRM process. Start by applying LLMs to automate questionnaires.



FAIR™ Approach for TPRM

FAIR TAM
THIRD-PARTY ASSESSMENT MODEL

Risk Based Prioritization → Comprehensive Continuous Monitoring → Actionable Mitigations

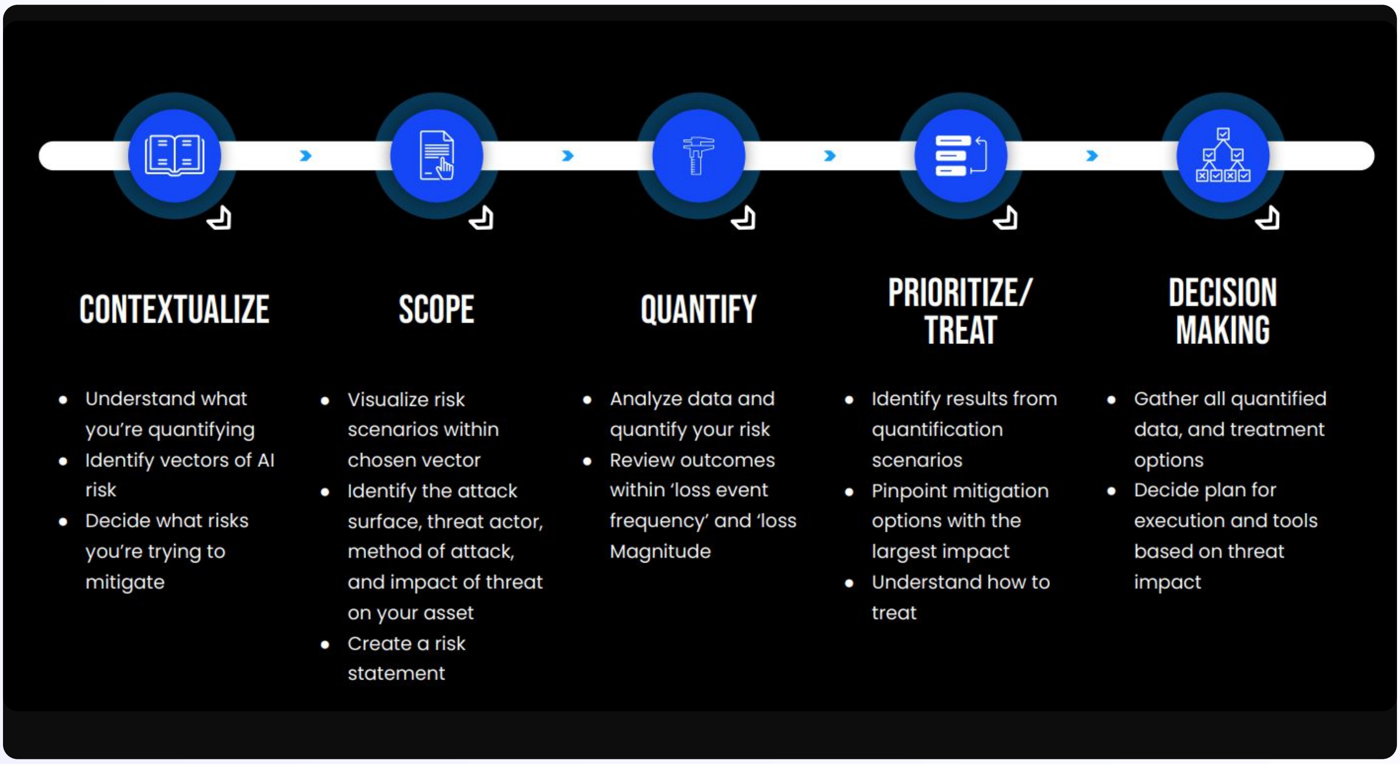
A FAIR Artificial Intelligence (AI) Cyber Risk Playbook

Right now, the disconnect between the security organization and the business is becoming clear once again. With the FAIR-AIR™ Approach, you will be able to speak the same language as the business and work as a partner in AI adoption rather than an impediment.

What is FAIR-AIR™

- The FAIR-AIR™ Approach will help you identify your AI loss exposure and make risk-based decisions on how to treat your identified loss event scenarios.
- You will need to work across teams to ensure proper data and alignment for scenarios and use cases.
- The purpose of this approach is to meet the business needs, not create additional obstacles to AI deployment.

FAIR AI Playbook - Steps to Risk Analysis



CONTEXTUALIZE

- Understand what you're quantifying
- Identify vectors of AI risk
- Decide what risks you're trying to mitigate

SCOPE

- Visualize risk scenarios within chosen vector
- Identify the attack surface, threat actor, method of attack, and impact of threat on your asset
- Create a risk statement

QUANTIFY

- Analyze data and quantify your risk
- Review outcomes within 'loss event frequency' and 'loss Magnitude

PRIORITIZE/ TREAT

- Identify results from quantification scenarios
- Pinpoint mitigation options with the largest impact
- Understand how to treat

DECISION MAKING

- Gather all quantified data, and treatment options
- Decide plan for execution and tools based on threat impact

What Is FAIR™ Automation?

The ideal FAIR™ automated system would ingest threat data up to the minute, actively monitor the status of controls and assets at risk and pull in the latest loss data from trusted vendors of industry statistics and from the organization's own logs.

Based on those inputs, the system would deliver automated, on-demand FAIR™ analysis that quantifies the probable frequency of cyber events and probable magnitude of losses – in the dollar terms that drive business decisions.

Benefits of Automating FAIR™

- Rapid prioritization for cybersecurity spending projects based on return on investment for risk reduction.
- Quick identification and reporting on material risks to the board and regulators to meet regulations like the SEC's 4-day risk disclosure rule.
- Streamline security operations – consolidate tools and staff to focus on the risks that matter most, when they most matter.

The 3 Must-Haves to Do FAIR™ Automation Right

1. A clear scope of what's being measured – the assets at risk, the relevant threats, the type of event (outage, data compromise, fraud, etc.) that together inform the creation of a risk scenario that can be analyzed in FAIR™ terms. If the scope is off, the analysis fails; ideally, an automated system would predefined scenarios to control for errors.
2. The FAIR™ model – FAIR™ sets the parameters needed to perform the analysis, and how data are used to generate a result. But as FAIR™ author Jack Jones has written, the FAIR™ model by itself "does not fully support automation" because it doesn't account for how controls affect risk; a complete automated solution also requires the FAIR Controls Analytics Model (FAIR-CAM™). Learn about FAIR-CAM™.
3. Data – We have more data for cybersecurity than ever before from threat intel, vulnerability scans, SIEM reporting, endpoints and many more forms of telemetry. The data challenge for FAIR™ automation is aggregating data into a coherent view.

Become an Institute Member

Learn the leading practices in Cyber Risk Quantification

- Experience how your organization can make better decisions with the FAIR™ Model

Connect with over 15,000 Industry Thought Leaders Worldwide

- Hear from the experts who are quantifying and managing their risk effectively

Take advantage of the Member Resource Library

- Network with your peers to share success stories and check out case studies, white papers, and webinars

Be Invited to Exclusive to Institute Events

- Discounts on the annual FAIR Conference (FAIRCON) and Local Chapter Meetings

https://www.fairinstitute.org/get-involved-apply-today

Notes

FAIR INSTITUTE

https://www.fairinstitute.org/