A FAIR Framework for Effective Cyber Risk Management

Leveraging the FAIR Model, FAIR-CAM, and FAIR-MAM to Align Cybersecurity Efforts with Business Priorities and Regulatory Compliance

January 3, 2025

Authors:

Pankaj Goyal
Director, Standards & Research
FAIR Institute
Pankaj@FAIRInstitute.org

Nick Sanna
Founder
FAIR Institute
NSanna@FAIRInstitute.org

Todd Tucker
Managing Director
FAIR Institute
TTucker@FAIRInstitute.org

©2025 FAIR Institute. All Rights Reserved.

www.FAIRInstitute.org

Table of Contents

Executive Summary

The FAIR Institute has developed and maintains three distinct but interrelated risk management standards: the FAIR Model™ (v3.0), the FAIR Controls Analytics Model™ (FAIR-CAM™, v1.0), and the FAIR Materiality Assessment Model™ (FAIR-MAM™, v1.0). These standard models are each described in their own standards artifacts and have been covered in other white papers, blogs, workshops, and courses from the FAIR Institute and other organizations.

This paper discusses how these three standard models fit together for a comprehensive framework for quantifying and managing cyber risk. As extensions of the FAIR Model, FAIR-CAM and FAIR-MAM help cyber risk managers understand the impact of controls on risk and quantify losses using a more detailed taxonomy.

This paper does not dive deep into each of the models. Instead, readers should use the following resources:

- Measuring and Managing Information Risk: A FAIR Approach by Jack Freund and Jack Jones
- Factor Analysis of Information Risk (FAIR) Standard (Version 3.0)
- FAIR Controls Analytics Model (FAIR-CAM) Standard (Version 1.0)
- FAIR Materiality Assessment Model (FAIR-MAM) Standard (Version 1.0)

This paper will be part one of a series describing FAIR Cyber Risk Management. The other topics are:

- Identifying, Defining, and Prioritizing Cyber Risk Scenarios with FAIR
- Common Data Sources and Their Roles in FAIR Cyber Risk Management
- How to Use the FAIR Controls Analytics Model for Cyber Risk Management
- How to Use the FAIR Materiality Assessment Model to Estimate Cyber Losses

We welcome feedback and questions about this paper. Please email us at feedback@fairinstitute.org.

©2025 FAIR Institute. All Rights Reserved.

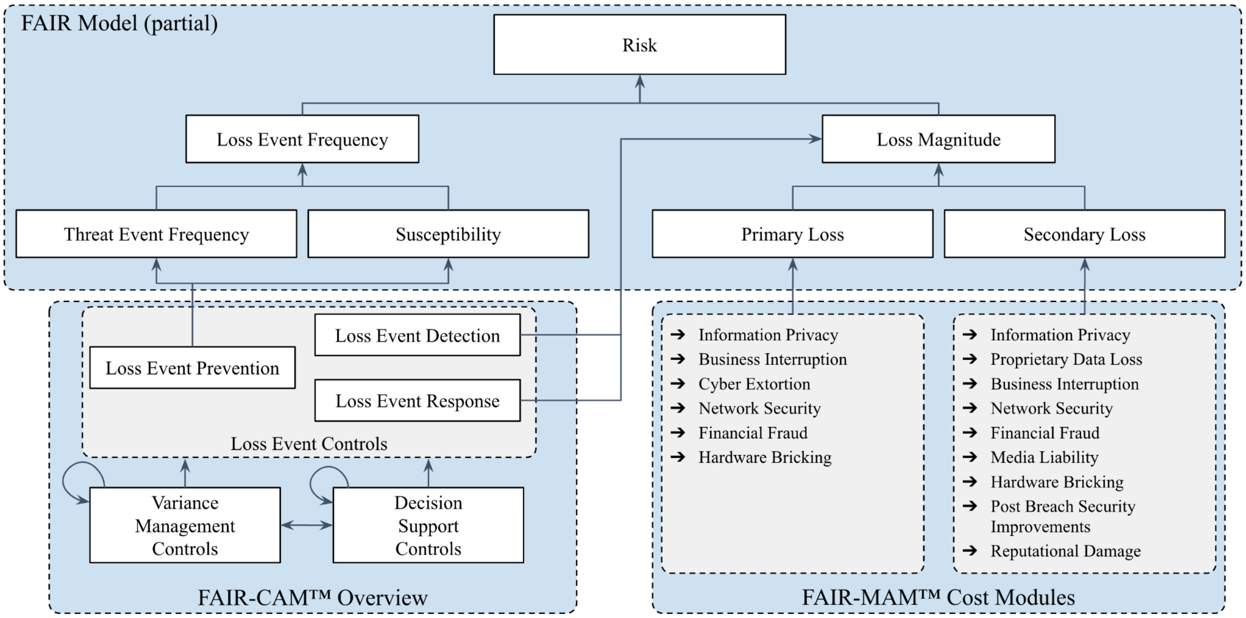
Introduction

Factor Analysis of Information Risk was developed as a general risk quantification model, primarily applied to “information” or “information technology” risks. However, it can also be applied to other forms of risk. FAIR quantifies the risk of loss from events caused by threats targeting valuable assets and exploiting control deficiencies. While this model can describe many types of risks, it is well-suited for cybersecurity (or cyber) risks. These risks often involve malicious threat actors or privileged users who accidentally or unintentionally cause harm. Among FAIR Institute members, most FAIR practitioners focus on assessing and managing cyber risks.

Recently, two new ancillary standards to the original FAIR model have been released to help with two key cyber risk management requirements. The first standard, the FAIR Controls Analytics Model (FAIR-CAM), describes and helps measure the effect of controls on risk. The second one, the FAIR Materiality Assessment Model (FAIR-MAM), provides a more detailed taxonomy of the various forms of cyber losses than the original FAIR model, similar to how a CFO or a cyber insurance company would account for them. Together with the original FAIR standard, FAIR-CAM and FAIR-MAM form the *FAIR Framework for Cyber Risk Management™*.

This paper explains how the FAIR Framework is applied to assessing and managing cyber risks. The FAIR Framework is illustrated below.

Figure 1: The FAIR Framework for Cyber Risk Management



Two significant benefits of the FAIR Framework for Cyber Risk Management are:

©2025 FAIR Institute. All Rights Reserved.

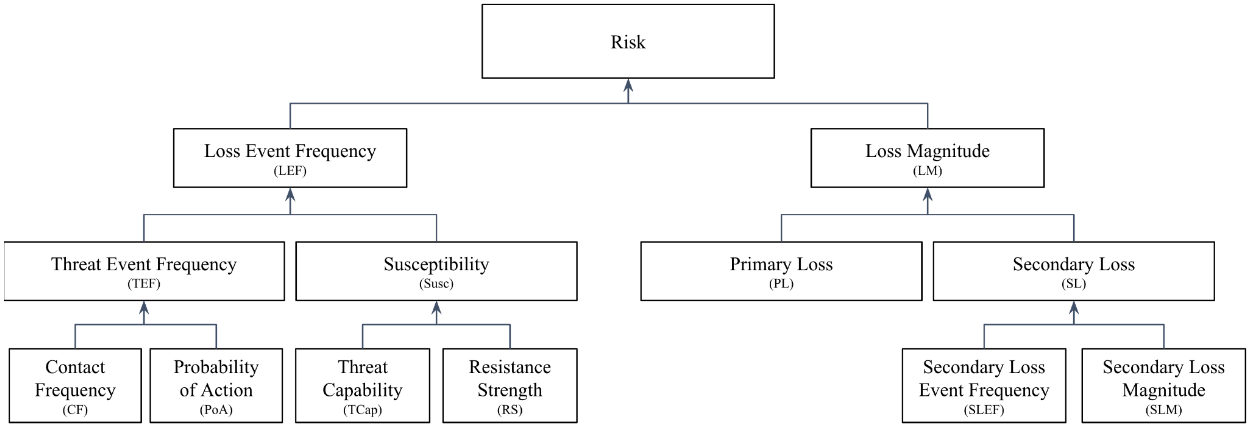
1. The framework supports a data-driven approach to quantifying and managing cyber risk by clearly defining how controls and granular cost data impact risk factors.
2. The framework enables the automation of cyber risk assessment tasks (including quantification), which has eluded the industry until now.

These benefits can be realized via the use of a Cyber Risk Management System, a technology platform purpose-built on the FAIR Framework that supports users throughout every step of the cyber risk management process, including the identification of risks, the quantification and prioritization of risks, the evaluation and recommendation of risk mitigation options, the reporting of risk, and the continuous monitoring of risk against stated risk objectives. We'll discuss the role of the Cyber Risk Management System later in this paper.

The FAIR Model: A Foundation for Risk Quantification

FAIR is an analytic model of the factors that drive risk. It aids in understanding, analyzing, measuring, and communicating risk. FAIR decomposes risk into its fundamental components, enabling better analytic focus, data application, and quantitative risk measurement and management. This offers a more straightforward pathway to understanding and cost-effectively managing loss exposure.

Figure 2: The FAIR Model



The FAIR Model describes the underlying factors that comprise risk and can be quantified to estimate it. Traditionally, risk analysts have performed this quantification based on subject matter estimates. Analysts can work at different levels of the model depending on the availability of data. With robust historical data, they can operate at a higher level of abstraction. When data is scarce, they may need to work at more granular levels within the model.

While the original FAIR Model defines a practical risk assessment structure, it does not describe how controls impact the various risk factors. It is up to the risk analyst to estimate how resistive controls reduce the susceptibility of a cyber loss event. This limitation has been addressed with the FAIR-CAM standard (v1.0), which extends the original FAIR model.

FAIR Controls Analytics Model: A “Controls Physiology” Approach

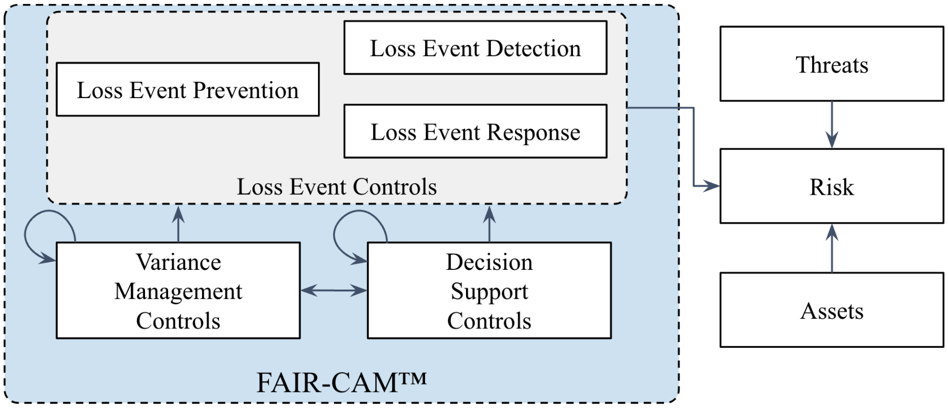
To understand and measure risk, analysts need to understand the controls they have in place. By definition, controls reduce the frequency or magnitude of loss. The FAIR Controls Analytics Model (FAIR-CAM™) goes beyond a simple description of the effects of controls on risk and provides a rigorous description of how the controls landscape works. FAIR-CAM describes this landscape as a complex set of interdependent functions that act as a system in risk management. This is analogous to how human physiology describes how the different parts of the body operate as a system. This “controls physiology” view fills a void in how risk management has historically been practiced, which has focused almost exclusively on the parts of the system (the controls) versus how those parts operate as a system.

FAIR-CAM goes beyond the standard FAIR Model (which mentions only resistive controls) in describing controls by articulating three distinct ways in which controls affect risk:

- By directly affecting the frequency or magnitude of loss (Loss Event Controls)
- By affecting the reliability of controls (Variance Management Controls)
- By affecting decisions (Decision Support Controls)

Recognizing these distinctions provides the structure for how controls affect risk, which lays the foundation for reliable measurement. The diagram below provides a high-level illustration of how these domains relate to one another in risk management:

Figure 3: FAIR-CAM Overview

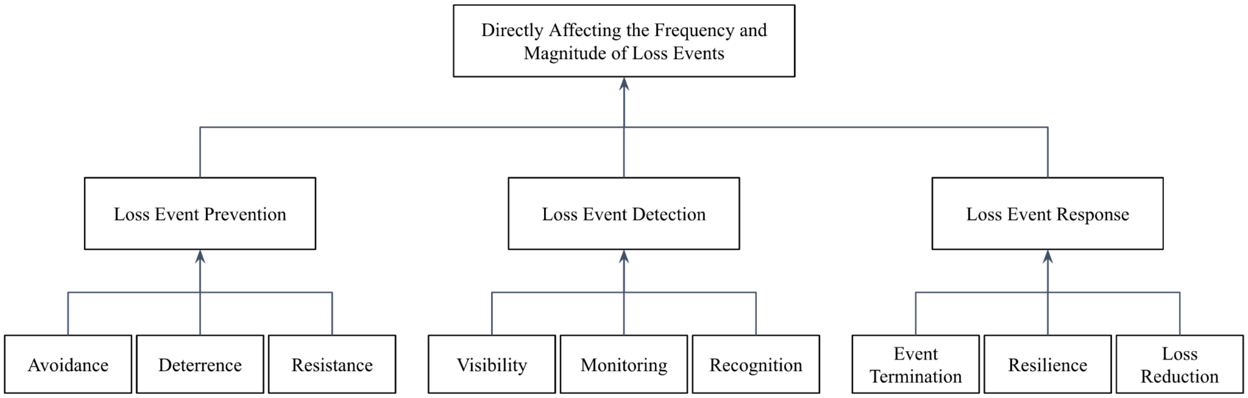


As you can see from the diagram, FAIR-CAM describes the direct impact of Loss Event Controls on risk. For analysts, this means using data about controls to assess their effects on Threat Event Frequency (TEF) and Loss Magnitude (LM). FAIR-CAM then describes Variance Management Controls, which seek to maintain the operational effectiveness of other controls. Finally, FAIR-CAM describes Decision Support Controls, which help ensure that decisions are aligned with organizational objectives and expectations.

Loss Event Controls

Loss Event Controls directly affect the frequency and magnitude of loss. These controls are depicted below among the three functional domains (Prevention, Detection, and Response):

Figure 4: FAIR-CAM Loss Event Controls



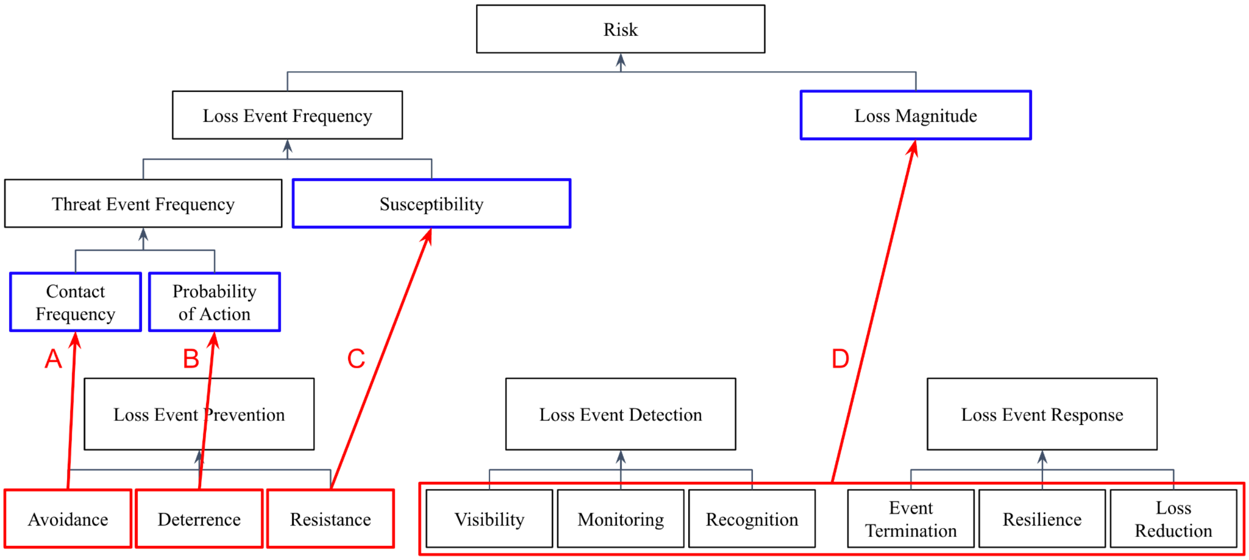
As illustrated, there are three control functions within each functional domain, resulting in nine (9) overall functions:

- **Avoidance:** Reduce the frequency of contact between threat agents and the assets they could adversely affect.
- **Deterrence:** Reduce the probability of potentially harmful actions after a threat agent has come into contact with an asset.
- **Resistance:** Reduce the likelihood that a threat agent's action(s) will result in a loss event.
- **Visibility:** Provide evidence of activity that may be anomalous or illicit.
- **Monitoring:** Review data provided by Visibility controls.
- **Recognition:** Enable differentiation of regular activity/conditions from abnormal activity/conditions that may indicate a loss event has occurred or is in progress.
- **Event Termination:** Enable termination of threat agent activities that could continue to be harmful.
- **Resilience:** Maintain or restore normal operations.
- **Loss Reduction:** Reduce the amount of realized losses from an event.

©2025 FAIR Institute. All Rights Reserved.

Coupling FAIR-CAM with the FAIR Model shows how Loss Event Controls impact different risk factors, as shown in Figure 5 with the red arrows:

Figure 5: Effect of Loss Event Controls on Factors of Risk



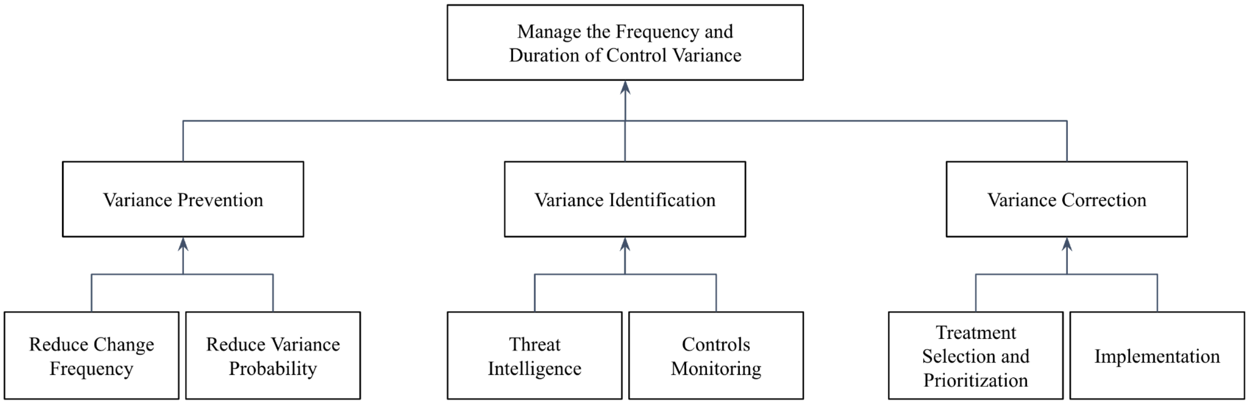
A. Avoidance controls reduce Contact Frequency between threats and assets
B. Deterrence controls reduce the Probability of Action if contact occurs
C. Resistive controls reduce Susceptibility, the probability of successful illicit actions
D. Detection and Response controls reduce the Loss Magnitude when an event occurs

Note that many controls fulfill more than one FAIR-CAM function. For example, EDR (Endpoint Detection & Response) solutions can, depending on how they're configured, fulfill the following functions of Prevention (Resistance), Detection (Visibility, Monitoring, Recognition), and Response (Containment).

Variance Management Controls

The **Variance Management Control** (VMC) domain, illustrated below, focuses on improving the operational performance of controls by addressing deviations or variances from their intended effectiveness.

Figure 6: FAIR-CAM Variance Management Controls



These controls are not limited to enhancing the reliability of loss event controls but also influence other VMCs and decision support controls (DSCs). For instance, technologies like asset discovery tools can act as VMCs by identifying and rectifying variances in asset data, thereby ensuring the accuracy of asset databases, a critical DSC function.

One key aspect of VMCs is **variance prevention**, which involves minimizing the frequency and likelihood of variances in control performance. Variance often arises during changes, such as software updates, configuration adjustments, or the introduction of new technologies. Organizations can reduce these occurrences by limiting the frequency of changes or ensuring robust practices are in place to mitigate risks associated with those changes. However, some variances, like those caused by emerging threats (e.g., zero-day exploits), cannot be prevented and must be identified and addressed as they occur.

Variance identification is another critical function within the VMC domain. It involves detecting changes that degrade control efficacy, whether due to modifications in the controls themselves or shifts in the threat landscape. Threat intelligence plays a crucial role here, as it helps organizations anticipate and react to emerging vulnerabilities, such as new exploits targeting specific software. Additionally, control monitoring enables the timely detection of variances in control conditions, with the frequency of monitoring tailored to the risk posed by these variances.

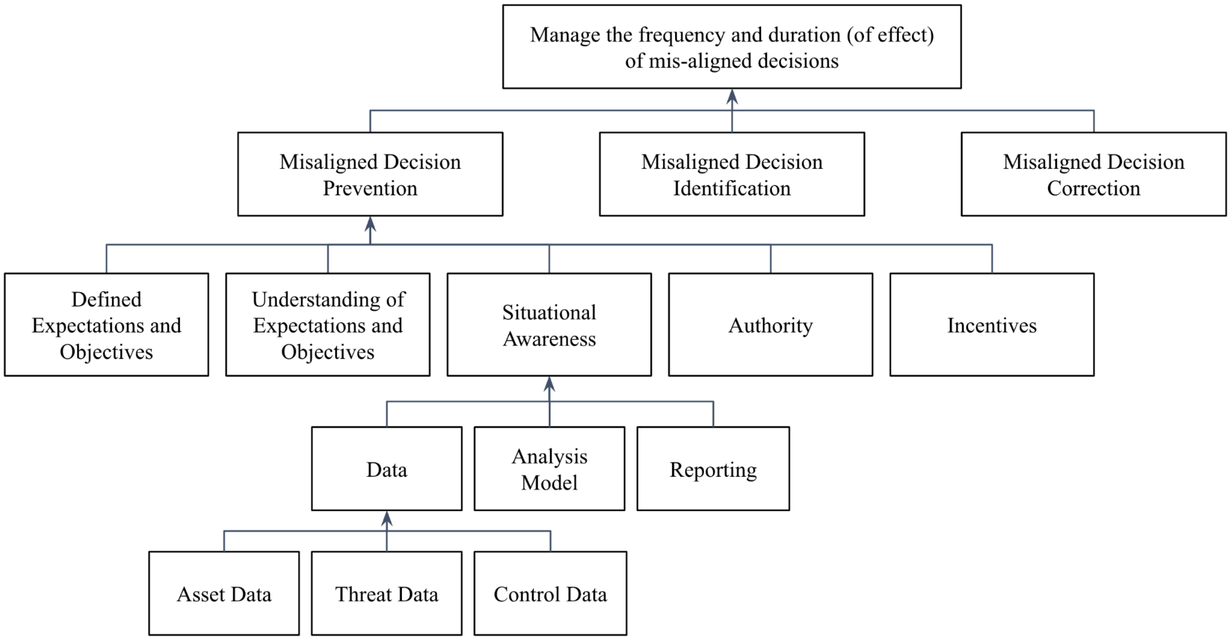
The final step in managing variances is **variance correction**, which involves selecting, prioritizing, and implementing corrective actions. This process relies heavily on DSCs, which provide the data and analysis needed to make informed decisions. Once corrective measures are prioritized, actions such as patching, reconfigurations, or process revisions are executed to restore control performance. The efficiency of this process is measured by the time taken from identifying a variance to fully implementing corrections.

In summary, VMCs play an essential role in maintaining the effectiveness of cybersecurity controls by preventing, identifying, and correcting variances. They safeguard against degradation in control performance and help organizations adapt to an ever-changing threat landscape. By integrating VMCs into a broader risk management framework, organizations can enhance their resilience and ensure consistent control efficacy.

Decision Support Controls

As illustrated below, Decision Support Controls (DSCs) are integral to ensure that organizational decisions align with objectives and expectations, particularly in achieving cost-effective risk management. Organizations must carefully balance limited resources while maintaining an acceptable level of risk. Misaligned decisions—whether they result in exceeding risk appetite, unnecessarily reducing risk, or inefficiently allocating resources—can undermine strategic and operational goals. DSCs are designed to minimize these risks by establishing clear expectations, providing necessary insights, and reinforcing alignment through incentives and situational awareness.

Figure 7: FAIR-CAM Decision Support Controls


Manage the frequency and duration (of effect) of mis-aligned decisions
Misaligned Decision Prevention
Misaligned Decision Identification
Misaligned Decision Correction
Defined Expectations and Objectives
Understanding of Expectations and Objectives
Situational Awareness
Authority
Incentives
Data
Analysis Model
Reporting
Asset Data
Threat Data
Control Data

At their core, DSCs operate across all levels of an organization, from executive strategy and budgeting decisions to individual employee actions. Weaknesses in decision-making processes can lead to systemic issues that materially increase risk exposure. For instance, a lack of clear communication, inadequate data quality, or conflicting incentives can significantly disrupt alignment with organizational objectives. By addressing these deficiencies, DSCs improve the quality of decisions, ensuring consistency and alignment with risk management priorities.

©2025 FAIR Institute. All Rights Reserved.

A key function of DSCs is to **prevent misaligned decisions** by clearly defining and communicating expectations. This involves translating abstract goals, such as a "low-risk appetite," into specific, measurable thresholds that guide decision-making. When expectations are unclear or poorly communicated, decision-makers are more likely to act based on personal judgment or bias, increasing the likelihood of inefficiency or excessive risk. Providing accurate and timely situational awareness further enhances decision quality, equipping decision-makers with the insights needed to evaluate current risks and anticipate the consequences of their actions.

Despite robust prevention measures, some misaligned decisions are inevitable. To mitigate their impact, it is essential to proactively identify misaligned decisions through mechanisms like audits, reviews, and postmortems. This process addresses immediate issues and helps uncover systemic weaknesses that may lead to recurring misalignment. **Correcting misaligned decisions** is often straightforward, such as adjusting a misconfigured system, but addressing the root causes typically requires refining controls related to expectations, communication, or situational awareness.

One illustrative example of DSCs in action is their role in managing control variance. Imagine an organization where access privileges are not consistently updated when employees change roles or leave. This widespread issue reduces the operational performance of controls and increases the risk of loss events. Using the DSC framework, root cause analysis might reveal that while expectations and processes are in place, there are no incentives to motivate compliance. Formal incentives, such as adding access management responsibilities to management objectives, help realign decision-making, reduce access privilege variances, and ultimately lower associated risks and audit costs.

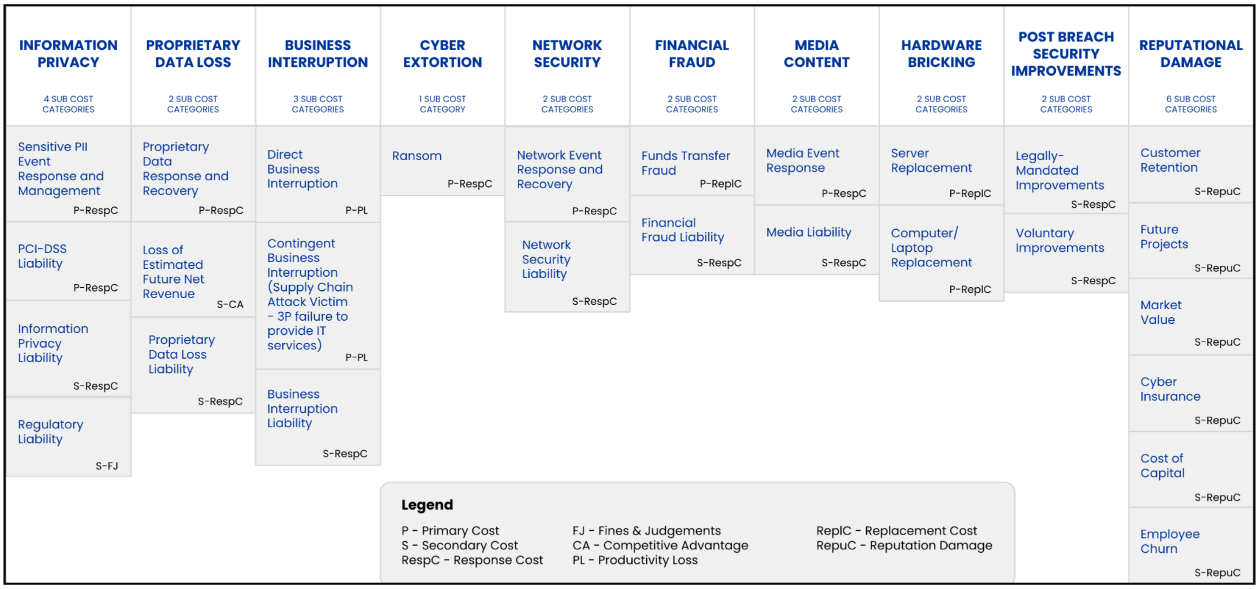
Another example highlights DSCs' role in control choices, such as deciding whether to upgrade a multi-factor authentication (MFA) solution. While an existing MFA may have been effective, changes in the threat landscape can reduce its efficacy. DSCs provide situational awareness through data and analysis in this scenario, enabling decision-makers to assess risks and predict outcomes for various solutions. However, proper alignment ensures decision-makers are incentivized to balance risk management objectives with cost and operational goals. Without such incentives, even robust risk analysis may fail to prompt necessary upgrades, leaving the organization vulnerable.

DSCs are pivotal in aligning decisions with organizational objectives, ensuring that resources are used efficiently and risks are managed effectively. By fostering clarity, accountability, and informed decision-making, DSCs enhance an organization's overall resilience and operational performance. Their implementation is crucial for maintaining alignment with strategic goals while navigating the complexities of modern risk landscapes.

FAIR Materiality Assessment Model: Granular Loss Magnitude Analysis

The FAIR Materiality Assessment Model (FAIR-MAM™) expands upon the FAIR Model's loss magnitude factor and provides a more detailed taxonomy and breakdown of cyber incident losses across 10 categories and 26 sub-categories, as illustrated below. As such, it is specifically designed for cyber risk management use cases but could be extended by risk analysts to include other loss categories.

Figure 8: FAIR-MAM Overview



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-RespC	Proprietary Data Response and Recovery P-RespC	Direct Business Interruption P-PL	Ransom P-RespC	Network Event Response and Recovery P-RespC	Funds Transfer Fraud P-ReplC	Media Event Response P-RespC	Server Replacement P-ReplC	Legally-Mandated Improvements S-RespC	Customer Retention S-RepuC
PCI-DSS Liability P-RespC	Loss of Estimated Future Net Revenue S-CA	Contingent Business Interruption (Supply Chain Attack Victim - 3P failure to provide IT services) P-PL		Network Security Liability S-RespC	Financial Fraud Liability S-RespC	Media Liability S-RespC	Computer/ Laptop Replacement P-ReplC	Voluntary Improvements S-RespC	Future Projects S-RepuC
Information Privacy Liability S-RespC	Proprietary Data Loss 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	FJ - Fines & Judgements	ReplC - Replacement Cost
S - Secondary Cost	CA - Competitive Advantage	RepuC - Reputation Damage
RespC - Response Cost	PL - Productivity Loss	

FAIR-MAM was developed to address the need for better cyber incident loss analysis and reporting, as required by the recent cybersecurity disclosure rules[1] published by the U.S. Securities and Exchange Commission (SEC) and the incident reporting requirements of the NIS 2 Directive[2] in the European Union. Those rules highlight a gap in existing cyber risk management practices, as many organizations lack the means to report on "material" risks from cybersecurity incidents in a timely, accurate, defensible, and comparable way.

[1] U.S. Securities and Exchange Commission. (2023). "Fact Sheet: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." Retrieved from https://www.sec.gov/files/33-11216-fact-sheet.pdf

[2] European Parliament. (14 December 2022). "Directive (EU) 2022/2555 of the European Parliament and of the Council." Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555

Contrary to what one may think based on its name, FAIR-MAM does not help define whether a loss is material. Instead, it helps cyber risk managers and other stakeholders consider all applicable forms of loss given specific risk scenarios and develop more accurate and defensible loss estimates using historical or industry benchmark data, which can then be used to determine materiality.

FAIR-MAM can be used reactively during a cybersecurity event and proactively when performing quantitative cyber risk assessments. Reactively, FAIR-MAM helps organizations more accurately and granularly assess the loss magnitude (cost) of a cybersecurity event. When considered with other *qualitative* aspects of an event, FAIR-MAM helps organizations determine when a cyber incident reaches a material threshold that warrants disclosure[3].

Proactively, FAIR-MAM allows analysts to model potential losses from high-risk scenarios before an incident occurs, helping prioritize risk mitigation efforts and optimize cyber insurance coverage. FAIR-MAM may be used standalone to provide a transparent, standardized, and thorough framework for incident loss estimation, or it may be used in concert with the FAIR Model to support Loss Magnitude estimation.

Figure 8 shows how FAIR-MAM connects to the original FAIR Model by tagging each of its loss categories with the FAIR attributes **Primary** (P) and **Secondary** (S) Losses (referring respectively to the direct and indirect types of losses) and the six (6) forms of losses[4] (**Productivity Loss**; **Response Costs**; **Replacement Costs**; **Fines and Judgments**; **Reputation Damage**; and **Competitive Advantage Loss).**

A Necessary Complement to Risk Management Processes

The FAIR Framework complements risk management processes like those defined by ISO/IEC 27005:2022 by enhancing quantitative analysis capabilities and decision-making along each process step. The following table illustrates how they align with and complement each other:

[3] FAIR-MAM does not and is not intended to help an organization define the threshold at which materiality occurs. The materiality threshold, based on both quantitative and qualitative factors, is a legal decision. Instead, FAIR-MAM gives those decision makers more specific facts to make the decision.

[4] These attributes and their definitions can be found in the Factor Analysis of Information Risk (FAIR) Model Standard.

Attribute	ISO 27005:2022	FAIR Framework
Focus on Quantitative Risk Analysis	Primarily supports qualitative or semi-quantitative methods for assessing risks.	Offers a structured approach to quantifying risk in monetary terms, making it easier to prioritize and justify mitigation strategies based on potential financial impact.
Enhancing Risk Identification and Assessment	Provides detailed guidance on identifying, assessing, and treating information security risks but leaves room for different methodologies to quantify risk.	Provides a clear methodology for analyzing cyber risks in detail, focusing on understanding loss event frequency and magnitude. This complements the broader identification and classification processes in ISO 27005.
Prioritization of Risks	Typically relies on qualitative (high, medium, and low) categories to prioritize risks.	Helps refine this prioritization by quantifying the impact of risks, enabling data-driven decisions about where to allocate resources effectively.
Integration with the Risk Treatment Process	Describes steps to select and implement appropriate risk treatments (controls).	Quantitatively measures the effectiveness of proposed controls to perform "what-if" scenarios, assessing how control changes would alter risk exposure.
Facilitating Communication	Offers guidance on documenting and communicating risk management processes but doesn’t specify how to express risks clearly to business stakeholders.	Translates technical risk into business language by focusing on financial implications, improving communication with non-technical stakeholders, and aligning cybersecurity with business objectives.
Aligning with Governance Standards	Part of the broader ISO/IEC 27000 series, it ensures alignment with international information security management standards like ISO/IEC 27001.	Complements these standards (and other similar risk management standards) by offering an advanced cyber risk quantification mechanism that fits within ISO/IEC 27005's flexible framework.
Iterative Improvement and Automation	Both frameworks encourage iterative refinement of risk management processes.	The FAIR Framework’s detailed quantification capabilities can provide feedback to enhance and refine the implementation of ISO 27005 and automate it when used as part of a Cyber Risk Management System.

By using FAIR in conjunction with risk management processes such as ISO 27005, organizations gain a robust foundation for:

- Comprehensive identification and classification of risks.
- Detailed quantitative analysis and prioritization of risks.
- Aligning cybersecurity efforts with business outcomes through financial quantification.

This combination ensures organizations can effectively manage risks, optimize resource allocation, and communicate risk management insights to all stakeholders.

The Role of a Cyber Risk Management System

A Cyber Risk Management System (CRMS) is necessary for operationalizing the FAIR Framework by ensuring that processes are efficient, repeatable, and actionable. By centralizing the data and workflows needed for managing the entire cyber risk management process, a CRMS provides a single platform where FAIR principles can be operationalized effectively via the following features and capabilities:

- **Supporting an objective, data-driven approach**: Within the CRMS, the FAIR Framework is supported by live data from threat intelligence, vulnerability management systems, and other sources to calculate risks in terms of likelihood and probable impact.
- **Continuous risk monitoring:** Integrating live security data and risk models allows for dynamic and continuous risk monitoring, eliminating the need to manually refresh analyses as conditions change.
- **Risk management automation:** The CRMS automates many of the risk assessment and management tasks that otherwise can be very manual and time-consuming.

The CRMS bridges the FAIR Framework and the risk management process, integrating data and workflows to provide a holistic view of cyber risk. For example, while FAIR-CAM ensures controls are effectively mapped to reduce risks identified by the FAIR Model, FAIR-MAM provides the financial context to assess whether those risks are material and require disclosure or mitigation. By automating many of these processes, the CRMS reduces the risk assessment burden on analysts, ensuring that risk quantification is accurate and scalable.

Ultimately, a CRMS built on the FAIR Framework provides organizations with a comprehensive solution for managing cyber risks in a measurable and actionable way. By quantifying risk in financial terms, assessing the effectiveness of controls, and providing detailed insights into loss magnitude, the system enables better alignment between cybersecurity initiatives and business priorities. This integration improves decision-making at all levels of the organization, ensures compliance with regulatory risk reporting and management requirements, and strengthens overall resilience against cyber threats.

Conclusion

Integrating the FAIR Model, FAIR-CAM, and FAIR-MAM into a cohesive framework provides a comprehensive and quantifiable approach to managing cyber risks. Together, these standards enable organizations to assess cyber risks in financial terms, evaluate the effectiveness of controls, and analyze potential losses with greater precision and reliability. The FAIR Model serves as the foundational structure by breaking down risk into Loss Event Frequency and Loss Magnitude, while FAIR-CAM builds on this by detailing the impact of controls on risk factors. FAIR-MAM adds depth by providing a detailed taxonomy for analyzing loss magnitude and aligning risk management practices with regulatory requirements and organizational priorities.

The Cyber Risk Management System (CRMS) is instrumental in operationalizing these standards as part of a risk management process. By centralizing data, automating workflows, and integrating insights from FAIR Models, the CRMS ensures consistent, efficient, and accurate risk analyses. This system allows organizations to monitor risks in real time, adjust strategies dynamically, and provide timely and defensible reporting. By bridging the gaps between cybersecurity operations and business objectives, the CRMS enhances decision-making, ensuring risk management efforts are strategically aligned.

Adopting a unified framework based on FAIR standards in a rapidly evolving cyber threat landscape positions organizations to address complex challenges proactively. This integration improves risk mitigation strategies and strengthens organizational resilience and compliance. By quantifying risks meaningfully and aligning security initiatives with business goals, organizations can make informed, data-driven decisions, demonstrating a mature and practical approach to cyber risk management.