How to Use FAIR to Mature Your Cyber Risk Management Program with NIST CSF 2.0

A Practical Guide

March 12, 2025

Authors:

Heather Dart, Ph.D.
Cybersecurity Risk Lead
Danaher Corporation
heather.dart@danaher.com

Jack Jones
Chair, Standards Committee
FAIR Institute
jjones@fairinstitute.org

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

Michael Smilanich
Risk Advisory Manager
Safe Security
michael.s@safe.security

Todd Tucker
Managing Director
FAIR Institute
TTucker@FAIRInstitute.org

Table of Contents

Executive Summary

This guide provides a practical, advanced approach to building a Cybersecurity Risk Management Program (CRMP), emphasizing integration with the NIST Cybersecurity Framework (CSF) 2.0 and broader governance methodologies to address sophisticated threats in complex technical ecosystems. It leverages the CSF's Govern function as the structural foundation for defining, measuring, and maturing cybersecurity risk governance to create actionable steps for bridging technical execution with strategic decision-making.

- **WHAT**: A CRMP establishes a structured, risk-driven framework that systematically identifies, assesses, mitigates, and monitors cybersecurity risks, integrating with organizational objectives and regulatory requirements to provide a repeatable process for safeguarding critical systems and data.
- **WHY**: A strong CRMP is essential for defending against cyber threats, ensuring business continuity, and meeting regulatory requirements like NIST CSF, ISO 27001, GDPR, and PCI-DSS. It provides a structured approach to risk management, aligning security efforts with business goals while preventing financial and reputational damage.
- **WHO**: Stakeholders in the CRMP include executives and board members, as well as IT, legal, cyber, and business function or operational teams, all of whom rely on the program's outputs to align security efforts with their related roles in governance, finance, technical execution, and regulatory adherence.
- **WHERE**: Within an organization, the CRMP operates through the Governance, Risk, and Compliance (GRC) function, supported by risk analysts and operational teams. It embeds risk management practices into daily processes and strategic planning across all departments.
- **HOW**: Leveraging the CSF's Govern function, the CRMP defines implementation tiers that guide organizations in assessing their current governance maturity, establishing risk management policies, and enhancing program effectiveness through a structured, scalable roadmap tailored to the organization's unique risk profile..
- **WHEN**: The CRMP is a continuous, ongoing process rather than a point-in-time exercise; it incorporates real-time threat monitoring, period risk assessments, and iterative improvements to effectively address dynamic cybersecurity threats and organizational changes.

- Shift Right: By integrating the Factor Analysis of Information Risk (FAIR) model, the CRMP advances to a more data-driven and forward-looking approach. This allows for the quantification of risk in financial terms and provides an avenue for precise, predictive decision-making designed to optimize outcomes.

This guide assumes familiarity with the overall NIST cybersecurity methodology and aims to equip organizations with actionable insights to develop, refine, and sustain an effective cyber risk governance strategy.

What: Overview of the Cybersecurity Risk Management Program

In today's complex digital landscape, organizations must take a proactive, structured approach to managing cybersecurity risks, making a Cybersecurity Risk Management Program (CRMP) a strategic necessity. A CRMP implements a repeatable framework for identifying, assessing, prioritizing, mitigating, and continuously monitoring cyber risks, ensuring alignment with business objectives, regulatory mandates, legal priorities, and industry best practices.

A well-designed CRMP enables informed, risk-based decision-making, balancing security needs with business goals to support and sustain the organization's mission. It leverages frameworks like NIST CSF 2.0 to guide policies, processes, and controls while addressing compliance with regulations such as the SEC cybersecurity disclosure rule, PCI DSS, and NERC CIP. By embedding cyber risk into governance and decision-making, the CRMP transforms security from a technical concern into a business enabler, strengthening resilience and stakeholder confidence.

NIST Cybersecurity Framework (CSF) 2.0

The **NIST Cybersecurity Framework (CSF) 2.0** is a globally recognized standard that helps organizations strengthen cybersecurity through a flexible, business-oriented approach. It defines high-level cybersecurity outcomes without prescribing specific methods, making it adaptable across industries. Implementing the Govern function in CSF 2.0 enhances alignment with enterprise governance, risk management, and business priorities by clarifying roles, defining risk strategies, and ensuring oversight. This integration makes the CSF a critical tool for proactive risk management, stakeholder alignment, and bridging cybersecurity with business objectives in today's evolving threat landscape.

The NIST CSF 2.0 Govern function is provided below:

Table 1: The NIST CSF 2.0 Govern Categories and Subcategories

Category	Subcategory
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders
	GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties

Category	Subcategory
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions
Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.
	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.
	GV.RR-04: Cybersecurity is included in human resources practices.
Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced	GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities, and are communicated and enforced.
	GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks

Category	Subcategory
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
	GV.SC-04: Suppliers are known and prioritized by criticality
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

Category	Subcategory
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Why: The Need for a Strong CRMP

In today's cyber threat landscape, where attackers relentlessly exploit vulnerabilities with increasing sophistication, every stakeholder has a vested interest in a strong, effective CRMP. A well-structured program ensures cybersecurity efforts align with business objectives while defending against ransomware, data breaches, operational disruptions, and other threats.

A strategic CRMP empowers governance and leadership teams to safeguard long-term business goals while enabling operational teams to maintain system reliability under constant cyber pressure. It also plays a critical role in regulatory compliance, helping organizations meet stringent requirements such as NIST CSF, ISO 27001, GDPR, CCPA, SEC cybersecurity disclosure rules, and industry-specific mandates like HIPAA and PCI-DSS. The CRMP shields organizations from legal penalties, fines, and reputational damage by providing structured risk assessments, security controls, and audit-ready documentation.

Cyber risk is no longer just an IT issue but a business imperative. A well-executed CRMP protects systems and data and ensures regulatory adherence, business resilience, and long-term success in an era of evolving threats and increasing compliance expectations.

Who: Stakeholders in a CRMP

The success of a CRMP depends on strong engagement from diverse stakeholders, each with unique roles and vested interests. These stakeholders fall into two categories: **internal constituents**, who drive and implement the program, and **external constituents**, who rely on it for security and assurance.

Internal Constituents

Internal stakeholders typically include the following:

- **Board of Directors** – Provides governance and strategic oversight. A strong CRMP reassures the board that cybersecurity risks are well-managed, regulatory requirements are met, and shareholder value is protected.

- **CEO** – Accountable for business success and reputation. The CRMP helps mitigate cyber risks that could disrupt operations, erode trust, or lead to financial losses, aligning security with business objectives.
- **CFO** – Focused on financial health and risk exposure. An effective CRMP prevents costly breaches, regulatory fines, and legal liabilities, ensuring budget allocations support informed risk priorities.
- **CISO** – Responsible for security strategy. The CRMP delivers risk insights and mitigation strategies, helping justify security investments and strengthen the organization's defenses.
- **IT Managers & Directors** – Manage technical infrastructure. CRMP outputs, such as risk assessments and mitigation plans, guide resource allocation, system hardening, and incident response to ensure reliability.
- **Legal & Compliance Officers** – Ensure regulatory adherence. The CRMP provides documentation and risk-based security controls, reducing liability and demonstrating due diligence.

External Constituents

External stakeholders typically include:

- **Customers** – Expect secure, uninterrupted services. A strong CRMP protects their data, builds trust, and prevents breaches that could impact privacy or disrupt business.
- **Shareholders** – Invest in financial stability. A CRMP enhances transparency, reduces cybersecurity risks, and safeguards stock performance and dividends from the impact of cyber losses (e.g., reputation damage, business interruption)..
- **Auditors** - Assess the organization's controls and control environment. A CRMP helps demonstrate the effective management of internal (cybersecurity) controls.
- **Regulators** — Mandate and assess compliance with cybersecurity standards. A CRMP is often mandated by regulations or helps ensure other mandates are satisfied.

A **well-implemented CRMP is not just a security measure—it's a business enabler**. It aligns cybersecurity with business priorities, delivering measurable benefits such as reduced risk, enhanced resilience, and regulatory compliance. Organizations can transform cyber risk from a liability into a strategic advantage by engaging all stakeholders.

Where: The CRMP in Organizational Structure

The CRMP must be thoughtfully positioned within an organization to maximize its impact on strategic alignment, business enablement, and risk-driven decision making. We make the following recommendations on the organizational structure to support the CRMP.

1. **Alignment with the CISO**: The CRMP should ideally report directly to the CISO. This ensures it remains independent, has direct access to cybersecurity initiatives, and can escalate risks without interference from operational, IT, or business units.
2. **Ownership under the VP/Director of GRC**: The GRC leader should oversee the CRMP, integrating risk, compliance, and governance. This role must have clear decision-making authority and a dedicated budget to drive meaningful outcomes.
3. **Investment in Risk Capabilities**: Building a skilled risk team is critical. The GRC leader should focus on strengthening expertise in risk assessment, mitigation, and reporting.
4. **Cultural Change Leadership**: Cyber risk management is as much about culture as it is about processes. The CISO and GRC leader must champion education and awareness, ensuring the entire organization understands the CRMP's value and their role in it.

This structure ensures the CRMP is not just a compliance function but a strategic enabler of business resilience.

How: Implementing a CRMP

At the highest level, to build a Cyber Risk Management Program (CRMP), organizations must focus on three foundational areas:

1. **Governance & Strategy**
    - Establish program documentation that serves as the "North Star" and answers the critical WHO, WHAT, WHEN, WHERE, WHY, and HOW.
    - Align cybersecurity goals with business objectives.
    - Ensure adequate executive & key stakeholder sponsorship.
2. **Risk Assessment & Management**
    - Identify key assets and threats.

- Conduct risk assessments using documented qualitative and/or quantitative methods to inform decision-making.
- Document assessment results, inform stakeholders, and implement risk mitigation, transfer, or acceptance strategies.

3. **Operational Execution & Continuous Monitoring**
    - Continuously monitor the environment and track risk assessment results over time by
        i. Integrating technology and security stacks with risk assessment practices
        ii. Consume compliance audit results as inputs to risk assessment activities
    - Partner with stakeholders to ingest security concerns and perform appropriate analysis to return information relevant to documented concerns, enabling risk-informed decision making or Risk Management as a Service.

CRMP Implementation Tiers based on NIST CSF 2.0

NIST does not explicitly define implementation tier criteria for CRMPs. To solve this, we are recommending implementation descriptions for each Tier. These definitions can be used to assess your organization's Governance Function based on NIST:

GV.OC: Organizational Context

"The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	The organization lacks a clearly defined and communicated mission and vision, leading to an unclear relationship between cybersecurity and strategic goals. As a result, cyber risks are difficult to assess, and cybersecurity remains an afterthought, with little to no alignment with evolving organizational strategy.	The organization's mission and vision are defined, but the link between cybersecurity and strategic goals is clear only at the management level. Cybersecurity is considered during planning but treated as a checklist item, with alignment to evolving strategy remaining ad-hoc.	The organization's mission and vision are defined, and cybersecurity is clearly integrated into strategic goals, continuously informing risk management. Cybersecurity is viewed as a business enabler, with a structured process ensuring alignment as the strategy evolves.	The organization's mission and vision are defined, and cybersecurity is fully integrated into strategic goals and continuously informs risk management. Cybersecurity is treated as a business enabler with a proactive, structured alignment process and a well-established learning loop for continuous improvement.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Stakeholders are identified informally as needed, with a limited understanding of their expectations and reactive responses. Their needs are rarely explicitly considered in cybersecurity risk management decisions.	Stakeholders are identified, but the list is incomplete and not regularly updated. Efforts to understand their expectations are informal, and while acknowledged, these expectations are not systematically integrated into cybersecurity risk management.	A formal process ensures all relevant stakeholders are identified and documented, with regular assessments to understand their needs. Their expectations are systematically integrated into cybersecurity risk management policies and procedures.	Stakeholder identification is continuously updated to reflect organizational and environmental changes, with proactive engagement to anticipate needs. Their input drives a dynamic, responsive cybersecurity risk management strategy that evolves with expectations.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	Legal, regulatory, and contractual requirements are identified only when necessary, with no structured tracking process. Compliance efforts are reactive and not integrated into risk management, and there is little to no internal communication or training on cybersecurity compliance.	Regulatory and contractual requirements are identified and documented, but compliance is primarily driven by external audits rather than internal strategy. Security planning considers these requirements, but application is inconsistent, with gaps in mapping controls to compliance frameworks. Compliance training exists but is informal, with limited organization-wide awareness.	The organization maintains a formal, regularly updated process for identifying and mapping legal, regulatory, and contractual obligations to cybersecurity policies. Compliance is fully integrated into risk management, with regular assessments to ensure adherence to evolving requirements. Scheduled training programs ensure employees understand compliance obligations, with documented policies enforced across all business units.	The organization proactively tracks and adapts to evolving legal, regulatory, and contractual requirements using automated compliance monitoring. Compliance is seamlessly integrated into risk management, continuously improving through predictive analysis and industry collaboration. Training is role-specific and embedded in security awareness programs, fostering a culture where compliance is seen as a business enabler rather than a checkbox exercise.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	The organization has limited awareness of the critical objectives, capabilities, and services that external stakeholders rely on. There is no formal process for identifying or communicating these dependencies, leading to a reactive approach in addressing stakeholder concerns.	The organization recognizes key external dependencies but lacks a consistent, structured approach to documenting and communicating them. Some efforts address stakeholder expectations, but engagement is ad-hoc and reactive rather than proactive.	A formal process exists to identify, document, and communicate critical services and capabilities that external stakeholders depend on. These dependencies are regularly reviewed, and stakeholder engagement is structured to ensure alignment with expectations.	The organization has a dynamic and proactive approach, continuously assessing and adapting to stakeholder needs. Communication is seamless, and the organization actively collaborates with stakeholders to enhance resilience and service reliability.
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	The organization has a limited understanding of the outcomes, capabilities, and services it depends on, with no formal process for identification or communication. Dependencies are reactively addressed, often only during incidents or disruptions.	Key outcomes, capabilities, and services are recognized but not comprehensively documented. Some communication occurs, but it is informal and inconsistent across departments. Dependencies are considered in decision-making but not systematically integrated into risk management.	The organization has a structured and well-documented approach to identifying and communicating dependencies. Dependencies are regularly assessed, and the organization ensures consistent communication across teams, integrating them into risk management and strategic planning.	Dependencies are continuously monitored and dynamically updated using processes and automated data-driven insights. Communication is proactive and embedded into decision-making at all levels, ensuring resilience and agility in response to changing risks and business needs.

GV.RM: Risk Management Strategy

"The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	Risk management objectives are not clearly defined or formally established. Objectives either don't exist or are set reactively.	Risk management objectives are defined but not consistently documented or communicated. Alignment across the organization is weak, risk objectives are considered but not fully integrated into business strategy.	The organization has a structured and documented approach to establishing risk management objectives, with regular reviews. Objectives are aligned with business goals and consistently integrated into risk management processes.	Risk management objectives are continuously refined and dynamically updated based on emerging threats, business changes, and stakeholder input. A collaborative, data-driven approach ensures objectives are well-communicated and proactively influence strategic decisions.
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	No formal risk tolerance established; decisions made without accurate data in an ad hoc or reactive method.	Risk tolerance is defined but not consistently applied across the organization. Organization lacks a defined risk appetite.	Risk appetite and tolerance are clearly defined and consistently applied against risk tolerance.	The organization's risk appetite vs. actual risk is reviewed on a regular basis. Continuous refinement occurs based on analyzed risk data and threat intelligence.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	Risk prioritization is ad hoc and inconsistent, cybersecurity risks are not aggregated and rolled up into ERM processes.	While cybersecurity risks are included or rolled up into the ERM process, mitigation efforts are not actively tracked.	Cybersecurity risks and associated Plan of Actions and Milestones (POA&Ms) are monitored and reported on through the organization's ERM processes.	The organization's cybersecurity risk, along with the associated POA&Ms, are regularly normalized and aggregated into the ERM processes; cybersecurity risks show the evolution of the related risks based on mitigation investment.
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	No structured risk mitigation approach exists; risk responses are ad hoc or reactive.	Basic risk mitigation strategies are documented but not consistently applied.	Risk mitigation plans are strategically aligned and integrated into IT and business operation functions. Risk mitigation investments are actively monitored through a POA&M and prioritized based on quantifiable risk data.	Risk mitigation strategies are strategically aligned and optimized using predictive analytics. Risk mitigation investments are based on quantified risk levels and implemented in an agile manner.
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Risk reporting is ad hoc, inconsistent, or lacking standardization.	Risk reports are generated and reviewed periodically but may not be comprehensive or actionable.	Standardized, actionable, and regularly scheduled risk reporting is in place with defined metrics.	Real-time, continuous monitoring risk management dashboards are in place with strategic, actionable, and executive-level insights.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Methods of managing risks are either ad hoc or not existent.	A standardized method of managing and prioritizing risks exists but heavily relies on subjective or qualitative measures . Stakeholder communication exists but lacks integration with risk management processes.	A documented method of risk lifecycle management exists that incorporates a level of quantitative measurement of risk in financial terms. The lifecycle includes a proactive and structured risk communication strategy, aligned with business needs.	A fully implemented risk management program exists incorporating quantitative measurement of risk using integrated threat, control, and assessment data.
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Risk management processes, if they exist, are ad hoc and do not consider strategic opportunities.	Strategic risk responses are considered in some areas but without active integration.	Fully integrated strategic risk management responses are in place and strategically aligned with the organization's enterprise.	Strategic risk management responses are continuously considered through the use of data-informed predictive analytics..

GV.RR: Roles, Responsibilities and Authorities

"Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	Leadership lacks formal responsibility for cybersecurity risk; no defined risk culture.	Leadership acknowledges cybersecurity risks but addresses them reactively. A basic risk-aware culture exists.	Leadership is actively accountable for cybersecurity and promotes a strong risk-aware culture. Stakeholders understand how to consider cybersecurity risks in the context of their business.	Leadership continuously fosters a cybersecurity-informed culture. Stakeholders regularly consider cybersecurity risks in the context of their business, including financial outcomes.
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	Cybersecurity roles and responsibilities are unclear or undocumented.	Roles and responsibilities are defined but not consistently understood or enforced across teams.	Clearly documented cybersecurity roles, responsibilities, and authorities, with training to ensure alignment.	Roles and responsibilities dynamically evolve with emerging risks, supported by continuous learning and incentive alignment.
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	Cybersecurity resources are minimal, insufficient, and reactive.	Cybersecurity receives some dedicated resources, but allocation is inconsistent and not aligned with risk levels.	Adequate cybersecurity resources are systematically allocated based on risk assessments and business needs.	Cybersecurity resources are continuously optimized using insights from proactive risk modeling.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.RR-04: Cybersecurity is included in human resources practices.	Cybersecurity considerations are absent from HR processes (e.g., hiring, training, offboarding).	Basic cybersecurity training exists, but HR processes do not systematically enforce cybersecurity policies.	Cybersecurity is embedded in HR policies, including structured training, onboarding, and offboarding protocols.	HR practices integrate real-time threat intelligence, training programs, and adaptive security measures.

GV.PO: Policy

"Organizational cybersecurity policy is established, communicated, and enforced."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities, and are communicated and enforced.	Cybersecurity risk management policies and procedures are informal, undocumented, or inconsistently applied.	Basic cybersecurity risk management policies exist but are not consistently enforced or communicated across the organization.	Well-defined, documented, and enforced cybersecurity risk management policies exist and are aligned with business strategy. Regular staff training ensures compliance.	Cybersecurity risk management policies are created, communicated, implemented and maintained with clear objectives and stakeholder alignment; Policies are regularly refined based on evolving threats, business changes, and real-time feedback, leveraging automation and incentives for enforcement.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Cybersecurity policies are static and rarely reviewed or updated.	Policies are reviewed periodically, but updates may lag behind emerging threats and technological advancements.	Policies undergo regular, systematic reviews to reflect new threats, regulations, and organizational priorities.	Policies are dynamically updated using real-time threat intelligence and continuous stakeholder feedback.

GV.OV: Category: Oversight

"Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	No baseline risk measurement exists, resulting in an inability to measure risk burndown over time.	The risk baseline is established with some decisions risk-informed, however, risk burndown measurement is not tracked.	Risk burndown - based on operational and strategic investments and risk-informed decisions - is measured to understand the effectiveness of the cyber risk management program.	The baseline of risk is clearly established. Risk burndown - based on operational and strategic investments and risk-informed decisions - is measured to understand the effectiveness of a cyber program; continuous adjustments are made to the risk burndown strategy to adjust based on real-time data and insights from internal and external environments.
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	Cybersecurity risk management strategy is undocumented or ad hoc with limited consideration of evolving organizational requirements and emerging risks.	The CRMP strategy is reviewed periodically, but updates may not fully address all organizational requirements or emerging threats.	The CRMP strategy ensures comprehensive coverage of organizational requirements and identified risks.	The CRMP strategy undergoes continuous refinement, leveraging data inputs from audit findings, cyber incidents, threat environment, and predictive analytics to anticipate and address emerging risks and organizational changes.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	CRMP performance evaluations are informal, infrequent, and lack clear metrics; adjustments are made ad hoc or reactively.	Basic performance metrics are established, and CRMP evaluations occur periodically, but they may not lead to timely or effective adjustments.	Comprehensive CRMP performance metrics are defined and regularly assessed; evaluation results drive systematic improvements in risk management practices.	CRMP performance management is an ongoing process that utilizes advanced analytics and real-time monitoring; continuous improvements are made through feedback mechanisms and adaptive strategies.

GV.SC: Supply Chain Risk Management

"Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders."

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Infrequent or ad hoc reviews of cybersecurity risk management outcomes; adjustments are reactive and lack a structured approach.	Supply chain risk management is very reactive - focused on a checklist exercise instead of being risk-based. No clear strategy is defined at the organizational level, and the teams are working independently	A cross-functional strategy for supply chain risk management is built with clear objectives, policies, and procedures. A risk-based program is also built. The strategy aligns cross-organizational teams such as IT, cybersecurity, operations, legal, and HR.	A cross-functional strategy for supply chain risk management is built with clear objectives, policies, and procedures. The strategy aligns cross-organizational teams such as IT, cybersecurity, operations, legal, and HR. Continuous improvement of the strategy based on outcomes and the evolving risk environment is built into the processes.
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Undefined or informal roles and responsibilities; lack of coordination.	Roles are defined but not consistently communicated or enforced; limited internal coordination.	Roles and responsibilities are continuously assessed, documented, and refined; one or more specific positions are present; performance goals are defined	Roles and responsibilities are continuously assessed, documented, and refined; one or more specific positions are present; performance goals are defined, and proactive collaboration with all stakeholders is practiced.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Supply chain risk management is siloed and not integrated into broader risk processes.	Partial integration with enterprise risk management; inconsistently applied.	Fully integrated into enterprise risk management, risk assessments, and improvement processes.	Seamless integration with enterprise risk management, including supply chain risks in enterprise risk registers and adaptive strategies informed by continuous monitoring and analysis.
GV.SC-04: Suppliers are known and prioritized by criticality	Suppliers are not assessed or prioritized by criticality.	Limited discovery and tiering of third parties. Tiering is subjectively defined and not measured.	Most third parties are discovered, and a 'shadow' third-party attack surface might exist. Clear criteria to tier third parties based on the risk posed to your business has been developed. The risk can be measured based on access to sensitive data, access to the network, and potential disruption to business. The criteria are objectively defined based on quantified risk measurements.	All third parties are discovered and assessed. Develop clear criteria to tier third parties based on the risk posed to your business; the risk can be measured based on access to sensitive data, access to network, and potential disruption to business. The criteria are objectively defined based on quantified risk measurements. The criteria are proactively assessed based on organizational risk thresholds and evolving risk environments.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Cybersecurity requirements are absent or inconsistently included in supplier contracts.	Some contracts include basic cybersecurity clauses, but they are not standardized.	Standardized cybersecurity requirements are established and integrated into all relevant supplier agreements.	Contracts are dynamically updated to reflect evolving threats and compliance requirements; cybersecurity requirements are clearly documented in contracts based on criticality of a third party; collaborative development of security standards with suppliers.
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Minimal or no due diligence conducted before engaging suppliers.	Basic due diligence is performed for select suppliers; consistency is lacking.	Comprehensive planning and due diligence processes are standardized and applied to all supplier engagements.	Advanced due diligence incorporates risk-based control assessments, threat intelligence and continuous monitoring; proactive risk mitigation strategies before formalizing relationships. Looking at both internal and third party controls for managing risk; proactively evolving the due diligence process based on new threats and business relationships.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Supplier risks are assessed infrequently or reactively.	Periodic assessments conducted, but not consistently monitored.	Based on due diligence, clearly understand the prioritized actions for managing risk - for the third party. Document and Monitor the completion of the actions continuously.	Based on due diligence, clearly understand the prioritized actions for managing risk - both for the third party and the first party. Document and Monitor the completion of the actions continuously. Monitor any changes in business relationships continuously.
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Suppliers are excluded from incident response planning and activities.	Limited inclusion of key suppliers in incident response plans.	Relevant suppliers are actively involved in incident planning, response, and recovery efforts.	Collaborative incident response with suppliers; joint simulations and continuous improvement of response strategies.
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Supply chain security practices are ad hoc and not integrated into broader programs.	Some integration exists, but practices are not consistently applied or monitored.	Risk reporting is provided to the leaders, risk driven metrics are monitored and used to measure the effectiveness of the supply chain risk program.	Risk reporting is provided to the leaders, risk driven metrics are monitored and used to measure the effectiveness of the supply chain risk program, continuous enhancement of supply chain security through innovation, real-time monitoring, and alignment with industry best practices.

Subcategory	Tier 1 - Partial	Tier 2 - Risk-Informed	Tier 3 - Repeatable	Tier 4 - Adaptive
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	No provisions for cybersecurity after the conclusion of supplier relationships.	Limited consideration of post-contractual cybersecurity activities.	Defined plans addressing cybersecurity activities post-contract, including data handling and access termination.	Established processes for terminating third party relationships; verify that assets/data/identities are returned and/or deactivated; Proactive management of post-contract cybersecurity; lessons learned are integrated into future supplier engagements and policies.

When: Continuous CRMP Operations

CRMP is a continuous, dynamic process, not a one-time effort. It ensures constant monitoring of systems, risks, and assets. Regular updates to risk assessments and controls address new threats and business changes. This ongoing cycle enables proactive defense, regulatory alignment, and business resilience.

A static, point-in-time cyber risk management approach leaves organizations exposed to evolving threats. Cyber risks don't pause, and neither should your defenses. A continuous Cyber Risk Management Program (CRMP) transforms cybersecurity from a compliance checkbox into a proactive, strategic advantage—protecting operations, financial stability, and stakeholder trust.

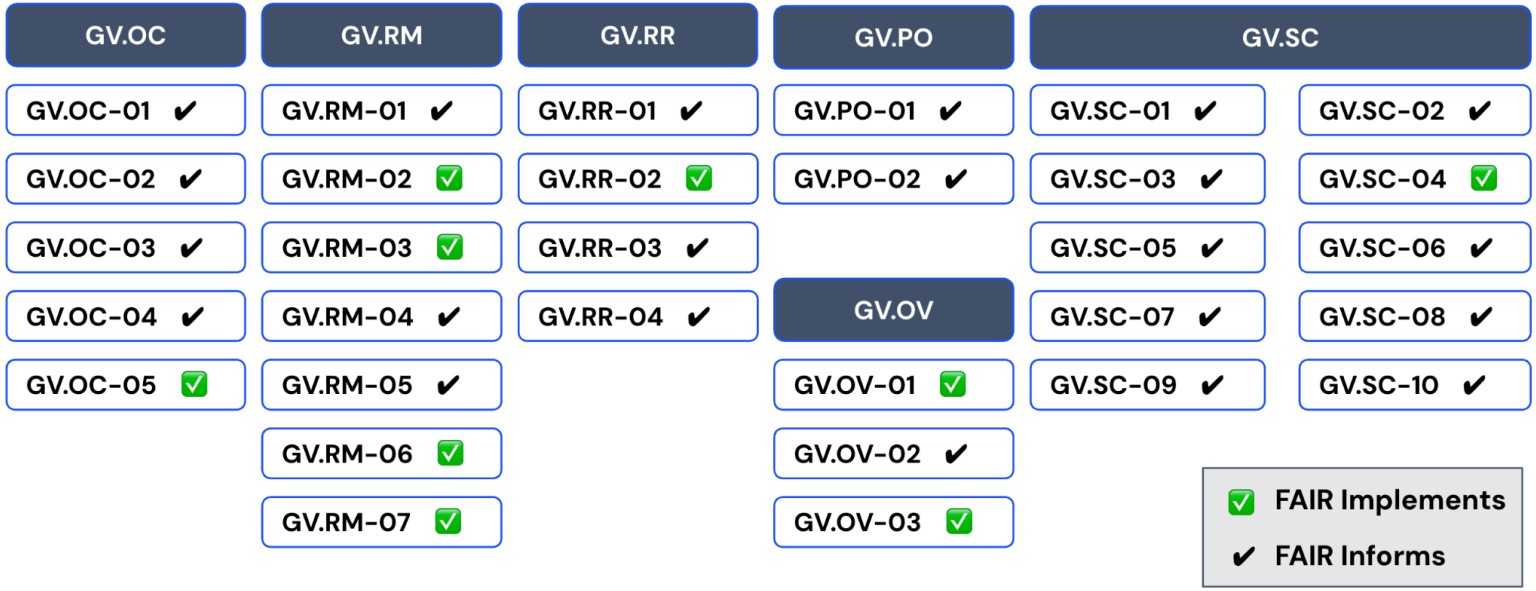
Shift Right: Enhancing CRMP Maturity with FAIR

The Factor Analysis of Information Risk (FAIR) model provides a quantitative approach to cybersecurity risk management, helping organizations:

- Translate cybersecurity risks into financial terms for business decision-making.
- Conduct risk quantification to prioritize security investments based on impact likelihood.
- Establish a structured methodology for assessing, mitigating, and reporting cyber risks.

The following (Figure 1) illustrates where FAIR implements or informs each of the NIST CSF 2.0 Govern function categories.

Figure 1: Mapping Support of FAIR for NIST Govern Function



The following table describes in more detail how FAIR helps CRMP leaders address each of the subcategories in the Govern function.

Subcategory	How FAIR Helps	Explanation
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Informs**	FAIR-based quantification can align business and cyber objectives based on the common language of dollars and cents.
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Informs**	FAIR can be used to assess stakeholder-related risks by quantifying the potential impact of cybersecurity risks on internal and external stakeholders.
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	**Informs**	FAIR does not directly track legal and regulatory compliance but can help quantify the financial and operational impact of non-compliance risks.
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	**Informs**	FAIR can support understanding of critical objectives by modeling the financial and operational impact of risks affecting external stakeholder expectations.
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	**Implements**	FAIR helps assess risks to services and capabilities the organization depends on by quantifying their potential impact and likelihood.
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	**Informs**	FAIR supports establishing risk management objectives by providing a structured approach to quantifying and prioritizing cyber risks.
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	**Implements**	FAIR aids in defining risk appetite and tolerance by translating qualitative statements into quantifiable risk thresholds.

Subcategory	How FAIR Helps	Explanation
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	**Implements**	FAIR can help establish a common framework to measure risk across the enterprise, including cyber risk
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	**Informs**	FAIR helps in evaluating strategic risk response options by quantifying the cost-benefit of different mitigation strategies.
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Informs**	FAIR supports risk communication by providing a standardized framework for expressing cyber risks in business-relevant terms.
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Implements**	FAIR provides a standardized method for quantifying, categorizing, and prioritizing cybersecurity risks, improving risk assessments.
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	**Implements**	FAIR primarily focuses on loss events but can be adapted to consider strategic opportunities by evaluating positive risk scenarios.
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	**Informs**	FAIR fosters a risk-aware culture by enabling leadership to understand and prioritize cybersecurity risks in financial terms.
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	**Implements**	FAIR can define quantitative levels of authority for accepting risk at different organizational levels.
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	**Informs**	FAIR helps in resource allocation by quantifying risk exposure and justifying cybersecurity investments based on risk reduction.
GV.RR-04: Cybersecurity is included in human resources practices.	**Informs**	FAIR can inform the cybersecurity-linked incentive structure for the organization

Subcategory	How FAIR Helps	Explanation
GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities, and are communicated and enforced.	**Informs**	FAIR analyses can inform different policy decisions on cybersecurity, such as password policy, third party due diligence, business resiliency, regulatory responses.
GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	**Informs**	If the FAIR quantified risk changes significantly, it can warrant a comprehensive review of the policy.
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	**Implements**	FAIR can help quantify the organizational risk; and the impact of operational and strategic actions to reduce risk
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	**Informs**	FAIR can help assess the magnitude of change in risk due to changing internal and external factors. This magnitude of change can inform the level of adjustment required in the risk management strategy.
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	**Implements**	FAIR can measure the risk - providing a quantified objective metric for measuring performance of the risk program.
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	**Informs**	FAIR can inform the third party program structure - such as tiering - to run the program in the most efficient and effective way possible.
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	**Informs**	FAIR can inform the incentive structure of team members.

Subcategory	How FAIR Helps	Explanation
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	**Informs**	FAIR Framework can provide a uniform framework to measure enterprise and third party risk - allowing for a uniform measurement and integration.
GV.SC-04: Suppliers are known and prioritized by criticality	**Implements**	FAIR can be used to quantify the risk exposure of third parties in defensible quantitative terms.
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	**Informs**	FAIR can help assess the criticality of a third party - based on which different contractual requirements can be set with a third party.
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Informs**	FAIR helps assess risks before entering supplier agreements by quantifying potential loss exposure.
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	**Informs**	FAIR helps in prioritizing actions based on quantified risks.
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	**Informs**	FAIR can help identify the riskiest vendors for this planning exercise
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	**Informs**	FAIR helps in quantifying risk of the overall third party program - that can be used to measure the effectiveness of the third party program overall.

Subcategory	How FAIR Helps	Explanation
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Informs**	Offboarding requirements and processes can vary based on the quantified risk tier of a third party.

Conclusion

Implementing a Cyber Risk Management Program (CRMP) based on a Cyber Risk Management Framework (CRMF) is essential for modern enterprises, but success depends on translating principles into actionable organizational decision-support. Cyber risk is no longer just an IT issue—it's a business-critical challenge.

By leveraging FAIR-based quantification organizations can measure progress, justify investments, and make data-driven decisions.

A strong Cyber Risk Management Program (CRMP) extends beyond implementation to strategic, continuous risk management. Positioned under the CISO for independence, it safeguards against cyber threats, preventing disruptions, financial loss, and eroded trust. Rooted in the NIST CSF's Govern function and powered by data, automation, and risk analysts, it transforms cybersecurity from a technical burden into a business advantage, ensuring resilience and competitive strength.

Appendix

Other Approaches to Defining Governance

There are many international standards an organization can leverage in the development of their CRMP, NIST includes a large cybersecurity platform including the NIST Risk Management Framework (RMF) and the NIST Security Control Catalog (SP 800-53 revision 5.1.1). NIST is just one of many frameworks that are widely available and supported with continuous updates. See the list below for suggestions:

1. ISO 27001:2022/27002 (International Organization for Standardization)

- A globally recognized standard for information security management systems (ISMS).
- ISO 27001 focuses on risk management and security controls.
- ISO 27002 provides best practices and implementation guidelines.

2. CIS (Center for Internet Security) CSC (Critical Security Controls) v8.1

- A prioritized set of cybersecurity best practices focused on practical defense strategies.
- Useful for organizations looking for a straightforward approach to securing their systems.
- Often used in conjunction with other frameworks like NIST CSF.

3. ISACA (Information Systems Audit and Control Association) COBIT (Control Objectives for Information and Related Technologies) 2019

- A governance framework developed by ISACA.
- Focuses on aligning IT security with business goals.
- Useful for risk management and compliance in enterprise environments.

4. AICPA (Association of International Certified Professional Accountants) TSC (Trust Services Criteria) SOC (Service Organization Control) 2

- A framework for managing customer data based on five trust service criteria: security, availability, processing integrity, confidentiality, and privacy.
- Frequently used by SaaS providers and cloud service companies.

5. PCI DSS (Payment Card Industry Data Security Standard)

- A mandatory framework for organizations handling credit card transactions.
- Ensures secure handling of cardholder data and payment security.

6. HITRUST CSF (Health Information Trust Alliance Common Security Framework)

- A security and compliance framework designed for the healthcare industry.
- Integrates multiple standards, including NIST, ISO, and HIPAA.

7. FFIEC (Federal Financial Institutions Examination Council) Cybersecurity Assessment Tool

- A framework designed for the financial sector.
- Helps banks and financial institutions assess their cybersecurity maturity.

8. GDPR (General Data Protection Regulation) & CCPA (California Consumer Privacy Act)

- While not traditional cybersecurity frameworks, they establish data privacy and security guidelines.
- Companies processing personal data must comply with these regulations.