SAFE

How to Use SAFE to Mature Your Cybersecurity Risk Management Program with NIST CSF 2.0

Authors:
Pankaj Goyal; Michael Smilanich; Chris Khadan

March 2025

Executive Summary

This guide builds on the white paper published by the FAIR Institute on using FAIR to build a robust Cybersecurity Risk Management Program (CRMP). It leverages the definitions of the implementation tiers of NIST CSF 2.0 GOVERN framework, and focuses on how the SAFE platform can help organizations build a continuous data-driven CRMP.

The guide will recap the What, Why, Who, Where of the original white paper; and then discuss building this program using the SAFE platform.

- **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 Cybersecurity 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, embedding 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 address dynamic cybersecurity threats and organizational changes effectively.
- **Shift Right**: By leveraging the SAFE Platform, the CRMP advances to a more data-driven and forward-looking approach, allowing for quantification of risk in financial terms and providing 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 Cybersecurity risk governance strategy.

We will start with the recap of the content from the original white paper, and conclude with how SAFE can help in Chapters 7-8.

Chapter 1 - **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 provides a repeatable framework for identifying, assessing, prioritizing, mitigating, and continuously monitoring cybersecurity risks, ensuring alignment with business objectives, regulatory mandates, 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 cybersecurity 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. The introduction of 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.

An overview of the Govern function is below:

Category	Sub-Category
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
	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

Category	Sub-Category
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
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed

Category	Sub-Category
Cybersecurity Supply Chain Risk Management (GV.SC): Cybersecurity 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
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Table 1: The NIST CSF 2.0 Govern Categories and Sub-Categories

Chapter 2 - **Why:**

The Need for a Strong CRMP

In today's cybersecurity 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 threats like ransomware, data breaches, and operational disruptions.

A strategic CRMP empowers governance and leadership teams to safeguard long-term business goals while enabling operational teams to maintain system confidentiality, availability, and integrity under constant 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. By providing structured risk assessments, security controls, and audit-ready documentation, the CRMP shields organizations from legal penalties, fines, and reputational damage.

Cybersecurity risk is no longer just an IT issue—it is a business imperative. A well-executed CRMP not only protects systems and data but also ensures regulatory adherence, business resilience, and long-term success in an era of evolving threats and increasing compliance expectations.

Chapter 3 - **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:

1) Internal constituents, who drive and implement the program, and
2) External constituents, who rely on it for security and assurance.

Internal Stakeholders

- **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 Cybersecurity 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 Stakeholders

- **Customers** – Expect secure, uninterrupted services. A strong CRMP protects their data, builds trust, and prevents breaches that could impact privacy or disrupt business.
- **Shareholders** – Invested in financial stability. A CRMP enhances transparency, reduces cybersecurity risks, and safeguards stock performance and dividends.
- **Partners – third parties, vendors, and other organizations. An effective CRMP assures that their relationship with your organization is secure, stable, and worth investing time/money into.**

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. By engaging all stakeholders, organizations can transform cybersecurity risk from a liability into a strategic advantage.

Chapter 4 - **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**: Cybersecurity 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.

Chapter 5 - **How:**

Implementing a CRMP

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

1 Governance & Strategy	2 Risk Assessment & Management	3 Operational Execution & Continuous Monitoring
● 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.	● 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.	● Continuously monitor the environment and track risk assessment results over time by ○ **Integrating** technology and **security stacks** with risk assessment practices ○ 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 a CRMP. 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. Detailed definitions are given in the white paper by the FAIR Institute. Further definitions for NIST CSF 2.0 CMMI and more frameworks will be added to this series of publications in the future.

Chapter 6 - **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.

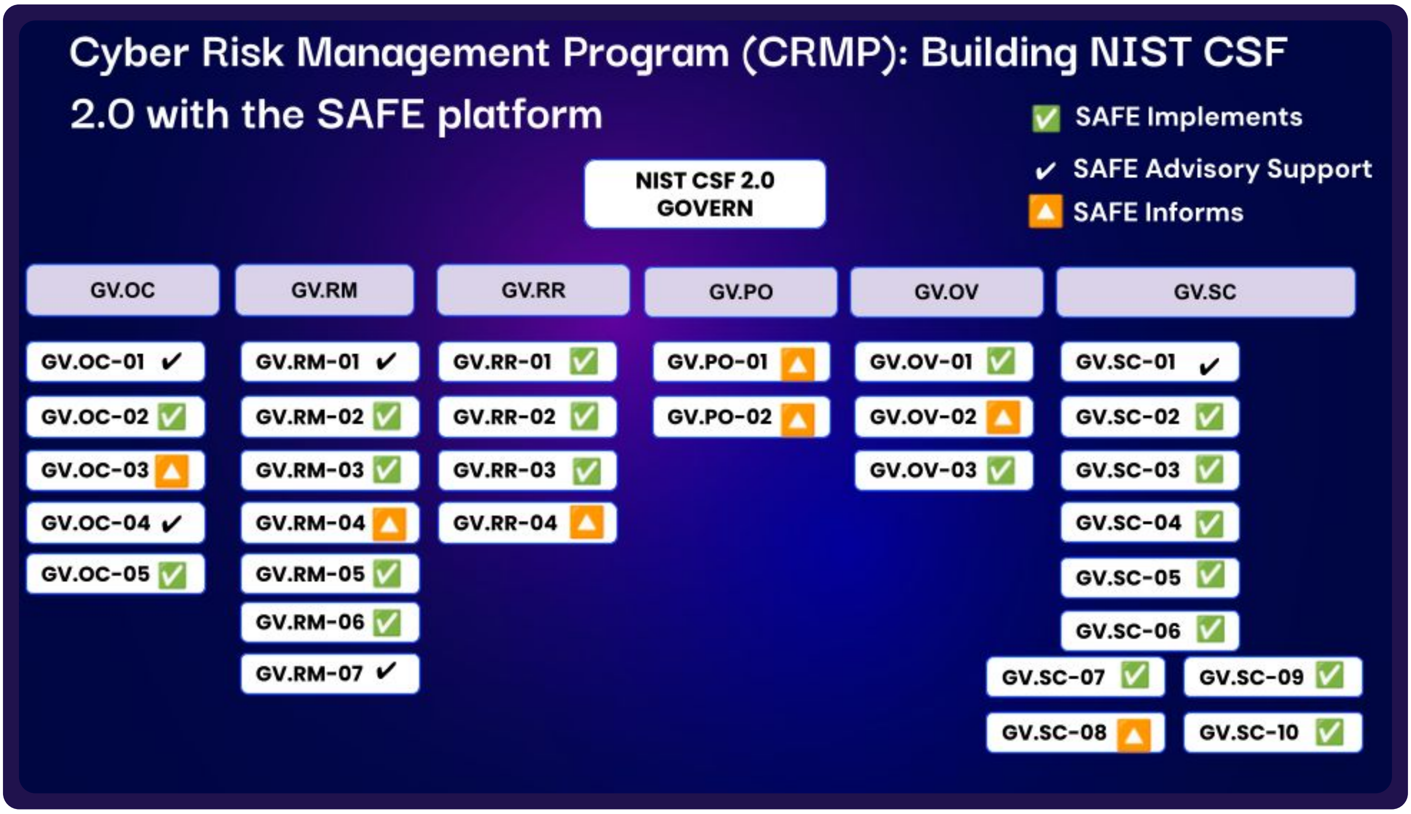
A static and point in time CRMP is like bringing a knife to a gun fight.

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

Chapter 7 - **Shift Right:**

Building a CRMP with Safe

The SAFE platform, combined with Safe's risk advisory services, can help you build and run a continuous CRMP:



Cyber Risk Management Program (CRMP): Building NIST CSF 2.0 with the SAFE platform

✅ SAFE Implements
✓ SAFE Advisory Support
⚠ SAFE Informs

NIST CSF 2.0 GOVERN

GV.OC	GV.RM	GV.RR	GV.PO	GV.OV	GV.SC
GV.OC-01 ✓	GV.RM-01 ✓	GV.RR-01 ✅	GV.PO-01 ⚠	GV.OV-01 ✅	GV.SC-01 ✓
GV.OC-02 ✅	GV.RM-02 ✅	GV.RR-02 ✅	GV.PO-02 ⚠	GV.OV-02 ⚠	GV.SC-02 ✅
GV.OC-03 ⚠	GV.RM-03 ✅	GV.RR-03 ✅		GV.OV-03 ✅	GV.SC-03 ✅
GV.OC-04 ✓	GV.RM-04 ⚠	GV.RR-04 ⚠			GV.SC-04 ✅
GV.OC-05 ✅	GV.RM-05 ✅				GV.SC-05 ✅
	GV.RM-06 ✅				GV.SC-06 ✅
	GV.RM-07 ✓				GV.SC-07 ✅ GV.SC-09 ✅
					GV.SC-08 ⚠ GV.SC-10 ✅

Sub-Category	How SAFE helps	Explanation
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Advisory Support**	SAFE aligns cybersecurity risks with business objectives by providing insights into how security posture impacts organizational mission.
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Implements**	SAFE helps map internal and external stakeholder risks by offering visibility into risk exposure across the ecosystem. Customers utilize SAFE for Risk Management as a Service (RMaaS) offerings that can ingest their needs and expectations around cybersecurity risk management to inform decision-making.
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity – including privacy and civil liberties obligations – are understood and managed	**Informs**	SAFE tracks compliance requirements and provides automated reporting to manage legal, regulatory, and contractual obligations like cybersecurity incident materiality disclosure and framework adherence. SAFE can also help understand the negative impact of not meeting such requirements.
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	**Advisory Support**	SAFE enables assessment and communication of critical services by quantifying the impact of cybersecurity risks on external stakeholders.
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	**Implements**	SAFE helps organizations understand dependencies by visualizing risk exposure in relation to business operations and services.
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	**Advisory Support**	SAFE supports risk management objectives by providing a structured, data-driven approach to measuring, mitigating, and socializing cybersecurity risks. SAFE's advisory team can help build the objectives of the risk management program.
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	**Implements**	SAFE assists in defining and tracking risk appetite and tolerance by offering real-time risk quantification and threshold management. SAFE helps in proactively managing the appetite/tolerance limits based on changing threats and internal environment.
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	**Implements**	SAFE can integrate into ERM platforms for a uniform view of risk across the enterprise.
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	**Informs**	SAFE can help define the thresholds that trigger specific responses.
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Implements**	SAFE facilitates risk communication across the organization by providing persona-based reporting (board, executives, risk owners, vulnerability management teams, etc.,) and real-time risk dashboards.
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Implements**	SAFE offers a standardized method for calculating, documenting, and prioritizing cybersecurity risks through its risk quantification engine based on open standards like FAIR and MITRE ATT&CK.

Sub-Category	How SAFE helps	Explanation
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	**Advisory Support**	SAFE can be used to quantify the return on strategic investments in terms of risk reduction.
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	**Implements**	Through SAFE roles and groups, an organization can hold risk owners accountable for managing the risk. SAFE's risk quantification translates Cybersecurity risk into business terms - helping business leaders understand Cybersecurity risk and hold themselves accountable.
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	**Implements**	SAFE's quantified output can be linked to incentive plans of the organization to drive accountability and performance on cybersecurity metrics.
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	**Implements**	SAFE optimizes resource allocation by identifying high-priority risks and guiding investment decisions in security controls.
GV.RR-04: Cybersecurity is included in human resources practices.	**Informs**	SAFE's controls around people security can be used to measure the cybersecurity effectiveness of employees. SAFE's output can also be used for incentive alignment.
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**	SAFE can provide the cybersecurity context and best practices to build a robust Cybersecurity risk management policy. Policy thresholds can be set based on quantified risks.
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 SAFE-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**	Through SAFE, an organization can establish a quantified risk baseline. Using risk scenarios and risk treatment plans, the risk burndown can be automatically tracked in the SAFE platform for measurement of performance. Operational decisions (like vulnerability prioritization) and strategic decisions (like investments) can be made through the SAFE platform in a defensible way.
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	**Informs**	Through SAFE, an organization can track all external and internal environmental changes, and the corresponding change in risk. If the risk changes significantly, it might warrant an adjustment in the risk management strategy.
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	**Implements**	SAFE helps an organization to measure risk continuously - thus providing objective metrics for performance evaluation of ybersecurity budget and teams.

Sub-Category	How SAFE helps	Explanation
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	**Advisory Support**	SAFE Advisory team can build the strategy and foundation for a risk-driven cybersecurity risk management strategy and program.
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	**Implements**	Through role-based access, SAFE supports suppliers, partners, and customers to engage and collaborate with the organization's risk assessment
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	**Implements**	SAFE integrates into Enterprise risk management systems (like ServiceNow) to enable integration of enterprise and third-party risk management
GV.SC-04: Suppliers are known and prioritized by criticality	**Implements**	SAFE automatically tiers and quantifies the business risk based on data/network/business disruption; SAFE allows users to tier third parties quantifiably. SAFE helps in auto discovery of third parties through external scans and internal SSO integrations.
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	**Implements**	SAFE can recommend security controls to be included in contracts; SAFE platform can also automatically read the contracts to understand the gaps.
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Implements**	SAFE implements comprehensive due diligence - from outside-in scanning, control questionnaires, to inside-out assessments. SAFE automates the process by using AI to ingest and process evidence and externally available information.
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	**Implements**	SAFE's AI agents continuously monitor the risk posed by third parties - based on internal and external threat intelligence, and raise alerts.
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	**Informs**	SAFE helps identify the riskiest third parties for this exercise. SAFE also provides insight into the weakest controls of third parties.
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	**Implements**	SAFE helps organizations track supply chain security performance by providing ongoing cybersecurity risk insights throughout the lifecycle.
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Implements**	SAFE implements offboarding of third parties with internal and external due diligence.

Table 2: How SAFE Can Support Maturing NIST-Based Cybersecurity Risk Program

Chapter 8 - **Shift Right:**

Building a roadmap with the SAFE Platform

Building a robust Cybersecurity Risk Management Program is a journey. Different organizations are at different stages today. Each organization will have its own target state, and Tier 4 across all categories is not required or realistic for all organizations. We recommend the following steps for a CISO or a GRC leader, to build and execute towards the target end state for their CRMP.

Step 0: Begin with the Why, and the Organization should agree to the Why

Begin with the 'Why' - why should you, your CISO, your organization - care about a CRMP. The Why can be around:

1. Improving the responsiveness and resilience of the cybersecurity program
2. Meeting compliance and regulatory requirements
3. Building a more data-driven decision-making framework in the organization
4. Improving the ROI of cybersecurity investments
5. Getting better cyberinsurance coverage

The 'Why' should be clearly documented and aligned with the stakeholders. Without an explicit alignment on the Why, your efforts are likely doomed.

Step 1: Understand the current maturity state

We recommend using the NIST CSF 2.0 as the framework to assess the current maturity of the organization. Even if you don't use the broader NIST CSF framework, we think that NIST does a good job at defining the maturity requirements. Use the definitions of the implementation tiers, as defined in the white paper by the FAIR Institute, to workshop out the current maturity state of your program. Involve the relevant stakeholders.

Step 2: Define and align on the target maturity state

Next step is to define the end state. Where do you want to get to?

You might not want to land in Maturity 3 / 4 for every category or subcategory - based on your organization's risk posture, complexity, and external threat environment. Do not constrain your discussion based on today's resource availability or priorities. These constraints should be accounted for in the execution plan.

Step 3: Identify and empower the owners

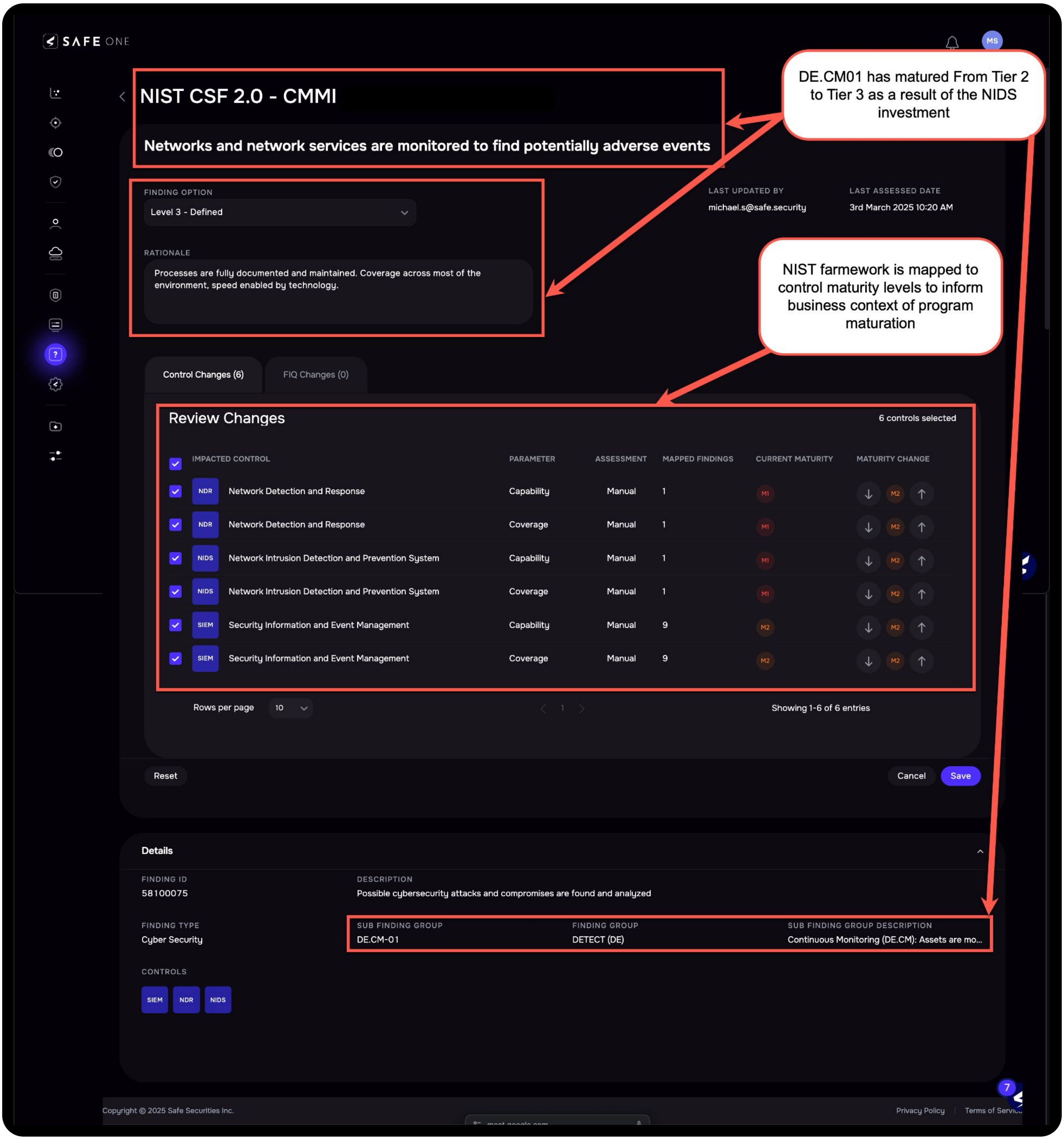
For each workstream, identify a clear owner. The incentives of the owner should be aligned with the success of his/her workstream. At the same time, the owner should be empowered with the right decision making authority and resources to be successful.

Step 4: Define a sprint-like execution plan

Create a tactical execution plan. Progress can happen in parallel on different workstreams, but identify the cross dependencies. Having a dedicated program manager can be a game changer for this effort.

Step 5: Quantify the impacts of your efforts in SAFE

In the example below, **network security controls matured from Tier 2 to Tier 3** under **DE.CM-01 (Continuous Monitoring)** due to a **NIDS investment**.



NIST CSF 2.0 - CMMI

Networks and network services are monitored to find potentially adverse events

FINDING OPTION
Level 3 - Defined

RATIONALE
Processes are fully documented and maintained. Coverage across most of the environment, speed enabled by technology.

LAST UPDATED BY
michael.s@safe.security

LAST ASSESSED DATE
3rd March 2025 10:20 AM

DE.CM01 has matured From Tier 2 to Tier 3 as a result of the NIDS investment

NIST farmework is mapped to control maturity levels to inform business context of program maturation

Review Changes

6 controls selected

☑	IMPACTED CONTROL	PARAMETER	ASSESSMENT	MAPPED FINDINGS	CURRENT MATURITY	MATURITY CHANGE
☑	NDR Network Detection and Response	Capability	Manual	1	M1	↓ M2 ↑
☑	NDR Network Detection and Response	Coverage	Manual	1	M1	↓ M2 ↑
☑	NIDS Network Intrusion Detection and Prevention System	Capability	Manual	1	M1	↓ M2 ↑
☑	NIDS Network Intrusion Detection and Prevention System	Coverage	Manual	1	M1	↓ M2 ↑
☑	SIEM Security Information and Event Management	Capability	Manual	9	M2	↓ M2 ↑
☑	SIEM Security Information and Event Management	Coverage	Manual	9	M2	↓ M2 ↑

Rows per page 10

Showing 1-6 of 6 entries

Details

FINDING ID
58100075

DESCRIPTION
Possible cybersecurity attacks and compromises are found and analyzed

FINDING TYPE
Cyber Security

SUB FINDING GROUP
DE.CM-01

FINDING GROUP
DETECT (DE)

SUB FINDING GROUP DESCRIPTION
Continuous Monitoring (DE.CM): Assets are mo...

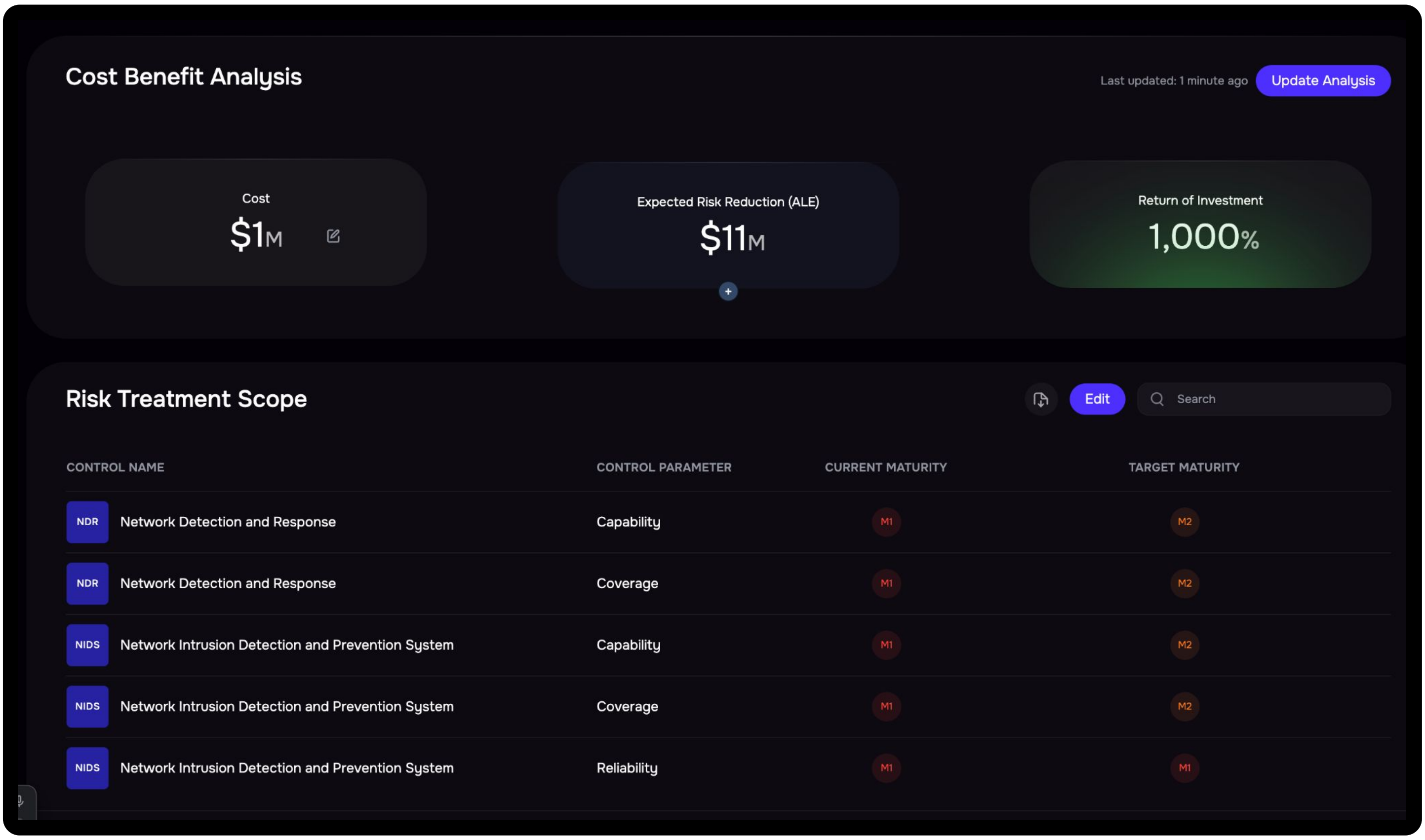
CONTROLS
SIEM NDR NIDS

Copyright © 2025 Safe Securities Inc.

Cost-Benefit Analysis: Cyber Risk in Financial Terms

SAFE supports quantification of cybersecurity ROI, demonstrating how a **$1M investment** results in **$11M in expected risk reduction** —a **1,000% ROI**. This allows security teams to:

- Prioritize initiatives based on **financial impact**.
- Optimize spending on **high-impact security controls**.
- Communicate **cybersecurity value to executives in monetary terms**.



Cost Benefit Analysis

Cost: $1M

Expected Risk Reduction (ALE): $11M

Return of Investment: 1,000%

Risk Treatment Scope

CONTROL NAME	CONTROL PARAMETER	CURRENT MATURITY	TARGET MATURITY
NDR Network Detection and Response	Capability	M1	M2
NDR Network Detection and Response	Coverage	M1	M2
NIDS Network Intrusion Detection and Prevention System	Capability	M1	M2
NIDS Network Intrusion Detection and Prevention System	Coverage	M1	M2
NIDS Network Intrusion Detection and Prevention System	Reliability	M1	M1

For strategic or tactical support and resources (workbooks) to build your CRMP, please contact your Customer Success / Risk Advisory partner.

Conclusion

Building a continuous Cyber Risk Management Program is a must-have for any large organization. It is a compliance requirement. The SAFE platform can help you mature your program using the NIST CSF 2.0 framework and others. With a combination of risk advisory and platform capabilities, the SAFE platform enables you to understand your current state and shift right towards a continuous risk management program.

Appendix

Building a robust Cybersecurity risk program helps you achieve Compliance

Most Compliances require a robust Cybersecurity Risk Management Programs. If an organization builds a strong continuous Cybersecurity Risk Management program, it helps the organization to achieve compliance with the following frameworks:

1. ISO 27001 (International Organization for Standardization)

- A globally recognized standard for information security management systems (ISMS).
- ISO 27001 focuses on risk management and security controls.
- Often used in conjunction with other frameworks like NIST CSF.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

SAFE