

THE CYBER RISK MANAGEMENT PROGRAM (CRMP) FRAMEWORK





The Cyber Risk Management Program (CRMP) Framework v1.0

CRMP.info

In the ever evolving landscape shaped by digital transformation, it's critical to recognize that cybersecurity is not just an IT concern but rather an intrinsic part of business strategy and decision making. With this realization comes the need for enterprises to operationalize a comprehensive cyber risk management program within their business operations. This document introduces a framework designed to holistically establish a cyber risk management program.

Purpose and Context

Recent years have brought an extraordinary surge in cyber threats and incidents. Authorities and regulatory bodies have highlighted the pressing need for organizations to strengthen their cybersecurity postures, and to ensure effective communication to stakeholders about cyber risks. Boards and executives must be able to provide proper oversight of their cyber risk environment. Many existing standards and references, when viewed in isolation, may fall short of providing a comprehensive program that truly serves the requirements of the business. This gap underscores the critical need for a unified framework that harmonizes and interprets the authoritative guidance, regulations, and standards, ensuring that businesses can properly manage and oversee their cyber risks.

The cyber risk management program framework synthesizes insights from leading practices and standards, providing a structured and comprehensive approach to a cyber risk management program. The program can be tailored to the unique needs and regulatory landscape of each enterprise. It serves as a guide to operationalize a cyber risk management program, enabling businesses to make informed risk decisions and evolve their security strategies to survive and thrive in the digital age.

Structure of the Cyber Risk Management Program Framework

The framework is organized into four core components:

- Agile governance
- Risk-informed system
- Risk-based strategy and execution
- Risk escalation and disclosure

Each of these components is further broken down into multiple supporting principles, which provide considerations for implementation. To facilitate practical application and deeper understanding, the principles within these components are then mapped to relevant informative references.

These references offer insights and practical guidelines, enhancing the robustness and applicability of the cyber risk management program framework.



The Cyber Risk Management Program (CRMP) Framework v1.0 CRMP.info

Note: Framework Disclosure

While the framework aligns closely with these references, it's important to recognize that no single standard or guidance can comprehensively cover all facets of a mature cyber risk management program as required for today's environment. Thus, the motivation behind developing this framework and the writing of the "Building a Cyber Risk Management Program" book to provide a holistic, synthesized view that integrates insights across multiple sources. Depending on the specific circumstances and nuances of your organization, you might find relevance in other standards or additional mappings.

In sum, this framework seeks to encapsulate the essence of a comprehensive cyber risk management program as guided by authoritative sources. It serves as a guide, aiding enterprises and their decision makers in understanding, implementing, and operationalizing a cyber risk management program. The guide also ensures enterprises can remain resilient and adaptive in the face of digital challenges while it also protects them from evolving liability and regulatory risks. As you navigate the intricacies of the framework, remember that its ultimate goal is to provide clarity, align with industry standards, and empower the business to make better decisions and thrive securely in the digital age.



The Cyber Risk Management Program (CRMP) Framework v1.0

CRMP.info

Component	Principle	Informative Reference
Agile Governance	<p>Principle 1: Establish Policies and Processes</p> <p><i>Enterprisewide policies and processes must be in place for establishing a cyber risk management program.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.PO-01, GV.PO.02 ISO/IEC 27001:2022 5.2 ISO 31000:2018 6.1 2018 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures Page 18 Paragraph 2, 3 2017 AICPA CRMP Description Criteria DC4, DC7, DC19</p>
	<p>Principle 2: Establish Governance and Roles and Responsibilities Across the “Three Lines Model”</p> <p><i>Cyber risk governance must be established with clearly defined roles, responsibilities, and outputs across the “Three Lines Model.”</i></p>	<p>2023 SEC Regulation S–K Item 106(c)—Governance and Form 20-F 2023 Draft NIST CSF 2.0 GV.RR 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 6 ISO/IEC 27001:2022 5.1, 5.3 ISO 31000:2018 5.2, 5.4.3 2020 IIA Three Lines Model Principle 2 - 4</p>
	<p>Principle 3: Align Governance Practices with Existing Risk Frameworks</p> <p><i>Cyber risk governance practices should be aligned with any existing enterprise or organizational risk frameworks.</i></p>	<p>2023 NACD Cyber Risk Oversight Handbook Principle 1, 4 2023 Draft NIST CSF 2.0 GV.RM-03 NISTIR 8286</p>
	<p>Principle 4: Board of Directors and Senior Executives Define Scope</p> <p><i>The scope of an enterprise’s cyber risk practices should be defined and approved by its board of directors and senior executives.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.OC-01, GV.RR-01 ISO 31000:2018 5.2</p>
	<p>Principle 5: Board of Directors and Senior Executives Provide Oversight</p> <p><i>The board of directors and senior executives should provide proper oversight of the enterprise’s cyber risk practices.</i></p>	<p>SEC Regulation S–K Item 106(c)—Governance and Form 20–F 2023 Draft NIST CSF 2.0 GV.RR-01 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 3 2020 IIA Three Lines Model Principle 1 ISO 31000:2018 5.4.2 2017 AICPA CRMP Description Criteria DC8</p>
	<p>Principle 6: Audit Governance Processes</p> <p><i>Audit processes should provide appropriate review and assessment of the enterprise’s cyber risk governance practices.</i></p>	<p>2020 IIA Three Lines Model Principle 4 2018 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures Page 18 Paragraph 3 ISO 31000:2018 5.6 2017 AICPA CRMP Description Criteria DC15</p>



The Cyber Risk Management Program (CRMP) Framework v1.0 CRMP.info

	<p>Principle 7: Align Resources to the Defined Roles and Responsibilities</p> <p><i>Appropriate resources and skill sets should be aligned to the defined roles and responsibilities with ongoing training in place.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.RR-03 ISO/IEC 27001:2022 7.1 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 3 2017 AICPA CRMP Description Criteria DC10</p>
Risk Informed System	<p>Principle 1: Define a Risk Assessment Framework and Methodology</p> <p><i>A risk framework and methodology must be defined and executed on to identify, assess, and measure cyber risk within the organizational context.</i></p>	<p>SEC Regulation S–K Item 106(b)—Risk Management and Strategy 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 1, 4, 5 Draft NIST CSF 2.0 GV.RM, ID.RA ISO/IEC 27001:2022 6.1.2, 6.1.3 2017 AICPA CRMP Description Criteria DC11 ISO 31000:2018 6.1</p>
	<p>Principle 2: Establish a Methodology for Risk Thresholds</p> <p><i>An approved and repeatable methodology for acceptable risk thresholds—both appetite and tolerance—must be established.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.RM-02 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 1, 5</p>
	<p>Principle 3: Establish Understanding of Risk-Informed Needs</p> <p><i>The governance body should be identified and engaged in establishing a comprehensive understanding of its cyber risk–informed needs.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.OC-02 2017 AICPA CRMP Description Criteria DC13 2020 IIA Three Lines Model Principle 1 ISO 31000:2018 6.2</p>
	<p>Principle 4: Agree on a Risk Assessment Interval</p> <p><i>The risk assessment process should be performed according to an agreed-on interval with its results regularly evaluated.</i></p>	<p>SEC Regulation S–K Item 106(b)—Risk Management and Strategy 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 5 2023 Draft NIST CSF 2.0 ID.RA, ID.IM 2017 AICPA CRMP Description Criteria DC11, DC12, DC15</p>
	<p>Principle 5: Enable Reporting Processes</p> <p><i>Reporting processes should equip the governance body with insights on the impact of cyber risks on existing practices and strategic decisions.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.OV 2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 5 2017 AICPA CRMP Description Criteria DC13, DC16 2020 IIA Three Lines Model Principle 6</p>
Risk-based Strategy and Execution	<p>Principle 1: Define Acceptable Risk Thresholds</p>	<p>2023 NACD Director’s Handbook on Cyber-Risk Oversight Principle 1 2023 Draft NIST CSF 2.0 GV.RM-02</p>



The Cyber Risk Management Program (CRMP) Framework v1.0

CRMP.info

	<p><i>Acceptable cyber risk thresholds must be clearly understood, established, and approved by the risk owners based on the risk framework and methodology.</i></p>	
	<p>Principle 2: Align Strategy and Budget with Approved Risk Thresholds</p> <p><i>The cyber risk treatment plan and budget should be aligned with the approved risk thresholds.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.RM-04 2023 NACD Director's Handbook on Cyber-Risk Oversight Principle 1 ISO 31000 6.5.1, 6.5.2 2017 AICPA CRMP Description Criteria DC17</p>
	<p>Principle 3: Execute to Meet Approved Risk Thresholds</p> <p><i>The cyber risk treatment plan should be executed to meet the approved risk thresholds.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.RR-03 ISO 31000 6.5.3</p>
	<p>Principle 4: Monitor on an Ongoing Basis</p> <p><i>The execution of the cyber risk treatment plan should be monitored on an ongoing basis with established performance indicators and operational metrics.</i></p>	<p>2023 NACD Director's Handbook on Cyber-Risk Oversight Principle 5 2023 Draft NIST CSF 2.0 GV.OV 2017 AICPA CRMP Description Criteria DC15, DC16</p>
	<p>Principle 5: Audit Against Risk Thresholds</p> <p><i>The audit function should review and assess proper execution of the cyber risk treatment plan based on the approved risk thresholds.</i></p>	<p>2020 IIA Three Lines Model Principle 4 2017 AICPA CRMP Description Criteria</p>
	<p>Principle 6: Include Third Parties in Risk Treatment Plan</p> <p><i>The cyber risk treatment plan should consider third parties including partners, suppliers, and supply chain participants.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.SC, ID.IM-02 SEC Regulation S–K Item 106(b)—Risk Management and Strategy</p>
Risk Escalation and Disclosure	<p>Principle 1: Establish Escalation Processes</p> <p><i>Formal cyber risk escalation processes must be established.</i></p>	<p>SEC Regulation S–K Item 106(c)—Governance 2023 NACD Director's Handbook on Cyber-Risk Oversight Principle 2 2018 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures Page 18 Paragraph 3, Page 20 Paragraph 1 2017 AICPA CRMP Description Criteria DC13, DC16</p>
	<p>Principle 2: Establish Disclosure Processes—All Enterprises</p> <p><i>The enterprise's cyber disclosure processes should address its specific risk factors, organizational context, and requirements.</i></p>	<p>2023 Draft NIST CSF 2.0 GV.OC-03 2023 NACD Director's Handbook on Cyber-Risk Oversight Principle 2 2017 AICPA CRMP Description Criteria DC6, DC14</p>



The Cyber Risk Management Program (CRMP) Framework v1.0 CRMP.info

	<p>Principle 3: Establish Disclosure Processes—Public Companies</p> <p><i>Public companies must disclose their material risks, risk factors, cyber risk management processes, governance, and material incident reporting.</i></p>	<p>2023 SEC Final Rule Cybersecurity Risk Management, Strategy, Governance, Incident Disclosure Rule 2023 Draft NIST CSF 2.0 GV.OC-03 2018 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures Page 4 Paragraph 1, Page 6 Paragraph 3, Page 7 Paragraph 4, Page 11 Paragraph 1</p>
	<p>Principle 4: Test Escalation and Disclosure Processes</p> <p><i>Cyber risk escalation and disclosure processes should be challenged, tested, and updated on an ongoing basis to incorporate lessons learned.</i></p>	<p>2023 SEC Final Rule Cybersecurity Risk Management, Strategy, Governance, Incident Disclosure Rule 2023 Draft NIST CSF 2.0 ID.IM</p>
	<p>Principle 5: Audit Escalation and Disclosure Processes</p> <p><i>Audit should review and assess the enterprise's cyber risk escalation and disclosure processes to ensure their effectiveness, consistency, and compliance with relevant regulations and policies.</i></p>	<p>2020 IIA Three Lines Model Principle 4, 5</p>