CYBERSECURITY
RISK FOUNDATION

S
2025

SAFEGUARDS

An aggregate, comprehensive
library of cybersecurity safeguards

crfsecure.org

TABLE OF CONTENTS

INTRODUCTION

As organizations navigate the evolving complexities of safeguarding digital assets against increasingly sophisticated threats, the Cybersecurity Risk Foundation (CRF) presents the *CRF–Safeguards (CRF–S) 2025*, an enhanced and comprehensive library of cybersecurity safeguards grounded in industry best practices. Designed to strengthen organizations' defenses, the *CRF–S* offers a structured approach to cybersecurity enhancement that aligns with the *CRF–Maturity Model* and integrates the safeguards established by leading cybersecurity standards and regulations. This initiative reaffirms our commitment to fostering a more secure digital ecosystem through collaboration, knowledge sharing, and continuous improvement.

The *CRF–Safeguards (CRF–S) 2025* represents a dynamic initiative synthesizing cybersecurity best practices from more than 80 recognized cybersecurity standards, frameworks, and regulations. By aggregating and prioritizing these diverse sources, the *CRF–S* provides a structured and adaptable array of safeguards, enabling organizations—regardless of their cybersecurity maturity level—to efficiently identify and implement the most effective security measures.

New for 2025 is the introduction of the Artificial Intelligence (AI) Management safeguard category, which recognizes the growing role of AI in cybersecurity operations. As organizations increasingly deploy AI-driven security solutions and integrate machine learning models into critical business functions, the need for structured AI governance, risk mitigation, and ethical considerations has become paramount. This new category provides guidance on securing AI systems, ensuring transparency in AI-driven decision-making, and managing associated risks, reinforcing the CRF's commitment to proactive and responsible cybersecurity.

The *CRF–S* remains a prioritized collection of cybersecurity safeguards, methodically organized to help organizations advance from foundational to more sophisticated cybersecurity maturity levels. By adopting these safeguards, organizations can systematically improve their security posture, address emerging vulnerabilities, and build resilience against evolving cyber threats. Each safeguard is categorized according to its maturity level, allowing organizations to efficiently align their cybersecurity initiatives with their current capabilities and strategic goals.

More than just a reference, this whitepaper serves as a roadmap for continuous cybersecurity improvement. The collaborative nature of the *CRF–S* reflects our belief in the power of a community-driven approach to elevating cybersecurity standards across all industries. By sharing expert insights, real-world experiences, and best practices, the *CRF–S* empowers organizations to confidently navigate the cybersecurity landscape and achieve their security objectives in an era of rapid digital transformation.

A COMMUNITY APPROACH TO DEFINING CYBERSECURITY SAFEGUARDS

The *Cybersecurity Risk Foundation–Safeguards (CRF–S)* is the culmination of an extensive review and synthesis process that examined over 80 unique cybersecurity standards and regulations globally. This comprehensive evaluation encompassed a broad spectrum of authoritative sources, including the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Center for Internet Security (CIS), as well as various U.S. federal and state laws, international regulations, and industry-specific standards. This rigorous analysis aimed to create an aggregated library of cybersecurity safeguards designed to offer organizations a unified and actionable guide for enhancing their cybersecurity posture. By distilling the essence of these diverse standards, the *CRF–S* provides a consolidated reference that bridges the gap between multiple cybersecurity frameworks and regulatory requirements, facilitating a cohesive approach to cybersecurity defense.

The *CRF–S* initiative is grounded in a collaborative community effort, drawing upon the expertise and contributions of multiple cybersecurity organizations. This collective endeavor ensures the *CRF–S* remains a dynamic and evolving resource, with ongoing contributions from a broad spectrum of cybersecurity professionals and entities dedicated to enhancing digital defenses. By pooling knowledge, insights, and best practices from the cybersecurity community, the *CRF–S* benefits from a wealth of experience and diverse perspectives, ensuring it remains relevant and effective in the face of new challenges and technological advancements. This collaborative approach enriches the *CRF–S* and fosters a sense of unity and shared purpose among cybersecurity practitioners, reinforcing the importance of cooperation in the continual quest to safeguard digital assets and infrastructures.

The prioritization of safeguards within the *CRF–S* has been meticulously designed in alignment with the *CRF–Maturity Model*, categorizing these protections based on their levels of effectiveness and the maturity they represent within an organization's cybersecurity framework. This structured approach ensures that organizations can systematically enhance their cybersecurity posture by implementing safeguards that are most effective against current threats and appropriate for their stage of cybersecurity development. By following this prioritized guidance, organizations are equipped to make strategic decisions on which safeguards to adopt, enabling a progressive strengthening of their defenses as they advance through the maturity levels, from foundational security measures to advanced, monitored environments. This methodical prioritization serves as a roadmap, guiding organizations to invest in the most impactful safeguards that facilitate immediate security improvements and long-term cybersecurity resilience.

The principal aim of the *CRF–S* project is to assist organizations in pinpointing the most relevant cybersecurity safeguards necessary to attain their specific goals, thereby optimizing their resource allocation towards essential defensive actions. By prioritizing and aggregating safeguards from many recognized sources, the *CRF–S* offers a strategic blueprint that guides organizations in identifying the critical security measures they should implement. This approach eliminates the often overwhelming task of deciphering which actions to prioritize for effective defense, providing a clear, structured pathway. Consequently, organizations can focus on implementing proven cybersecurity practices that significantly bolster their defenses, ensuring they are well-equipped to protect their digital assets and operational integrity.

CYBERSECURITY SAFEGUARDS

The CRF-Safeguards are organized into seven domains: Cybersecurity Governance, Operational Cybersecurity, Computing System Cybersecurity, Identity and Access Cybersecurity, Network Cybersecurity, Cloud Cybersecurity, and Development Cybersecurity. This structured categorization is designed to offer a comprehensive overview of the critical areas within cybersecurity, facilitating easy navigation and implementation for organizations. Each safeguard listed in the following sections is accompanied by its domain classification and a priority ranking derived from the consolidated insights of leading cybersecurity frameworks and regulations. This approach ensures that organizations can efficiently identify and prioritize the implementation of safeguards that are most crucial to their cybersecurity posture for cybersecurity enhancement.

CYBERSECURITY GOVERNANCE SAFEGUARDS

Cybersecurity Governance forms the strategic foundation of an organization’s cybersecurity program, emphasizing establishing policies, procedures, and oversight mechanisms to ensure that cybersecurity strategies align with business objectives. This domain focuses on leadership, risk management, and compliance to create a cohesive framework that supports informed decision-making and accountability. By prioritizing governance, organizations can ensure a top-down approach to cybersecurity, where leadership actively promotes a culture of security awareness and resilience.

Program Management

Effective cybersecurity begins with a structured, well-documented program aligning security initiatives with business objectives. The Program Management safeguards establish the foundation for an organization's cybersecurity strategy by defining its security program's scope, authority, and governance structure. These safeguards ensure a formal cybersecurity charter is in place, clearly outlining objectives, responsibilities, and regulatory compliance requirements. Additionally, they emphasize the importance of executive sponsorship, stakeholder engagement, and ongoing program oversight to maintain an adaptive and resilient cybersecurity posture.

Safeguard ID	Safeguard Description	Level
PRG-01	Maintain a cybersecurity program charter that authorizes the existence of a program and gives authority to the program team to use organizational resources to achieve the program objectives.	Governed (Level 3)
PRG-02	Ensure that the organization's cybersecurity program charter defines its scope and applicability to each of its business units or related entities.	Governed (Level 3)
PRG-03	Ensure that the organization's cybersecurity program charter defines the ultimate goal of the cybersecurity program as the confidentiality, integrity, and availability of the organization's information systems.	Governed (Level 3)
PRG-04	Ensure that the organization's cybersecurity program charter defines all the cybersecurity regulations and standards it shall use to define its goals for specific cybersecurity safeguards.	Governed (Level 3)
PRG-05	Ensure that the organization's cybersecurity program charter or supporting documentation formally defines the organization's approach to cybersecurity governance and risk management.	Governed (Level 3)
PRG-06	Ensure that the organization's cybersecurity program charter defines the executive leadership sponsor for the organization's cybersecurity program.	Governed (Level 3)
PRG-07	Ensure that the organization's cybersecurity program charter establishes the authority of the stakeholder committee responsible for the program.	Governed (Level 3)
PRG-08	Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific stakeholder committee members responsible for the organization's cybersecurity program.	Governed (Level 3)
PRG-09	Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific members of the stakeholder committee responsible for its cybersecurity program and that they are from a diverse set of business units, not simply the technology teams.	Governed (Level 3)
PRG-10	Ensure that the organization's cybersecurity program charter or supporting documentation defines the roles and responsibilities of the stakeholder committee members responsible for the organization's cybersecurity program.	Governed (Level 3)
PRG-11	Ensure that the organization's cybersecurity program charter or supporting documentation defines the logistics details (such as meeting cadence and rules of order) for the stakeholder committee responsible for the organization's cybersecurity program.	Governed (Level 3)
PRG-12	Ensure that the organization's cybersecurity program charter has been formally reviewed and updated by the organization's board of directors or executive leadership team.	Governed (Level 3)
PRG-13	Ensure that the organization's board has formally approved the organization's cybersecurity program charter of directors or executive leadership team.	Governed (Level 3)

Safeguard Selection Management

Selecting the proper cybersecurity safeguards is essential to mitigating threats effectively and aligning with organizational risk tolerance. The Safeguard Selection Management safeguards focus on establishing a structured approach to defining, prioritizing, and documenting the security measures an organization implements. This includes maintaining an up-to-date threat taxonomy, mapping safeguards to emerging risks, and ensuring security policies align with regulatory requirements and industry standards. Organizations can proactively strengthen their defenses and address the most critical security gaps by methodically evaluating and selecting safeguards..

Safeguard ID	Safeguard Description	Level
SAF-01	Maintain a detailed and documented taxonomy of all cybersecurity threats that could harm the organization's information systems.	Controlled (Level 4)
SAF-02	Regularly evaluate cybersecurity threats to the organization and define, document, and approve cybersecurity safeguards to address these threats.	Controlled (Level 4)
SAF-03	Maintain subscriptions to relevant cybersecurity threat intelligence feeds to ensure the organization's threat taxonomy is updated with the latest cybersecurity threats.	Controlled (Level 4)
SAF-04	Maintain a detailed and documented list of characteristics that will be used to model each threat in the organization's cybersecurity threat taxonomy.	Controlled (Level 4)
SAF-05	Ensure that the organization's threat model prioritizes each of the threats in the organization's cybersecurity threat taxonomy.	Controlled (Level 4)
SAF-06	Maintain a documented board of directors-level cybersecurity policy that defines the high-level categories of cybersecurity safeguards that will be implemented to achieve the goals defined in the organization's cybersecurity program charter.	Governed (Level 3)
SAF-07	Maintain a detailed and documented list of all appropriate cybersecurity safeguards the organization must implement to achieve the goals defined in its cybersecurity program charter.	Governed (Level 3)
SAF-08	Ensure that the organization has aspirationally defined a complete list of the appropriate cybersecurity safeguards it must implement to achieve the goals defined in its cybersecurity program charter.	Governed (Level 3)
SAF-09	Ensure that the organization's cybersecurity safeguard documentation clearly defines the scope of applicability for each documented cybersecurity safeguard.	Governed (Level 3)
SAF-10	Ensure that the organization's cybersecurity safeguard documentation clearly defines the sanctions imposed if the documented cybersecurity safeguards are violated.	Governed (Level 3)
SAF-11	Ensure that the organization's cybersecurity safeguard documentation clearly defines mappings to regulatory or standards-based requirements for each documented cybersecurity safeguard.	Governed (Level 3)
SAF-12	Ensure that the organization's cybersecurity safeguard documentation clearly defines a business stakeholder responsible for each documented cybersecurity safeguard.	Governed (Level 3)
SAF-13	Ensure that the organization's cybersecurity safeguard documentation clearly defines the job roles that must be aware of each of the documented cybersecurity safeguards.	Governed (Level 3)
SAF-14	Ensure that the organization's cybersecurity safeguard documentation clearly defines a quantifiable measure of compliance for each of the documented cybersecurity safeguards.	Governed (Level 3)
SAF-15	Maintain detailed and documented acceptable use statements that define how an organization's workforce members shall appropriately utilize information systems.	Governed (Level 3)
SAF-16	Ensure that each prioritized threat in the organization's cybersecurity threat model is mapped against each of the corresponding cybersecurity safeguards in the organization's list of documented safeguards.	Controlled (Level 4)
SAF-17	Regularly review the documentation used to define the organization's cybersecurity safeguards to ensure they are appropriate and up-to-date.	Governed (Level 3)

Education Management

A well-informed workforce is a fundamental line of defense against cyber threats. The Education Management safeguards ensure that employees, developers, and privileged users receive role-specific cybersecurity training and awareness programs. These safeguards emphasize the need for documented training requirements, a centralized learning management system, and regular security education to reinforce best practices. Additionally, they highlight the importance of educating users on secure authentication, data handling, social engineering awareness, and incident reporting, fostering a culture of security accountability across the organization.

Safeguard ID	Safeguard Description	Level
EDU-01	Ensure that all workforce members have access to the documentation defining the cybersecurity safeguards related to their roles and responsibilities.	Governed (Level 3)
EDU-02	Maintain a technology platform for delivering cybersecurity-related education to workforce members (such as a Learning Management System (LMS)).	Governed (Level 3)
EDU-03	Maintain a technology platform (such as a Learning Management System (LMS)) for tracking cybersecurity-related education delivered to workforce members.	Governed (Level 3)
EDU-04	Ensure that all workforce members (including engineers, developers, and privileged users) regularly receive appropriate education on cybersecurity safeguards related to their roles and responsibilities.	Governed (Level 3)
EDU-05	Ensure that all workforce members regularly receive appropriate cybersecurity awareness training related to their roles and responsibilities.	Governed (Level 3)
EDU-06	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely authenticating to information systems.	Governed (Level 3)
EDU-07	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely communicating over untrusted networks.	Governed (Level 3)
EDU-08	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely handling data, including the most likely reasons data may be exposed.	Governed (Level 3)
EDU-09	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely responding to social engineering techniques, including identifying and handling such activities.	Governed (Level 3)
EDU-10	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely reporting cybersecurity safeguard failures.	Governed (Level 3)
EDU-11	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely reporting potential cybersecurity incidents to the organization.	Governed (Level 3)
EDU-12	Regularly perform educational activities that reinforce the organization's cybersecurity education program and validate the effectiveness of the program.	Governed (Level 3)
EDU-13	Regularly validate the effectiveness of the organization's cybersecurity education program using quantifiable measures that can be reported to business stakeholders.	Governed (Level 3)
EDU-14	Regularly report the results of validating the effectiveness of the organization's cybersecurity education program to business stakeholders.	Governed (Level 3)

Asset Management

A comprehensive understanding of an organization's technology assets is critical for effective cybersecurity risk management. The Asset Management safeguards focus on maintaining an accurate, centralized inventory of all computing devices, servers, and mobile assets, ensuring that each is appropriately tracked and secured. These safeguards require organizations to implement automated asset discovery, maintain detailed ownership and criticality records, and enforce approval processes for new assets. By establishing strong asset management practices, organizations can reduce the risk of unauthorized devices, unpatched vulnerabilities, and unmanaged endpoints.

Safeguard ID	Safeguard Description	Level
AST-01	Maintain one centralized information system asset inventory tracking system to track each of the organization's logical computing information systems.	Hygiene (Level 2)
AST-02	Ensure the organization's asset tracking system includes all endpoint computing devices (such as workstations or laptops), whether onsite or remote.	Hygiene (Level 2)
AST-03	Ensure that the organization's asset tracking system includes all server computing devices (such as physical or virtualized server instances), whether onsite or remote.	Hygiene (Level 2)
AST-04	Ensure the organization's asset tracking system includes all mobile computing devices (such as phones and tablets), whether onsite or remote.	Hygiene (Level 2)
AST-05	Ensure that the organization's asset tracking system records essential technical information about each information asset (including name, hardware address, and network address).	Hygiene (Level 2)
AST-06	Ensure that the organization's asset tracking system records essential business information about each information asset (including business owner, criticality, business unit, and approvals).	Hygiene (Level 2)
AST-07	Maintain an automated asset discovery platform to discover information assets (actively or passively) to ensure the organization's asset tracking system is accurate and automatically updated regularly.	Hygiene (Level 2)
AST-08	Define a process the organization shall use to approve each information asset in the organization's asset tracking system.	Governed (Level 3)
AST-09	Define a process the organization shall use to remove unauthorized information assets from the organization's network and decommission unauthorized assets.	Governed (Level 3)

Safeguard Implementation Management

Deploying cybersecurity safeguards effectively requires structured project management and oversight. The Safeguard Implementation Management safeguards help organizations track and prioritize the rollout of security measures, ensuring resources are allocated efficiently. These safeguards include maintaining a cybersecurity project tracking system, documenting exceptions when safeguards cannot be implemented, and managing issues that arise during deployment. Organizations can ensure that security investments translate into tangible risk reduction by following a disciplined implementation approach.

Safeguard ID	Safeguard Description	Level
IMP-01	Define a process the organization will use to document and track each of its cybersecurity projects (such as a formal Project Management Office (PMO)).	Governed (Level 3)
IMP-02	Maintain a cybersecurity project tracking system (such as a Project Management Office (PMO) tool) to track each organization's cybersecurity projects.	Governed (Level 3)
IMP-03	Ensure the organization's cybersecurity project tracking system is used to document each of the organization's active cybersecurity projects.	Governed (Level 3)
IMP-04	Ensure the organization's cybersecurity project tracking system prioritizes each active cybersecurity project.	Governed (Level 3)
IMP-05	Ensure the organization's cybersecurity project tracking system tracks the capital implementation costs for each active cybersecurity project.	Governed (Level 3)
IMP-06	Ensure the organization's cybersecurity project tracking system is used to track the personnel implementation costs for each organization's active cybersecurity project.	Governed (Level 3)
IMP-07	Ensure the organization's cybersecurity project tracking system is used to track the status of each organization's active cybersecurity project.	Governed (Level 3)
IMP-08	Define a process the organization shall use to document and track each of the organization's approved cybersecurity exceptions when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.	Governed (Level 3)
IMP-09	Define a process the organization shall use to document which business stakeholder(s) are authorized to approve cybersecurity exceptions in the organization's cybersecurity exception process.	Governed (Level 3)
IMP-10	Maintain a system to track all approved and documented cybersecurity exceptions to the organization's approved cybersecurity safeguards (such as a Governance, Risk, and Compliance (GRC) system or risk register).	Governed (Level 3)
IMP-11	Define a process the organization shall use to document and track each of the organization's issues (or defects) when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.	Governed (Level 3)
IMP-12	Ensure that the organization assigns appropriate resources to address each of its cybersecurity projects and issues in a timely manner.	Governed (Level 3)
IMP-13	Regularly review each of the cybersecurity projects, cybersecurity exceptions, and cybersecurity issues to the organization's approved cybersecurity safeguards and report the status of each to the organization's leadership team.	Monitored (Level 5)

Safeguard Validation Management

A cybersecurity program is only as effective as its ability to verify the success of implemented safeguards. The Safeguard Validation Management safeguards focus on developing a formal audit and assessment strategy, ensuring that security controls are tested, measured, and continuously improved. These safeguards define a multi-year audit plan, establish penetration testing and security assessments, and implement ongoing compliance monitoring. Organizations can detect weaknesses, validate security effectiveness, and reinforce their cybersecurity resilience by maintaining a rigorous validation process.

Safeguard ID	Safeguard Description	Level
VAL-01	Maintain a cybersecurity safeguard validation (audit) plan that documents the assessments the organization shall perform to validate the quality of the organization's cybersecurity safeguards.	Monitored (Level 5)
VAL-02	Ensure that the organization's cybersecurity safeguard validation (audit) plan is a multi-year plan that regularly addresses all the scopes the organization should assess.	Monitored (Level 5)
VAL-03	Ensure that the organization's cybersecurity safeguard validation (audit) plan establishes criticality rankings for each of the assessment scopes in its assessment plan.	Monitored (Level 5)
VAL-04	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines who should perform each assessment scope in its assessment plan.	Monitored (Level 5)
VAL-05	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes each of the cybersecurity penetration testing scopes it should assess regularly.	Monitored (Level 5)
VAL-06	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes software application penetration tests in its assessment plan.	Monitored (Level 5)
VAL-07	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes red team cybersecurity assessments in its assessment plan.	Monitored (Level 5)
VAL-08	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines where cybersecurity penetration testing should be performed only against test systems due to the sensitivity of such systems.	Monitored (Level 5)
VAL-09	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how cybersecurity penetration testing should utilize vulnerability scanners as a part of the assessments.	Monitored (Level 5)
VAL-10	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines when cybersecurity penetration testing should be documented in machine-readable formats (such as SCAP).	Monitored (Level 5)
VAL-11	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how the organization will monitor user accounts during cybersecurity penetration tests.	Monitored (Level 5)
VAL-12	Ensure that the organization's leadership stakeholders regularly approve the organization's cybersecurity safeguard validation (audit) plan.	Monitored (Level 5)
VAL-13	Ensure that the organization's leadership stakeholders regularly allocate and assign resources to the safeguard validation (audit) plan and complete each assessment according to the defined schedule.	Monitored (Level 5)
VAL-14	Ensure that the organization documents the results of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).	Monitored (Level 5)
VAL-15	Ensure that the organization tracks the progress of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).	Monitored (Level 5)
VAL-16	Ensure that the organization regularly reports the results of each cybersecurity assessment to its leadership stakeholders.	Monitored (Level 5)

Third Party Risk Management

External vendors and service providers introduce additional security risks that must be effectively managed. The Third-Party Risk Management safeguards establish a governance framework for assessing and monitoring the cybersecurity posture of third-party partners. These safeguards include maintaining an up-to-date inventory of third-party relationships, enforcing contractually defined security requirements, and continuously evaluating vendors for compliance. Organizations can mitigate supply chain threats by applying a structured third-party risk management approach and ensuring that external partners adhere to security best practices.

Safeguard ID	Safeguard Description	Level
TPR-01	Maintain a process for approving each of the organization's third parties that store or process any of the organization's technology systems or data.	Governed (Level 3)
TPR-02	Maintain a Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data.	Governed (Level 3)
TPR-03	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data maintains a complete inventory of all such third parties.	Governed (Level 3)
TPR-04	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data documents the demographics of all such third parties (such as business owner, criticality, whether data is shared).	Governed (Level 3)
TPR-05	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data maintains a complete data inventory of all data stored or processed by such third-parties.	Governed (Level 3)
TPR-06	Maintain consistent, appropriate, and approved contract language for each organization's third parties that store or process any of the organization's technology systems or data.	Governed (Level 3)
TPR-07	Ensure that the organization's third-party contract language includes provisions requiring any third party that experiences a significant cybersecurity event (such as a data breach) to promptly report it to the organization.	Governed (Level 3)
TPR-08	Ensure that the organization's third-party contract language includes provisions that all third parties must implement cybersecurity safeguards.	Governed (Level 3)
TPR-09	Ensure that the organization's third-party contract language includes provisions requiring all third parties to implement a defined set of cybersecurity safeguards, also defining which safeguards are optional versus mandatory.	Governed (Level 3)
TPR-10	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data signs the agreed-upon contract terms.	Governed (Level 3)
TPR-11	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data is regularly assessed for the appropriate cybersecurity safeguards (utilizing third-party reports such as SOC2 where appropriate).	Monitored (Level 5)
TPR-12	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data is monitored for significant cybersecurity events.	Monitored (Level 5)
TPR-13	Ensure that each of the organization's third parties that store or process any of its technology systems or data are given an aggregate cybersecurity rating based on their criticality, implementation of appropriate cybersecurity safeguards, and occurrence of significant cybersecurity events.	Monitored (Level 5)
TPR-14	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data are appropriately decommissioned when there is no longer a need for the third party to perform such services.	Controlled (Level 4)

Risk Communication Management

Effective cybersecurity risk management relies on transparent reporting and communication with key stakeholders. The Risk Communication Management safeguards focus on leveraging governance, risk, and compliance (GRC) platforms to document, track, and report security risks. These safeguards emphasize the importance of integrating risk intelligence from cybersecurity tools, maintaining executive dashboards for real-time risk visibility, and ensuring that cybersecurity insights are effectively conveyed to business, technical, and executive teams. By prioritizing clear risk communication, organizations can enhance decision-making, drive continuous security improvements, and maintain alignment between cybersecurity efforts and business objectives.

Safeguard ID	Safeguard Description	Level
COM-01	Maintain a Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform to document, track, and report on the organization's cybersecurity risks.	Monitored (Level 5)
COM-02	Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform maps its cybersecurity tools against approved and prioritized cybersecurity safeguards.	Monitored (Level 5)
COM-03	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform automatically integrates with all appropriate cybersecurity technologies to aggregate data regarding potential cybersecurity risks.	Monitored (Level 5)
COM-04	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform manually records the status of cybersecurity safeguards that cannot be automatically entered into the system.	Monitored (Level 5)
COM-05	Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform defines quality thresholds for each aggregated, quantified data point.	Monitored (Level 5)
COM-06	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk on a safeguard basis.	Monitored (Level 5)
COM-07	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk per business unit.	Monitored (Level 5)
COM-08	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk in a way that takes approved exceptions into account and in a way that does not take approved exceptions into account.	Monitored (Level 5)
COM-09	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to executive leadership stakeholders.	Monitored (Level 5)
COM-10	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to business stakeholders.	Monitored (Level 5)
COM-11	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to technical stakeholders.	Monitored (Level 5)

Resilience Management

Cyber resilience ensures an organization can maintain operations and recover swiftly from cyber incidents. The Resilience Management safeguards focus on establishing comprehensive business continuity, disaster recovery, and incident response plans. These safeguards require organizations to implement enterprise-wide backup strategies, maintain immutable data copies, define clear incident response roles, and conduct regular tabletop exercises. By proactively preparing for disruptions, organizations can minimize downtime, mitigate damage, and ensure continued business operations in the face of cyber threats.

Safeguard ID	Safeguard Description	Level
RES–01	Maintain a documented Business Continuity and Disaster Recovery (BCP / DR) program that documents the organization's safeguards to address business continuity.	Governed (Level 3)
RES–02	Maintain a documented cybersecurity Incident Management (IM) program that documents the organization's safeguards to address cybersecurity incident management.	Governed (Level 3)
RES–03	Ensure that the organization's documented Incident Management (IM) plan defines workforce members' roles and responsibilities during a cybersecurity incident.	Governed (Level 3)
RES–04	Ensure that the organization's documented Incident Management (IM) plan defines workforce members' leadership and decision–making responsibilities during a cybersecurity incident.	Governed (Level 3)
RES–05	Ensure that the organization's documented Incident Management (IM) plan defines a communications plan the organization should use during a cybersecurity incident.	Governed (Level 3)
RES–06	Ensure that the organization's documented Incident Management (IM) plan defines how incidents should be reported to the organization (including how to handle whistleblowing cases).	Governed (Level 3)
RES–07	Ensure that the organization's documented Incident Management (IM) plan defines how to report to external groups (such as partners, law enforcement, regulators, and others) during a cybersecurity incident.	Governed (Level 3)
RES–08	Ensure that the organization's documented Incident Management (IM) plan defines how to report a cybersecurity incident to those impacted by the incident.	Governed (Level 3)
RES–09	Ensure that the organization's documented Incident Management (IM) plan defines the roles and responsibilities of the technical incident response team or security operations center during a cybersecurity incident.	Governed (Level 3)
RES–10	Ensure the organization's documented Incident Management (IM) plan defines how and where to document cybersecurity incidents.	Governed (Level 3)
RES–11	Ensure that the organization's documented Incident Management (IM) plan defines categories or classifications levels of cybersecurity incidents and how to classify incidents at each level.	Governed (Level 3)
RES–12	Ensure that the organization's documented Incident Management (IM) plan requires the organization to perform a root cause analysis of each cybersecurity incident.	Governed (Level 3)

Resilience Management (continued)

Safeguard ID	Safeguard Description	Level
RES–13	Define a process the organization shall use to ensure that the organization's documented Incident Management (IM) plan defines how the documentation will be regularly reviewed and updated.	Governed (Level 3)
RES–14	Define a process for regularly testing the organization's Incident Management (IM) plans.	Controlled (Level 4)
RES–15	Regularly perform tabletop exercises with key stakeholders to test the organization's Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) plans.	Controlled (Level 4)
RES–16	Define a process the organization shall use to report Incident Management (IM) statistics to the organization's business stakeholders.	Monitored (Level 5)
RES–17	Maintain technical cybersecurity tools to help the organization detect and respond to cybersecurity incidents as described in the organization's Incident Management (IM) plans.	Controlled (Level 4)
RES–18	Regularly test the organization's cybersecurity Incident Management (IM) tools to ensure they function as expected to help it detect and respond to cybersecurity incidents.	Controlled (Level 4)
RES–19	Maintain a cybersecurity forensics and threat-hunting program to help the organization detect and respond to cybersecurity incidents.	Monitored (Level 5)
RES–20	Maintain cybersecurity forensics tools to help the organization create forensics images of computing systems to detect and respond to cybersecurity incidents.	Monitored (Level 5)
RES–21	Define a process the organization shall use to update its Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) documentation after changes to its information technologies.	Governed (Level 3)
RES–22	Maintain an enterprise backup architecture to regularly create backups of the organization's computing systems and data.	Foundational (Level 1)
RES–23	Maintain a trusted system image for each class of computing endpoint to ensure that it can be quickly restored in the case of a cybersecurity incident.	Foundational (Level 1)
RES–24	Maintain a trusted system image for each computing server to ensure that it can be quickly restored in the case of a cybersecurity incident.	Foundational (Level 1)
RES–25	Maintain technical access controls on each of the organization's backups to ensure that only authorized users have access to them (including encrypting physical access controls).	Hygiene (Level 2)
RES–26	Maintain immutable backups for each of the organization's computing systems and data to ensure they cannot be accidentally deleted or by malicious individuals.	Hygiene (Level 2)
RES–27	Define a process the organization shall use to test the organization's backups regularly.	Hygiene (Level 2)

Artificial Intelligence Management

Managing their security and ethical implications is crucial as AI technologies become integral to cybersecurity and business operations. Artificial intelligence management safeguards address the governance, risk assessment, and security controls necessary to ensure that AI systems operate safely and transparently. These safeguards focus on monitoring AI model integrity, preventing adversarial attacks, enforcing ethical AI principles, and securing AI-driven decision-making processes. By embedding structured AI risk management, organizations can harness the power of AI while mitigating unintended consequences and security vulnerabilities.

Safeguard ID	Safeguard Description	Level
AI-01	Maintain an artificial intelligence acceptable use standard to govern the organization's adoption and use of artificial intelligence technologies.	Controlled (Level 4)
AI-02	Ensure the organization's artificial intelligence acceptable use standard defines the types of data that may be entered into AI systems, ensuring compliance with the organization's data classification requirements.	Controlled (Level 4)
AI-03	Ensure the organization's artificial intelligence acceptable use standard establishes guidelines distinguishing between AI systems maintained on-premises and publicly available AI solutions, in alignment with the organization's data classification requirements.	Controlled (Level 4)
AI-04	Ensure the organization's artificial intelligence acceptable use standard defines criteria for evaluating and approving new AI technologies before they are adopted within the organization.	Controlled (Level 4)
AI-05	Ensure the organization's artificial intelligence acceptable use standard defines the acceptable use of AI embedded in software in accordance with the organization's software inventory requirements.	Controlled (Level 4)
AI-06	Ensure the organization's artificial intelligence acceptable use standard defines the authorization requirements for AI usage, ensuring that only authorized users can access and utilize AI systems in accordance with the organization's access control policies.	Controlled (Level 4)
AI-07	Ensure the organization's artificial intelligence acceptable use standard addresses intellectual property and copyright considerations to ensure compliance with legal and regulatory requirements.	Controlled (Level 4)
AI-08	Ensure the organization's artificial intelligence acceptable use standard includes provisions for managing the use of high-risk AI systems to mitigate potential security, privacy, and operational risks.	Controlled (Level 4)
AI-09	Ensure the organization's artificial intelligence acceptable use standard defines guidelines for identifying, mitigating, and addressing bias in AI systems.	Controlled (Level 4)
AI-10	Ensure the organization's artificial intelligence acceptable use standard ensures that all AI usage aligns with ethical guidelines and principles to prevent misuse or unintended consequences.	Controlled (Level 4)
AI-11	Ensure the organization's artificial intelligence acceptable use standard defines monitoring requirements to detect and prevent AI misuse, abuse, or unintended consequences, including mechanisms for reporting and responding to incidents.	Controlled (Level 4)
AI-12	Ensure the organization's artificial intelligence acceptable use standard defines the necessity of human oversight in AI-assisted decision-making, including requirements for human intervention, review, and curation of AI-generated outputs where appropriate.	Controlled (Level 4)
AI-13	Maintain an approved artificial intelligence software inventory to track and manage authorized AI solutions.	Controlled (Level 4)
AI-14	Ensure the organization's artificial intelligence inventory includes AI solutions developed and managed by the organization to ensure proper governance and oversight.	Controlled (Level 4)
AI-15	Ensure the organization's artificial intelligence inventory tracks Software-as-a-Service (SaaS) AI solutions utilized within the organization.	Controlled (Level 4)
AI-16	Ensure the organization's artificial intelligence inventory accounts for AI capabilities embedded within approved software applications to maintain visibility and control over AI use.	Controlled (Level 4)
AI-17	Ensure the organization's artificial intelligence inventory tracks third-party AI use to ensure acceptable use of AI by such third parties, especially as it relates to the use of the organization's data.	Controlled (Level 4)

Physical Security Management

Protecting physical infrastructure is an essential component of a comprehensive cybersecurity strategy. The Physical Security Management safeguards define the measures needed to secure facilities, prevent unauthorized access, and protect physical assets from tampering. These safeguards include implementing access controls for restricted areas, monitoring visitor activity, ensuring secure disposal of sensitive materials, and enforcing environmental protections for critical systems. By integrating physical security controls with digital defenses, organizations can reduce the risk of breaches from on-site vulnerabilities.

Safeguard ID	Safeguard Description	Level
PHY-01	Maintain a documented physical security program for the organization that documents the safeguards it will implement to address physical security.	Governed (Level 3)
PHY-02	Define a process the organization shall use to monitor and detect violations of the organization's physical security program.	Monitored (Level 5)
PHY-03	Ensure that the organization's documented physical security program defines safeguards for securely disposing of physical assets.	Hygiene (Level 2)
PHY-04	Ensure that the organization's documented physical security program defines safeguards for perimeter access controls to the organization's facilities.	Hygiene (Level 2)
PHY-05	Ensure that the organization's documented physical security program defines safeguards for authorizing, identifying, and monitoring visitors at the organization's facilities.	Monitored (Level 5)
PHY-06	Ensure that the organization's documented physical security program defines safeguards for addressing internal physical access controls at the organization's facilities.	Controlled (Level 4)
PHY-07	Ensure the organization's documented physical security program defines safeguards for securely handling physical access devices (such as keys or cards).	Hygiene (Level 2)
PHY-08	Ensure that the organization's documented physical security program defines safeguards to visibly mark the classification level of the organization's technology assets.	Controlled (Level 4)
PHY-09	Ensure that the organization's documented physical security program defines environmental safeguards to protect the organization's facilities and technology assets.	Hygiene (Level 2)
PHY-10	Ensure the organization's documented physical security program defines safeguards to address access controls for physical computing devices.	Controlled (Level 4)
PHY-11	Ensure that the organization's documented physical security program defines safeguards for how individuals can remove technology assets from the organization's facilities.	Governed (Level 3)
PHY-12	Ensure that the organization's documented physical security program defines safeguards and how the organization will secure unattended spaces (such as clean desk policies).	Governed (Level 3)
PHY-13	Ensure the organization's documented physical security program defines safeguards to secure technology assets such as printers, copiers, or multi-function devices.	Controlled (Level 4)
PHY-14	Ensure that the organization's documented physical security program defines safeguards for logging physical access to its facilities.	Monitored (Level 5)
PHY-15	Regularly perform physical penetration tests at each facility to ensure the organization's physical security safeguards operate as expected.	Monitored (Level 5)

Privacy Management

Protecting personal and sensitive data is every organization's legal and ethical responsibility. The Privacy Management safeguards ensure compliance with global privacy regulations and best practices for handling personal information. These safeguards focus on defining clear data handling policies, maintaining records of processing activities, implementing privacy-by-design principles, and enabling user consent management. By prioritizing privacy protections, organizations can maintain regulatory compliance, build customer trust, and minimize the risk of data misuse or exposure.

Safeguard ID	Safeguard Description	Level
PRV-01	Maintain a transparent, documented privacy program that documents the organization's safeguards to address data privacy.	Governed (Level 3)
PRV-02	Ensure that the organization's documented privacy program defines a process for performing data processing authorizations (authorizing, maintaining, and revoking).	Governed (Level 3)
PRV-03	Ensure that the organization's documented privacy program defines a process for reviewing, transferring, disclosing, modifying, or deleting data from the organization's information systems for privacy purposes.	Governed (Level 3)
PRV-04	Ensure that the organization's documented privacy program defines a process for recording and maintaining an individual's privacy preferences.	Governed (Level 3)
PRV-05	Ensure that the organization's documented privacy program defines a process for recording, maintaining, and reviewing stakeholder goals for data privacy.	Governed (Level 3)
PRV-06	Ensure that the organization's documented privacy program defines a process for evaluating the organization's use of data for bias.	Controlled (Level 4)
PRV-07	Ensure that the organization's documented privacy program defines a process for recording and evaluating data provenance and lineage.	Controlled (Level 4)
PRV-08	Ensure that the organization's documented privacy program defines a process for limiting the identification or inference of individuals when processing data.	Controlled (Level 4)
PRV-09	Ensure that the organization's documented privacy program defines a process for replacing attribute values with attribute references in the organization's information systems for privacy purposes.	Controlled (Level 4)
PRV-10	Ensure that the organization's documented privacy program defines a process for informing customers and external business partners about how their data is being used and the organization's privacy goals.	Governed (Level 3)
PRV-11	Ensure that the organization's documented privacy program defines a process to obtain feedback from individuals regarding the organization's use of data and the associated privacy risks.	Governed (Level 3)
PRV-12	Ensure that the organization's documented privacy program defines a process to allow individuals to request data corrections to their data.	Governed (Level 3)
PRV-13	Ensure that the organization's documented privacy program defines a process to allow individuals to request data deletions of their data (right to be forgotten).	Governed (Level 3)
PRV-14	Ensure that the organization's documented privacy program defines a process for sharing only appropriate data with third parties.	Governed (Level 3)
PRV-15	Maintain a technology platform to record the organization's efforts related to its data privacy program.	Governed (Level 3)
PRV-16	Ensure the organization's privacy record system tracks individuals' stated privacy preferences.	Governed (Level 3)
PRV-17	Ensure that the organization's privacy record system tracks data correction and deletion requests and the organization's response.	Governed (Level 3)
PRV-18	Ensure the organization's privacy record system tracks data disclosures or sharing personal information with third-parties.	Governed (Level 3)

Identity Management

Managing digital identities is a fundamental safeguard against unauthorized access and insider threats. The Identity Management safeguards establish secure identity verification, authentication, and account lifecycle processes. These safeguards require organizations to maintain an inventory of identity providers, enforce strong authentication policies, implement single sign-on (SSO) solutions, and regularly review identity access rights. Organizations can strengthen access control and reduce the risk of credential-based attacks by ensuring secure identity management.

Safeguard ID	Safeguard Description	Level
ID-01	Maintain a Human Resources (HR) program to formally manage the organization's workforce members.	Governed (Level 3)
ID-02	Maintain a Human Resources Information System (HRIS) to track the status of each organization's workforce member.	Governed (Level 3)
ID-03	Ensure that the organization's Human Resources (HR) program performs background screening for each workforce member.	Governed (Level 3)
ID-04	Ensure that the organization's Human Resources (HR) program requires workforce members to agree to the organization's terms and conditions of employment or similar appropriate contracts.	Governed (Level 3)
ID-05	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return physical assets after their work with the organization.	Governed (Level 3)
ID-06	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return information assets after their work with the organization.	Governed (Level 3)
ID-07	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return authentication credentials after their work with the organization.	Governed (Level 3)
ID-08	Maintain an inventory of each Identity Provider (IDP) the organization approves.	Hygiene (Level 2)
ID-09	Ensure that the organization minimizes the number of Identity Providers (IDPs) it uses and utilizes centralized Single Sign On (SSO) solutions whenever possible.	Hygiene (Level 2)
ID-10	Maintain an inventory of each user account authorized by the Identity Provider (IDP).	Governed (Level 3)
ID-11	Maintain a configuration benchmark for each of the organization's authorized Identity Providers (IDPs).	Controlled (Level 4)
ID-12	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) do not allow workforce members to share accounts.	Controlled (Level 4)
ID-13	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) do not allow concurrent account logins.	Controlled (Level 4)
ID-14	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) do not allow account names to be reused within a defined period of time.	Controlled (Level 4)
ID-15	Define a process the organization shall use to regularly perform identity reviews of each of the organization's Identity Providers (IDPs) to ensure only authorized accounts exist in the system.	Governed (Level 3)

Identity Management (continued)

Safeguard ID	Safeguard Description	Level
ID-16	Maintain an identity management system to provision accounts for workforce members once automatically added to the organization's Human Resources Information System (HRIS).	Controlled (Level 4)
ID-17	Maintain an identity management system to automatically de-provision accounts for workforce members once they are tagged as inactive in the organization's Human Resources Information System (HRIS).	Controlled (Level 4)
ID-18	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require strong passwords.	Foundational (Level 1)
ID-19	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require account lockouts if a defined threshold of failed login attempts is exceeded.	Foundational (Level 1)
ID-20	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) require that passwords be stored encrypted and hashed using salts.	Hygiene (Level 2)
ID-21	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require passwords to be transmitted only when encrypted.	Hygiene (Level 2)
ID-22	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require a process for secure password provisioning by the organization's helpdesk.	Governed (Level 3)
ID-23	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require using Multi-Factor Authentication (MFA).	Hygiene (Level 2)
ID-24	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require that unused accounts are automatically disabled after a period of not being used and/or require the use of expiration dates on each account.	Controlled (Level 4)
ID-25	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging logon events for standard accounts (whether successful or failed).	Hygiene (Level 2)
ID-26	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging access to deactivated accounts.	Monitored (Level 5)
ID-27	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging User Behavior Analytics (UBA) events.	Monitored (Level 5)

Privileged Account Management

Privileged accounts present a high-risk target for attackers and must be secured with strict controls. The Privileged Account Management safeguards focus on inventorying and protecting privileged accounts across endpoint, server, network, and application environments. These safeguards require organizations to implement multi-factor authentication (MFA) for privileged access, enforce role-based access controls, remove default system credentials, and monitor privileged activity for suspicious behavior. Organizations can significantly reduce the risk of insider threats and privilege escalation attacks by securing privileged accounts.

Safeguard ID	Safeguard Description	Level
PAM-01	Maintain an inventory of all privileged accounts configured on endpoint computing systems.	Governed (Level 3)
PAM-02	Maintain an inventory of all privileged accounts configured on server computing systems.	Governed (Level 3)
PAM-03	Maintain an inventory of all privileged accounts configured on network devices.	Governed (Level 3)
PAM-04	Maintain an inventory of all privileged accounts configured on enterprise business applications.	Governed (Level 3)
PAM-05	Ensure all privileged accounts on endpoint computing systems are authorized and dedicated privileged accounts are required.	Hygiene (Level 2)
PAM-06	Ensure that all privileged accounts on server computing systems are authorized and require dedicated privileged accounts.	Hygiene (Level 2)
PAM-07	Ensure all privileged accounts on network devices are authorized and require dedicated privileged accounts.	Hygiene (Level 2)
PAM-08	Ensure that all privileged accounts on enterprise business applications are authorized and require dedicated privileged accounts.	Hygiene (Level 2)
PAM-09	Ensure that all default privileged accounts are not using their default system credentials to authenticate to the system.	Hygiene (Level 2)
PAM-10	Ensure that the organization does not allow shared privileged accounts for workforce members except in documented cases for emergency access or via a Privileged Account Management (PAM) system.	Controlled (Level 4)
PAM-11	Maintain a Privileged Account Management (PAM) or Password Manager (PM) system for documenting service, shared accounts, or shared secrets between workforce members.	Controlled (Level 4)
PAM-12	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each endpoint or server computing system.	Controlled (Level 4)
PAM-13	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each network device.	Controlled (Level 4)
PAM-14	Ensure the organization's Identity Providers (IDPs) require Multi-Factor Authentication (MFA) for all privileged accounts.	Hygiene (Level 2)
PAM-15	Ensure the organization's Identity Providers (IDPs) logs and alerts when changes are made to privileged group memberships.	Monitored (Level 5)
PAM-16	Ensure the organization's Identity Providers (IDPs) log and alert account logon events (successful and failed) for all privileged accounts.	Monitored (Level 5)

Data Management

Effective data management protects sensitive information from loss, theft, or corruption. Data management safeguards ensure that organizations establish clear policies for data classification, ownership, and secure storage. These safeguards require organizations to inventory data assets, define data retention policies, restrict access to sensitive information, and implement encryption for data at rest and in transit. By enforcing strong data management practices, organizations can minimize data exposure risks and improve compliance with regulatory requirements.

Safeguard ID	Safeguard Description	Level
DTA-01	Maintain a data inventory management system to track data managed by the organization.	Controlled (Level 4)
DTA-02	Ensure the organization's data inventory management system maintains an Inventory of data managed by the organization and under its control.	Controlled (Level 4)
DTA-03	Ensure the organization's data inventory management system maintains an Inventory of data managed by the organization and under the control of third parties.	Controlled (Level 4)
DTA-04	Ensure the organization's data inventory management system maintains documented definitions of the categories of data it manages.	Controlled (Level 4)
DTA-05	Ensure the organization's data inventory management system defines data owners for all data the organization manages.	Controlled (Level 4)
DTA-06	Ensure the organization's data inventory management system tracks the necessity of the data managed by the organization when the organization's data owners approve it.	Controlled (Level 4)
DTA-07	Ensure the organization's data inventory management system tracks the business purpose of all data managed by the organization.	Controlled (Level 4)
DTA-08	Ensure the organization's data inventory management system tracks data that should be masked in information systems.	Controlled (Level 4)
DTA-09	Ensure the organization's data inventory management system tracks the classification, criticality, and sensitivity of all data it manages.	Controlled (Level 4)
DTA-10	Ensure the organization's data inventory management system documents the location of all data managed during the processing lifecycle.	Controlled (Level 4)
DTA-11	Maintain a system to automatically inventory and classify items managed by the organization (whether onsite or located at a third party).	Controlled (Level 4)
DTA-12	Ensure that the organization's data inventory system automatically discovers data managed by the organization (whether onsite or at a third party).	Controlled (Level 4)
DTA-13	Ensure that the organization's data inventory system automatically classifies and labels data managed by the organization (whether onsite or located at a third party).	Controlled (Level 4)
DTA-14	Ensure that the organization's data inventory system automatically discovers when its private data is located in publicly available locations.	Controlled (Level 4)
DTA-15	Ensure that the organization's data inventory system is integrated with the organization's asset inventory system.	Controlled (Level 4)
DTA-16	Ensure that the organization's data inventory system logs and alerts events related to the data it manages (such as access, changes, and deletions).	Monitored (Level 5)
DTA-17	Ensure that the organization's data inventory system logs and alerts events related to the system configuration files managed by the organization (such as access, changes, and deletions).	Monitored (Level 5)
DTA-18	Define a process the organization shall use to define data retention periods for different types of data managed by the organization.	Controlled (Level 4)
DTA-19	Define a process the organization shall use to archive data managed by the organization whenever possible.	Controlled (Level 4)

Access Management

Controlling and monitoring user access to critical systems is vital for preventing unauthorized activity. Access Management safeguards define the principles for granting, modifying, and revoking user access to ensure security and the least privileged enforcement. These safeguards require organizations to maintain access control lists (ACLs), implement automated provisioning and deprovisioning, enforce segregation of duties, and monitor access logs for anomalies. Organizations can prevent unauthorized system interactions and data breaches by managing access effectively.

Safeguard ID	Safeguard Description	Level
AM-01	Define a process for creating and documenting roles and responsibilities for each of the organization's workforce members.	Governed (Level 3)
AM-02	Ensure that the organization's documented roles and responsibilities for workforce members consider the principle of separation of duties when defining roles.	Governed (Level 3)
AM-03	Maintain documented Access Control Lists (ACLs) for each computing system and business application system.	Hygiene (Level 2)
AM-04	Ensure that the organization's documented Access Control Lists (ACLs) for computing systems and business applications are based on the organization's defined roles for workforce members.	Controlled (Level 4)
AM-05	Maintain Access Control Lists (ACLs) on computing system objects based on approved documentation, roles, and the principle of least privilege.	Controlled (Level 4)
AM-06	Maintain Access Control Lists (ACLs) on computing system functions based on approved documentation, roles, and the principle of least privilege.	Controlled (Level 4)
AM-07	Maintain Access Control Lists (ACLs) on code repositories based on approved documentation, roles, and the principle of least privilege.	Controlled (Level 4)
AM-08	Ensure that the organization's Access Control Lists (ACLs) enforce encryption of data at rest on each of the organization's computing systems.	Controlled (Level 4)
AM-09	Ensure that the organization's Access Control Lists (ACLs) enforce data encryption in transit on each computing system.	Controlled (Level 4)
AM-10	Define a process for reviewing the organization's documented Access Control Lists (ACLs) on a regular basis.	Governed (Level 3)
AM-11	Define a process for reviewing the organization's Access Control List (ACL) documentation on a regular basis.	Governed (Level 3)
AM-12	Define a process the organization shall use to regularly review the organization's group or role membership used by the organization's Access Control Lists (ACLs) on a regular basis.	Governed (Level 3)
AM-13	Ensure the organization's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).	Hygiene (Level 2)

Log Management

Comprehensive log management enables security teams to detect, investigate, and respond to cyber threats efficiently. The Log Management safeguards ensure that organizations implement centralized logging, retain logs for forensic analysis, and monitor logs for suspicious activity. These safeguards focus on maintaining enterprise-managed time sources, enforcing log integrity protections, and ensuring that logs are aggregated and correlated across systems. Organizations can enhance threat detection and incident response capabilities by maintaining robust log management practices.

Safeguard ID	Safeguard Description	Level
LOG-01	Maintain at least three enterprise-managed time sources that the organization's information systems can use to synchronize time.	Hygiene (Level 2)
LOG-02	Ensure the organization's operating system configuration benchmarks enable appropriate logging on all computing systems.	Hygiene (Level 2)
LOG-03	Ensure the organization's network device configuration benchmarks enable appropriate logging on all network devices.	Monitored (Level 5)
LOG-04	Ensure the organization's business application configuration benchmarks enable appropriate logging on all business applications.	Monitored (Level 5)
LOG-05	Ensure the organization's cloud configuration benchmarks enable appropriate logging on all Cloud Service Providers (CSPs) and Software-as-a-Service (SaaS) platforms.	Monitored (Level 5)
LOG-06	Maintain a system to aggregate all appropriate logs from each organization's information system.	Hygiene (Level 2)
LOG-07	Ensure the organization's aggregated information system logs are only accessible to authorized workforce members.	Controlled (Level 4)
LOG-08	Ensure the organization's aggregated information system logs and alerts when logs have not been received from an information system after a defined period.	Monitored (Level 5)
LOG-09	Ensure the organization's aggregated information system is regularly tuned to ensure appropriate log events are alerted to the appropriate workforce members.	Monitored (Level 5)
LOG-10	Define a process the organization shall use to regularly review the logs aggregated from the organization's information systems.	Monitored (Level 5)
LOG-11	Ensure that the organization's regular log review process includes clear Service Level Agreements (SLAs) for who should monitor aggregated information system logs (such as a Security Operations Center (SOC)).	Monitored (Level 5)
LOG-12	Define a process the organization shall use to automate the review of aggregated logs.	Monitored (Level 5)
LOG-13	Define a process the organization will use to automate alerting on threats discovered by its aggregate log management system.	Monitored (Level 5)
LOG-14	Define a process the organization shall use to retain information systems logs over time (including how long to retain logs of particular types).	Monitored (Level 5)
LOG-15	Maintain a log management system (such as a SIEM, SOAR, or service management platform) to track the status of alerts generated by the organization's log management system.	Monitored (Level 5)

System Protection Management

Securing computing systems against cyber threats is fundamental to an organization's security posture. The System Protection Management safeguards ensure that endpoint devices, servers, and infrastructure are protected through advanced security controls. These safeguards include maintaining endpoint detection and response (EDR) systems, enforcing whole-disk encryption, implementing host-based firewalls, and restricting the use of removable media. Organizations can defend against malware, unauthorized access, and data exfiltration by strengthening system protections.

Safeguard ID	Safeguard Description	Level
SYS-01	Maintain an Endpoint Detection and Response (EDR) system to detect and alert malicious activity on the organization's computing systems, whether onsite or remote.	Foundational (Level 1)
SYS-02	Ensure that the organization's Endpoint Detection and Response (EDR) system utilizes software agents that cannot be disabled by standard computing system users.	Foundational (Level 1)
SYS-03	Ensure the organization's Endpoint Detection and Response (EDR) system is centrally managed and cloud-based.	Foundational (Level 1)
SYS-04	Ensure that the organization's Endpoint Detection and Response (EDR) system's anti-malware signature is regularly updated on all computing systems.	Foundational (Level 1)
SYS-05	Ensure the organization's Endpoint Detection and Response (EDR) system automatically scans removable media for potentially malicious files.	Foundational (Level 1)
SYS-06	Ensure that the organization's Endpoint Detection and Response (EDR) system logs and tracks all running processes for cybersecurity incident response.	Monitored (Level 5)
SYS-07	Ensure that the organization's Endpoint Detection and Response (EDR) system generates a database of the signatures (hashes) for all the files on each of the organization's computing systems for cybersecurity incident response.	Monitored (Level 5)
SYS-08	Ensure that the organization's Endpoint Detection and Response (EDR) system logs and alerts on appropriate events for cybersecurity incident response.	Foundational (Level 1)
SYS-09	Maintain host-based firewalls on each of the organization's computing systems.	Controlled (Level 4)
SYS-10	Ensure the organization's host-based firewalls are configured with a default rule to deny all network traffic.	Controlled (Level 4)
SYS-11	Maintain a whole-disk encryption system on the organization's endpoint computing systems.	Hygiene (Level 2)
SYS-12	Maintain a host-based Data Loss Prevention (DLP) system on each organization's computing system.	Controlled (Level 4)
SYS-13	Maintain removable media safeguards on each of the organization's endpoint computing systems.	Hygiene (Level 2)
SYS-14	Ensure the organization's removable media safeguard system creates an inventory of authorized storage and peripheral devices.	Governed (Level 3)
SYS-15	Ensure the organization's removable media safeguard system tracks data owners on approved devices responsible for the media.	Governed (Level 3)
SYS-16	Ensure the organization's removable media safeguard system disables removable storage media on computing systems that do not require such devices.	Controlled (Level 4)
SYS-17	Ensure the organization's removable media safeguard system disables unauthorized peripheral devices on computing systems that do not require such devices.	Controlled (Level 4)
SYS-18	Ensure the organization's removable media safeguard system only allows reading and writing on authorized removable media devices.	Controlled (Level 4)
SYS-19	Ensure the organization's removable media safeguard system only allows writing to authorized removable media devices utilizing encryption.	Controlled (Level 4)

Software Management

Managing software assets effectively reduces the risk of unpatched vulnerabilities and unauthorized applications. The Software Management safeguards focus on maintaining an inventory of approved software, ensuring regular patching, and enforcing application control policies. These safeguards require organizations to validate software against vendor support lifecycles, monitor for unauthorized installations, and restrict the execution of unapproved binaries, libraries, and scripts. Organizations can minimize exposure to software-based security risks by maintaining strict software management policies.

Safeguard ID	Safeguard Description	Level
SW-01	Maintain a system to maintain an inventory of the organization's approved software.	Hygiene (Level 2)
SW-02	Ensure the organization's software inventory system records appropriate demographics for each software application.	Hygiene (Level 2)
SW-03	Ensure the organization's software inventory system regularly updates the software inventory via an automated discovery tool.	Hygiene (Level 2)
SW-04	Ensure the organization's software inventory system correlates the organization's hardware and software inventories in the same system.	Hygiene (Level 2)
SW-05	Ensure the organization's software inventory system validates that all software in the inventory is still supported by the software vendor.	Hygiene (Level 2)
SW-06	Ensure the organization's software inventory system validates that all operating system software in the organization's software inventory is kept up to date.	Hygiene (Level 2)
SW-07	Ensure the organization's software inventory system validates that all application software in the organization's software inventory is kept up to date.	Hygiene (Level 2)
SW-08	Maintain a Service Level Agreement (SLA) for the organization to define how often software updates must be performed on each software application.	Governed (Level 3)
SW-09	Define a process the organization shall use to ensure all software adheres to the organization's approved software-update Service Level Agreement (SLA).	Governed (Level 3)
SW-10	Maintain a software application control system on each organization's computing systems to ensure that only authorized software can execute.	Hygiene (Level 2)
SW-11	Ensure the organization's application control system only allows the execution of authorized binaries on each of the organization's computing systems.	Hygiene (Level 2)
SW-12	Ensure the organization's application control system only allows authorized software libraries (such as DLLs) on each of the organization's computing systems.	Controlled (Level 4)
SW-13	Ensure the organization's application control system only allows the use of authorized software scripts on each of the organization's computing systems.	Controlled (Level 4)
SW-14	Ensure the organization's application control system only allows the use of authorized operating system shells (such as Microsoft PowerShell or BASH) on each of its computing systems.	Hygiene (Level 2)
SW-15	Define a process the organization shall use to remove unauthorized software from each of its computing systems in a timely manner.	Controlled (Level 4)

Configuration Management

Ensuring that systems are securely configured is critical to reducing cyber risk. The Configuration Management safeguards establish standardized security benchmarks for operating systems, applications, and cloud services. These safeguards require organizations to enforce secure baseline configurations, disable unnecessary services, enable advanced logging, and implement secure boot processes. By maintaining a well-defined configuration management framework, organizations can prevent misconfigurations that could lead to security breaches.

Safeguard ID	Safeguard Description	Level
CFG-01	Maintain a library of approved operating system configuration benchmarks to ensure that each of the organization's operating systems are configured securely.	Governed (Level 3)
CFG-02	Ensure that the organization's approved operating system configuration benchmark defines the organization as able to disable all unnecessary services in the operating system.	Governed (Level 3)
CFG-03	Ensure that the organization's approved operating system configuration benchmark defines that the organization shall define configuration benchmarks for each necessary service, including databases, SMB services, tiny services, VoIP, and similar services.	Governed (Level 3)
CFG-04	Ensure that the organization's approved operating system configuration benchmark defines the organization as having unnecessary scripting languages in the operating system.	Governed (Level 3)
CFG-05	Ensure that the organization's approved operating system configuration benchmark defines it as enabling advanced logging for operating system shells (such as Microsoft PowerShell or BASH).	Governed (Level 3)
CFG-06	Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enforce cybersecurity services such as Data Execution Protection (DEP), Address Space Layout Randomization (ASLR), and User Account Control (UAC).	Governed (Level 3)
CFG-07	Ensure that the organization's approved operating system configuration benchmark defines its ability to disable autorun on its operating system.	Governed (Level 3)
CFG-08	Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enable machine locks (screensavers) after a defined period of inactivity.	Governed (Level 3)
CFG-09	Ensure that the organization's approved operating system configuration benchmark defines the organization as requiring a secure boot process to verify the integrity of the operating system before loading (such as UEFI).	Governed (Level 3)
CFG-10	Ensure that the organization's approved operating system configuration benchmark defines that the organization shall disable unnecessary wireless protocols and networks on the organization's endpoints.	Governed (Level 3)
CFG-11	Maintain a library of approved software application configuration benchmarks that will be used to ensure that each of the organization's software applications is configured securely.	Controlled (Level 4)
CFG-12	Maintain a configuration enforcement system to enforce the organization's approved operating system and application configurations on each of the organization's computing systems.	Controlled (Level 4)
CFG-13	Ensure that the organization's configuration enforcement system enforces the organization's approved operating system and application configurations, regardless of the computing system's location (whether onsite or operating remotely).	Controlled (Level 4)

Vulnerability Management

Identifying and remediating security vulnerabilities is essential for maintaining a strong defense against cyber threats. The Vulnerability Management safeguards ensure organizations deploy vulnerability scanning tools, prioritize discovered weaknesses, and track remediation efforts over time. These safeguards require organizations to scan for outdated software, misconfigurations, and open network ports while ensuring that remediation efforts are measured and reported to leadership. Organizations can reduce the attack surface and mitigate known security risks by implementing proactive vulnerability management.

Safeguard ID	Safeguard Description	Level
VUL-01	Maintain a Vulnerability Management (VM) system to detect and track weaknesses in the organization's information systems.	Hygiene (Level 2)
VUL-02	Ensure the organization's Vulnerability Management (VM) system uses agents and/or authenticated scans to detect weaknesses in the organization's information systems.	Hygiene (Level 2)
VUL-03	Ensure the organization's Vulnerability Management (VM) system scans for weaknesses caused by outdated, vulnerable software (based on CVEs).	Hygiene (Level 2)
VUL-04	Ensure the organization's Vulnerability Management (VM) system scans for weaknesses caused by software misconfigurations (based on CCEs).	Hygiene (Level 2)
VUL-05	Ensure the organization's Vulnerability Management (VM) system scans for open, dangerous network ports or services.	Hygiene (Level 2)
VUL-06	Ensure the organization's Vulnerability Management (VM) system prioritizes the vulnerabilities it detects in its information systems.	Governed (Level 3)
VUL-07	Ensure the organization's Vulnerability Management (VM) system compares the results of consecutive vulnerability scans to track the progress of remediation efforts over time.	Governed (Level 3)
VUL-08	Ensure the organization's Vulnerability Management (VM) system tracks open vulnerabilities in the organization's information systems.	Governed (Level 3)
VUL-09	Ensure the organization's Vulnerability Management (VM) system tracks approved exceptions when vulnerabilities are discovered on the organization's information systems.	Governed (Level 3)
VUL-10	Ensure the organization's Vulnerability Management (VM) system reports discovered vulnerabilities to the organization's technical staff regularly.	Monitored (Level 5)
VUL-11	Ensure the organization's Vulnerability Management (VM) system regularly reports discovered vulnerabilities to the organization's business unit staff.	Monitored (Level 5)
VUL-12	Ensure the organization's Vulnerability Management (VM) system reports discovered vulnerabilities to the organization's business leadership staff regularly.	Monitored (Level 5)

Mobile Device Management

The widespread use of mobile devices introduces unique security risks that must be managed effectively. The Mobile Device Management safeguards focus on enforcing security controls for corporate and personal mobile devices used for business operations. These safeguards require organizations to enforce mobile security policies, restrict the installation of unauthorized applications, require device encryption, enable remote wipe capabilities, and detect jailbroken or compromised devices. By securing mobile devices, organizations can protect sensitive data across all endpoints.

Safeguard ID	Safeguard Description	Level
MDM-01	Maintain a Mobile Device Management (MDM) system to enforce cybersecurity safeguards on each organization's mobile device (such as phones and tablets).	Controlled (Level 4)
MDM-02	Ensure the organization's Mobile Device Management (MDM) system limits enterprise data on mobile devices to containerized, enterprise-managed applications.	Controlled (Level 4)
MDM-03	Ensure the organization's Mobile Device Management (MDM) system enforces approved configurations on each of the organization's approved enterprise applications.	Controlled (Level 4)
MDM-04	Ensure the organization's Mobile Device Management (MDM) system enforces application control on the organization's managed mobile devices, only allowing authorized applications (including mobile application stores) to execute on the devices.	Controlled (Level 4)
MDM-05	Ensure the organization's Mobile Device Management (MDM) system enforces an unlock code to access each of the organization's mobile devices (6 characters or longer).	Controlled (Level 4)
MDM-06	Ensure the organization's Mobile Device Management (MDM) system enforces mobile operating system updates on each of the organization's mobile devices.	Controlled (Level 4)
MDM-07	Ensure the organization's Mobile Device Management (MDM) system enforces application updates on each mobile device.	Controlled (Level 4)
MDM-08	Ensure the organization's Mobile Device Management (MDM) system detects and blocks jailbroken mobile devices.	Controlled (Level 4)
MDM-09	Ensure the organization's Mobile Device Management (MDM) system can remotely wipe data from its mobile devices if they are lost or stolen.	Controlled (Level 4)

Network Device Management

Securing network infrastructure is critical for protecting data flows and preventing unauthorized access. Network Device Management safeguards ensure that routers, switches, firewalls, and other network appliances are correctly configured, updated, and monitored. These safeguards require organizations to maintain an inventory of network devices, enforce multi-factor authentication (MFA) for administrative access, implement encrypted, remote management protocols, and monitor network status in real-time. By managing network devices securely, organizations can reduce the risk of misconfigurations and unauthorized access.

Safeguard ID	Safeguard Description	Level
NDM-01	Maintain an inventory of each of the organization's approved network devices.	Governed (Level 3)
NDM-02	Maintain network device cybersecurity configuration benchmarks for the organization's authorized network devices.	Governed (Level 3)
NDM-03	Ensure the organization's network devices are managed from an approved, dedicated management network subnet.	Controlled (Level 4)
NDM-04	Ensure the organization's network devices are not managed from a remote (or Internet-based) network.	Controlled (Level 4)
NDM-05	Ensure the organization's network devices are managed from an approved Privileged Account Management (PAM) system or management jump box.	Controlled (Level 4)
NDM-06	Ensure the organization's network devices require using Multi-Factor Authentication (MFA) to access the device.	Hygiene (Level 2)
NDM-07	Ensure the organization's network devices use encrypted remote management protocols (such as SSH or TLS).	Hygiene (Level 2)
NDM-08	Maintain a network device management system to manage each organization's approved network device.	Hygiene (Level 2)
NDM-09	Ensure the organization's network device management system regularly scans for new network devices to add to the organization's network device inventory.	Hygiene (Level 2)
NDM-10	Ensure the organization's network device management system monitors each network device's status and logs and alerts when it is offline.	Hygiene (Level 2)
NDM-11	Ensure the organization's network device management system performs IP Address Management (IPAM) for each network (including DHCP scopes).	Monitored (Level 5)
NDM-12	Ensure the organization's network device management system records netflow data from each network device.	Monitored (Level 5)
NDM-13	Ensure the organization's network device management system compares each network device's configuration on a regular basis to log and alert any changes to the configuration.	Monitored (Level 5)
NDM-14	Ensure the organization's network device management system ensures that each network device utilizes the latest firmware for the network device.	Hygiene (Level 2)

Perimeter Network Access Management

Defending the network perimeter is essential to preventing unauthorized external access to internal systems. The Perimeter Network Access Management safeguards focus on implementing firewalls, intrusion detection and prevention systems (IDS/IPS), and secure remote access solutions. These safeguards require organizations to enforce IP-based and user-based filtering, require MFA for remote access, encrypt all remote authentication channels, and block malicious traffic at the network boundary. Organizations can minimize the risk of external cyber threats breaching internal networks by securing perimeter access points.

Safeguard ID	Safeguard Description	Level
PNA-01	Maintain an inventory of the organization's approved perimeter network connections (including Internet and third-party connections).	Governed (Level 3)
PNA-02	Maintain documented Access Control Lists (ACLs) for the organization's approved perimeter network connections.	Governed (Level 3)
PNA-03	Maintain perimeter network firewalls at the organization's approved perimeter network connections.	Foundational (Level 1)
PNA-04	Ensure the organization's approved perimeter network firewalls perform IP-based filtering of perimeter network connections.	Hygiene (Level 2)
PNA-05	Ensure the organization's approved perimeter network firewalls perform protocol-based (TCP, UDP, or similar) inbound filtering of perimeter network connections.	Foundational (Level 1)
PNA-06	Ensure the organization's approved perimeter network firewalls perform protocol-based (TCP, UDP, or similar) outbound filtering of perimeter network connections.	Controlled (Level 4)
PNA-07	Ensure the organization's approved perimeter network firewalls perform application-based filtering of perimeter network connections.	Controlled (Level 4)
PNA-08	Ensure that the organization's approved perimeter network firewalls perform user-based filtering of network connections, ensuring that only authorized users can remotely connect to an organization's network.	Foundational (Level 1)
PNA-09	Ensure the organization's approved perimeter network firewalls require Multi-Factor Authentication (MFA) when authenticating all remote connections.	Hygiene (Level 2)
PNA-10	Ensure the organization's approved perimeter network firewalls use encrypted channels (such as TLS) when authenticating all remote connections.	Foundational (Level 1)
PNA-11	Ensure the organization's approved perimeter network firewalls require User Behavior Analytics (UBA) when authenticating all remote connections.	Controlled (Level 4)
PNA-12	Maintain a system to perform full packet capture for all of the organization's perimeter network traffic.	Monitored (Level 5)
PNA-13	Maintain perimeter network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) at the organization's approved perimeter network connections.	Foundational (Level 1)
PNA-14	Maintain a perimeter web-based URL filtering system at the organization's Internet connections.	Foundational (Level 1)
PNA-15	Ensure the organization's web-based URL filtering systems block network connections to unapproved web-based services (such as email, storage, or similar).	Controlled (Level 4)
PNA-16	Ensure the organization's web-based URL filtering systems decrypt all TLS-encrypted traffic to facilitate web-based URL filtering.	Controlled (Level 4)
PNA-17	Ensure that the organization's web-based URL filtering systems utilize Data Loss Prevention (DLP) on each of its Internet connections.	Controlled (Level 4)
PNA-18	Ensure that the organization's perimeter network firewalls log appropriate events observed by the system.	Monitored (Level 5)
PNA-19	Ensure that the organization's web-based URL filtering systems log all URLs observed by the system.	Monitored (Level 5)

Perimeter Network Access Management (continued)

PNA-20	Ensure that the organization's Domain Name System (DNS) systems log all DNS queries observed by the system.	Monitored (Level 5)
PNA-21	Ensure that the organization's Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) systems log all appropriate events observed by the system.	Monitored (Level 5)
PNA-22	Ensure that the organization's perimeter network firewalls log all remote user connections observed by the system.	Monitored (Level 5)
PNA-23	Maintain network deception technologies at the organization's perimeter network connections to facilitate incident detection and management.	Monitored (Level 5)

Internal Network Access Management

Controlling access within internal networks is crucial for preventing attackers' lateral movement. Internal Network Access Management safeguards ensure organizations enforce network segmentation, implement role-based access controls, and monitor internal network activity. These safeguards require organizations to maintain network authentication controls, enforce secure wireless protocols, and restrict access to critical systems based on business needs. Organizations can contain potential threats and limit unauthorized access within the corporate environment by securing internal network access.

Safeguard ID	Safeguard Description	Level
INA-01	Maintain documented Virtual Local Area Networks (VLANs) for the organization's endpoint computing system networks.	Governed (Level 3)
INA-02	Maintain documented Virtual Local Area Networks (VLANs) for the organization's server computing system networks.	Governed (Level 3)
INA-03	Maintain documented Virtual Local Area Networks (VLANs) for the organization's hypervisor management system networks.	Governed (Level 3)
INA-04	Maintain documented Virtual Local Area Networks (VLANs) for the organization's software development networks.	Governed (Level 3)
INA-05	Maintain dedicated computing systems on dedicated Virtual Local Area Networks (VLANs) for high-risk computing activities.	Controlled (Level 4)
INA-06	Maintain network authentication systems (802.1x) for each organization's wired network.	Controlled (Level 4)
INA-07	Ensure that the organization's network authentication systems (802.1x) for each wired network require certificate-based authentication.	Controlled (Level 4)
INA-08	Maintain network authentication systems (802.1x) for each of the organization's wireless networks.	Foundational (Level 1)
INA-09	Ensure that the organization's network authentication systems (802.1x) for each wireless network require certificate-based authentication.	Controlled (Level 4)
INA-10	Ensure the organization's network authentication systems (802.1x) for each of the organization's wireless networks require the use of AES-CCMP to encrypt all wireless connections.	Foundational (Level 1)
INA-11	Ensure the organization's network authentication systems (802.1x) for each of the organization's wireless networks require the use of a dedicated wireless network for all devices (guests) not managed by the organization.	Foundational (Level 1)
INA-12	Ensure the organization's network authentication systems (802.1x) for each of its wired or wireless networks require health checks of computing systems before allowing them access to the network.	Controlled (Level 4)
INA-13	Ensure that each of the organization's endpoint computing systems' Virtual Local Area Networks (VLANs) enforces privatization to prevent computing systems from communicating with other systems on the same VLAN.	Controlled (Level 4)

Cloud Service Provider Management

Managing cloud environments securely is vital as organizations increasingly rely on cloud-based services. The Cloud Service Provider Management safeguards and establishes controls for selecting, configuring, and monitoring cloud service providers (CSPs). These safeguards require organizations to enforce cloud security policies, validate CSP compliance with industry standards, implement cloud access controls, and monitor cloud infrastructure for misconfigurations. Organizations can maintain data integrity and prevent unauthorized access to cloud resources by securing cloud environments.

Safeguard ID	Safeguard Description	Level
CSP-01	Maintain an inventory of each of the organization's authorized Cloud Service Providers (CSPs).	Governed (Level 3)
CSP-02	Maintain an inventory of each service authorized for use in each authorized Cloud Service Provider (CSP).	Governed (Level 3)
CSP-03	Maintain an inventory of the organization's authorized Software-as-a-Service (SaaS) providers.	Governed (Level 3)
CSP-04	Maintain an inventory of the accounts authorized for use in each of the authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers.	Governed (Level 3)
CSP-05	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Cloud Service Providers (CSPs).	Controlled (Level 4)
CSP-06	Maintain a cybersecurity configuration benchmark for each of the services authorized for use in each of the organization's authorized Cloud Service Providers (CSPs).	Controlled (Level 4)
CSP-07	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Software-as-a-Service (SaaS) providers.	Controlled (Level 4)
CSP-08	Maintain a cloud configuration vulnerability management system to regularly scan each of the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers for potential cybersecurity vulnerabilities.	Monitored (Level 5)
CSP-09	Maintain a Data Loss Prevention (DLP) system to log and alert on potential data loss events in the organization's Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers regularly.	Controlled (Level 4)
CSP-10	Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are enabled on the cloud platform.	Monitored (Level 5)
CSP-11	Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are aggregated into the organization's log management system.	Monitored (Level 5)

Email Management

Email remains a primary attack vector for phishing, malware, and data leaks. The Email Management safeguards focus on implementing strong email security policies, filtering mechanisms, and authentication controls. These safeguards require organizations to deploy email filtering solutions, enforce domain-based message authentication (DMARC, SPF, and DKIM), scan for malicious attachments, and prevent data exfiltration via email. By securing email communications, organizations can reduce the risk of phishing attacks and email-based cyber threats.

Safeguard ID	Safeguard Description	Level
EM-01	Maintain an inventory of each of the domain names authorized to use email.	Governed (Level 3)
EM-02	Maintain an inventory of Mail Transfer Agents (MTAs) authorized for each of the organization's approved email domains.	Governed (Level 3)
EM-03	Maintain appropriate Domain Name System (DNS) records for each of the organization's approved email domains (including SPF, DKIM, and DMARC).	Foundational (Level 1)
EM-04	Ensure that the organization's email systems require encrypted connections (TLS) between all email servers, whether internal or external.	Controlled (Level 4)
EM-05	Ensure that the organization's email systems block emails from domains not utilizing the appropriate Domain Name System (DNS) records (including SPF, DKIM, and DMARC).	Controlled (Level 4)
EM-06	Ensure that the organization's email systems perform spam content filtering for all emails (received by or sent by the organization).	Foundational (Level 1)
EM-07	Ensure that the organization's email systems perform malware content filtering for all emails (received by or sent by the organization).	Foundational (Level 1)
EM-08	Ensure that the organization's email systems perform anti-phishing content filtering for all emails (received or sent by the organization).	Hygiene (Level 2)
EM-09	Ensure that the organization's email systems perform anti-phishing URL filtering for all emails (received by or sent by the organization).	Hygiene (Level 2)
EM-10	Ensure that the organization's email systems filter data content for all emails (received by or sent by the organization).	Controlled (Level 4)
EM-11	Ensure that the organization's email systems perform attachment filtering for all emails (received by or sent by the organization), including utilizing sandboxes to validate each attachment.	Hygiene (Level 2)
EM-12	Maintain a file transfer portal system that is separate from the organization's email system and that the organization can use to send large files to individuals outside of the organization.	Controlled (Level 4)

Software Development Management

Secure software development practices are essential for preventing vulnerabilities in custom applications. The Software Development Management safeguards ensure organizations integrate security throughout the software development lifecycle (SDLC). These safeguards require organizations to enforce secure coding practices, conduct static and dynamic application security testing (SAST/DAST), implement version control, and restrict production access. Organizations can prevent software-related security flaws from reaching production by embedding security into development workflows.

Safeguard ID	Safeguard Description	Level
SDM-01	Ensure the organization's software development program adheres to the organization's cybersecurity governance safeguards.	Governed (Level 3)
SDM-02	Ensure that each of the organization's software application development teams is governed by the organization's approved cybersecurity governance program.	Governed (Level 3)
SDM-03	Maintain a documented Software Development Lifecycle (SDLC) to govern the organization's development and maintenance of software applications.	Governed (Level 3)
SDM-04	Ensure that each of the organization's software application development teams follows the organization's approved Software Development Lifecycle (SDLC).	Governed (Level 3)
SDM-05	Maintain an approved inventory of each software development coding language used by the organization's software application development teams (by team).	Governed (Level 3)
SDM-06	Maintain a documented set of coding standards for each software development coding language used by the organization's software application development teams.	Controlled (Level 4)
SDM-07	Ensure that each organization's software development coding standards define how software application developers perform input validation in their software applications.	Controlled (Level 4)
SDM-08	Ensure that each organization's software development coding standards define how software application developers will only utilize organization and industry-approved encryption algorithms in their software applications.	Controlled (Level 4)
SDM-09	Ensure that each organization's software development coding standard defines how software application developers will only utilize organization and industry-approved data exchange protocols in their software applications.	Controlled (Level 4)
SDM-10	Ensure that each of the organization's software development coding standards specifically defines how software application developers will perform error handling in their software applications.	Controlled (Level 4)
SDM-11	Ensure that each of the organization's software development coding standards defines how software application developers will include data privacy values in their software applications.	Controlled (Level 4)
SDM-12	Maintain technical safeguards to create separation between the organization's development and production application systems.	Controlled (Level 4)
SDM-13	Ensure that the organization's non-production application systems do not contain any sensitive or personally identifiable information.	Controlled (Level 4)
SDM-14	Ensure that the organization's software application development teams do not have privileged access to the organization's production application systems.	Controlled (Level 4)

Software Development Vulnerability Management

Proactively identifying and remediating application security flaws is critical for reducing software-related risks. The Software Development Vulnerability Management safeguards focus on integrating security testing and risk assessments into the software development lifecycle. These safeguards require organizations to conduct regular vulnerability scans, perform penetration testing on applications, address security defects before release, and track vulnerability remediation over time. Organizations can minimize the risk of exploitable software vulnerabilities by prioritizing application security.

Safeguard ID	Safeguard Description	Level
SDV-01	Maintain an issue-tracking system for each cybersecurity vulnerability identified in the organization's custom software applications.	Governed (Level 3)
SDV-02	Ensure that the organization's issue-tracking system tracks cybersecurity vulnerabilities identified in its custom software applications and tracks the criticality of each custom software application to assist the organization with threat modeling.	Governed (Level 3)
SDV-03	Ensure that the organization's issue-tracking system tracks cybersecurity vulnerabilities identified in its custom software application, calculating the criticality of each vulnerability to assist the organization with threat modeling.	Governed (Level 3)
SDV-04	Maintain a software application code vulnerability scanner to scan each organization's custom software application for cybersecurity vulnerabilities.	Hygiene (Level 2)
SDV-05	Ensure that each of the organization's software application development teams is utilizing its software application code vulnerability scanner to scan each of their custom software applications.	Hygiene (Level 2)
SDV-06	Ensure that each cybersecurity vulnerability identified by the software application code vulnerability scanner is reported to the organization's issue-tracking system.	Governed (Level 3)
SDV-07	Maintain an approved inventory of each software library and third-party module used by the organization's software application development teams.	Governed (Level 3)
SDV-08	Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is maintained and supported by its creator.	Controlled (Level 4)
SDV-09	Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is updated with the latest cybersecurity-related updates.	Controlled (Level 4)
SDV-10	Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is scanned regularly for cybersecurity vulnerabilities.	Controlled (Level 4)
SDV-11	Ensure that each cybersecurity vulnerability identified by the software library and third-party module scanner is reported to the organization's issue-tracking system.	Controlled (Level 4)
SDV-12	Maintain a process for individuals inside or outside the organization to report software application vulnerabilities to the organization's issue-tracking system.	Controlled (Level 4)
SDV-13	Maintain documented Service Level Agreements (SLAs) that define the organization's timing targets for mitigating cybersecurity vulnerabilities discovered in the organization's custom software applications.	Monitored (Level 5)
SDV-14	Ensure that each of the cybersecurity vulnerabilities tracked by the organization's issue tracking system are remediated in accordance with the organization's documented Service Level Agreements (SLAs).	Monitored (Level 5)
SDV-15	Ensure that each cybersecurity vulnerability tracked by the organization's issue-tracking system is reported to the appropriate stakeholders on a regular basis.	Monitored (Level 5)

CONCLUSION

In conclusion, we hope the Cybersecurity Risk Foundation - Safeguards (CRF-S) will be a resource for organizations navigating the complex landscape of cybersecurity defense. By aggregating the most pertinent and effective cybersecurity safeguards from the most esteemed standards and regulations into a single, accessible framework, the CRF-S empowers organizations to streamline their cybersecurity efforts. This consolidation is designed to simplify the decision-making process for cybersecurity investments and ensure that organizations can confidently address their most critical security challenges with proven strategies. The prioritization of these safeguards, in alignment with the CRF - Maturity Model, offers a strategic path forward for organizations at varying stages of cybersecurity maturity, enabling them to enhance their defenses and resilience against cyber threats rapidly.

Moreover, the collaborative nature of the CRF-S underscores the project's foundational belief in the power of community and collective expertise in the fight against cyber threats. The involvement of multiple cybersecurity organizations in the maintenance and evolution of the CRF-S ensures that it remains a living document, reflective of the latest in cybersecurity best practices and responsive to the emerging landscape of digital threats. This communal effort not only enriches the CRF-S but also cultivates a broader culture of sharing, learning, and mutual support among cybersecurity professionals and organizations worldwide.

As organizations continue to face an ever-expanding array of cyber threats, the CRF-S provides a beacon of guidance and clarity. It is a testament to the cybersecurity community's commitment to collective defense and the empowerment of organizations to achieve their cybersecurity goals. In embracing the CRF-S, organizations can take decisive steps toward securing their digital futures, leveraging a comprehensive, prioritized, and community-supported framework of cybersecurity safeguards. The journey toward enhanced cybersecurity is ongoing and complex. Yet, with resources like the CRF-S, organizations have a solid foundation to build a more secure and resilient digital presence.

ABOUT US

The Cybersecurity Risk Foundation's (CRF) purpose is to encourage global collaboration and knowledge-sharing among cybersecurity professionals. Established with the mission to address the practical challenges of cybersecurity that organizations face, the CRF embodies a collective endeavor to fortify digital landscapes against ever-evolving threats. Our foundation is built on the principle that unity in action and thought can significantly impact cybersecurity, promoting safer and more resilient digital environments for businesses and institutions across various sectors.

At the heart of the CRF is a vibrant community of experts, practitioners, and thought leaders who bring a wealth of experience and insights from diverse cybersecurity fields. This rich tapestry of knowledge forms the foundation of our collaborative efforts to develop, refine, and disseminate practical strategies and solutions to common cybersecurity challenges. Through workshops, whitepapers, forums, and collaborative research initiatives, the CRF facilitates the exchange of ideas and best practices, encouraging innovation and continuous learning among its members. Our goal is to create a dynamic repository of cybersecurity knowledge that addresses current threats and anticipates future challenges, equipping organizations with the tools and strategies they need to navigate the digital age securely.

We invite cybersecurity professionals and organizations to join our mission, contribute to our body of knowledge, and engage in collaborative initiatives. Whether through sharing experiences, participating in discussions, or contributing to our ongoing research efforts, your involvement can make a significant difference. Together, we can create a powerful force for change, driving the advancement of cybersecurity practices and fostering a culture of security that transcends organizational boundaries. The CRF is more than just a foundation; it is a community of shared purpose committed to making the digital world a safer place for everyone.

CYBERSECURITY
RISK FOUNDATION

crfsecure.org