

SKILLWEED NIST CSF 2.0 RUM: RISK UNDERSTANDING MODEL

YOUR GUIDE TO QUESTIONNAIRES, DOCUMENTATION,
AND POINT OF CONTACTS FOR EVERY DOMAIN!



 SkillWeed

TABLE OF CONTENTS

Executive Summary.....	3
Background	4
Key Elements of the NIST CSF.....	5
Assessment Questionnaire, Evidence and point of contact	9
Summary Breakdown of the controls.....	92
Conclusion	121

EXECUTIVE SUMMARY



In today's digital landscape, cybersecurity is a critical concern for organizations of all sizes and industries. To effectively manage cybersecurity risks, it is essential to establish a comprehensive framework that addresses various aspects of risk management, policy development, supply chain security, incident response, and recovery. This executive summary provides an overview of key concepts and practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and identifies the importance of each element in building a robust cybersecurity posture.

BACKGROUND



The NIST CSF serves as a foundational guide for organizations seeking to strengthen their cybersecurity capabilities and mitigate cyber threats. It encompasses a wide range of cybersecurity practices organized into several categories, including governance, risk management, supply chain security, incident response, and recovery. By implementing the recommendations outlined in the CSF, organizations can enhance their resilience to cyberattacks and safeguard their critical assets and information.

KEY ELEMENTS OF THE NIST CSF

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles Responsibilities and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management Authentication and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

This summary provides a comprehensive overview of the key element of the NIST CSF 2.0 Controls

GOVERN (GV): THE ORGANIZATION'S CYBERSECURITY RISK MANAGEMENT STRATEGY EXPECTATIONS AND POLICY ARE ESTABLISHED, COMMUNICATED, AND MONITORED.

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood. This includes understanding the organizational mission, stakeholders' expectations regarding cybersecurity risk management, legal and regulatory requirements, and critical objectives reliant on external stakeholders.
- **Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance, and appetite statements and assumptions are established, communicated, and used to support operational risk decisions. This involves establishing risk management objectives, defining risk appetite and tolerance, integrating cybersecurity risk management activities into enterprise risk management processes, and ensuring strategic direction for risk response.
- **Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.
- **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced.
- **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.
- **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

IDENTIFY (ID): THE ORGANIZATION'S CURRENT CYBERSECURITY RISKS ARE UNDERSTOOD.

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
- **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization.
- **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF Functions.

PROTECT (PR): SAFEGUARDS TO MANAGE THE ORGANIZATION'S CYBERSECURITY RISKS ARE USED.

- **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.
- **Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.
- **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- **Platform Security (PR.PS):** The hardware, software, and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.
- **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

DETECT (DE): POSSIBLE CYBERSECURITY ATTACKS AND COMPROMISES ARE FOUND AND ANALYZED.

- **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.
- **Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

RESPOND (RS): ACTIONS REGARDING A DETECTED CYBERSECURITY INCIDENT ARE TAKEN.

- **Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed.
- **Incident Analysis (RS.AN):** Investigations are conducted to ensure effective response and support forensics and recovery activities.
- **Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.
- **Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects.

RECOVER (RC): ASSETS AND OPERATIONS AFFECTED BY A CYBERSECURITY INCIDENT ARE RESTORED.

- **Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.
- **Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties.

ASSESSMENT QUESTIONNAIRE, EVIDENCE AND POINT OF CONTACT

In the assessment process, you may encounter a questionnaire, requests for evidence, and contact points. Keep in mind, these elements can differ based on the organization you're dealing with.

Function	Category	Subcategory	Assessment Questions	Evidence Requested	Point of Contact
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	1. How is the organizational mission defined and communicated within the organization? 2. How are cybersecurity risk management activities aligned with the organizational mission? 3. Can you provide examples of how the organizational mission guides decision-making in cybersecurity risk management? 4. How are changes in the organizational mission reflected in cybersecurity risk management priorities? 5. How is the importance of cybersecurity risk management communicated in the context of achieving the organizational mission?	1. Organizational mission statement 2. Documents showing alignment of cybersecurity strategies with organizational goals 3. Reports or presentations demonstrating the integration of cybersecurity risk management with organizational mission objectives 4. Records of meetings or discussions where cybersecurity decisions were influenced by the organizational mission 5. Training materials or communications emphasizing the relationship between cybersecurity and organizational mission success	CEO
		GV.OC-02: Internal and	1. How does the organization	1. Stakeholder analysis	Compliance Officer

	external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	<p>identify internal stakeholders relevant to cybersecurity risk management?</p> <p>2. How are the needs and expectations of internal stakeholders regarding cybersecurity risk management determined and documented?</p> <p>3. How does the organization identify external stakeholders relevant to cybersecurity risk management?</p> <p>4. What mechanisms are in place to gather feedback from internal and external stakeholders regarding cybersecurity?</p> <p>5. How are stakeholder needs and expectations incorporated into cybersecurity risk management processes and decisions?</p>	<p>documents</p> <p>2. Surveys or feedback mechanisms used to gather stakeholder input on cybersecurity risk management</p> <p>3. Records of meetings or consultations with stakeholders regarding cybersecurity priorities and concerns</p> <p>4. Reports or presentations demonstrating consideration of stakeholder needs and expectations in cybersecurity risk management decisions</p> <p>5. Correspondence or communications discussing stakeholder feedback and its impact on cybersecurity strategies</p>	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	<p>1. How does the organization stay informed about legal, regulatory, and contractual requirements related to cybersecurity?</p> <p>2. How are legal, regulatory, and contractual requirements assessed for relevance and applicability to the organization?</p> <p>3. How does the organization</p>	<p>1. Legal and regulatory compliance documentation</p> <p>2. Records of legal assessments or consultations related to cybersecurity compliance</p> <p>3. Contracts or agreements containing cybersecurity-related clauses or requirements</p> <p>4. Reports or presentations</p>	CTO

		<p>ensure compliance with cybersecurity-related laws, regulations, and contracts?</p> <p>4. What mechanisms are in place to monitor changes or updates to cybersecurity-related legal and regulatory requirements?</p> <p>5. How are privacy and civil liberties considerations integrated into cybersecurity risk management processes?</p>	<p>demonstrating compliance with cybersecurity-related laws and regulations</p> <p>5. Training materials or communications addressing cybersecurity legal and regulatory requirements</p>	
	GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	<p>1. How does the organization identify critical objectives, capabilities, and services?</p> <p>2. What mechanisms are in place to determine stakeholder expectations regarding organizational objectives, capabilities, and services?</p> <p>3. How are critical objectives, capabilities, and services communicated within the organization?</p> <p>4. What measures are taken to ensure alignment between stakeholder expectations and organizational objectives?</p> <p>5. How are changes in</p>	<p>1. Organizational objectives and mission statements</p> <p>2. Stakeholder feedback or surveys regarding expectations and requirements</p> <p>3. Communications or presentations detailing critical organizational capabilities and services</p> <p>4. Records of meetings or discussions regarding alignment of organizational objectives with stakeholder expectations</p> <p>5. Reports or assessments demonstrating the impact of stakeholder expectations on cybersecurity risk management priorities</p>	HR Manager

			stakeholder expectations or organizational objectives reflected in cybersecurity risk management priorities?		
		GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	1. How does the organization identify outcomes, capabilities, and services critical to its operations? 2. What mechanisms are in place to assess the dependencies between organizational functions and external services or capabilities? 3. How are critical outcomes, capabilities, and services communicated within the organization? 4. What measures are taken to ensure continuity of critical outcomes, capabilities, and services in the face of cybersecurity risks? 5. How are changes in dependencies or critical services reflected in cybersecurity risk management strategies?	1. Business impact analysis documents 2. Dependency mapping or assessment reports 3. Communications or presentations detailing critical organizational outcomes, capabilities, and services 4. Records of discussions or meetings regarding continuity planning for critical services 5. Reports or assessments demonstrating the integration of critical services dependencies into cybersecurity risk management strategies	CEO
	Risk Management	GV.RM-01: Risk management	1. How are risk management	1. Risk management	CFO

	Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	objectives are established and agreed to by organizational stakeholders	objectives developed within the organization? 2. What mechanisms are in place to ensure alignment between risk management objectives and organizational goals? 3. How are risk management objectives communicated to relevant stakeholders? 4. How are conflicts or disagreements regarding risk management objectives resolved? 5. What measures are taken to ensure ongoing review and adjustment of risk management objectives?	objective documents or statements 2. Meeting minutes or records demonstrating stakeholder agreement on risk management objectives 3. Communications or presentations detailing risk management objectives and their alignment with organizational goals 4. Reports or assessments showing the implementation of risk management objectives in practice 5. Correspondence or communications discussing changes or updates to risk management objectives	
		GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	1. How does the organization define its risk appetite and risk tolerance? 2. What mechanisms are in place to communicate risk appetite and tolerance statements to relevant stakeholders? 3. How are risk appetite and tolerance statements integrated into risk management	1. Risk appetite and tolerance statements or policies 2. Communications or presentations explaining risk appetite and tolerance to stakeholders 3. Records of meetings or discussions regarding the integration of risk appetite/tolerance into risk management processes	Operations Lead

		<p>processes and decisions?</p> <p>4. How often are risk appetite and tolerance statements reviewed and updated?</p> <p>5. What measures are taken to ensure consistency and alignment between risk appetite/tolerance and organizational goals?</p>	<p>4. Reports or assessments demonstrating the application of risk appetite/tolerance in risk management decisions</p> <p>5. Documentation showing the periodic review and update of risk appetite/tolerance statements</p>	
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	<p>1. How does the organization integrate cybersecurity risk management into broader enterprise risk management processes?</p> <p>2. What mechanisms are in place to ensure that cybersecurity risks are considered alongside other types of risks?</p> <p>3. How are cybersecurity risk management activities coordinated with other risk management functions?</p> <p>4. What measures are taken to ensure consistency and alignment between cybersecurity risk management and enterprise risk management objectives?</p> <p>5. How are lessons learned from cybersecurity incidents</p>	<p>1. Documentation showing integration of cybersecurity risk management into enterprise risk management frameworks</p> <p>2. Reports or presentations demonstrating consideration of cybersecurity risks alongside other types of risks</p> <p>3. Records of meetings or discussions regarding coordination between cybersecurity risk management and enterprise risk management functions</p> <p>4. Reports or assessments demonstrating alignment between cybersecurity risk management outcomes and enterprise risk management objectives</p> <p>5. Documentation</p>	CEO

		incorporated into enterprise risk management practices?	showing the incorporation of cybersecurity incident lessons learned into enterprise risk management processes	
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	1. How does the organization determine appropriate risk response options? 2. What mechanisms are in place to communicate risk response options to relevant stakeholders? 3. How are risk response options tailored to specific types of cybersecurity risks or scenarios? 4. What measures are taken to ensure consistency and alignment between risk response options and organizational goals? 5. How are changes in risk response options communicated and implemented across the organization?	1. Strategic direction documents or policies outlining risk response options 2. Communications or presentations explaining risk response options to stakeholders 3. Records of meetings or discussions regarding the selection and communication of risk response options 4. Reports or assessments demonstrating the application of risk response options in practice 5. Documentation showing the implementation of changes or updates to risk response options	CTO
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	1. How does the organization facilitate communication about cybersecurity risks across different departments or units? 2. What mechanisms are in place to ensure that cybersecurity risks from	1. Communication protocols or procedures for cybersecurity risk management 2. Records of meetings or discussions involving cross-departmental communication on cybersecurity risks 3.	HR Manager

		<p>suppliers and third parties are communicated effectively?</p> <p>3. How are communication channels tailored to the needs and preferences of different stakeholders?</p> <p>4. What measures are taken to ensure that relevant cybersecurity risk information reaches decision-makers in a timely manner?</p> <p>5. How are feedback and input from stakeholders incorporated into cybersecurity risk communication processes?</p>	<p>Communications or presentations detailing cybersecurity risk communication strategies</p> <p>4. Reports or assessments demonstrating the effectiveness of communication channels for cybersecurity risks</p> <p>5. Documentation showing the incorporation of stakeholder feedback into cybersecurity risk communication processes</p>	
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	<p>1. What method or framework does the organization use for calculating, documenting, categorizing, and prioritizing cybersecurity risks?</p> <p>2. How is the chosen method or framework communicated to relevant stakeholders?</p> <p>3. How are cybersecurity risks categorized and prioritized based on the chosen method or framework?</p> <p>4. What measures are taken to ensure consistency and accuracy in risk calculations and</p>	<p>1. Cybersecurity risk management frameworks or methodologies</p> <p>2. Training materials or communications explaining the chosen method or framework to stakeholders</p> <p>3. Records of risk assessments or categorizations using the established method or framework</p> <p>4. Reports or assessments demonstrating the consistency and accuracy of risk calculations and documentation</p> <p>5. Documentation showing the periodic review</p>	Compliance Officer

			documentation? 5. How often is the method or framework reviewed and updated based on changes in the threat landscape or organizational priorities?	and update of the method or framework based on changes in the threat landscape or organizational priorities	
		GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	1. How does the organization identify and assess strategic opportunities related to cybersecurity risks? 2. What mechanisms are in place to ensure that strategic opportunities are considered alongside potential negative risks? 3. How are strategic opportunities incorporated into cybersecurity risk management discussions and decisions? 4. What measures are taken to capture and capitalize on strategic opportunities identified through cybersecurity risk management? 5. How are lessons learned from successful risk-taking incorporated into future risk management practices?	1. Documentation of identified strategic opportunities related to cybersecurity risks 2. Records of meetings or discussions involving consideration of strategic opportunities in risk management 3. Communications or presentations highlighting strategic opportunities identified through cybersecurity risk management 4. Reports or assessments demonstrating the impact of strategic opportunities on risk management outcomes 5. Documentation showing the incorporation of lessons learned from successful risk-taking into future risk management practices	CTO
	Roles, Responsibilities, and Authorities (GV.RR):	GV.RR-01: Organizational leadership is responsible and	1. How does organizational leadership demonstrate	1. Statements or policies outlining leadership responsibilities for	CTO

	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	responsibility and accountability for cybersecurity risk management? 2. What mechanisms are in place to foster a risk-aware culture within the organization? 3. How does leadership promote ethical behavior and decision-making in cybersecurity risk management? 4. What measures are taken to encourage continuous improvement in cybersecurity risk management practices? 5. How does leadership respond to cybersecurity incidents or failures, and what lessons are learned from these events?	cybersecurity risk management 2. Records of leadership communications or directives regarding risk-aware culture and ethical behavior 3. Reports or assessments demonstrating leadership support for continuous improvement in cybersecurity risk management practices 4. Documentation of lessons learned from cybersecurity incidents and failures, along with actions taken to address them 5. Training materials or communications promoting risk awareness and ethical decision-making among employees	
		GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	1. How are roles, responsibilities, and authorities related to cybersecurity risk management defined within the organization? 2. What mechanisms are in place to communicate and ensure understanding of these roles and responsibilities? 3. How does the organization enforce compliance with assigned roles,	1. Organizational charts or role descriptions outlining cybersecurity risk management responsibilities 2. Training materials or communications explaining roles, responsibilities, and authorities related to cybersecurity risk management 3. Records of discussions or meetings regarding enforcement of	Operations Lead

		responsibilities, and authorities? 4. How are changes or updates to roles and responsibilities communicated and implemented? 5. How are conflicts or overlaps in roles and responsibilities resolved?	roles and responsibilities 4. Reports or assessments demonstrating compliance with assigned roles and responsibilities 5. Documentation showing the resolution of conflicts or overlaps in roles and responsibilities	
	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	1. How does the organization determine resource requirements for cybersecurity risk management? 2. What mechanisms are in place to ensure that resources allocated to cybersecurity risk management are sufficient and appropriate? 3. How are resource allocation decisions made and communicated within the organization? 4. What measures are taken to monitor and evaluate the effectiveness of resource allocation for cybersecurity risk management? 5. How does the organization adjust resource allocation in response to changes in the threat landscape	1. Resource allocation plans or budgets for cybersecurity risk management 2. Records of resource assessments or evaluations to determine adequacy for risk management 3. Communications or presentations explaining resource allocation decisions for cybersecurity risk management 4. Reports or assessments demonstrating the effectiveness of resource allocation for risk management 5. Documentation showing adjustments to resource allocation based on changes in the threat landscape or organizational priorities	Finance Director

			or organizational priorities?		
		GV.RR-04: Cybersecurity is included in human resources practices	1. How does the organization incorporate cybersecurity considerations into human resources practices? 2. What mechanisms are in place to ensure that employees are aware of their cybersecurity responsibilities? 3. How are cybersecurity skills and competencies assessed during the hiring process? 4. What measures are taken to ensure ongoing training and development in cybersecurity for employees? 5. How does the organization address cybersecurity breaches or incidents involving employees?	1. Human resources policies or guidelines including cybersecurity responsibilities 2. Training materials or programs addressing cybersecurity awareness and responsibilities for employees 3. Records of cybersecurity training or competency assessments for employees 4. Reports or assessments demonstrating the integration of cybersecurity into human resources practices 5. Documentation showing disciplinary actions or responses to cybersecurity breaches involving employees	HR Manager
	Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	1. How is the cybersecurity risk management policy developed within the organization? 2. What mechanisms are in place to ensure that the policy reflects organizational context, strategy, and priorities? 3. How is the cybersecurity risk management policy communicated to	1. Cybersecurity risk management policy documents or statements 2. Records of policy development processes including stakeholder consultations and assessments 3. Communications or presentations explaining the cybersecurity risk management policy to	Security Analyst

			relevant stakeholders? 4. What measures are taken to enforce compliance with the cybersecurity risk management policy? 5. How is the policy reviewed and updated to reflect changes in requirements, threats, and technology?	stakeholders 4. Reports or assessments demonstrating compliance with the cybersecurity risk management policy 5. Documentation showing the periodic review and update of the policy based on changes in requirements, threats, and technology	
		GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	1. How often is the cybersecurity risk management policy reviewed and updated within the organization? 2. What mechanisms are in place to identify changes in requirements, threats, technology, and organizational mission that may impact the policy? 3. How is the updated policy communicated to relevant stakeholders? 4. What measures are taken to enforce compliance with the updated policy? 5. How are feedback and input from stakeholders incorporated into policy review and update processes?	1. Records of policy review and update cycles, including dates and revisions made 2. Documentation showing assessments of changes in requirements, threats, technology, and organizational mission 3. Communications or presentations announcing policy updates to stakeholders 4. Reports or assessments demonstrating compliance with the updated policy 5. Documentation showing the incorporation of stakeholder feedback into policy review and update processes	CTO
	Oversight (GV.OV): Results of organization-	GV.OV-01: Cybersecurity risk management	1. How often are cybersecurity risk management strategy	1. Records of cybersecurity risk management strategy review	Finance Director

	wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	strategy outcomes are reviewed to inform and adjust strategy and direction	outcomes reviewed within the organization? 2. What mechanisms are in place to assess the effectiveness of cybersecurity risk management strategies? 3. How are lessons learned from cybersecurity incidents or breaches incorporated into strategy review processes? 4. What measures are taken to adjust strategy and direction based on review outcomes? 5. How is the impact of strategy adjustments communicated to relevant stakeholders?	cycles, including dates and outcomes 2. Reports or assessments evaluating the effectiveness of cybersecurity risk management strategies 3. Documentation showing lessons learned from cybersecurity incidents and breaches 4. Communications or presentations announcing strategy adjustments to stakeholders 5. Documentation showing the incorporation of stakeholder feedback into strategy review processes	
		GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	1. How does the organization ensure that the cybersecurity risk management strategy remains aligned with organizational requirements and risks? 2. What mechanisms are in place to identify changes in organizational requirements and risks that may impact the strategy? 3. How often is the cybersecurity risk management strategy adjusted based on changing requirements and risks?	1. Records of cybersecurity risk management strategy review cycles, including dates and outcomes 2. Documentation showing assessments of changes in organizational requirements and risks 3. Reports or assessments demonstrating adjustments to the cybersecurity risk management strategy 4. Documentation showing the implementation of strategy adjustments 5.	Security Analyst

			<p>4. What measures are taken to ensure that adjustments to the strategy are implemented effectively?</p> <p>5. How are changes to the strategy communicated to relevant stakeholders?</p>	<p>Communications or presentations announcing changes to the strategy to stakeholders</p>	
		GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	<p>1. How does the organization evaluate and review its cybersecurity risk management performance?</p> <p>2. What mechanisms are in place to collect data and metrics related to cybersecurity risk management?</p> <p>3. How often are performance evaluations and reviews conducted?</p> <p>4. What measures are taken to identify areas for improvement in cybersecurity risk management?</p> <p>5. How are adjustments based on performance evaluations communicated and implemented?</p> <p>6. How does the organization ensure accountability for cybersecurity risk management performance?</p>	<p>1. Records of cybersecurity risk management performance evaluations and reviews, including dates and outcomes</p> <p>2. Metrics and data collected related to cybersecurity risk management performance</p> <p>3. Reports or assessments identifying areas for improvement in cybersecurity risk management</p> <p>4. Documentation showing adjustments made based on performance evaluations</p> <p>5. Communications or presentations announcing performance evaluation outcomes and adjustments to stakeholders</p> <p>6. Documentation outlining accountability measures for cybersecurity risk management performance</p>	HR Manager
	Cybersecurity Supply Chain	GV.SC-01: A cybersecurity	1. How does the organization	1. Documentation outlining the	IT Manager

	<p>Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders</p>	<p>supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders</p>	<p>establish its cybersecurity supply chain risk management program?</p> <p>2. What mechanisms are in place to develop and communicate objectives, policies, and processes for supply chain risk management?</p> <p>3. How are organizational stakeholders involved in the establishment and agreement of supply chain risk management initiatives?</p> <p>4. What measures are taken to ensure compliance with supply chain risk management policies and processes?</p> <p>5. How often are supply chain risk management strategies and objectives reviewed and updated?</p>	<p>cybersecurity supply chain risk management program, including objectives, policies, and processes</p> <p>2. Records of stakeholder consultations and agreements regarding supply chain risk management initiatives</p> <p>3. Communications or presentations explaining supply chain risk management objectives, policies, and processes to stakeholders</p> <p>4. Reports or assessments demonstrating compliance with supply chain risk management policies and processes</p> <p>5. Documentation showing the periodic review and update of supply chain risk management strategies and objectives</p>	
--	--	---	---	---	--

	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	<p>1. How does the organization establish roles and responsibilities for cybersecurity within its supply chain?</p> <p>2. What mechanisms are in place to communicate cybersecurity expectations to suppliers, customers, and partners?</p> <p>3. How are internal and external stakeholders coordinated to ensure alignment of cybersecurity roles and responsibilities?</p> <p>4. What measures are taken to ensure that cybersecurity roles and responsibilities are understood and fulfilled by suppliers, customers, and partners?</p> <p>5. How are changes or updates to cybersecurity roles and responsibilities communicated and implemented?</p>	<p>1. Documentation outlining cybersecurity roles and responsibilities for suppliers, customers, and partners</p> <p>2. Communications or presentations explaining cybersecurity expectations to internal and external stakeholders</p> <p>3. Records of coordination efforts to align cybersecurity roles and responsibilities</p> <p>4. Reports or assessments demonstrating understanding and fulfillment of cybersecurity roles and responsibilities by suppliers, customers, and partners</p> <p>5. Documentation showing the communication and implementation of changes or updates to cybersecurity roles and responsibilities</p>	CFO
--	--	--	---	-----

		GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	<ol style="list-style-type: none"> 1. How does the organization integrate supply chain risk management into broader cybersecurity and enterprise risk management processes? 2. What mechanisms are in place to ensure that supply chain risks are considered alongside other types of risks? 3. How are risk assessments conducted to identify and prioritize supply chain risks? 4. How are supply chain risk management practices evaluated and improved over time? 5. How does the organization ensure that lessons learned from supply chain incidents are incorporated into risk management processes? 	<ol style="list-style-type: none"> 1. Documentation showing integration of supply chain risk management into broader risk management frameworks 2. Reports or presentations demonstrating consideration of supply chain risks alongside other types of risks 3. Records of risk assessments specifically focused on supply chain risks 4. Assessments or audits evaluating supply chain risk management practices 5. Documentation showing incorporation of lessons learned from supply chain incidents into risk management processes 	Finance Director
--	--	---	--	---	------------------

		GV.SC-04: Suppliers are known and prioritized by criticality	<ol style="list-style-type: none"> 1. How does the organization identify and assess suppliers in terms of criticality to its operations? 2. What mechanisms are in place to ensure that critical suppliers are identified and prioritized for risk management? 3. How are critical suppliers monitored and evaluated for changes in risk profile? 4. What measures are taken to ensure continuity of operations in the event of disruptions involving critical suppliers? 5. How does the organization communicate with critical suppliers regarding cybersecurity expectations and requirements? 	<ol style="list-style-type: none"> 1. Records of supplier assessments and evaluations, including criticality rankings 2. Documentation outlining processes for identifying and prioritizing critical suppliers 3. Reports or assessments demonstrating monitoring and evaluation of critical suppliers for changes in risk profile 4. Documentation showing continuity planning efforts involving critical suppliers 5. Communications or agreements outlining cybersecurity expectations and requirements for critical suppliers 	COO
--	--	---	--	--	-----

		<p>GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties</p>	<ol style="list-style-type: none"> 1. How does the organization identify cybersecurity requirements for its supply chain relationships? 2. What mechanisms are in place to prioritize and communicate these requirements to suppliers and other third parties? 3. How are cybersecurity requirements integrated into contracts and agreements with suppliers and third parties? 4. What measures are taken to ensure compliance with cybersecurity requirements by suppliers and third parties? 5. How are changes or updates to cybersecurity requirements communicated and implemented across the supply chain? 	<ol style="list-style-type: none"> 1. Documentation outlining cybersecurity requirements for supply chain relationships 2. Communications or presentations explaining cybersecurity requirements to suppliers and third parties 3. Contracts or agreements containing cybersecurity clauses or requirements 4. Reports or assessments demonstrating compliance with cybersecurity requirements by suppliers and third parties 5. Documentation showing the communication and implementation of changes or updates to cybersecurity requirements 	IT Manager
--	--	---	--	--	------------

		GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	<ol style="list-style-type: none"> 1. How does the organization assess cybersecurity risks associated with potential suppliers or third-party relationships? 2. What mechanisms are in place to conduct due diligence and risk assessments before entering into formal agreements? 3. How are findings from risk assessments used to inform decision-making regarding supplier or third-party relationships? 4. What measures are taken to mitigate identified risks before formalizing relationships? 5. How does the organization ensure that risk assessments are documented and retained for future reference? 	<ol style="list-style-type: none"> 1. Records of risk assessments conducted for potential suppliers or third-party relationships 2. Documentation outlining due diligence processes for supplier or third-party relationships 3. Reports or assessments demonstrating the use of risk assessment findings in decision-making processes 4. Documentation showing the implementation of risk mitigation measures before formalizing relationships 5. Procedures or policies outlining documentation and retention requirements for risk assessments 	CFO
--	--	---	---	--	-----

		GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	<p>1. How does the organization assess and record risks posed by suppliers, their products and services, and other third parties?</p> <p>2. What mechanisms are in place to prioritize and assess these risks over the course of the relationship?</p> <p>3. How are responses to identified risks determined and implemented?</p> <p>4. What measures are taken to monitor and evaluate risks and responses throughout the relationship?</p> <p>5. How does the organization ensure that lessons learned from risk management activities are incorporated into future relationship management?</p>	<p>1. Risk assessment reports or records specific to suppliers, their products and services, and other third parties</p> <p>2. Documentation outlining processes for prioritizing and assessing risks over the course of supplier relationships</p> <p>3. Records of risk response decisions and actions taken</p> <p>4. Reports or assessments demonstrating monitoring and evaluation of risks and responses</p> <p>5. Documentation showing the incorporation of lessons learned from risk management activities into relationship management processes</p>	Operations Lead
--	--	--	---	--	-----------------

		GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	<ol style="list-style-type: none"> 1. How does the organization involve suppliers and other third parties in incident planning and response? 2. What mechanisms are in place to ensure coordination and communication with suppliers and third parties during incident response activities? 3. How are roles and responsibilities defined and communicated to suppliers and third parties in the event of an incident? 4. What measures are taken to ensure that incident response plans account for supplier and third-party dependencies? 5. How does the organization evaluate the effectiveness of supplier and third-party involvement in incident response activities? 	<ol style="list-style-type: none"> 1. Records of supplier involvement in incident planning and response activities 2. Documentation outlining communication and coordination processes with suppliers and third parties during incidents 3. Agreements or contracts detailing roles and responsibilities of suppliers and third parties in incident response 4. Reports or assessments evaluating the impact of supplier and third-party involvement on incident response effectiveness 5. Documentation showing adjustments made to incident response plans based on supplier and third-party dependencies 	CEO
--	--	--	---	--	-----

		<p>GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle</p>	<ol style="list-style-type: none"> 1. How does the organization integrate supply chain security practices into broader cybersecurity and enterprise risk management programs? 2. What mechanisms are in place to monitor the performance of supply chain security practices over the technology product and service life cycle? 3. How are supply chain security practices assessed and evaluated for effectiveness? 4. What measures are taken to ensure that supply chain security practices evolve with changes in technology and threats? 5. How does the organization ensure accountability for the performance of supply chain security practices? 	<ol style="list-style-type: none"> 1. Documentation outlining integration of supply chain security practices into broader risk management programs 2. Reports or assessments monitoring the performance of supply chain security practices over the product and service life cycle 3. Records of assessments and evaluations of supply chain security practices 4. Documentation showing adjustments made to supply chain security practices based on changes in technology and threats 5. Procedures or policies outlining accountability measures for supply chain security practice performance 	Compliance Officer
--	--	---	---	---	--------------------

		GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	<p>1. How does the organization plan for cybersecurity risks that may arise after the conclusion of supplier partnerships or service agreements?</p> <p>2. What mechanisms are in place to ensure that post-agreement activities are included in supply chain risk management plans?</p> <p>3. How are responsibilities defined and communicated for managing cybersecurity risks after the conclusion of agreements?</p> <p>4. What measures are taken to ensure that post-agreement activities are monitored and evaluated for compliance and effectiveness?</p> <p>5. How does the organization ensure that lessons learned from post-agreement activities are incorporated into future risk management practices?</p>	<p>1. Documentation outlining provisions for post-agreement cybersecurity risk management activities</p> <p>2. Records of discussions or meetings regarding the inclusion of post-agreement activities in risk management plans</p> <p>3. Agreements or contracts detailing responsibilities for managing cybersecurity risks after agreement conclusion</p> <p>4. Reports or assessments monitoring compliance and effectiveness of post-agreement risk management activities</p> <p>5. Documentation showing the incorporation of lessons learned from post-agreement activities into risk management practices</p>	COO
--	--	---	---	---	-----

IDENTIFY (ID): The organization's current cybersecurity risks are understood	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	ID.AM-01: Inventories of hardware managed by the organization are maintained	1. ID.AM-01: Inventories of hardware managed by the organization are maintained 2. How is the inventory of hardware assets managed and updated within the organization? 3. What information is included in the hardware inventory, and how is it organized? 4. How often are inventory audits conducted to ensure accuracy and completeness?	1. Asset inventory databases or systems 2. Reports or records of hardware acquisitions and disposals 3. Documentation outlining procedures for maintaining hardware inventories 4. Periodic audits or assessments of hardware inventory accuracy 5. Documentation showing reconciliation of inventory records with physical assets	Operations Lead
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	1. ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained 2. How are inventories of software, services, and systems tracked and maintained? 3. What methods are used to ensure all software and services are accounted for in the inventory? 4. How are changes to software and services documented and updated in the inventory?	1. Software asset management tools or databases 2. Records or logs of software installations and removals 3. Documentation outlining procedures for maintaining software inventories 4. Periodic audits or assessments of software inventory accuracy 5. Documentation showing reconciliation of inventory records with software licenses	HR Manager

		ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	1. ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained 2. How are representations of network communication and data flows documented and updated? 3. What tools or methodologies are used to visualize and manage network data flows? 4. How are changes to network communication and data flows reviewed and approved?	1. Network diagrams or topology maps 2. Documentation of network access control lists and firewall rules 3. Records of network configuration changes 4. Documentation outlining procedures for maintaining network representations 5. Reports or assessments of network security posture based on maintained representations	Operations Lead
		ID.AM-04: Inventories of services provided by suppliers are maintained	1. ID.AM-04: Inventories of services provided by suppliers are maintained 2. How are inventories of services provided by suppliers documented and managed? 3. What information is included in the service inventory, and how is it categorized? 4. How are changes or updates to supplier services tracked and recorded?	1. Supplier service catalogs or inventories 2. Contracts or agreements detailing services provided by suppliers 3. Documentation outlining procedures for maintaining supplier service inventories 4. Periodic audits or assessments of supplier service inventories 5. Documentation showing reconciliation of inventory records with contracted services	CEO

		ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	<ol style="list-style-type: none"> 1. ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission 2. What criteria are used to prioritize assets within the organization? 3. How are assets classified and categorized based on their criticality and impact? 4. How is resource allocation aligned with asset priorities and organizational mission objectives? 	<ol style="list-style-type: none"> 1. Asset prioritization frameworks or matrices 2. Documentation of asset classification criteria and definitions 3. Records of asset classification and prioritization decisions 4. Documentation outlining procedures for asset prioritization 5. Reports or assessments of asset prioritization effectiveness 	HR Manager
		ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	<ol style="list-style-type: none"> 1. ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained 2. How are inventories of data and metadata organized and maintained within the organization? 3. What methods are used to classify and categorize different data types? 4. How often are data inventories reviewed and updated to ensure accuracy? 	<ol style="list-style-type: none"> 1. Data inventory databases or systems 2. Data classification and metadata standards documentation 3. Records of data classification and metadata assignments 4. Documentation outlining procedures for maintaining data inventories 5. Periodic audits or assessments of data inventory accuracy 6. Documentation showing reconciliation of inventory records with actual data assets 	COO

		ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	1. ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles 2. What processes are in place to manage the life cycle of systems, hardware, software, services, and data? 3. How are changes and updates to these assets tracked and documented? 4. How is disposal or decommissioning handled at the end of their life cycle?	1. Policies or procedures for asset life cycle management 2. Records or logs of asset acquisition, deployment, maintenance, and disposal 3. Documentation outlining asset management processes and responsibilities 4. Reports or assessments of asset life cycle management compliance 5. Documentation showing implementation of asset management controls and measures	CEO
	Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	1. ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded 2. How are vulnerabilities in assets identified and validated within the organization? 3. What tools or techniques are used for vulnerability assessment? 4. How are vulnerabilities prioritized and addressed based on their severity and potential impact?	1. Vulnerability scanning or assessment reports 2. Records of vulnerability remediation activities 3. Documentation outlining vulnerability identification and validation processes 4. Periodic audits or assessments of vulnerability management practices 5. Reports or assessments of vulnerability risk exposure	Security Analyst

		<p>ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources</p>	<p>1. ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources</p> <p>2. What sources are used to gather cyber threat intelligence?</p> <p>3. How is threat intelligence shared and disseminated within the organization?</p> <p>4. How does the organization ensure the relevance and accuracy of the threat intelligence received?</p>	<p>1. Records of subscriptions to threat intelligence feeds</p> <p>2. Reports or briefings on emerging threats and indicators of compromise</p> <p>3. Documentation outlining procedures for threat intelligence collection and dissemination</p> <p>4. Periodic assessments of threat intelligence relevance and effectiveness</p> <p>5. Records of threat intelligence-driven actions or responses</p>	<p>Compliance Officer</p>
		<p>ID.RA-03: Internal and external threats to the organization are identified and recorded</p>	<p>1. ID.RA-03: Internal and external threats to the organization are identified and recorded</p> <p>2. How are internal and external threats identified and categorized?</p> <p>3. What methods are used to monitor and detect potential threats?</p> <p>4. How are threat data and intelligence sources integrated into threat identification processes?</p>	<p>1. Threat intelligence reports or assessments</p> <p>2. Incident reports documenting detected threats</p> <p>3. Security event logs or monitoring alerts</p> <p>4. Documentation outlining threat identification and recording processes</p> <p>5. Reports or assessments of threat identification coverage and accuracy</p>	<p>COO</p>

		ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	1. ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded 2. How are potential impacts and likelihoods of threats assessed within the organization? 3. What factors are considered when determining the impact and likelihood of threats? 4. How is this information documented and recorded for analysis?	1. Risk assessment reports or matrices 2. Documentation of threat likelihood and impact assessments 3. Records of risk scoring and prioritization 4. Documentation outlining processes for threat impact and likelihood assessment 5. Periodic audits or assessments of risk assessment effectiveness	Security Analyst
		ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	1. ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization 2. How is inherent risk calculated and assessed based on threats, vulnerabilities, likelihoods, and impacts? 3. How does the organization prioritize risk responses based on this understanding?	1. Risk assessment reports or dashboards 2. Documentation of risk scoring and prioritization criteria 3. Records of risk response decisions based on threat and vulnerability assessments 4. Documentation outlining processes for risk response prioritization 5. Reports or assessments of risk response effectiveness	CFO

		ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	<ol style="list-style-type: none"> 1. ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated 2. How are risk responses developed and prioritized within the organization? 3. What criteria are used to determine the most appropriate response to identified risks? 4. How are these responses tracked, monitored, and communicated to relevant stakeholders? 	<ol style="list-style-type: none"> 1. Risk treatment plans or registers 2. Documentation of risk response options and decisions 3. Records of risk response implementation and progress 4. Documentation outlining processes for risk response planning and tracking 5. Reports or assessments of risk response plan effectiveness 	COO
		ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	<ol style="list-style-type: none"> 1. ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked 2. How does the organization manage changes and exceptions to established risk management processes? 3. What procedures are in place to assess the risk impact of proposed changes or exceptions? 4. How are these changes documented and tracked over time? 	<ol style="list-style-type: none"> 1. Change management logs or databases 2. Records of change requests and approvals 3. Documentation outlining change control procedures and responsibilities 4. Reports or assessments of change management compliance 5. Documentation showing risk impact assessment for changes and exceptions 	CFO

		ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	<ol style="list-style-type: none"> 1. ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established 2. How does the organization receive vulnerability disclosures from internal and external sources? 3. What procedures are in place to analyze and assess the validity of vulnerability disclosures? 4. How are responses formulated and communicated to relevant parties? 	<ol style="list-style-type: none"> 1. Vulnerability disclosure policies or procedures 2. Records of reported vulnerabilities and their analysis 3. Documentation outlining vulnerability disclosure handling processes 4. Periodic audits or assessments of vulnerability disclosure procedures 5. Documentation showing response actions taken for disclosed vulnerabilities 	HR Manager
		ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	<ol style="list-style-type: none"> 1. ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use 2. How does the organization verify the authenticity and integrity of hardware and software before acquisition? 3. What measures are in place to ensure the integrity of acquired assets during the procurement process? 4. How are these assessments documented and retained? 	<ol style="list-style-type: none"> 1. Records of hardware and software authenticity verification 2. Documentation of integrity checks and validation processes 3. Documentation outlining procedures for authenticity and integrity assessment 4. Reports or assessments of authenticity and integrity verification compliance 	Security Analyst

		ID.RA-10: Critical suppliers are assessed prior to acquisition	1. ID.RA-10: Critical suppliers are assessed prior to acquisition 2. What criteria are used to identify critical suppliers within the organization? 3. How are these suppliers assessed for cybersecurity risks before acquisition? 4. How do these assessments influence the decision-making process when engaging with suppliers?	1. Supplier risk assessment reports or profiles 2. Contracts or agreements detailing supplier risk management requirements 3. Documentation outlining supplier assessment criteria and processes 4. Records of supplier assessment findings and decisions 5. Documentation showing supplier risk assessment integration into procurement processes	Compliance Officer
	Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	ID.IM-01: Improvements are identified from evaluations	1. ID.IM-01: Improvements are identified from evaluations 2. What evaluation methods or frameworks are used to assess cybersecurity practices and processes? 3. How are improvement opportunities identified from these evaluations? 4. How are evaluation findings translated into actionable improvements within the organization?	1. Evaluation reports or findings 2. Records of improvement recommendations or initiatives 3. Documentation outlining evaluation criteria and methodologies 4. Reports or assessments of evaluation effectiveness 5. Documentation showing implementation of identified improvements	CEO

		<p>ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties</p>	<p>1. ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties</p> <p>2. How does the organization conduct security tests and exercises?</p> <p>3. What role do suppliers and third parties play in these activities?</p> <p>4. How are improvement opportunities identified and addressed based on test results?</p>	<p>1. Security test reports or exercise debriefings</p> <p>2. Records of identified weaknesses or vulnerabilities</p> <p>3. Documentation outlining test and exercise objectives and scenarios</p> <p>4. Reports or assessments of test and exercise effectiveness</p> <p>5. Documentation showing implementation of test and exercise findings</p>	CTO
		<p>ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities</p>	<p>1. ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities</p> <p>2. How are operational processes and procedures reviewed for potential improvements?</p> <p>3. What mechanisms are in place to capture feedback from staff regarding process execution?</p> <p>4. How are identified improvements implemented and tracked over time?</p>	<p>1. Operational incident reports or post-mortems</p> <p>2. Records of process or procedure deviations or inefficiencies</p> <p>3. Documentation outlining operational process improvement mechanisms</p> <p>4. Reports or assessments of operational process effectiveness</p> <p>5. Documentation showing implementation of process improvements</p>	Operations Lead

		ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	1. ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved 2. How does the organization develop and establish incident response plans? 3. Can you describe the process for communicating incident response plans to relevant stakeholders? 4. How often are incident response plans reviewed and updated, and what triggers these updates? 5. How are lessons learned from incidents incorporated into plan improvements?	1. Incident response plans and playbooks 2. Documentation of plan review and update cycles 3. Records of plan dissemination and training activities 4. Documentation outlining incident response plan maintenance procedures 5. Reports or assessments of incident response plan effectiveness 6. Documentation showing improvements made to incident response plans	IT Manager
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	1. PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization 2. How are identities and credentials managed within the organization? 3. Can you describe the process for provisioning and deprovisioning user accounts? 4. What measures are in place to ensure the secure storage and	1. User account management policies or procedures 2. Identity and access management systems or tools 3. Records of user account creation, modification, and deletion 4. Documentation outlining identity and credential management processes 5. Reports or assessments of identity and credential management compliance	Compliance Officer

			transmission of credentials? 5. How is multi-factor authentication implemented for sensitive accounts?		
		PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	1. PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions 2. How does the organization verify the identity of users before granting access? 3. Can you describe the methods used for identity proofing? 4. What factors or attributes are considered during the proofing process? 5. How are different levels of proofing determined based on the context of user interactions?	1. Identity proofing policies or procedures 2. Records of identity verification and validation activities 3. Documentation outlining context-based credential binding processes 4. Reports or assessments of identity proofing and credential binding effectiveness	Security Analyst

		<p>PR.AA-03: Users, services, and hardware are authenticated</p>	<p>1. PR.AA-03: Users, services, and hardware are authenticated</p> <p>2. What authentication methods are employed within the organization?</p> <p>3. Can you describe the process for authenticating users, services, and hardware?</p> <p>4. How are authentication mechanisms adapted to different types of users and devices?</p> <p>5. What measures are in place to prevent unauthorized access through authentication bypass or exploitation of weaknesses?</p>	<p>1. Authentication mechanisms or protocols in use</p> <p>2. Logs or records of authentication attempts and outcomes</p> <p>3. Documentation outlining authentication methods and requirements</p> <p>4. Reports or assessments of authentication effectiveness</p>	CTO
--	--	--	--	--	-----

		PR.AA-04: Identity assertions are protected, conveyed, and verified	<p>1. PR.AA-04: Identity assertions are protected, conveyed, and verified</p> <p>2. How are identity assertions protected during transmission and storage?</p> <p>3. Can you describe the mechanisms used for conveying identity assertions?</p> <p>4. What measures are in place to verify the authenticity and integrity of identity assertions?</p> <p>5. How are identity-related risks mitigated to prevent impersonation or identity theft attacks?</p>	<p>1. Single sign-on (SSO) systems or federated identity solutions</p> <p>2. Records of identity assertion issuance and validation</p> <p>3. Documentation outlining identity assertion protection and verification processes</p> <p>4. Reports or assessments of identity assertion management compliance</p>	Compliance Officer
		PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	<p>1. PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties</p> <p>2. How are access permissions and entitlements defined and managed within the organization?</p> <p>3. Can you describe the policy framework used for managing access permissions?</p>	<p>1. Access control policies or matrices</p> <p>2. Access control lists or permissions configurations</p> <p>3. Records of access requests, grants, modifications, and revocations</p> <p>4. Documentation outlining access control policy enforcement mechanisms</p> <p>5. Reports or assessments of access control policy compliance</p>	Security Analyst

			<p>4. What mechanisms are in place for enforcing the principles of least privilege and separation of duties?</p> <p>5. How are access permissions and entitlements reviewed and updated to reflect changes in roles and responsibilities?</p>		
		<p>PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk</p>	<p>1. PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk</p> <p>2. How does the organization manage physical access to its assets?</p> <p>3. Can you describe the measures in place for monitoring physical access?</p> <p>4. What controls are implemented to enforce physical access policies?</p> <p>5. How is the level of access control adjusted based on the risk associated with different assets and locations?</p>	<p>1. Physical access control policies or procedures</p> <p>2. Logs or records of physical access events</p> <p>3. Documentation outlining physical access control measures and monitoring</p> <p>4. Reports or assessments of physical access control effectiveness</p>	Finance Director

	<p>Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks</p>	<p>PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind</p>	<p>1. PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind</p> <p>2. How does the organization provide cybersecurity awareness and training to personnel?</p> <p>3. Can you describe the topics covered in general cybersecurity awareness training?</p> <p>4. How often are training sessions conducted, and how is the effectiveness of training evaluated?</p> <p>5. What measures are in place to ensure ongoing awareness and knowledge retention among personnel?</p>	<p>1. Security awareness training materials or modules</p> <p>2. Training completion records or certifications</p> <p>3. Documentation outlining security awareness and training requirements</p> <p>4. Reports or assessments of security awareness program effectiveness</p>	<p>Finance Director</p>
--	--	---	---	--	-------------------------

		<p>PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind</p>	<p>1. PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind</p> <p>2. How are specialized roles identified within the organization for cybersecurity training?</p> <p>3. Can you describe the content and focus areas of specialized cybersecurity training?</p> <p>4. How is the relevance of training content tailored to specific job roles and responsibilities?</p> <p>5. What mechanisms are in place to assess the proficiency and effectiveness of specialized training for different roles?</p>	<p>1. Role-specific cybersecurity training programs or materials</p> <p>2. Training completion records or certifications for specialized roles</p> <p>3. Documentation outlining role-based cybersecurity training requirements</p> <p>4. Reports or assessments of role-based training effectiveness</p>	CFO
--	--	---	---	---	-----

	<p>Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information</p>	<p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p>	<p>1. PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>2. How does the organization protect the confidentiality, integrity, and availability of data stored at rest?</p> <p>3. Can you describe the encryption mechanisms used to protect data-at-rest?</p> <p>4. What measures are in place to prevent unauthorized access or tampering with stored data?</p> <p>5. How are data protection controls adjusted based on the sensitivity and criticality of stored data?</p>	<p>1. Data encryption policies or standards</p> <p>2. Data encryption tools or technologies in use</p> <p>3. Records of encrypted data storage configurations</p> <p>4. Documentation outlining data-at-rest protection measures</p> <p>5. Reports or assessments of data-at-rest protection effectiveness</p>	<p>Compliance Officer</p>
--	---	---	--	--	---------------------------

		PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	<p>1. PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>2. What measures are in place to protect the confidentiality, integrity, and availability of data during transit?</p> <p>3. Can you describe the encryption protocols and technologies used for securing data-in-transit?</p> <p>4. How are data protection measures adapted to different types of network communications?</p> <p>5. What monitoring mechanisms are in place to detect and respond to unauthorized access or tampering during data transit?</p>	<p>1. Network encryption protocols or technologies in use</p> <p>2. Records of encrypted communication sessions</p> <p>3. Documentation outlining data-in-transit protection mechanisms</p> <p>4. Reports or assessments of data-in-transit protection effectiveness</p>	Finance Director
--	--	---	--	--	------------------

		<p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p>	<p>1. PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>2. How does the organization protect the confidentiality, integrity, and availability of data while in use?</p> <p>3. Can you describe the security measures applied to data-in-use?</p> <p>4. What controls are in place to prevent unauthorized access or leakage of sensitive data during processing?</p> <p>5. How are encryption and access controls implemented to safeguard data during processing activities?</p>	<p>1. Data loss prevention (DLP) policies or solutions</p> <p>2. Records of protected data usage and access</p> <p>3. Documentation outlining data-in-use protection controls</p> <p>4. Reports or assessments of data-in-use protection effectiveness</p>	<p>Security Analyst</p>
--	--	--	--	--	-------------------------

		<p>PR.DS-11: Backups of data are created, protected, maintained, and tested</p>	<p>1. PR.DS-11: Backups of data are created, protected, maintained, and tested</p> <p>2. What processes are in place for creating backups of critical data?</p> <p>3. Can you describe the backup storage and protection mechanisms used?</p> <p>4. How often are backups performed, and what data retention policies are followed?</p> <p>5. What procedures are in place for testing the integrity and reliability of backups?</p> <p>6. How are backup and recovery plans adapted to changes in data volume and criticality?</p>	<p>1. Backup and recovery policies or procedures</p> <p>2. Backup schedules and retention policies</p> <p>3. Records of backup creation, storage, and testing activities</p> <p>4. Documentation outlining backup and recovery processes</p> <p>5. Reports or assessments of backup and recovery effectiveness</p>	CFO
--	--	---	---	--	-----

	<p>Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability</p>	<p>PR.PS-01: Configuration management practices are established and applied</p>	<p>1. PR.PS-01: Configuration management practices are established and applied</p> <p>2. How does the organization manage configuration changes to its systems and assets?</p> <p>3. Can you describe the configuration management practices followed?</p> <p>4. What tools or systems are used to automate configuration management processes?</p> <p>5. How are changes authorized, documented, and reviewed to ensure compliance with configuration standards?</p> <p>6. What measures are in place to detect unauthorized or unauthorized configuration changes?</p>	<p>1. Configuration management policies or standards</p> <p>2. Configuration management tools or systems in use</p> <p>3. Records of configuration baselines and changes</p> <p>4. Documentation outlining configuration management procedures</p> <p>5. Reports or assessments of configuration management compliance</p>	<p>Security Analyst</p>
--	--	---	--	--	-------------------------

		<p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p>	<p>1. PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p> <p>2. How does the organization manage the lifecycle of software applications?</p> <p>3. Can you describe the processes for software maintenance, replacement, and removal?</p> <p>4. What criteria are used to determine the risk associated with software applications?</p> <p>5. How are outdated or vulnerable software applications identified</p>	<p>1. Software inventory management systems or tools</p> <p>2. Records of software lifecycle management activities</p> <p>3. Documentation outlining software maintenance and retirement procedures</p> <p>4. Reports or assessments of software maintenance effectiveness</p>	CFO
--	--	---	--	--	-----

		<p>PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk</p>	<p>1. PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk</p> <p>2. How does the organization manage the lifecycle of hardware assets?</p> <p>3. Can you describe the processes for hardware maintenance, replacement, and decommissioning?</p> <p>4. What criteria are used to assess the risk associated with hardware assets?</p> <p>5. How are outdated or end-of-life hardware components identified and retired from production environments?</p> <p>6. What measures are in place to securely dispose of decommissioned hardware and prevent data exposure?</p>	<p>1. Hardware asset management systems or tools</p> <p>2. Records of hardware maintenance and replacement cycles</p> <p>3. Documentation outlining hardware maintenance and retirement procedures</p> <p>4. Reports or assessments of hardware maintenance effectiveness</p>	<p>Compliance Officer</p>
--	--	---	---	---	---------------------------

		<p>PR.PS-04: Log records are generated and made available for continuous monitoring</p>	<ol style="list-style-type: none"> 1. PR.PS-04: Log records are generated and made available for continuous monitoring 2. How does the organization generate and manage log records from its systems and applications? 3. Can you describe the types of information captured in log records? 4. What mechanisms are in place for centralizing and storing log data? 5. How are log records protected from tampering or unauthorized access? 6. What tools or systems are used for log analysis and continuous monitoring? 7. How is the integrity and reliability of log records ensured over time? 	<ol style="list-style-type: none"> 1. Logging and monitoring policies or procedures 2. Log management solutions or platforms in use 3. Records of log generation and storage 4. Documentation outlining log retention and access controls 5. Reports or assessments of log management compliance 	CTO
--	--	---	--	---	-----

		<p>PR.PS-05: Installation and execution of unauthorized software are prevented</p>	<p>1. PR.PS-05: Installation and execution of unauthorized software are prevented</p> <p>2. What measures are in place to prevent the installation and execution of unauthorized software?</p> <p>3. Can you describe the methods used for software whitelisting and blacklisting?</p> <p>4. How are software installation policies enforced on endpoints and servers?</p> <p>5. What controls are in place to prevent unauthorized software downloads from the internet?</p> <p>6. How is the organization alerted or notified about attempts to install unauthorized software?</p> <p>7. How are exceptions handled for legitimate software installations that may not be whitelisted?</p>	<p>1. Application whitelisting or blacklisting solutions</p> <p>2. Records of software installation attempts and outcomes</p> <p>3. Documentation outlining software control mechanisms</p> <p>4. Reports or assessments of unauthorized software prevention effectiveness</p>	CEO
--	--	--	--	--	-----

		<p>PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p>	<p>1. PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development lifecycle</p> <p>2. How does the organization integrate secure software development practices?</p> <p>3. Can you describe the secure development methodologies followed?</p> <p>4. What security controls are integrated into the software development lifecycle?</p> <p>5. How are security requirements defined and tracked throughout the development process?</p> <p>6. What measures are in place to ensure compliance with security standards and best practices?</p> <p>7. How is the performance of secure software development practices monitored and evaluated?</p>	<p>1. Secure software development frameworks or methodologies</p> <p>2. Code review and testing reports or metrics</p> <p>3. Documentation outlining secure development practices and controls</p> <p>4. Reports or assessments of secure software development effectiveness</p>	COO
--	--	--	---	--	-----

	Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	1. PR.IR-01: Networks and environments are protected from unauthorized logical access and usage 2. What measures are in place to protect networks and environments from unauthorized logical access? 3. Can you describe the network segmentation and access control mechanisms implemented? 4. How are network boundaries and trust zones defined and enforced? 5. What monitoring tools are used to detect and respond to unauthorized access attempts? 6. How are user permissions and access rights managed and reviewed to prevent unauthorized access? 7. What measures are in place to detect and mitigate insider threats?	1. Network access control policies or solutions 2. Records of access control violations or anomalies 3. Documentation outlining logical access control mechanisms 4. Reports or assessments of logical access control effectiveness	CTO
--	--	--	--	--	-----

		<p>PR.IR-02: The organization's technology assets are protected from environmental threats</p>	<ol style="list-style-type: none"> 1. PR.IR-02: The organization's technology assets are protected from environmental threats 2. How does the organization protect its technology assets from environmental threats? 3. Can you describe the physical security controls implemented for data centers and server rooms? 4. What measures are in place to protect hardware assets from power outages, floods, fires, or other environmental risks? 5. How are environmental monitoring systems utilized to detect and respond to threats? 6. What redundancy and failover mechanisms are implemented to ensure continuity of operations in case of environmental disruptions? 7. How are environmental risk assessments conducted to identify vulnerabilities and plan mitigation strategies? 	<ol style="list-style-type: none"> 1. Environmental monitoring systems or sensors 2. Records of environmental threat events or incidents 3. Documentation outlining environmental threat protection measures 4. Reports or assessments of environmental threat protection effectiveness 	HR Manager
--	--	--	--	---	------------

		<p>PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations</p>	<p>1. PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations</p> <p>2. What mechanisms are in place to ensure resilience in both normal and adverse situations?</p> <p>3. Can you describe the redundancy and failover strategies implemented for critical systems?</p> <p>4. How is data replication and synchronization managed to ensure availability and consistency?</p> <p>5. What business continuity and disaster recovery plans are in place to maintain operations during adverse events?</p> <p>6. How are resilience requirements defined, tested, and validated?</p> <p>7. What measures are taken to ensure that critical services can be quickly restored in case of disruptions?</p>	<p>1. Resilience and redundancy strategies or plans</p> <p>2. Records of resilience mechanism implementation and testing</p> <p>3. Documentation outlining resilience requirements and measures</p> <p>4. Reports or assessments of resilience mechanism effectiveness</p>	Security Analyst
--	--	---	--	--	------------------

		<p>PR.IR-04: Adequate resource capacity to ensure availability is maintained</p>	<p>1. PR.IR-04: Adequate resource capacity to ensure availability is maintained</p> <p>2. How does the organization ensure adequate resource capacity to maintain availability?</p> <p>3. Can you describe the capacity planning and resource allocation processes?</p> <p>4. What tools or metrics are used to monitor resource utilization and performance?</p> <p>5. How are scalability requirements assessed and addressed for growing demand?</p> <p>6. What measures are in place to prevent resource exhaustion and performance degradation under high loads?</p> <p>7. How are contingency plans activated to allocate additional resources during peak usage periods?</p>	<p>1. Capacity planning and monitoring tools or solutions</p> <p>2. Records of resource utilization and performance metrics</p> <p>3. Documentation outlining resource capacity requirements and thresholds</p> <p>4. Reports or assessments of resource capacity management effectiveness</p>	<p>HR Manager</p>
--	--	--	---	--	-------------------

<p>DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed</p>	<p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p>	<p>DE.CM-01: Networks and network services are monitored to find potentially adverse events</p>	<p>1. DE.CM-01: Networks and network services are monitored to find potentially adverse events 2. How does the organization monitor its networks and network services for potential adverse events? 3. Can you describe the network monitoring tools and technologies used? 4. What types of events or anomalies are considered indicators of potential threats or vulnerabilities? 5. How are network traffic patterns analyzed to detect abnormal behavior or security incidents? 6. What measures are in place to ensure timely detection and response to network security events? 7. How are network monitoring activities coordinated with other security controls and incident response processes?</p>	<p>1. Network monitoring tools or solutions 2. Logs or records of network traffic and service activity 3. Documentation outlining network monitoring criteria and thresholds 4. Reports or assessments of network monitoring effectiveness</p>	<p>CTO</p>
--	---	---	--	---	------------

		DE.CM-02: The physical environment is monitored to find potentially adverse events	<ol style="list-style-type: none"> 1. DE.CM-02: The physical environment is monitored to find potentially adverse events 2. What measures are in place to monitor the physical environment for potential adverse events? 3. Can you describe the physical security controls and surveillance systems deployed? 4. What types of events or activities are considered indicators of potential physical threats? 5. How are access logs and entry records used to track and investigate physical security incidents? 6. What measures are in place to detect and respond to unauthorized access attempts or breaches of physical security perimeters? 7. How are physical security monitoring activities integrated with overall security operations? 	<ol style="list-style-type: none"> 1. Physical security monitoring systems or sensors 2. Logs or records of physical access events and environmental conditions 3. Documentation outlining physical environment monitoring measures 4. Reports or assessments of physical environment monitoring effectiveness 	CFO
--	--	--	---	--	-----

		<p>DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events</p>	<ol style="list-style-type: none"> 1. DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events 2. How does the organization monitor personnel activity and technology usage for potential adverse events? 3. Can you describe the user activity monitoring tools and technologies implemented? 4. What types of user behaviors or actions are considered indicators of potential security incidents? 5. How are user access logs and audit trails analyzed to identify suspicious activities or policy violations? 6. What measures are in place to detect insider threats or unauthorized access by employees? 7. How is technology usage monitored to identify unauthorized software installations or non-compliant activities? 	<ol style="list-style-type: none"> 1. User activity monitoring solutions or tools 2. Logs or records of user actions and system events 3. Documentation outlining personnel and technology usage monitoring criteria 4. Reports or assessments of activity and usage monitoring effectiveness 	COO
--	--	---	--	---	-----

		<p>DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p>	<p>1. DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p> <p>2. What measures are in place to monitor the activities and services of external service providers?</p> <p>3. Can you describe the monitoring controls and contractual requirements for third-party vendors?</p> <p>4. What types of events or activities are considered indicators of potential risks or breaches by external providers?</p> <p>5. How are service level agreements (SLAs) and performance metrics used to track vendor compliance and service quality?</p> <p>6. What measures are in place to ensure timely detection and response to security incidents involving external service providers?</p> <p>7. How are</p>	<p>1. Service provider monitoring agreements or arrangements</p> <p>2. Logs or reports of service provider activities and service levels</p> <p>3. Documentation outlining service provider monitoring requirements</p> <p>4. Reports or assessments of service provider monitoring effectiveness</p>	COO
--	--	---	---	---	-----

		DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events			IT Manager
	Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	1. DE.AE-02: Potentially adverse events are analyzed to better understand associated activities 2. How does the organization analyze potentially adverse events to understand associated activities? 3. Can you describe the process for incident analysis and investigation? 4. What tools or techniques are used to correlate and analyze event data? 5. How are incident timelines reconstructed to identify root causes and attack vectors? 6. What measures are in place to preserve the integrity and confidentiality of incident data during analysis? 7. How are findings from incident analysis used to improve security controls and response procedures?	1. Incident analysis reports or summaries 2. Records of incident response actions and outcomes 3. Documentation outlining incident analysis processes and techniques 4. Reports or assessments of incident analysis effectiveness	COO

		<p>DE.AE-03: Information is correlated from multiple sources</p>	<ol style="list-style-type: none"> 1. DE.AE-03: Information is correlated from multiple sources 2. How does the organization correlate information from multiple sources to identify potential security threats? 3. Can you describe the sources of security information used for correlation? 4. What tools or platforms are employed for aggregating and correlating security data? 5. How is threat intelligence integrated into the correlation process? 6. What measures are in place to ensure data consistency and accuracy across correlated sources? 7. How are correlation rules and algorithms customized to address specific threats or attack patterns? 8. How is the correlation process automated to improve detection and response capabilities? 	<ol style="list-style-type: none"> 1. Correlation rules or algorithms used in security information and event management (SIEM) systems 2. Records or logs of correlated security events or incidents 3. Documentation outlining information correlation processes and tools 4. Reports or assessments of information correlation effectiveness 	CEO
--	--	--	--	--	-----

		DE.AE-04: The estimated impact and scope of adverse events are understood	<ol style="list-style-type: none"> 1. DE.AE-04: The estimated impact and scope of adverse events are understood 2. How does the organization assess the estimated impact and scope of adverse events? 3. Can you describe the criteria used for assessing the severity and consequences of security incidents? 4. What factors are considered when estimating the potential impact on business operations? 5. How are stakeholders informed about the potential impact and implications of security events? 6. What measures are in place to mitigate or contain the impact of security incidents? 7. How is the scope of incidents determined to assess the breadth and depth of potential exposure? 8. How are incident response plans adjusted based on the estimated impact and scope of security events? 	<ol style="list-style-type: none"> 1. Impact assessment reports or analyses 2. Records of incident impact estimation and scoping 3. Documentation outlining impact assessment methodologies 4. Reports or assessments of impact assessment accuracy 	COO
--	--	---	---	---	-----

		<p>DE.AE-06: Information on adverse events is provided to authorized staff and tools</p>	<ol style="list-style-type: none"> 1. DE.AE-06: Information on adverse events is provided to authorized staff and tools 2. How does the organization disseminate information on adverse events to authorized staff and tools? 3. Can you describe the communication channels and protocols used for incident notification? 4. What measures are in place to ensure timely and accurate reporting of security incidents? 5. How are incident notifications prioritized and escalated based on severity? 6. What tools or platforms are used for incident alerting and notification? 7. How are incident responders coordinated and mobilized to address reported security events? 8. What mechanisms are in place to verify incident notifications and prevent false positives? 	<ol style="list-style-type: none"> 1. Incident notification procedures or mechanisms 2. Records of incident notifications and recipients 3. Documentation outlining incident notification criteria and channels 4. Reports or assessments of incident notification effectiveness 	CTO
--	--	--	--	--	-----

		<p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p>	<ol style="list-style-type: none"> 1. DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis 2. How does the organization integrate cyber threat intelligence into incident analysis? 3. Can you describe the sources of threat intelligence used for analysis? 4. What types of contextual information are considered during incident investigation? 5. How is threat intelligence correlated with internal security events and indicators? 6. What measures are in place to validate and verify the accuracy of threat intelligence? 7. How are threat actor tactics, techniques, and procedures (TTPs) incorporated into incident response strategies? 8. How is threat intelligence shared with other organizations or industry groups to enhance collective defense? 	<ol style="list-style-type: none"> 1. Threat intelligence feeds or sources integrated with analysis tools 2. Records of threat intelligence utilization in incident analysis 3. Documentation outlining threat intelligence integration processes 4. Reports or assessments of threat intelligence integration effectiveness 	IT Manager
--	--	--	--	--	------------

		<p>DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria</p>	<p>1. DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria</p> <p>2. How does the organization determine when adverse events meet the criteria for declaring incidents?</p> <p>3. Can you describe the incident classification and categorization process?</p> <p>4. What criteria are used to distinguish between security incidents and normal operational events?</p> <p>5. How are incident thresholds and severity levels defined and documented?</p> <p>6. What measures are in place to ensure consistency and objectivity in incident classification?</p> <p>7. How are incident declaration criteria adjusted to account for evolving threats and changes in business requirements?</p> <p>8. How are stakeholders notified and informed when incidents are officially declared?</p>	<p>1. Incident declaration policies or procedures</p> <p>2. Records of incident declaration decisions</p> <p>3. Documentation outlining incident declaration criteria and thresholds</p> <p>4. Reports or assessments of incident declaration accuracy</p>	CTO
--	--	--	--	--	-----

RESPOND (RS): Actions regarding a detected cybersecurity incident are taken	Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	1. RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared 2. How does the organization coordinate incident response with relevant third parties? 3. Can you describe the process for involving external stakeholders in incident response? 4. What types of third-party organizations or entities are typically involved in incident management? 5. How are communication channels established and maintained with external responders? 6. What measures are in place to ensure alignment and collaboration between internal and external incident response teams? 7. How is sensitive information shared securely with external parties during incident response?	1. Incident response plan documentation 2. Records of coordination activities with third parties during incident response 3. Documentation outlining roles and responsibilities of third parties in incident response 4. Reports or assessments of incident response plan execution effectiveness	CTO
--	---	---	---	--	-----

		<p>RS.MA-02: Incident reports are triaged and validated</p>	<p>1. RS.MA-02: Incident reports are triaged and validated</p> <p>2. How does the organization triage and validate incident reports?</p> <p>3. Can you describe the criteria and procedures used for incident prioritization?</p> <p>4. What measures are in place to verify the authenticity and accuracy of reported incidents?</p> <p>5. How are incident reports categorized based on severity and impact?</p> <p>6. What tools or systems are used for incident tracking and management?</p> <p>7. How are incident response timelines established and monitored?</p> <p>8. How are incident reports documented and archived for future reference and analysis?</p>	<p>1. Incident triage and validation procedures</p> <p>2. Records of incident reports and their triage status</p> <p>3. Documentation outlining incident report validation criteria</p> <p>4. Reports or assessments of incident report triage and validation effectiveness</p>	<p>Operations Lead</p>
--	--	---	--	---	------------------------

		<p>RS.MA-03: Incidents are categorized and prioritized</p>	<p>1. RS.MA-03: Incidents are categorized and prioritized</p> <p>2. What criteria are used to categorize and prioritize security incidents?</p> <p>3. Can you describe the incident prioritization framework or matrix used?</p> <p>4. How are incident categories and priorities communicated to response teams?</p> <p>5. What measures are in place to ensure consistency and fairness in incident prioritization?</p> <p>6. How are response resources allocated based on incident categories and priorities?</p> <p>7. How are incident categories and priorities adjusted in real-time based on changing circumstances or threat intelligence?</p> <p>8. What metrics or KPIs are used to evaluate the effectiveness of incident prioritization?</p>	<p>1. Incident categorization and prioritization criteria</p> <p>2. Records of incident categorization and prioritization decisions</p> <p>3. Documentation outlining incident categorization and prioritization processes</p> <p>4. Reports or assessments of incident categorization and prioritization effectiveness</p>	IT Manager
--	--	--	--	---	------------

		<p>RS.MA-04: Incidents are escalated or elevated as needed</p>	<p>1. RS.MA-04: Incidents are escalated or elevated as needed</p> <p>2. How does the organization determine when incidents need to be escalated or elevated?</p> <p>3. Can you describe the escalation procedures and levels used?</p> <p>4. What criteria are used to trigger incident escalation?</p> <p>5. How are stakeholders informed about incident escalations and status changes?</p> <p>6. What measures are in place to ensure timely and effective escalations?</p> <p>7. How are incident escalations coordinated between different response teams and organizational levels?</p> <p>8. What communication channels are used for incident escalation and how are they</p>	<p>1. Incident escalation and elevation procedures</p> <p>2. Records of incident escalation or elevation actions</p> <p>3. Documentation outlining incident escalation and elevation criteria</p> <p>4. Reports or assessments of incident escalation and elevation effectiveness</p>	CTO
--	--	--	--	---	-----

		<p>RS.MA-05: The criteria for initiating incident recovery are applied</p>	<ol style="list-style-type: none"> 1. RS.MA-05: Incident response actions are coordinated with stakeholders 2. How does the organization coordinate incident response actions with stakeholders? 3. Can you describe the communication channels and protocols used for stakeholder engagement? 4. What roles and responsibilities do stakeholders have in the incident response process? 5. How are stakeholders kept informed about incident response progress and outcomes? 6. What measures are in place to ensure alignment and collaboration between internal teams and stakeholders? 7. How are stakeholder expectations managed during incident response? 8. What mechanisms are in place for obtaining stakeholder feedback and incorporating it into incident response improvements? 	<ol style="list-style-type: none"> 1. Incident recovery criteria or thresholds 2. Records of incident recovery initiation decisions 3. Documentation outlining incident recovery initiation processes 4. Reports or assessments of incident recovery initiation effectiveness 	Operations Lead
--	--	--	---	---	-----------------

	Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	1. How does the organization conduct analysis to determine what occurred during an incident? 2. Can you describe the methodology used to establish the root cause of security incidents? 3. What types of data sources and evidence are analyzed during incident analysis? 4. How are different analysis techniques employed to reconstruct incident timelines and sequences of events? 5. What measures are in place to ensure the accuracy and reliability of incident analysis findings? 6. How is incident analysis used to identify underlying vulnerabilities or weaknesses in security controls?	1. Incident analysis methodologies or frameworks 2. Analysis reports detailing incident timelines, actions, and root cause analysis 3. Documentation outlining incident analysis processes and techniques 4. Reports or assessments of incident analysis effectiveness	Operations Lead
--	--	--	--	---	-----------------

		<p>RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved</p>	<ol style="list-style-type: none"> 1. How does the organization record actions taken during incident investigations? 2. Can you describe the process for documenting investigation activities and findings? 3. What measures are in place to ensure the integrity and authenticity of investigation records? 4. How are timestamps and audit trails used to track the chronology of investigation actions? 5. What mechanisms are in place to prevent tampering or unauthorized modification of investigation records? 6. How are investigation records stored, secured, and retained for future reference or legal purposes? 	<ol style="list-style-type: none"> 1. Investigation documentation and records 2. Logs or records of investigation activities and findings 3. Documentation outlining investigation record management processes 4. Reports or assessments of investigation record integrity and provenance 	IT Manager
--	--	--	---	---	------------

		<p>RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved</p>	<ol style="list-style-type: none"> 1. What methods are used to collect incident data and metadata? 2. Can you describe the types of information included in incident data and metadata? 3. How is the integrity of collected data and metadata maintained throughout the investigation process? 4. What measures are in place to ensure the accuracy and completeness of collected data? 5. How are data provenance and chain of custody maintained for forensic purposes? 6. What tools or technologies are used for data collection and preservation during incident response? 	<ol style="list-style-type: none"> 1. Incident data collection and preservation procedures 2. Records of incident data and metadata collection activities 3. Documentation outlining incident data integrity and provenance preservation measures 4. Reports or assessments of incident data integrity and provenance 	HR Manager
--	--	---	--	---	------------

		<p>RS.AN-08: An incident's magnitude is estimated and validated</p>	<ol style="list-style-type: none"> 1. How does the organization estimate the magnitude or impact of security incidents? 2. Can you describe the factors considered when assessing the severity and scale of incidents? 3. What metrics or criteria are used to validate the estimated magnitude of incidents? 4. How are incident impact assessments used to prioritize response actions? 5. What measures are in place to ensure consistency and objectivity in magnitude estimation? 6. How are incident magnitude assessments communicated to stakeholders and decision-makers? 	<ol style="list-style-type: none"> 1. Incident magnitude estimation methodologies 2. Records of incident magnitude estimation and validation processes 3. Documentation outlining incident magnitude estimation criteria and techniques 4. Reports or assessments of incident magnitude estimation effectiveness 	CFO
--	--	---	--	--	-----

	Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	RS.CO-02: Internal and external stakeholders are notified of incidents	1. How does the organization notify internal stakeholders about security incidents? 2. Can you describe the communication channels and protocols used for internal incident notifications? 3. What information is typically included in incident notifications to internal stakeholders? 4. How are external stakeholders informed about security incidents affecting them? 5. What measures are in place to ensure timely and accurate incident notifications? 6. How are incident notification procedures adapted for different types of incidents or stakeholders?	1. Incident notification procedures or protocols 2. Records of incident notifications to stakeholders 3. Documentation outlining stakeholder notification criteria and channels 4. Reports or assessments of stakeholder notification effectiveness	CEO
--	--	---	--	--	-----

		<p>RS.CO-03: Information is shared with designated internal and external stakeholders</p>	<ol style="list-style-type: none"> 1. How does the organization share information about security incidents with designated stakeholders? 2. Can you describe the process for identifying and engaging relevant internal stakeholders? 3. What criteria are used to determine which external stakeholders should receive incident information? 4. How is incident information packaged and communicated to different stakeholder groups? 5. What measures are in place to protect sensitive or confidential information when sharing incident details? 6. How are feedback and insights from stakeholders incorporated into incident response efforts? 	<ol style="list-style-type: none"> 1. Information sharing policies or agreements 2. Records of information sharing activities with stakeholders 3. Documentation outlining information sharing processes and criteria 4. Reports or assessments of information sharing effectiveness 	CFO
--	--	---	---	--	-----

	Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	RS.MI-01: Incidents are contained	1. How does the organization ensure incidents are contained effectively? 2. Can you describe the process for isolating and limiting the impact of security incidents? 3. What measures are in place to prevent the spread or escalation of incidents? 4. How are containment measures tailored to different types of incidents or threat scenarios? 5. What role do automated response mechanisms play in incident containment? 6. How is the effectiveness of incident containment measures evaluated and validated? 7. What steps are taken to prevent recurrence of incidents after containment?	1. Incident containment procedures and protocols 2. Records of incident containment actions and outcomes 3. Documentation outlining incident containment measures 4. Reports or assessments of incident containment effectiveness	COO
--	---	--------------------------------------	---	--	-----

		<p>RS.MI-02: Incidents are eradicated</p>	<ol style="list-style-type: none"> 1. How does the organization ensure incidents are completely eradicated? 2. Can you describe the process for identifying and removing malicious artifacts or unauthorized access? 3. What measures are in place to ensure thoroughness and completeness in incident eradication? 4. How are systems and networks scanned or monitored to confirm eradication of threats? 5. What role do forensic analysis techniques play in incident eradication? 6. How is the success of eradication efforts measured and validated? 7. What steps are taken to prevent re-infection or persistence of threats post-eradication? 8. How are lessons learned from incident eradication applied to improve future response efforts? 	<ol style="list-style-type: none"> 1. Incident eradication procedures and techniques 2. Records of incident eradication activities and outcomes 3. Documentation outlining incident eradication measures 4. Reports or assessments of incident eradication effectiveness 	CEO
--	--	---	--	--	-----

RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored	Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	<ol style="list-style-type: none"> 1. How does the organization verify the integrity of restored assets after an incident? 2. Can you describe the process for validating the functionality and security of restored systems and services? 3. What measures are in place to ensure that restored assets are free from residual threats or vulnerabilities? 4. How is normal operating status defined and confirmed following restoration activities? 5. What mechanisms are used to monitor and assess the performance of restored systems and services? 6. How are user acceptance testing and validation conducted as part of the restoration process? 7. What safeguards are in place to prevent re-infection or recurrence of incidents post-restoration? 8. How are stakeholders and end-users involved in verifying the integrity of restored assets and services? 	<ol style="list-style-type: none"> 1. Incident response plan execution records 2. Records of recovery actions taken 3. Documentation outlining the execution process 4. Reports or assessments of incident recovery effectiveness 	COO
--	--	--	--	---	-----

		<p>RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed</p>	<ol style="list-style-type: none"> 1. How does the organization determine when incident recovery is complete? 2. Can you describe the criteria or indicators used to declare the end of incident recovery? 3. What documentation and reporting requirements are associated with the completion of incident recovery? 4. How are incident-related records and artifacts compiled and finalized post-recovery? 5. What measures are in place to ensure that all recovery activities and outcomes are documented? 6. How is the success or effectiveness of incident recovery efforts evaluated and assessed? 7. What steps are taken to transition from recovery to post-incident monitoring and evaluation? 8. How are incident recovery lessons learned captured and incorporated into future response planning? 	<ol style="list-style-type: none"> 1. Incident response plan execution records 2. Records of recovery actions taken 3. Documentation outlining the execution process 4. Reports or assessments of incident recovery effectiveness 	CTO
--	--	--	--	---	-----

		<p>RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration</p>	<ol style="list-style-type: none"> 1. How does the organization communicate progress in restoring operational capabilities after an incident? 2. Can you describe the channels and mechanisms used to share recovery updates with stakeholders? 3. What information is typically included in recovery status reports and communications? 4. How are stakeholders kept informed about potential impacts or delays in recovery activities? 5. What measures are in place to ensure transparency and accountability in recovery communications? 6. How are feedback and input from stakeholders integrated into recovery decision-making? 7. What role does timely and accurate communication play in maintaining stakeholder confidence during recovery efforts? 	<ol style="list-style-type: none"> 1. Recovery action plans or checklists 2. Documentation outlining recovery action selection criteria 3. Records of recovery action prioritization and execution 4. Reports or assessments of recovery action effectiveness 	Security Analyst
--	--	--	---	---	------------------

		8. How are recovery communications tailored to different stakeholder groups and their respective interests or concerns?		
--	--	---	--	--

SUMMARY BREAKDOWN OF THE CONTROLS



- **GV.OC-01 to GV.OC-05** focus on understanding the organizational context, including its mission, stakeholder needs, legal requirements, and dependencies. Expected outcomes are enhanced alignment with organizational objectives, improved stakeholder satisfaction, and increased resilience. Sample evidence includes documentation integrating the mission into cybersecurity processes and dependency mappings.
- **GV.RM-01 to GV.RM-07** emphasize the importance of establishing clear risk management objectives, communicating risk appetite, and integrating risk management into the broader organizational framework. The goals are to ensure a systematic approach to assessing and prioritizing cybersecurity risks, with records of stakeholder agreements and risk assessment methodologies as evidence.

- **GV.RR-01 to GV.RR-04** outline leadership roles and resource allocation for cybersecurity, aiming for strong support, clarity on roles, and integration of cybersecurity in human resources practices. Evidence includes leadership statements prioritizing cybersecurity and training programs.
- **GV.PO-01 and GV.PO-02** deal with establishing and maintaining policies for managing cybersecurity risks, ensuring their current relevance and alignment with organizational needs. Policy documents and records of updates serve as evidence.
- **GV.OV-01 to GV.OV-03** focus on reviewing and adjusting the cybersecurity risk management strategy to match organizational requirements, with reports showing strategy adjustments as evidence.
- **GV.SC-01 to GV.SC-10** highlight the need for a cybersecurity supply chain risk management program, identifying critical suppliers, and integrating supply chain security into broader risk management processes. Sample evidence includes supply chain risk management documentation and supplier agreements specifying cybersecurity requirements.
- **ID.AM-01 to ID.AM-08** cover asset management, including maintaining inventories of hardware, software, and data, with hardware inventory databases and network diagrams as examples of evidence.
- **ID.RA-01 to ID.RA-10** involve identifying and recording vulnerabilities and threats, assessing supplier risks, and ensuring the integrity of assets before use. Vulnerability scans and supplier risk assessments are types of evidence.
- **PR.AA-01 to PR.PS-06** and **PR.IR-01 to PR.IR-04** describe access management, protection of data, and resilience of networks and environments. Evidence includes identity management systems, encryption mechanisms, and business continuity plans.
- **DE.CM-01 to DE.CM-09** are concerned with monitoring for potentially adverse events and ensuring early detection and response. Security event logs and NIDS alerts are examples of evidence.
- **RS.MA-01 to RS.CO-03, RS.MI-01 and RS.MI-02, and RC.RP-01 to RC.CO-04** detail incident response and recovery processes, from execution and containment to recovery and communication. Incident response team logs, recovery action plans, and public updates on recovery efforts are forms of sample evidence.

The summary below encapsulates the control IDs, descriptions, expected outcomes, and examples of sample evidence across various aspects of cybersecurity risk management within an organization:

CONTROL ID: GV.OC-01

Control Description: Understanding the organizational mission and its influence on cybersecurity risk management

Expected Output: Enhanced alignment of cybersecurity practices with organizational objectives

Sample Evidence: Documentation demonstrating how the organizational mission is integrated into cybersecurity risk management processes

CONTROL ID: GV.OC-02

Control Description: Understanding internal and external stakeholder needs and expectations regarding cybersecurity risk management

Expected Output: Improved stakeholder satisfaction and trust in cybersecurity measures

Sample Evidence: Surveys, interviews, or feedback demonstrating stakeholder awareness and satisfaction with cybersecurity efforts

CONTROL ID: GV.OC-03

Control Description: Management of legal, regulatory, and contractual cybersecurity requirements

Expected Output: Compliance with relevant laws, regulations, and contracts

Sample Evidence: Documentation of compliance efforts, such as audit reports or legal assessments

CONTROL ID: GV.OC-04

Control Description: Understanding critical objectives, capabilities, and services expected by stakeholders

Expected Output: Clear communication of organizational priorities and goals

Sample Evidence: Stakeholder interviews or surveys confirming awareness and understanding of critical objectives

CONTROL ID: GV.OC-05

Control Description: Understanding organizational dependencies on outcomes, capabilities, and services

Expected Output: Improved resilience and continuity of operations

Sample Evidence: Dependency mapping or risk assessments demonstrating awareness of critical organizational dependencies

CONTROL ID: GV.RM-01

Control Description: Establishing risk management objectives agreed upon by stakeholders

Expected Output: Defined goals and priorities for managing cybersecurity risks

Sample Evidence: Records of stakeholder meetings or agreements outlining risk management objectives

CONTROL ID: GV.RM-02

Control Description: Establishment and communication of risk appetite and tolerance statements

Expected Output: Clear guidance on acceptable levels of risk exposure

Sample Evidence: Published risk appetite statements or risk tolerance thresholds

CONTROL ID: GV.RM-03

Control Description: Inclusion of cybersecurity risk management in enterprise risk management processes

Expected Output: Comprehensive risk management across organizational functions

Sample Evidence: Documentation showing integration of cybersecurity risk management into broader risk management frameworks

CONTROL ID: GV.RM-04

Control Description: Establishment and communication of strategic direction for risk response options

Expected Output: Clarity on response strategies aligned with organizational goals

Sample Evidence: Strategic documents outlining risk response options and decision-making processes

CONTROL ID: GV.RM-05

Control Description: Establishment of communication channels for cybersecurity risks across the organization

Expected Output: Effective risk communication and collaboration

Sample Evidence: Communication plans or protocols for sharing cybersecurity risk information

CONTROL ID: GV.RM-06

Control Description: Standardized method for calculating, documenting, and prioritizing cybersecurity risks

Expected Output: Consistent and systematic approach to risk assessment

Sample Evidence: Risk assessment frameworks or methodologies used consistently across the organization

CONTROL ID: GV.RM-07

Control Description: Identification and consideration of strategic opportunities in cybersecurity risk discussions

Expected Output: Proactive identification of positive risks

Sample Evidence: Records of risk discussions or analyses including consideration of strategic opportunities

CONTROL ID: GV.RR-01

Control Description: Leadership responsibility and accountability for cybersecurity risk management

Expected Output: Strong leadership support and commitment to cybersecurity

Sample Evidence: Leadership statements or directives emphasizing cybersecurity as a priority

CONTROL ID: GV.RR-02

Control Description: Establishment of roles, responsibilities, and authorities related to cybersecurity risk management

Expected Output: Clarity on individual accountabilities and decision-making authority

Sample Evidence: Organizational charts, job descriptions, or policy documents defining cybersecurity roles and responsibilities

CONTROL ID: GV.RR-03

Control Description: Allocation of adequate resources for implementing cybersecurity risk strategy

Expected Output: Sufficient budget, personnel, and technology for cybersecurity efforts

Sample Evidence: Budget allocations or resource plans demonstrating investment in cybersecurity

CONTROL ID: GV.RR-04

Control Description: Inclusion of cybersecurity in human resources practices

Expected Output: Integration of cybersecurity considerations into hiring, training, and personnel management

Sample Evidence: Training programs or job requirements incorporating cybersecurity competencies

CONTROL ID: GV.PO-01

Control Description: Establishment and enforcement of policy for managing cybersecurity risks

Expected Output: Clear guidelines for risk management practices

Sample Evidence: Policy documents outlining cybersecurity risk management requirements and procedures

CONTROL ID: GV.PO-02

Control Description: Regular review and updating of cybersecurity risk management policies

Expected Output: Currency and relevance of policy guidance

Sample Evidence: Records of policy reviews or updates reflecting changes in requirements or technology

CONTROL ID: GV.OV-01

Control Description: Review of cybersecurity risk management strategy outcomes

Expected Output: Informed adjustments to strategy and direction

Sample Evidence: Reports or analyses showing review outcomes and strategy adjustments

CONTROL ID: GV.OV-02

Control Description: Review and adjustment of cybersecurity risk management strategy to ensure coverage of organizational requirements and risks

Expected Output: Alignment of strategy with evolving organizational needs

Sample Evidence: Strategy documents or assessments indicating adjustments made for coverage improvements

CONTROL ID: GV.OV-03

Control Description: Evaluation and review of organizational cybersecurity risk management performance

Expected Output: Continuous improvement of risk management practices

Sample Evidence: Performance metrics or reports demonstrating ongoing evaluation and improvement efforts

CONTROL ID: GV.SC-01

Control Description: Establishment of cybersecurity supply chain risk management program and processes

Expected Output: Proactive management of supply chain risks

Sample Evidence: Documentation of supply chain risk management frameworks or programs

CONTROL ID: GV.SC-02

Control Description: Establishment and communication of cybersecurity roles and responsibilities for suppliers, customers, and partners

Expected Output: Clear expectations and accountability for supply chain cybersecurity

Sample Evidence: Contracts, agreements, or communication plans outlining cybersecurity roles and responsibilities

CONTROL ID: GV.SC-03

Control Description: Integration of cybersecurity supply chain risk management into broader risk management processes

Expected Output: Comprehensive risk management across supply chain relationships

Sample Evidence: Risk assessment or management frameworks incorporating supply chain cybersecurity

CONTROL ID: GV.SC-04

Control Description: Identification and prioritization of suppliers by criticality

Expected Output: Focus on critical suppliers for risk mitigation efforts

Sample Evidence: Supplier prioritization matrices or risk assessments

CONTROL ID: GV.SC-05

Control Description: Establishment of requirements to address cybersecurity risks in supply chains

Expected Output: Integration of cybersecurity requirements into supplier agreements

Sample Evidence: Contract clauses or agreements specifying cybersecurity requirements

CONTROL ID: GV.SC-06

Control Description: Performance of planning and due diligence to reduce risks before entering into formal supplier relationships

Expected Output: Risk-informed decision-making in supplier selection

Sample Evidence: Due diligence checklists or risk assessments for supplier relationships

CONTROL ID: GV.SC-07

Control Description: Understanding, recording, and assessment of risks posed by suppliers and third parties

Expected Output: Awareness and mitigation of supplier-related risks

Sample Evidence: Risk registers or assessments documenting supplier risks

CONTROL ID: GV.SC-08

Control Description: Inclusion of relevant suppliers and third parties in incident planning, response, and recovery activities

Expected Output: Collaborative incident management across supply chain partners

Sample Evidence: Incident response plans or communication protocols involving suppliers

CONTROL ID: GV.SC-09

Control Description: Integration of supply chain security practices into cybersecurity and enterprise risk management programs

Expected Output: Comprehensive risk management throughout the product lifecycle

Sample Evidence: Documentation showing integration of supply chain security practices

CONTROL ID: GV.SC-10

Control Description: Inclusion of provisions for post-agreement activities in cybersecurity supply chain risk management plans

Expected Output: Continued risk management beyond the conclusion of agreements

Sample Evidence: Risk management plans or agreements including post-agreement provisions

CONTROL ID: ID.AM-01

Control Description: Maintenance of inventories of hardware managed by the organization

Expected Output: Awareness and control of hardware assets

Sample Evidence: Hardware inventory databases or tracking systems

CONTROL ID: ID.AM-02

Control Description: Maintenance of inventories of software, services, and systems managed by the organization

Expected Output: Awareness and control of software assets

Sample Evidence: Software inventory databases or tracking systems

CONTROL ID: ID.AM-03

Control Description: Maintenance of representations of the organization's authorized network communication and data flows

Expected Output: Understanding of network configurations and data flows

Sample Evidence: Network diagrams or documentation showing authorized data flows

CONTROL ID: ID.AM-04

Control Description: Maintenance of inventories of services provided by suppliers

Expected Output: Awareness and control of supplier-provided services

Sample Evidence: Supplier service inventories or contractual documentation

CONTROL ID: ID.AM-05

Control Description: Prioritization of assets based on classification, criticality, resources, and impact on the mission

Expected Output: Focus on protecting high-value assets

Sample Evidence: Asset prioritization matrices or risk assessments

CONTROL ID: ID.AM-07

Control Description: Maintenance of inventories of data and corresponding metadata for designated data types

Expected Output: Awareness and control of organizational data assets

Sample Evidence: Data inventories or metadata repositories

CONTROL ID: ID.AM-08

Control Description: Management of systems, hardware, software, services, and data throughout their life cycles

Expected Output: Comprehensive lifecycle management of organizational assets

Sample Evidence: Lifecycle management plans or procedures

CONTROL ID: ID.RA-01

Control Description: Identification, validation, and recording of vulnerabilities in assets

Expected Output: Awareness and mitigation of asset vulnerabilities

Sample Evidence: Vulnerability scanning reports or risk registers

CONTROL ID: ID.RA-02

Control Description: Receipt of cyber threat intelligence from information sharing forums and sources

Expected Output: Awareness of current threats and vulnerabilities

Sample Evidence: Cyber threat intelligence reports or subscriptions

CONTROL ID: ID.RA-03

Control Description: Identification and recording of internal and external threats to the organization

Expected Output: Awareness of potential threats

Sample Evidence: Threat intelligence reports or incident logs

CONTROL ID: ID.RA-04

Control Description: Identification and recording of potential impacts and likelihoods of threats exploiting vulnerabilities

Expected Output: Understanding of potential risk scenarios

Sample Evidence: Risk assessment reports or matrices

CONTROL ID: ID.RA-05

Control Description: Use of threats, vulnerabilities, likelihoods, and impacts to understand inherent risk and inform risk response prioritization

Expected Output: Risk-informed decision-making for prioritizing risk responses

Sample Evidence: Risk assessment findings or risk prioritization criteria

CONTROL ID: ID.RA-06

Control Description: Choice, prioritization, planning, tracking, and communication of risk responses

Expected Output: Execution of risk mitigation actions

Sample Evidence: Risk treatment plans or action trackers

CONTROL ID: ID.RA-07

Control Description: Management, assessment, recording, and tracking of changes and exceptions

Expected Output: Control over changes affecting risk posture

Sample Evidence: Change management logs or exception reports

CONTROL ID: ID.RA-08

Control Description: Establishment of processes for receiving, analyzing, and responding to vulnerability disclosures

Expected Output: Responsiveness to reported vulnerabilities

Sample Evidence: Vulnerability disclosure procedures or incident response protocols

CONTROL ID: ID.RA-09

Control Description: Assessment of the authenticity and integrity of hardware and software prior to acquisition and use

Expected Output: Assurance of trustworthiness in acquired assets

Sample Evidence: Integrity verification logs or vendor assessments

CONTROL ID: ID.RA-10

Control Description: Assessment of critical suppliers prior to acquisition

Expected Output: Assurance of trustworthiness in supplier relationships

Sample Evidence: Supplier risk assessments or due diligence reports

CONTROL ID: ID.IM-01

Control Description: Identification of improvements from evaluations

Expected Output: Continual improvement of cybersecurity posture

Sample Evidence: Evaluation reports or improvement plans

CONTROL ID: ID.IM-02

Control Description: Identification of improvements from security tests and exercises

Expected Output: Strengthening of security controls and practices

Sample Evidence: Test reports or exercise findings

CONTROL ID: ID.IM-03

Control Description: Identification of improvements from execution of operational processes, procedures, and activities

Expected Output: Optimization of operational cybersecurity practices

Sample Evidence: Incident reports or operational reviews

CONTROL ID: ID.IM-04

Control Description: Establishment, communication, maintenance, and improvement of incident response plans and other cybersecurity plans affecting operations

Expected Output: Preparedness for and responsiveness to cybersecurity incidents

Sample Evidence: Incident response plans or post-incident reviews

CONTROL ID: PR.AA-01

Control Description: Management of identities and credentials for authorized users, services, and hardware

Expected Output: Control over access to organizational resources

Sample Evidence: Identity management systems or access control policies

CONTROL ID: PR.AA-02

Control Description: Proofing and binding of identities to credentials based on context

Expected Output: Assurance of identity trustworthiness

Sample Evidence: Identity verification logs or multi-factor authentication records

CONTROL ID: PR.AA-03

Control Description: Authentication of users, services, and hardware

Expected Output: Verification of identity before granting access

Sample Evidence: Authentication logs or access control systems

CONTROL ID: PR.AA-04

Control Description: Protection, conveyance, and verification of identity assertions

Expected Output: Assurance of identity integrity

Sample Evidence: Digital signatures or certificate revocation lists

CONTROL ID: PR.AA-05

Control Description: Definition, management, enforcement, and review of access permissions, entitlements, and authorizations

Expected Output: Control over access rights and privileges

Sample Evidence: Access control policies or permissions matrices

CONTROL ID: PR.AA-06

Control Description: Management, monitoring, and enforcement of physical access to assets commensurate with risk

Expected Output: Control over physical access to organizational facilities

Sample Evidence: Access control logs or security camera footage

CONTROL ID: PR.AT-01

Control Description: Provision of awareness and training to personnel to perform general tasks with cybersecurity risks in mind

Expected Output: Awareness of cybersecurity risks and best practices

Sample Evidence: Training materials or completion records

CONTROL ID: PR.AT-02

Control Description: Provision of awareness and training to individuals in specialized roles with cybersecurity risks in mind

Expected Output: Skill development for specialized cybersecurity tasks

Sample Evidence: Role-specific training modules or certification records

CONTROL ID: PR.DS-01

Control Description: Protection of the confidentiality, integrity, and availability of data-at-rest

Expected Output: Secure storage of sensitive information

Sample Evidence: Encryption mechanisms or data classification policies

CONTROL ID: PR.DS-02

Control Description: Protection of the confidentiality, integrity, and availability of data-in-transit

Expected Output: Secure transmission of sensitive information

Sample Evidence: Transport layer security protocols or network encryption logs

CONTROL ID: PR.DS-10

Control Description: Protection of the confidentiality, integrity, and availability of data-in-use

Expected Output: Secure processing of sensitive information

Sample Evidence: Application sandboxing or data masking techniques

CONTROL ID: PR.DS-11

Control Description: Creation, protection, maintenance, and testing of backups of data

Expected Output: Availability of critical data in case of data loss or corruption

Sample Evidence: Backup schedules or recovery point objectives

CONTROL ID: PR.PS-01

Control Description: Establishment and application of configuration management practices

Expected Output: Consistent and secure configuration of organizational assets

Sample Evidence: Configuration management policies or change control records

CONTROL ID: PR.PS-02

Control Description: Maintenance, replacement, and removal of software commensurate with risk

Expected Output: Timely patching and updating of software vulnerabilities

Sample Evidence: Patch management logs or software inventory reports

CONTROL ID: PR.PS-03

Control Description: Maintenance, replacement, and removal of hardware commensurate with risk

Expected Output: Timely retirement of outdated or vulnerable hardware

Sample Evidence: Hardware lifecycle management plans or decommissioning records

CONTROL ID: PR.PS-04

Control Description: Generation and availability of log records for continuous monitoring

Expected Output: Visibility into system activities for threat detection and analysis

Sample Evidence: Log management systems or security information and event management (SIEM) tools

CONTROL ID: PR.PS-05

Control Description: Prevention of installation and execution of unauthorized software

Expected Output: Control over software installations to mitigate security risks

Sample Evidence: Application whitelisting policies or unauthorized software detection reports

CONTROL ID: PR.PS-06

Control Description: Integration of secure software development practices throughout the software development life cycle

Expected Output: Reduction of software vulnerabilities and defects

Sample Evidence: Secure coding guidelines or code review reports

CONTROL ID: PR.IR-01

Control Description: Protection of networks and environments from unauthorized logical access and usage

Expected Output: Control over network access to prevent unauthorized activities

Sample Evidence: Network access control policies or intrusion detection system alerts

CONTROL ID: PR.IR-02

Control Description: Protection of the organization's technology assets from environmental threats

Expected Output: Mitigation of physical risks to hardware and infrastructure

Sample Evidence: Environmental controls or facility security assessments

CONTROL ID: PR.IR-03

Control Description: Implementation of mechanisms to achieve resilience requirements in normal and adverse situations

Expected Output: Continuity of operations and service availability under stress conditions

Sample Evidence: Business continuity plans or disaster recovery procedures

CONTROL ID: PR.IR-04

Control Description: Maintenance of adequate resource capacity to ensure availability

Expected Output: Scalability and reliability of IT infrastructure to meet demand

Sample Evidence: Capacity planning reports or resource utilization metrics

CONTROL ID: DE.CM-01

Control Description: Monitoring of networks and network services to find potentially adverse events

Expected Output: Early detection and response to network security incidents

Sample Evidence: Network intrusion detection system (NIDS) alerts or security event logs

CONTROL ID: DE.CM-02

Control Description: Monitoring of the physical environment to find potentially adverse events

Expected Output: Early detection and response to physical security incidents

Sample Evidence: Surveillance camera footage or environmental sensor alerts

CONTROL ID: DE.CM-03

Control Description: Monitoring of personnel activity and technology usage to find potentially adverse events

Expected Output: Early detection and response to insider threats or policy violations

Sample Evidence: User activity logs or security policy violation reports

CONTROL ID: DE.CM-06

Control Description: Monitoring of external service provider activities and services to find potentially adverse events

Expected Output: Early detection and response to security incidents involving third-party services

Sample Evidence: Service provider incident reports or service level agreement (SLA) compliance audits

CONTROL ID: DE.CM-09

Control Description: Monitoring of computing hardware and software, runtime environments, and their data to find potentially adverse events

Expected Output: Early detection and response to system compromises or data breaches

Sample Evidence: Endpoint security logs or system integrity checks

CONTROL ID: DE.AE-02

Control Description: Analysis of potentially adverse events to better understand associated activities

Expected Output: Improved incident response and mitigation strategies

Sample Evidence: Post-incident analysis reports or root cause analysis documentation

CONTROL ID: DE.AE-03

Control Description: Correlation of information from multiple sources to understand adverse events

Expected Output: Comprehensive understanding of the incident's context and impact

Sample Evidence: Incident correlation reports or threat intelligence feeds

CONTROL ID: DE.AE-04

Control Description: Understanding the estimated impact and scope of adverse events

Expected Output: Effective prioritization of incident response efforts

Sample Evidence: Impact assessment reports or severity scoring criteria

CONTROL ID: DE.AE-06

Control Description: Provision of information on adverse events to authorized staff and tools

Expected Output: Timely response and mitigation of security incidents

Sample Evidence: Incident notification emails or security incident management platform alerts

CONTROL ID: DE.AE-07

Control Description: Integration of cyber threat intelligence and other contextual information into the analysis

Expected Output: Enhanced understanding of the threat landscape and potential risks

Sample Evidence: Threat intelligence reports or threat actor profiles

CONTROL ID: DE.AE-08

Control Description: Declaration of incidents when adverse events meet the defined incident criteria

Expected Output: Formal recognition and response to security incidents

Sample Evidence: Incident declaration forms or incident response playbooks

CONTROL ID: RS.MA-01

Control Description: Execution of the incident response plan in coordination with relevant third parties

Expected Output: Collaborative incident response efforts to minimize impact

Sample Evidence: Incident response team communication logs or joint incident response exercises

CONTROL ID: RS.MA-02

Control Description: Triage and validation of incident reports

Expected Output: Efficient prioritization of incident response efforts

Sample Evidence: Incident triage reports or incident validation checklists

CONTROL ID: RS.MA-03

Control Description: Categorization and prioritization of incidents

Expected Output: Systematic handling of security incidents based on severity

Sample Evidence: Incident categorization matrices or incident prioritization guidelines

CONTROL ID: RS.MA-04

Control Description: Escalation or elevation of incidents as needed

Expected Output: Prompt escalation of critical incidents for higher-level attention

Sample Evidence: Incident escalation procedures or incident escalation logs

CONTROL ID: RS.MA-05

Control Description: Application of criteria for initiating incident recovery

Expected Output: Systematic assessment of when to initiate recovery efforts

Sample Evidence: Incident recovery decision matrices or incident recovery trigger conditions

CONTROL ID: RS.AN-03

Control Description: Performance of analysis to establish what has taken place during an incident and its root cause

Expected Output: Identification of incident details and underlying causes

Sample Evidence: Incident analysis reports or root cause analysis diagrams

CONTROL ID: RS.AN-06

Control Description: Recording of actions performed during an investigation

Expected Output: Documentation of incident response activities for future reference

Sample Evidence: Investigation activity logs or incident response documentation

CONTROL ID: RS.AN-07

Control Description: Collection of incident data and metadata, preserving their integrity and provenance

Expected Output: Preservation of evidence for forensic analysis and legal purposes

Sample Evidence: Incident data collection logs or chain of custody records

CONTROL ID: RS.AN-08

Control Description: Estimation and validation of an incident's magnitude

Expected Output: Understanding the severity and impact of security incidents

Sample Evidence: Incident magnitude assessment reports or severity validation procedures

CONTROL ID: RS.CO-02

Control Description: Notification of internal and external stakeholders of incidents

Expected Output: Timely communication to relevant parties about security incidents

Sample Evidence: Incident notification emails or stakeholder communication logs

CONTROL ID: RS.CO-03

Control Description: Sharing of information with designated internal and external stakeholders

Expected Output: Collaborative incident response efforts and transparency

Sample Evidence: Incident sharing agreements or stakeholder communication protocols

CONTROL ID: RS.MI-01

Control Description: Containment of incidents to prevent further spread or damage

Expected Output: Mitigation of security incidents to minimize impact

Sample Evidence: Incident containment reports or incident response action plans

CONTROL ID: RS.MI-02

Control Description: Eradication of incidents to remove their presence from systems

Expected Output: Complete removal of security threats from affected systems

Sample Evidence: Incident eradication confirmation reports or malware removal logs

CONTROL ID: RC.RP-01

Control Description: Execution of the recovery portion of the incident response plan

Expected Output: Restoration of affected systems and services to normal operation

Sample Evidence: Incident recovery task lists or recovery progress dashboards

CONTROL ID: RC.RP-02

Control Description: Selection, scoping, prioritization, and performance of recovery actions

Expected Output: Systematic approach to restoring affected systems and services

Sample Evidence: Recovery action plans or recovery task prioritization matrices

CONTROL ID: RC.RP-03

Control Description: Verification of the integrity of backups and restoration assets before use

Expected Output: Assurance that backup data is reliable for restoration purposes

Sample Evidence: Backup integrity verification logs or restoration asset validation procedures

CONTROL ID: RC.RP-04

Control Description: Consideration of critical mission functions and cybersecurity risk management to establish post-incident operational norms

Expected Output: Adaptation of operational practices to prevent future incidents

Sample Evidence: Post-incident operational norm reports or lessons learned documents

CONTROL ID: RC.RP-05

Control Description: Verification of the integrity of restored assets, restoration of systems and services, and confirmation of normal operating status

Expected Output: Assurance that restored systems operate as expected

Sample Evidence: System restoration verification reports or post-recovery testing results

CONTROL ID: RC.RP-06

Control Description: Declaration of the end of incident recovery based on criteria, and completion of incident-related documentation

Expected Output: Formal closure of the incident response process

Sample Evidence: Incident recovery completion forms or post-incident review meeting minutes

CONTROL ID: RC.CO-03

Control Description: Communication of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders

Expected Output: Transparency and accountability in the recovery process

Sample Evidence: Recovery progress updates or stakeholder communication logs

CONTROL ID: RC.CO-04

Control Description: Sharing of public updates on incident recovery using approved methods and messaging

Expected Output: Maintaining public trust and confidence during incident response

Sample Evidence: Public incident updates on organizational websites or press releases

CONCLUSION



In conclusion, these guides serve to fortify your organization's cyber landscape, enhancing resilience as you integrate NIST CSF 2.0 controls as your guiding principles.

