NIST CSF 2.0

AUDIT CHECKLIST

GOVERN | IDENTIFY | PROTECT
DETECT | RESPOND | RECOVER

MINISTRY OF MOS SECURITY

NIST CSF 2.0 AUDIT CHECKLIST

NIST CSF 2.0 Audit Checklist		
Function	**GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored**	
Category	**Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	1. Does the organization have a documented and communicated mission statement that clearly articulates the organization's purpose and strategic objectives? 2. Have the organization's key stakeholders (e.g., executive leadership, board of directors, department heads) been engaged to ensure a shared understanding of the organizational mission? 3. Has the organization assessed how its mission and strategic objectives could be impacted by cybersecurity risks and threats? 4. Are the organization's cybersecurity risk management policies, processes, and controls aligned with and designed to support the achievement of the organizational mission? 5. Do the organization's cybersecurity risk management activities (e.g., risk assessments, control implementation, monitoring) take the organizational mission into account when prioritizing and addressing risks? 6. Are cybersecurity roles and responsibilities defined in a way that ensures the organization's mission is considered when making risk-based decisions? 7. Does the organization periodically review and update its cybersecurity risk management approach to ensure it remains aligned with the evolving organizational mission and strategic priorities?	
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	1. Has the organization identified and documented its internal and external stakeholders? 2. Has the organization assessed the needs, expectations, and concerns of these stakeholders regarding cybersecurity? 3. Are the identified stakeholders and their cybersecurity-related needs and expectations communicated and understood throughout the organization? 4. Does the organization have a process in place to regularly engage with stakeholders to understand any changes or new cybersecurity-related needs and expectations?	

NIST CSF 2.0 AUDIT CHECKLIST

	5. Are the organization's cybersecurity risk management policies, processes, and controls designed to address the identified stakeholder needs and expectations? 6. Are there examples of how the organization has incorporated stakeholder feedback and input into its cybersecurity risk management approach? 7. Does the organization have a mechanism to monitor and address any gaps or misalignments between stakeholder needs and the organization's cybersecurity risk management activities?	
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	1. Has the organization identified and documented all relevant legal, regulatory, and contractual requirements that impact its cybersecurity practices? 2. Does the organization have a process in place to regularly review and update its understanding of applicable cybersecurity-related laws, regulations, and contractual obligations? 3. Are the identified legal, regulatory, and contractual requirements communicated to relevant stakeholders throughout the organization? 4. Has the organization assessed the potential impacts and risks associated with non-compliance with these requirements? 5. Are the organization's cybersecurity risk management policies, processes, and controls designed to ensure compliance with the identified legal, regulatory, and contractual requirements? 6. Does the organization have a mechanism to monitor and report on its compliance with cybersecurity-related legal, regulatory, and contractual requirements? 7. Are there any examples of how the organization has adapted its cybersecurity risk management approach to address changes in legal, regulatory, or contractual requirements?	
GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	1. Has the organization identified and documented its critical objectives, capabilities, and services that are essential for stakeholders (both internal and external)? 2. Are the dependencies and relationships between these critical objectives, capabilities, and services understood, including any interdependencies or external dependencies? 3. Has the organization assessed the potential impacts on stakeholders if these critical objectives, capabilities, and services are disrupted or compromised? 4. Are the organization's cybersecurity risk management policies, processes, and controls designed to protect the critical objectives, capabilities, and services proportionate to their importance and the associated	

	risks? 5. Does the organization monitor and review the status and security of the critical objectives, capabilities, and services on a regular basis? 6. Are there processes in place to manage changes or disruptions to the critical objectives, capabilities, and services, including incident response and recovery plans? 7. Are the organization's key stakeholders (e.g., leadership, service owners) aware of and engaged in the management of the critical objectives, capabilities, and services?	
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	1. Has the organization identified and documented the critical outcomes, capabilities, and services that it depends on to achieve its mission and objectives? 2. Are the dependencies and relationships between these critical outcomes, capabilities, and services understood, including any interdependencies or external dependencies? 3. Has the organization assessed the cybersecurity risks associated with these critical outcomes, capabilities, and services, including the potential impacts if they are disrupted or compromised? 4. Are the cybersecurity controls and risk management activities designed to protect the organization's critical outcomes, capabilities, and services proportionate to their importance and the associated risks? 5. Does the organization monitor and review the status and security of the critical outcomes, capabilities, and services on a regular basis? 6. Are there processes in place to manage changes or disruptions to the critical outcomes, capabilities, and services, including incident response and recovery plans? 7. Are the organization's key stakeholders (e.g., leadership, service owners) aware of and engaged in the management of the critical outcomes, capabilities, and services?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	1. Has the organization defined clear and measurable cybersecurity risk management objectives? 2. Were these objectives developed in collaboration with key stakeholders, such as executive leadership, business units, and IT/security teams? 3. Do the risk management objectives align with the organization's overall strategic goals and priorities? 4. Are the risk management objectives communicated and understood across the organization? 5. Are the risk management objectives regularly reviewed and updated to ensure they remain relevant and appropriate? 6. Are the risk management objectives used to guide the development and implementation of the organization's cybersecurity risk management program? 7. Does the organization have a process in place to measure and report on the achievement of the risk management objectives?	
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	1. Has the organization defined and documented its cybersecurity risk appetite and risk tolerance statements? 2. Were these statements developed in collaboration with key stakeholders, such as executive leadership, business units, and IT/security teams? 3. Do the risk appetite and tolerance statements align with the organization's strategic goals, risk management objectives, and overall risk management approach? 4. Are the risk appetite and tolerance statements communicated and understood across the organization? 5. Does the organization have a process in place to review and update the risk appetite and tolerance statements on a regular basis to ensure they remain relevant and appropriate? 6. Are the risk appetite and tolerance statements used to guide decision-making and risk management activities throughout the organization? 7. Are there examples of how the organization has applied the risk appetite and tolerance statements to address specific risks or risk scenarios?	

NIST CSF 2.0 AUDIT CHECKLIST

GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	1. Has the organization integrated its cybersecurity risk management activities and outcomes into the enterprise-wide risk management processes? 2. Are cybersecurity risk management strategies and treatment plans coordinated with the organization's overall enterprise risk management approach? 3. Are cybersecurity risk management responsibilities and accountabilities defined within the enterprise risk management framework? 4. Does the organization's enterprise risk management reporting and governance processes include information on cybersecurity risks and risk management activities? 5. Does the organization periodically review the integration of cybersecurity risk management within the enterprise risk management processes to identify any gaps or areas for improvement?	
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	1. Has the organization defined and documented its strategic direction for cybersecurity risk response options? 2. Does the strategic direction consider factors such as the organization's risk appetite, tolerance, and available resources? 3. Are the risk response options (e.g., accept, mitigate, transfer, avoid) clearly described and communicated to relevant stakeholders? 4. Are the criteria and decision-making processes for selecting appropriate risk response options defined and understood across the organization? 5. Are the risk response options aligned with the organization's overall cybersecurity risk management strategy and enterprise risk management approach? 6. Does the organization have a mechanism to monitor the effectiveness of the implemented risk response options and make adjustments as needed?	
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	1. Has the organization established and documented clear lines of communication for sharing information about cybersecurity risks across the organization? 2. Do these communication channels include both vertical (e.g., from leadership to operational teams) and horizontal (e.g., across business units, functions) information flows? 3. Are the roles and responsibilities for communicating and escalating cybersecurity risks, including risks from suppliers and other third parties, defined and understood? 4. Are the communication processes and protocols for sharing information about cybersecurity risks documented and communicated to relevant stakeholders? 5. Does the organization have a mechanism to ensure	

	timely and effective communication of cybersecurity risks to the appropriate decision-makers and stakeholders?	
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	1. Has the organization developed and documented a standardized methodology for assessing, categorizing, and prioritizing cybersecurity risks? 2. Does the methodology consider factors such as asset criticality, threat likelihood, impact, and risk tolerance? 3. Is the risk assessment methodology consistently applied across the organization? 4. Are the results of risk assessments documented in a centralized and standardized manner? 5. Are the risk categories and prioritization criteria communicated to relevant stakeholders throughout the organization? 6. Does the organization regularly review and update the risk assessment methodology to ensure it remains appropriate and effective?	
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	1. Has the organization identified and documented any strategic opportunities (i.e., positive risks) that could be realized through its cybersecurity risk management activities? 2. Are these strategic opportunities characterized in terms of their potential benefits, likelihood of success, and the resources required to pursue them? 3. Are the identified strategic opportunities incorporated into the organization's overall cybersecurity risk management discussions and decision-making processes? 4. Does the organization have a process in place to regularly review and update its assessment of potential strategic opportunities related to cybersecurity? 5. Are the organization's key stakeholders (e.g., executive leadership, business units) aware of and engaged in the consideration of strategic opportunities related to cybersecurity risk management?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	1. Has the organization's leadership (e.g., executive team, board of directors) clearly defined and communicated their responsibility and accountability for managing cybersecurity risks? 2. Do the organization's leadership team members actively demonstrate their commitment to cybersecurity risk management through their actions and decisions? 3. Has the organization established a culture that encourages risk awareness, ethical behaviour, and continuous improvement in cybersecurity practices? 4. Does the organization's leadership actively promote and support cybersecurity training, awareness,	
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	1. Has the organization documented and communicated roles, responsibilities, and authorities related to cybersecurity risk management? 2. Do personnel understand their assigned cybersecurity risk management roles and responsibilities, and does the organization monitor and enforce these? 3. Are the cybersecurity risk management roles and responsibilities aligned with the organization's overall risk management strategy and objectives? 4. Does the organization periodically review and update the cybersecurity risk management roles and responsibilities as needed? 5. Are the cybersecurity risk management roles and responsibilities clearly defined for both internal and external stakeholders?	
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	1. Has the organization defined cybersecurity risk strategy that outlines resource requirements? 2. Are the resources (financial, personnel, technological, etc.) allocated for cybersecurity risk management commensurate with the organization's cybersecurity risk strategy and policies? 3. How does the organization determine the appropriate level of resources required to effectively manage cybersecurity risks? 4. Does the organization's budgeting and resource allocation process consider the evolving cybersecurity threat landscape and the need for continuous improvement? 5. How does the organization ensure that the allocated cybersecurity resources are utilized efficiently and effectively? 6. Does the organization regularly review and adjust the	

	cybersecurity resource allocation to address changes in risks, threats, and organizational priorities? 7. How does the organization's leadership demonstrate their commitment to providing adequate resources for effective cybersecurity risk management?	
GV.RR-04: Cybersecurity is included in human resources practices	1. Are cybersecurity-related roles, responsibilities, and competencies incorporated into the organization's job descriptions and hiring criteria? 2. Does the organization's hiring process include cybersecurity-focused assessments, such as background checks, skills evaluations, or security clearance verifications? 3. Are cybersecurity awareness, training, and education requirements defined and incorporated into the organization's onboarding and ongoing professional development programs? 4. How does the organization ensure that personnel maintain the necessary cybersecurity knowledge and skills to perform their job functions effectively? 5. Does the organization have a process to identify and address cybersecurity competency gaps among personnel, and provide appropriate training or development opportunities? 6. How does the organization's human resources department collaborate with the cybersecurity team to ensure alignment between HR practices and cybersecurity requirements? 7. Does the organization have a process to manage the removal of access and privileges for departing or terminated employees in a timely manner? 8. How does the organization's human resources practices support the development of a cybersecurity-aware culture and the retention of skilled cybersecurity personnel?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	1. Has the organization established a comprehensive cybersecurity risk management policy that is aligned with its overall organizational context, cybersecurity strategy, and priorities? 2. Does the cybersecurity risk management policy clearly define the organization's approach to identifying, assessing, and mitigating cybersecurity risks? 3. How does the organization ensure that the cybersecurity risk management policy is communicated to all relevant internal and external stakeholders? 4. Are there processes in place to monitor and enforce compliance with the organization's cybersecurity risk management policy? 5. Does the policy address roles, responsibilities, and authorities related to cybersecurity risk management across the organization? 6. Does the organization provide training and awareness programs to ensure that personnel understand and adhere to the cybersecurity risk management policy? 7. How does the organization's leadership demonstrate their commitment to the cybersecurity risk management policy and its effective implementation? 8. Are there mechanisms in place to hold individuals and business units accountable for adherence to the cybersecurity risk management policy?	

NIST CSF 2.0 AUDIT CHECKLIST

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. Has the organization defined process for regularly reviewing and updating the cybersecurity risk management policy? 2. How does the organization identify and incorporate changes in requirements, threats, technology, and organizational mission into the policy review and update process? 3. Are there mechanisms in place to ensure that the updated cybersecurity risk management policy is effectively communicated to all relevant internal and external stakeholders? 4. How does the organization ensure that the updated cybersecurity risk management policy is understood and implemented by personnel across the organization? 5. What processes are in place to monitor and enforce compliance with the updated cybersecurity risk management policy? 6. Does the organization provide training and guidance to support the implementation of the updated cybersecurity risk management policy? 7. How does the organization evaluate the effectiveness of the updated cybersecurity risk management policy in addressing evolving risks and threats? 8. Are there clear accountabilities and consequences defined for non-compliance with the cybersecurity risk management policy? 9. How does the organization's leadership demonstrate their ongoing commitment to the review, update, and enforcement of the cybersecurity risk management policy?	
Category	**Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	1. Does the organization have a defined process for reviewing the outcomes of its cybersecurity risk management strategy? 2. How does the organization identify and collect relevant data and metrics to evaluate the effectiveness of its cybersecurity risk management strategy? 3. Are there clear roles and responsibilities assigned for the review and analysis of cybersecurity risk management strategy outcomes? 4. What mechanisms are in place to gather feedback and input from key stakeholders (e.g., leadership, business units, cybersecurity team) on the cybersecurity risk management strategy's effectiveness?	

NIST CSF 2.0 AUDIT CHECKLIST

	5. Does the organization's review process consider changes in the threat landscape, regulatory environment, technology, and business objectives that may impact the cybersecurity risk management strategy? 6. How does the organization analyse the results of the cybersecurity risk management strategy review to identify areas for improvement or adjustment? 7. Are there documented procedures for incorporating the findings from the cybersecurity risk management strategy review into the organization's decision-making processes and strategic planning? 8. How does the organization's leadership demonstrate their commitment to the continuous improvement of the cybersecurity risk management strategy based on the review outcomes? 9. Does the organization have a process to monitor the implementation and impact of any adjustments made to the cybersecurity risk management strategy based on the review findings?	
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	1. Does the organization have a defined process for periodically reviewing and adjusting its cybersecurity risk management strategy? 2. How does the organization identify and incorporate changes in organizational requirements, risks, and threats into the review and adjustment of the cybersecurity risk management strategy? 3. Are there mechanisms in place to gather input from key stakeholders (e.g., business units, IT, security team, leadership) on the effectiveness and relevance of the cybersecurity risk management strategy? 4. What criteria or metrics does the organization use to assess the adequacy and coverage of the cybersecurity risk management strategy in addressing its requirements and risks? 5. How does the organization analyze the results of the cybersecurity risk management strategy review to identify areas for improvement or adjustment? 6. Are the adjustments to the cybersecurity risk management strategy aligned with the organization's overall risk management approach and business objectives? 7. What processes are in place to ensure that the updated cybersecurity risk management strategy is effectively communicated and implemented across the organization? 8. Does the organization provide training or guidance to support the implementation of the adjusted cybersecurity risk management strategy? 9. How does the organization's leadership demonstrate their commitment to the regular review and	

	adjustment of the cybersecurity risk management strategy? 10. Are there mechanisms in place to monitor the effectiveness of the adjusted cybersecurity risk management strategy and make further refinements as needed?	
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	1. Does the organization have a defined process for evaluating and reviewing the performance of its cybersecurity risk management activities? 2. What metrics, key performance indicators (KPIs), and other measurements does the organization use to assess the effectiveness of its cybersecurity risk management program? 3. How does the organization collect and analyse data on the performance of its cybersecurity risk management activities? 4. Are there clear roles and responsibilities assigned for the evaluation and review of cybersecurity risk management performance? 5. Does the organization's performance evaluation process consider feedback from internal stakeholders (e.g., business units, IT, security team) and external stakeholders (e.g., customers, partners, regulators)? 6. How does the organization identify and address any gaps or areas for improvement in its cybersecurity risk management performance? 7. Are the findings from the cybersecurity risk management performance evaluation used to inform adjustments to the organization's cybersecurity risk management strategy, policies, and practices? 8. What processes are in place to ensure that the adjustments made based on the performance evaluation are effectively communicated and implemented across the organization? 9. Does the organization's leadership actively engage in the review of cybersecurity risk management performance and the decision-making process for necessary adjustments? 10. How does the organization monitor the impact and effectiveness of the adjustments made to its cybersecurity risk management program based on the performance evaluation?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	
Subcategory	**Audit Questionnaire**	**Compliance Status**
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	1. Has the organization established a comprehensive cybersecurity supply chain risk management program, strategy, objectives, and policies? 2. Are the cybersecurity supply chain risk management program, strategy, objectives, and policies aligned with the organization's overall cybersecurity and enterprise risk management frameworks? 3. Do the cybersecurity supply chain risk management policies and processes cover the entire lifecycle of third-party relationships, from onboarding to offboarding? 4. Are there defined processes for identifying, assessing, and mitigating cybersecurity risks associated with the organization's supply chain? 5. Does the organization periodically review and update the cybersecurity supply chain risk management program, strategy, objectives, and policies to address changes in requirements, threats, and technology? 6. Are there mechanisms in place to monitor and enforce compliance with the organization's cybersecurity supply chain risk management policies and processes? 7. Does the organization provide training and guidance to personnel involved in managing cybersecurity supply chain risks?	
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	1. Has the organization clearly defined the cybersecurity roles and responsibilities for its suppliers, customers, and partners? 2. How are the cybersecurity roles and responsibilities communicated to the organization's suppliers, customers, and partners? 3. What mechanisms are in place to coordinate the cybersecurity roles and responsibilities between the organization and its supply chain stakeholders? 4. Are there contractual agreements or memorandums of understanding that define the cybersecurity roles, responsibilities, and expectations for supply chain stakeholders? 5. Are there processes in place to address and resolve any gaps or conflicts in the cybersecurity roles and responsibilities with supply chain stakeholders? 6. How does the organization ensure that changes in cybersecurity roles and responsibilities are communicated to relevant supply chain stakeholders in a timely manner? 7. Does the organization have a process to periodically review and update the cybersecurity roles and	

	responsibilities of its supply chain stakeholders?	
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	1. Is the organization's cybersecurity supply chain risk management program integrated into its overall enterprise risk management framework? 2. How does the organization identify, assess, and mitigate cybersecurity risks associated with its supply chain as part of the enterprise risk management process? 3. Are the cybersecurity supply chain risk management processes aligned with the organization's risk assessment methodology and risk appetite? 4. Does the organization have a process to continuously monitor and update its understanding of cybersecurity risks within the supply chain? 5. How are the findings and insights from the cybersecurity supply chain risk management process incorporated into the organization's overall risk management decision-making? 6. Are there clear roles and responsibilities defined for the integration of cybersecurity supply chain risk management into the enterprise risk management processes? 7. Does the organization provide training and guidance to personnel involved in the integration of cybersecurity supply chain risk management into enterprise risk management? 8. How does the organization ensure that cybersecurity supply chain risks are considered in the organization's strategic planning, budgeting, and investment decisions? 9. Are there mechanisms in place to measure the effectiveness of the integration of cybersecurity supply chain risk management into the enterprise risk management processes? 10. Does the organization's leadership actively support and oversee the integration of cybersecurity supply chain risk management into the enterprise risk management framework?	
GV.SC-04: Suppliers are known and prioritized by criticality	1. Has the organization identified and documented all of its suppliers, vendors, and other third-party service providers? 2. How does the organization categorize and prioritize its suppliers based on their level of criticality to the organization's operations and cybersecurity risk exposure? 3. What criteria does the organization use to assess the criticality of its suppliers (e.g., access to sensitive data, impact on business continuity, cybersecurity controls)?	

NIST CSF 2.0 AUDIT CHECKLIST

	4. Are there clear roles and responsibilities assigned for the identification, categorization, and prioritization of suppliers based on criticality? 5. How often does the organization review and update its supplier criticality assessments to account for changes in the supplier landscape and risk environment? 6. Does the organization's supplier criticality prioritization align with its overall cybersecurity and enterprise risk management strategies? 7. How does the organization communicate the criticality assessments and priorities to relevant internal and external stakeholders? 8. Are there processes in place to monitor and validate the accuracy of the supplier criticality assessments over time? 9. Does the organization have a centralized repository or system to maintain and manage information on its suppliers and their criticality levels?	
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	1. Has the organization defined and documented the cybersecurity risk requirements that must be addressed in contracts and agreements with suppliers and other third parties? 2. How are the cybersecurity risk requirements prioritized and integrated into the organization's contracting and procurement processes? 3. Do the cybersecurity risk requirements cover aspects such as access controls, data protection, incident response, and security testing? 4. Are the cybersecurity risk requirements aligned with the organization's overall cybersecurity and enterprise risk management policies and standards? 5. What processes are in place to ensure that the cybersecurity risk requirements are communicated to and acknowledged by suppliers and other third parties during the contracting phase? 6. How does the organization monitor and enforce compliance with the cybersecurity risk requirements by its suppliers and other third parties? 7. Are there mechanisms in place to address and resolve any non-compliance or gaps in meeting the cybersecurity risk requirements with suppliers and other third parties? 8. Does the organization provide guidance or training to its procurement, legal, and contract management teams on the integration of cybersecurity risk requirements into supplier agreements? 9. How are the cybersecurity risk requirements in supplier agreements periodically reviewed and updated to reflect changes in the organization's risk landscape and regulatory environment?	

NIST CSF 2.0 AUDIT CHECKLIST

	10. Does the organization's leadership actively support and oversee the incorporation of cybersecurity risk requirements into supplier and third-party agreements?	
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	1. Does the organization have a defined process for conducting due diligence on potential suppliers and other third-party service providers before entering into a formal relationship? 2. What types of cybersecurity-related assessments and checks are performed as part of the due diligence process (e.g., security controls, risk assessments, incident history)? 3. How does the organization evaluate the potential cybersecurity risks associated with a supplier or third-party before onboarding them? 4. Are there clear criteria and thresholds established for determining the acceptability of cybersecurity risks posed by potential suppliers and third parties? 5. Does the organization's due diligence process include an assessment of the supplier's or third-party's financial stability, ownership structure, and overall business continuity capabilities? 6. How does the organization document and communicate the results of the due diligence process to the relevant stakeholders involved in the supplier or third-party selection decision?	
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	1. Has the organization established a process to identify, assess, and prioritize the cybersecurity risks posed by its suppliers and other third-party service providers? 2. What criteria and methodologies does the organization use to evaluate the cybersecurity risks associated with its suppliers and third parties (e.g., threat assessments, vulnerability scans, security control reviews)? 3. How does the organization maintain a centralized inventory or database of the identified cybersecurity risks related to its suppliers and third-party relationships? 4. Are the cybersecurity risks associated with suppliers and third parties integrated into the organization's overall enterprise risk management framework and risk register? 5. What processes are in place to regularly monitor and update the cybersecurity risk profiles of the organization's suppliers and third-party service providers? 6. How does the organization respond to and mitigate the identified cybersecurity risks posed by its suppliers and third parties, based on the risk prioritization and assessment?	

	7. Are there clear roles and responsibilities assigned for the ongoing management and monitoring of cybersecurity risks related to suppliers and third-party relationships? 8. Does the organization provide guidance or training to personnel responsible for supplier and third-party risk management activities? 9. How does the organization's leadership oversee and provide direction on the management of cybersecurity risks associated with the supply chain and third-party relationships? 10. Are there mechanisms in place to measure the effectiveness of the organization's supplier and third-party cybersecurity risk management processes and make improvements as needed?	
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	1. Has the organization identified and documented the roles and responsibilities of its suppliers and other third-party service providers in its incident planning, response, and recovery processes? 2. How are the incident response and recovery requirements communicated to and coordinated with the organization's suppliers and third-party service providers? 3. Are there clear processes in place for suppliers and third parties to report and escalate cybersecurity incidents that may impact the organization? 4. Does the organization's incident response and recovery plans include specific procedures for engaging and collaborating with suppliers and third parties during a cybersecurity incident? 5. How does the organization test and validate the involvement of suppliers and third parties in its incident planning, response, and recovery exercises? 6. Are there mechanisms in place to ensure that suppliers and third parties maintain and regularly test their own incident response and business continuity capabilities? 7. How does the organization monitor and enforce the compliance of its suppliers and third parties with the incident planning, response, and recovery requirements?	

NIST CSF 2.0 AUDIT CHECKLIST

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	1. Has the organization integrated its supply chain security practices into its overall cybersecurity and enterprise risk management programs? 2. How are the cybersecurity and enterprise risk management processes, policies, and controls applied to the organization's supply chain and third-party relationships? 3. Does the organization have a defined process to monitor and measure the performance of its supply chain security practices as part of its cybersecurity and enterprise risk management programs? 4. Are the supply chain security practices and their performance metrics aligned with the organization's overall cybersecurity and risk management objectives and key performance indicators (KPIs)? 5. How does the organization ensure that changes or updates to its cybersecurity and enterprise risk management programs are also reflected in its supply chain security practices? 6. Are there clear roles and responsibilities assigned for the integration and ongoing management of supply chain security practices within the organization's cybersecurity and enterprise risk management programs? 7. Are there mechanisms in place to review and continuously improve the integration of supply chain security practices into the organization's cybersecurity and enterprise risk management programs? 8. How does the organization ensure that the performance and results of its supply chain security practices are effectively communicated to relevant stakeholders?	
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	1. Does the organization's cybersecurity supply chain risk management plan include provisions for activities that occur after the conclusion of a partnership or service agreement with a supplier or third-party? 2. What processes are in place to ensure the secure transfer, return, or destruction of the organization's data and assets when a supplier or third-party relationship is terminated? 3. Are there defined procedures for the secure offboarding of supplier or third-party access, accounts, and privileges upon the conclusion of an agreement? 4. How does the organization ensure that intellectual property, confidential information, and other sensitive data are protected during and after the termination of a supplier or third-party relationship? 5. Are there contractual clauses or agreements that outline the post-relationship cybersecurity and data	

	handling requirements for suppliers and third parties? 6. Does the organization have a process to verify and validate the secure destruction or return of the organization's data and assets by suppliers and third parties upon the termination of an agreement? 7. Are there mechanisms in place to address and mitigate any cybersecurity risks that may arise from the termination of a supplier or third-party relationship?	

Function	**IDENTIFY (ID):** The organization's current cybersecurity risks are understood	
Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
ID.AM-01: Inventories of Hardware Managed by the Organization	8. Does the organization maintain a comprehensive inventory of all hardware assets under its management? 9. What types of hardware assets are included in the inventory (e.g., servers, workstations, network devices, mobile devices, IoT devices)? 10. How does the organization ensure that the hardware inventory is accurate and up-to-date? 11. Is there a defined process for adding new hardware assets to the inventory and removing decommissioned or retired assets? 12. Does the hardware inventory include relevant details such as asset owner, location, configuration, and security controls? 13. How is the hardware inventory information used to support cybersecurity risk management activities? 14. Are there mechanisms in place to monitor and detect unauthorized or unmanaged hardware assets within the organization's environment? 15. Does the organization have a centralized system or database for maintaining and managing the hardware inventory? 16. Are there clear roles and responsibilities assigned for maintaining the hardware inventory?	

NIST CSF 2.0 AUDIT CHECKLIST

ID.AM-02: Inventories of Software, Services, and Systems Managed by the Organization	8. Does the organization maintain inventories of all software, services, and systems under its management? 9. What types of software, services, and systems are included in the inventories (e.g., applications, databases, cloud services, operating systems, network services)? 10. How does the organization ensure that the software, services, and systems inventories are accurate and up-to-date? 11. Is there a defined process for adding new software, services, and systems to the inventories and removing decommissioned or retired items? 12. Do the inventories include relevant details such as software versions, licenses, configurations, and associated hardware assets? 13. How are the software, services, and systems inventories used to support cybersecurity risk management activities? 14. Are there mechanisms in place to monitor and detect unauthorized or unmanaged software, services, and systems within the organization's environment? 15. Does the organization have a centralized system or database for maintaining and managing the software, services, and systems inventories? 16. Are there clear roles and responsibilities assigned for maintaining the software, services, and systems inventories?	
ID.AM-03: Representations of Authorized Network Communication and Data Flows	8. Does the organization maintain representations of its authorized network communication and data flows, both internal and external? 9. What types of network communication and data flows are represented (e.g., application traffic, remote access, cloud services, partner connections)? 10. How does the organization ensure that the network communication and data flow representations are accurate and up-to-date? 11. Is there a defined process for updating the network communication and data flow representations when changes occur? 12. Do the network communication and data flow representations include relevant details such as source, destination, protocols, ports, and security controls? 13. How are the network communication and data flow representations used to support cybersecurity risk management activities? 14. Are there mechanisms in place to monitor and detect unauthorized or unmanaged network	

	communication and data flows? 15. Does the organization have a centralized system or database for maintaining and managing the network communication and data flow representations? 16. Are there clear roles and responsibilities assigned for maintaining the network communication and data flow representations?	
ID.AM-04: Inventories of Services Provided by Suppliers	8. Does the organization maintain an inventory of services provided by its suppliers and third-party service providers? 9. What types of services provided by suppliers are included in the inventory (e.g., cloud services, managed services, outsourced services, software-as-a-service)? 10. How does the organization ensure that the inventory of supplier-provided services is accurate and up-to-date? 11. Is there a defined process for adding new supplier-provided services to the inventory and removing discontinued services? 12. Does the inventory of supplier-provided services include relevant details such as service descriptions, service level agreements, security controls, and risk assessments? 13. Are there mechanisms in place to monitor and detect unauthorized or unmanaged services provided by suppliers?	
ID.AM-05: Asset Prioritization Based on Classification, Criticality, Resources, and Impact	8. Does the organization have a defined process for prioritizing its assets based on classification, criticality, resources, and impact on the mission? 9. What criteria or factors are used to determine the classification and criticality of assets (e.g., confidentiality, integrity, availability, regulatory requirements, business impact)? 10. How does the organization assess the resources required to protect and maintain different types of assets? 11. How does the organization evaluate the potential impact on its mission and objectives if specific assets are compromised or unavailable? 12. Are there mechanisms in place to periodically review and update the asset prioritization based on changes in the organization's risk landscape or mission requirements? 13. How is the asset prioritization information used to support cybersecurity risk management activities and resource allocation decisions? 14. Are there clear roles and responsibilities assigned for conducting asset prioritization activities? 15. Does the organization provide training or guidance	

NIST CSF 2.0 AUDIT CHECKLIST

	to personnel involved in asset prioritization processes? 16. How does the organization's leadership oversee and ensure the effectiveness of the asset prioritization process? 17. Are there mechanisms in place to validate and audit the asset prioritization results for accuracy and consistency?	
ID.AM-07: Inventories of Data and Corresponding Metadata	8. Does the organization maintain inventories of its data and corresponding metadata for designated data types? 9. What types of data are included in the inventories (e.g., sensitive data, proprietary data, customer data, intellectual property)? 10. What types of metadata are captured and maintained for the data inventories (e.g., data classification, data owners, access controls, retention policies)? 11. How does the organization ensure that the data and metadata inventories are accurate and up-to-date? 12. Is there a defined process for adding new data and metadata to the inventories and removing obsolete or decommissioned data? 13. Are there clear roles and responsibilities assigned for maintaining the data and metadata inventories?	
ID.AM-08: Life Cycle Management of Systems, Hardware, Software, Services, and Data	8. Does the organization have defined processes for managing systems, hardware, software, services, and data throughout their life cycles? 9. What stages of the life cycle are covered by the organization's management processes (e.g., acquisition, deployment, configuration, maintenance, disposal)? 10. How does the organization ensure that cybersecurity requirements and controls are integrated into the life cycle management processes? 11. Are there mechanisms in place to monitor and enforce compliance with the life cycle management processes? 12. How does the organization ensure that systems, hardware, software, services, and data are properly decommissioned or securely disposed of at the end of their life cycles? 13. Are there processes in place to address and mitigate any risks or vulnerabilities identified during the life cycle management activities?	

NIST CSF 2.0 AUDIT CHECKLIST

	14. Does the organization provide training or guidance to personnel involved in the life cycle management processes? 15. Are there mechanisms in place to measure and report on the performance of the life cycle management processes? 16. How does the organization incorporate lessons learned and best practices into the continuous improvement of its life cycle management processes?	
Category	**Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization	
Subcategory	**Audit Questionnaire**	**Compliance Status**
ID.RA-01: Identification, Validation, and Recording of Asset Vulnerabilities	5. Does the organization have a process in place to identify vulnerabilities in its assets (e.g., systems, applications, hardware, software)? 6. What sources of vulnerability information does the organization utilize (e.g., vendor advisories, threat intelligence feeds, vulnerability databases)? 7. How does the organization validate the identified vulnerabilities to ensure their relevance and applicability? 8. Is there a centralized repository or system for recording and tracking identified vulnerabilities? 9. Does the vulnerability information include details such as severity, impact, affected assets, and potential mitigations? 10. How does the organization ensure that vulnerability information is kept up-to-date and reflects the current state of its assets? 11. Are there clear roles and responsibilities assigned for the identification, validation, and recording of vulnerabilities? 12. Does the organization provide training or guidance to personnel involved in vulnerability management activities? 13. How does the organization's leadership oversee and monitor the effectiveness of the vulnerability identification and management processes? 14. Are there mechanisms in place to prioritize and address identified vulnerabilities based on risk assessments?	

NIST CSF 2.0 AUDIT CHECKLIST

ID.RA-02: Receiving Cyber Threat Intelligence from Information Sharing Forums and Sources	6. Does the organization have processes in place to receive and leverage cyber threat intelligence from information sharing forums and sources? 7. What types of information sharing forums and sources does the organization participate in or obtain intelligence from (e.g., industry groups, government agencies, threat intelligence providers)? 8. How does the organization evaluate the reliability and credibility of the threat intelligence sources? 9. Is there a centralized system or database for collecting, storing, and analyzing the received threat intelligence? 10. How is the threat intelligence integrated into the organization's risk assessment and decision-making processes? 11. Are there mechanisms in place to analyze and prioritize the threat intelligence based on its relevance and potential impact? 12. Does the organization share relevant threat intelligence with its partners, suppliers, or other stakeholders as appropriate? 13. Are there clear roles and responsibilities assigned for the management and utilization of cyber threat intelligence? 14. Does the organization provide training or guidance to personnel involved in threat intelligence activities?	
ID.RA-03: Identification and Recording of Internal and External Threats	8. Does the organization have a process in place to identify and record internal and external threats? 9. What sources of information does the organization utilize to identify internal threats (e.g., employee monitoring, data loss prevention, insider threat program)? 10. What sources of information does the organization utilize to identify external threats (e.g., threat intelligence feeds, security advisories, industry reports)? 11. Is there a centralized repository or system for recording and tracking identified internal and external threats? 12. Does the threat information include details such as threat actors, motivations, tactics, techniques, and potential impacts? 13. How does the organization ensure that threat information is kept up-to-date and reflects the current threat landscape? 14. Are there clear roles and responsibilities assigned for the identification and recording of internal and external threats? 15. Does the organization provide training or guidance	

	to personnel involved in threat identification and management activities? 16. How does the organization's leadership oversee and monitor the effectiveness of the threat identification and management processes? 17. Are there mechanisms in place to prioritize and address identified threats based on risk assessments?	
ID.RA-04: Identification and Recording of Potential Threat Impacts and Likelihoods	9. Does the organization have a process in place to identify and record the potential impacts and likelihoods of threats exploiting vulnerabilities? 10. What methodologies or frameworks does the organization use to assess the potential impacts of threats (e.g., business impact analysis, risk assessment frameworks)? 11. How does the organization determine the likelihood of threats being realized or vulnerabilities being exploited? 12. Is there a centralized repository or system for recording the assessed impacts and likelihoods of threats and vulnerabilities? 13. Does the impact and likelihood information include details such as risk scores, risk levels, and potential consequences? 14. How does the organization ensure that the impact and likelihood assessments are kept up-to-date and reflect changes in the risk landscape? 15. Are there clear roles and responsibilities assigned for the assessment and recording of threat impacts and likelihoods? 16. Does the organization provide training or guidance to personnel involved in risk assessment activities? 17. How does the organization's leadership oversee and monitor the effectiveness of the impact and likelihood assessment processes? 18. Are there mechanisms in place to prioritize and address identified risks based on their assessed impacts and likelihoods?	
ID.RA-05: Utilization of Threats, Vulnerabilities, Likelihoods, and Impacts for Risk Understanding and Response Prioritization	9. Does the organization utilize the information on threats, vulnerabilities, likelihoods, and impacts to understand its inherent cybersecurity risk? 10. How does the organization integrate and correlate the information on threats, vulnerabilities, likelihoods, and impacts to develop a comprehensive risk picture? 11. Are there methodologies or frameworks in place to analyze and prioritize risks based on the assessed threats, vulnerabilities, likelihoods, and impacts? 12. How does the organization determine its risk	

	tolerance and appetite levels, and how are these factored into the risk analysis and prioritization? 13. Is there a centralized system or dashboard for presenting and reporting the organization's overall cybersecurity risk posture? 14. How does the organization utilize the risk analysis and prioritization to inform its risk response strategies and decision-making? 15. Are there clear roles and responsibilities assigned for the analysis and prioritization of cybersecurity risks? 16. Does the organization provide training or guidance to personnel involved in risk analysis and decision-making activities? 17. How does the organization's leadership oversee and monitor the effectiveness of the risk analysis and prioritization processes? 18. Are there mechanisms in place to continuously monitor and update the risk analysis and prioritization based on changes in the threat landscape or organizational context?	

NIST CSF 2.0 AUDIT CHECKLIST

ID.RA-06: Selection, Prioritization, Planning, Tracking, and Communication of Risk Responses	10. Does the organization have a process in place for selecting, prioritizing, planning, tracking, and communicating risk responses? 11. What types of risk responses does the organization consider (e.g., accept, avoid, mitigate, transfer)? 12. How does the organization prioritize and select appropriate risk responses based on the assessed risks and organizational objectives? 13. Are there mechanisms in place to develop and document risk response plans, including assigned responsibilities and timelines? 14. How does the organization track the implementation and effectiveness of the selected risk responses? 15. Are there processes in place to communicate the selected risk responses and associated plans to relevant stakeholders within the organization? 16. Does the organization involve external stakeholders (e.g., partners, suppliers) in the risk response planning and communication processes, as appropriate? 17. Are there clear roles and responsibilities assigned for the selection, prioritization, planning, tracking, and communication of risk responses? 18. Does the organization provide training or guidance to personnel involved in risk response activities? 19. How does the organization's leadership oversee and monitor the effectiveness of the risk response processes?	
ID.RA-07: Management, Assessment, Recording, and Tracking of Changes and Exceptions	10. Does the organization have a process in place for managing, assessing, recording, and tracking changes and exceptions? 11. What types of changes and exceptions are subject to this process (e.g., changes to systems, configurations, policies, processes)? 12. How does the organization assess the potential risk impact of proposed changes or exceptions? 13. Is there a centralized repository or system for recording and tracking changes and exceptions, along with their associated risk assessments? 14. Does the change and exception management process include mechanisms for approving, rejecting, or deferring proposed changes or exceptions based on their risk impact? 15. How does the organization ensure that approved changes or exceptions are implemented and tracked according to established procedures? 16. Are there clear roles and responsibilities assigned for the management, assessment, recording, and	

	tracking of changes and exceptions? 17. Does the organization provide training or guidance to personnel involved in change and exception management activities? 18. How does the organization's leadership oversee and monitor the effectiveness of the change and exception management processes? 19. Are there mechanisms in place to continuously monitor and assess the risk impact of implemented changes or exceptions over time?	
ID.RA-08: Processes for Receiving, Analyzing, and Responding to Vulnerability Disclosures	11. Does the organization have established processes for receiving, analyzing, and responding to vulnerability disclosures? 12. What channels or mechanisms are in place for receiving vulnerability disclosures (e.g., vendor notifications, security researchers, public disclosures)? 13. How does the organization analyze and validate the credibility and severity of received vulnerability disclosures? 14. Does the organization have a centralized system or database for recording and tracking vulnerability disclosures? 15. What information is captured and maintained for each vulnerability disclosure (e.g., description, affected assets, severity, mitigation guidance)? 16. Are there defined criteria or processes for prioritizing the analysis and response to vulnerability disclosures? 17. How does the organization determine and implement appropriate mitigation or remediation actions in response to validated vulnerability disclosures? 18. Are there mechanisms in place to communicate relevant vulnerability information and mitigation guidance to stakeholders and affected parties? 19. Are there clear roles and responsibilities assigned for receiving, analyzing, and responding to vulnerability disclosures? 20. How does the organization's leadership oversee and ensure the effectiveness of the vulnerability disclosure management processes?	

NIST CSF 2.0 AUDIT CHECKLIST

ID.RA-09: Assessing the Authenticity and Integrity of Hardware and Software	1. Does the organization have processes in place to assess the authenticity and integrity of hardware and software prior to acquisition and use? 2. What methods or techniques are used to verify the authenticity and integrity of hardware and software (e.g., digital signatures, secure boot, trusted platform modules)? 3. How does the organization ensure that the authenticity and integrity assessments are performed consistently and effectively across different types of hardware and software? 4. Are there defined criteria or thresholds for determining the acceptable level of authenticity and integrity for hardware and software acquisitions? 5. Does the organization maintain records or documentation of the authenticity and integrity assessments performed for acquired hardware and software? 6. How does the organization handle situations where the authenticity or integrity of hardware or software cannot be verified or validated? 7. Are there mechanisms in place to monitor and detect potential tampering or unauthorized modifications to acquired hardware and software during their use or deployment? 8. Does the organization provide training or guidance to personnel responsible for conducting authenticity and integrity assessments? 9. Are there clear roles and responsibilities assigned for assessing the authenticity and integrity of hardware and software acquisitions?	

NIST CSF 2.0 AUDIT CHECKLIST

ID.RA-10: Assessing Critical Suppliers Prior to Acquisition	11. Does the organization have processes in place to assess critical suppliers prior to acquisition or engagement? 12. What criteria or factors are used to determine which suppliers are considered "critical" (e.g., access to sensitive data, impact on business continuity, cybersecurity controls)? 13. How does the organization gather and evaluate information about potential critical suppliers (e.g., reputation, financial stability, security posture, compliance certifications)? 14. Are there defined risk assessment methodologies or frameworks used to assess the potential risks associated with critical suppliers? 15. Does the organization maintain records or documentation of the critical supplier assessments performed? 16. How does the organization handle situations where the risk assessment of a critical supplier reveals significant concerns or issues? 17. Are there mechanisms in place to monitor and periodically reassess the risks associated with critical suppliers during the course of the engagement? 18. Does the organization provide training or guidance to personnel responsible for conducting critical supplier assessments?	
Category	**Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	
Subcategory	**Audit Questionnaire**	**Compliance Status**
ID.IM-01: Identifying Improvements from Evaluations	8. Does the organization have a process for conducting evaluations of its cybersecurity risk management program and related activities? 9. What types of evaluations are performed (e.g., internal audits, external assessments, maturity assessments, compliance reviews)? 10. How does the organization ensure that the evaluations are comprehensive, objective, and aligned with industry standards and best practices? 11. Does the organization maintain documentation or reports from the conducted evaluations? 12. Are there mechanisms in place to analyze the evaluation findings and identify opportunities for improvement? 13. How does the organization prioritize and select the improvements to be implemented based on the evaluation results? 14. Is there a defined process for planning,	

	implementing, and tracking the identified improvements? 15. Are there clear roles and responsibilities assigned for conducting evaluations and identifying improvements?	
ID.IM-02: Identifying Improvements from Security Tests and Exercises	8. Does the organization conduct security tests and exercises to identify potential improvements in its cybersecurity posture? 9. What types of security tests and exercises are performed (e.g., penetration testing, vulnerability assessments, tabletop exercises, incident response simulations)? 10. How does the organization ensure that the security tests and exercises are realistic, comprehensive, and aligned with its risk profile? 11. Are relevant suppliers and third parties involved in the planning and execution of security tests and exercises, where appropriate? 12. Does the organization maintain documentation or reports from the conducted security tests and exercises? 13. Are there mechanisms in place to analyze the results of security tests and exercises and identify opportunities for improvement? 14. How does the organization prioritize and select the improvements to be implemented based on the security test and exercise results? 15. Is there a defined process for planning, implementing, and tracking the identified improvements? 16. Are there clear roles and responsibilities assigned for conducting security tests and exercises, and identifying improvements?	
ID.IM-03: Identifying Improvements from Operational Processes, Procedures, and Activities	11. Does the organization have a process for identifying potential improvements during the execution of operational processes, procedures, and activities? 12. What types of operational processes, procedures, and activities are assessed for improvement opportunities (e.g., incident response, change management, access control, backup and recovery)? 13. How does the organization gather feedback and input from personnel involved in the execution of operational processes, procedures, and activities? 14. Are there mechanisms in place to analyze the feedback and identify potential areas for improvement or optimization? 15. How does the organization prioritize and select the improvements to be implemented based on the feedback and analysis?	

	16. Is there a defined process for planning, implementing, and tracking the identified improvements? 17. Are there clear roles and responsibilities assigned for identifying and implementing improvements to operational processes, procedures, and activities?	
ID.IM-04: Establishing, Communicating, Maintaining, and Improving Incident Response and Other Cybersecurity Plans	10. Does the organization have established incident response plans and other cybersecurity plans that affect operations? 11. How does the organization ensure that the incident response and other cybersecurity plans are comprehensive, up-to-date, and aligned with industry standards and best practices? 12. Are the incident response and other cybersecurity plans communicated to all relevant stakeholders, including personnel, suppliers, and relevant third parties? 13. Does the organization provide training or awareness programs to ensure that personnel understand and are prepared to execute the incident response and other cybersecurity plans? 14. Are there processes in place for regularly reviewing and updating the incident response and other cybersecurity plans to reflect changes in the organization's risk landscape, technologies, or operational environment? 15. Does the organization conduct tests or exercises to validate the effectiveness of the incident response and other cybersecurity plans? 16. Are there mechanisms in place to gather feedback and identify potential improvements to the incident response and other cybersecurity plans? 17. How does the organization prioritize and implement identified improvements to the incident response and other cybersecurity plans? 18. Are there clear roles and responsibilities assigned for establishing, maintaining, and improving the incident response and other cybersecurity plans?	

NIST CSF 2.0 AUDIT CHECKLIST

Function	**PROTECT (PR):** Safeguards to manage the organization's cybersecurity risks are used	
Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	17. Does the organization have a defined process for managing identities and credentials for authorized users, services, and hardware? 18. How does the organization ensure that identities and credentials are uniquely assigned and accurately associated with the corresponding users, services, or hardware? 19. What mechanisms are in place to create, modify, disable, and revoke identities and credentials in a timely and secure manner? 20. Does the organization maintain a centralized repository or system for managing and storing identities and credentials? 21. Are there processes in place to periodically review and validate the active identities and credentials to ensure their continued necessity and accuracy? 22. How does the organization monitor and detect the use of unauthorized or compromised identities and credentials? 23. Are there defined policies and procedures for the secure handling, storage, and protection of credentials (e.g., password policies, multi-factor authentication, encryption)? 24. Does the organization provide training or guidance to personnel on the proper management and use of identities and credentials? 25. Are there clear roles and responsibilities assigned for the management of identities and credentials across the organization? 26. How does the organization's leadership ensure the effectiveness of the identity and credential management processes?	
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	17. Does the organization have processes in place to proof identities and bind them to credentials based on the context of interactions? 18. What methods or techniques are used for identity proofing (e.g., document verification, biometric authentication, third-party identity services)? 19. How does the organization determine the appropriate level of identity proofing required based on the context and risk associated with different types of interactions? 20. Are there defined procedures for securely binding proofed identities to the corresponding credentials? 21. Does the organization maintain records or	

	documentation of the identity proofing and credential binding processes? 22. Are there mechanisms in place to detect and prevent the use of fraudulent or compromised identities and credentials?	
PR.AA-03: Users, services, and hardware are authenticated	17. Does the organization have processes in place to authenticate users, services, and hardware before granting access to systems or resources? 18. What authentication mechanisms or protocols are used (e.g., passwords, multi-factor authentication, biometrics, digital certificates, hardware tokens)? 19. How does the organization ensure that the authentication mechanisms are appropriate and commensurate with the risk associated with different types of access or interactions? 20. Are there defined procedures for securely managing and distributing authentication credentials or factors to authorized users, services, and hardware? 21. Does the organization maintain records or logs of authentication activities for auditing and monitoring purposes? 22. How does the organization ensure that authentication mechanisms are consistently applied across different systems, applications, or environments? 23. Are there mechanisms in place to detect and prevent unauthorized or brute-force authentication attempts?	
PR.AA-04: Identity assertions are protected, conveyed, and verified	14. Does the organization have processes in place to protect, convey, and verify identity assertions? 15. What mechanisms or protocols are used to ensure the confidentiality, integrity, and authenticity of identity assertions during transmission and storage (e.g., encryption, digital signatures, secure protocols)? 16. How does the organization ensure that identity assertions are conveyed and verified in a secure and trusted manner across different systems, applications, or environments? 17. Are there defined procedures for managing and validating the trust relationships between entities involved in the exchange of identity assertions? 18. Does the organization maintain records or logs of identity assertion activities for auditing and monitoring purposes? 19. Are there mechanisms in place to detect and prevent unauthorized or malicious modifications	

	to identity assertions?	
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	18. Does the organization have a defined policy for managing access permissions, entitlements, and authorizations? 19. How does the organization ensure that access permissions, entitlements, and authorizations are aligned with the principles of least privilege and separation of duties? 20. Are there processes in place to periodically review and validate the appropriateness of access permissions, entitlements, and authorizations based on user roles, responsibilities, and business requirements? 21. Does the organization maintain a centralized repository or system for managing and enforcing access permissions, entitlements, and authorizations across different systems and applications? 22. How does the organization monitor and detect unauthorized or excessive access permissions, entitlements, or authorizations? 23. Are there defined procedures for granting, modifying, and revoking access permissions, entitlements, and authorizations in a timely and secure manner? 24. Does the organization provide training or guidance to personnel on the proper assignment and management of access permissions, entitlements, and authorizations? 25. Are there clear roles and responsibilities assigned for the management and oversight of access permissions, entitlements, and authorizations? 26. How does the organization's leadership ensure the effectiveness and continuous improvement of the access management processes? 27. Are there mechanisms in place to audit and report on the compliance with the access management policy and procedures?	
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	14. Does the organization have processes in place to manage, monitor, and enforce physical access to assets commensurate with risk? 15. How does the organization identify and classify assets that require physical access controls based on their criticality and sensitivity? 16. What types of physical access controls are implemented (e.g., locks, access cards, biometrics, surveillance cameras, security guards)? 17. Are there defined procedures for granting,	

	modifying, and revoking physical access permissions to authorized personnel or visitors? 18. Does the organization maintain records or logs of physical access activities for auditing and monitoring purposes? 19. How does the organization monitor and detect unauthorized physical access attempts or breaches? 20. Are there mechanisms in place to prevent or mitigate the consequences of unauthorized physical access to assets? 21. Does the organization provide training or guidance to personnel on the proper physical security practices and access control procedures? 22. Are there clear roles and responsibilities assigned for the management and oversight of physical access to assets? 23. How does the organization's leadership ensure the effectiveness and continuous improvement of the physical access management processes?	
Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
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	15. Does the organization have a comprehensive cybersecurity awareness and training program for all personnel? 16. How does the organization determine the specific cybersecurity knowledge and skills required for personnel to perform their general tasks while considering cybersecurity risks? 17. What types of awareness and training activities are included in the program (e.g., online courses, classroom sessions, phishing simulations, security advisories)? 18. Are the awareness and training materials regularly reviewed and updated to reflect the latest cybersecurity threats, best practices, and organizational policies? 19. Does the organization have a mechanism to assess the effectiveness of the awareness and training program, such as knowledge assessments or practical exercises? 20. Are there processes in place to track and monitor personnel's completion of required cybersecurity awareness and training activities? 21. How does the organization ensure that personnel apply the acquired cybersecurity knowledge and skills in their day-to-day tasks and decision-making?	

NIST CSF 2.0 AUDIT CHECKLIST

	22. Does the organization provide refresher or ongoing cybersecurity awareness and training to reinforce the knowledge and skills of personnel? 23. Are there clear roles and responsibilities assigned for the development, delivery, and oversight of the cybersecurity awareness and training program? 24. How does the organization's leadership support and promote the importance of cybersecurity awareness and training among personnel?	
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	15. Does the organization have a specialized cybersecurity awareness and training program for individuals in specialized roles (e.g., cybersecurity professionals, IT administrators, developers)? 16. How does the organization identify the specialized roles that require advanced cybersecurity knowledge and skills to perform their tasks effectively? 17. What types of specialized awareness and training activities are included in the program (e.g., technical certifications, hands-on workshops, threat hunting exercises)? 18. Are the specialized awareness and training materials regularly reviewed and updated to reflect the latest cybersecurity technologies, techniques, and industry best practices? 19. Does the organization have a mechanism to assess the effectiveness of the specialized awareness and training program, such as practical assessments or simulations? 20. Are there processes in place to track and monitor the completion of required specialized cybersecurity awareness and training activities? 21. How does the organization ensure that individuals in specialized roles apply the acquired advanced cybersecurity knowledge and skills in their day-to-day tasks and responsibilities? 22. Does the organization provide opportunities for continuous learning and professional development in specialized cybersecurity areas? 23. Are there clear roles and responsibilities assigned for the development, delivery, and oversight of the specialized cybersecurity awareness and training program? 24. How does the organization's leadership support and promote the importance of specialized cybersecurity awareness and training among relevant personnel?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	
Subcategory	**Audit Questionnaire**	**Compliance Status**
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	1. Does the organization have processes and controls in place to protect the confidentiality, integrity, and availability of data-at-rest? 2. What types of data are considered "data-at-rest" (e.g., data stored on servers, databases, storage systems, backups, archives)? 3. How does the organization classify and identify sensitive or critical data-at-rest that requires additional protection measures? 4. What mechanisms are used to protect the confidentiality of data-at-rest (e.g., encryption, access controls, data masking)? 5. What mechanisms are used to protect the integrity of data-at-rest (e.g., digital signatures, hash functions, access controls)? 6. What mechanisms are used to ensure the availability of data-at-rest (e.g., redundancy, fault tolerance, backup and recovery processes)? 7. Are there defined processes for securely managing and rotating encryption keys or other data protection mechanisms for data-at-rest? 8. How does the organization monitor and detect unauthorized access or modifications to data-at-rest? 9. Are there defined roles and responsibilities for the management and protection of data-at-rest across the organization?	
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	19. Does the organization have processes and controls in place to protect the confidentiality, integrity, and availability of data-in-transit? 20. What types of data flows are considered "data-in-transit" (e.g., network communications, file transfers, remote access, cloud services)? 21. How does the organization identify and classify sensitive or critical data-in-transit that requires additional protection measures? 22. What mechanisms are used to protect the confidentiality of data-in-transit (e.g., encryption, secure protocols, access controls)? 23. What mechanisms are used to protect the integrity of data-in-transit (e.g., digital signatures, message authentication codes, secure protocols)? 24. What mechanisms are used to ensure the availability of data-in-transit (e.g., load balancing, redundancy, failover mechanisms)? 25. Are there defined processes for securely managing and rotating encryption keys or other data	

	protection mechanisms for data-in-transit? 26. How does the organization monitor and detect unauthorized access or modifications to data-in-transit? 27. Are there defined roles and responsibilities for the management and protection of data-in-transit across the organization?	
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	1. Does the organization have processes and controls in place to protect the confidentiality, integrity, and availability of data-in-use? 2. What types of data are considered "data-in-use" (e.g., data processed by applications, memory-resident data, data used in computations)? 3. How does the organization identify and classify sensitive or critical data-in-use that requires additional protection measures? 4. What mechanisms are used to protect the confidentiality of data-in-use (e.g., secure execution environments, memory protection, access controls)? 5. What mechanisms are used to protect the integrity of data-in-use (e.g., secure execution environments, input validation, access controls)? 6. What mechanisms are used to ensure the availability of data-in-use (e.g., redundancy, fault tolerance, failure isolation)? 7. Are there defined processes for securely managing and protecting data-in-use throughout its lifecycle (e.g., secure coding practices, secure runtime environments)? 8. How does the organization monitor and detect unauthorized access or modifications to data-in-use? 9. Are there defined roles and responsibilities for the management and protection of data-in-use across the organization?	

NIST CSF 2.0 AUDIT CHECKLIST

PR.DS-11: Backups of data are created, protected, maintained, and teste	20. Does the organization have processes and controls in place for creating, protecting, maintaining, and testing backups of data? 21. What types of data are included in the backup processes (e.g., databases, file systems, configurations, application data)? 22. How does the organization determine the appropriate frequency and retention periods for data backups based on criticality and recovery requirements? 23. What mechanisms are used to protect the confidentiality and integrity of backup data (e.g., encryption, access controls, secure storage)? 24. Are backup data stored in secure locations, both on-site and off-site, to ensure availability in case of disasters or incidents? 25. How does the organization monitor and ensure the successful completion of backup processes, including the verification of backup data integrity? 26. Are there defined processes for testing and validating the restoration of backup data on a regular basis? 27. Does the organization maintain documentation and procedures for executing backup and restoration processes? 28. Are there defined roles and responsibilities for the management and oversight of backup and data protection processes across the organization? 29. How does the organization's leadership ensure the effectiveness and continuous improvement of backup and data protection measures?	
Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
PR.PS-01: Configuration management practices are established and applied	16. Does the organization have documented configuration management practices and procedures? 17. How does the organization ensure that configuration management practices are consistently applied across all hardware, software, and service platforms? 18. What processes are in place for establishing and maintaining secure baseline configurations for systems, applications, and services? 19. Are there mechanisms to detect and report deviations from approved configurations? 20. How does the organization manage and approve changes to configurations, including testing and	

	validation processes? 21. Are configuration management activities and changes documented and tracked in a centralized repository or system? 22. Does the organization provide training and guidance to personnel involved in configuration management activities? 23. How does the organization ensure that configuration management practices are aligned with its risk management strategy and security requirements? 24. Are there processes in place to periodically review and update configuration management practices to address changes in the threat landscape, technology, or organizational needs?	
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	1. Does the organization have processes in place for maintaining, replacing, and removing software components (e.g., operating systems, applications, firmware)? 2. How does the organization determine when software needs to be updated, replaced, or removed based on risk considerations? 3. What processes are in place to ensure that software updates and replacements are tested, validated, and approved before deployment? 4. Are there mechanisms to detect and prevent the installation or execution of unauthorized or malicious software? 5. How does the organization manage and track software licenses, versions, and end-of-life cycles? 6. Are there documented procedures for securely removing or decommissioning software components, including data sanitization and secure disposal? 7. Does the organization provide training and guidance to personnel involved in software maintenance, replacement, and removal activities? 8. How does the organization ensure that software maintenance, replacement, and removal practices are aligned with its risk management strategy and security requirements? 9. Are there processes in place to periodically review and update software maintenance, replacement, and removal practices to address changes in the threat landscape, technology, or organizational needs?	

NIST CSF 2.0 AUDIT CHECKLIST

PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	1. Does the organization have processes in place for maintaining, replacing, and removing hardware components (e.g., servers, workstations, network devices)? 2. How does the organization determine when hardware needs to be updated, replaced, or removed based on risk considerations? 3. What processes are in place to ensure that hardware updates and replacements are tested, validated, and approved before deployment? 4. Are there mechanisms to detect and prevent the installation or connection of unauthorized or compromised hardware? 5. How does the organization manage and track hardware assets, including maintenance schedules and end-of-life cycles? 6. Are there documented procedures for securely removing or decommissioning hardware components, including data sanitization and secure disposal? 7. Does the organization provide training and guidance to personnel involved in hardware maintenance, replacement, and removal activities? 8. How does the organization ensure that hardware maintenance, replacement, and removal practices are aligned with its risk management strategy and security requirements? 9. Are there processes in place to periodically review and update hardware maintenance, replacement, and removal practices to address changes in the threat landscape, technology, or organizational needs?	
PR.PS-04: Log records are generated and made available for continuous monitoring	1. Does the organization have processes in place for generating and making log records available for continuous monitoring? 2. What types of log records are generated and collected (e.g., system logs, application logs, security logs, network logs)? 3. How does the organization ensure that log records are generated and collected consistently across all hardware, software, and service platforms? 4. Are there mechanisms in place to protect the integrity and confidentiality of log records? 5. How does the organization manage and store log records, including retention periods and archiving processes? 6. Are log records continuously monitored for security events, incidents, or anomalies? 7. Does the organization have processes for	

	analyzing and correlating log records from multiple sources to identify potential security issues? 8. Are there mechanisms in place to ensure that log records are available and accessible for analysis, reporting, and investigations? 9. Does the organization provide training and guidance to personnel involved in log management and monitoring activities?	
PR.PS-05: Installation and execution of unauthorized software are prevented	1. Does the organization have mechanisms in place to prevent the installation and execution of unauthorized software? 2. What technologies or controls are used to enforce software whitelisting or application control policies? 3. How does the organization define and maintain an approved list of authorized software for different user groups or system types? 4. Are there processes for granting exceptions or temporary approvals for installing or executing specific software? 5. How does the organization monitor and detect attempts to install or execute unauthorized software? 6. Are there mechanisms in place to automatically block or quarantine unauthorized software installations or executions? 7. Does the organization provide training and awareness programs to educate users about the risks of unauthorized software and the importance of adhering to software policies? 8. How does the organization ensure that software whitelisting or application control policies are consistently enforced across all hardware, software, and service platforms? 9. Are there processes in place to periodically review and update the approved software lists and whitelisting policies to address changes in the threat landscape, technology, or organizational needs?	
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	1. Does the organization have processes in place to integrate secure software development practices throughout the software development life cycle? 2. What secure software development methodologies, frameworks, or best practices are followed (e.g., secure coding practices, code reviews, security testing)? 3. How does the organization ensure that secure software development practices are consistently applied across all software development projects?	

NIST CSF 2.0 AUDIT CHECKLIST

	4. Are there mechanisms in place to monitor and assess the performance and effectiveness of secure software development practices? 5. How does the organization identify and address any gaps or weaknesses in the secure software development practices? 6. Are there processes for incorporating feedback and lessons learned from security incidents or vulnerabilities into the secure software development practices? 7. Does the organization provide training and guidance to software developers, testers, and project managers on secure software development practices? 8. How does the organization ensure that secure software development practices are aligned with its risk management strategy and security requirements? 9. Are there processes in place to periodically review and update the secure software development practices to address changes in the threat landscape, technology, or organizational needs?	
Category	**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	
Subcategory	**Audit Questionnaire**	**Compliance Status**
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	1. Does the organization have implemented controls and mechanisms to protect its networks and environments from unauthorized logical access and usage? 2. What types of controls are in place to prevent unauthorized access to the organization's networks and environments (e.g., firewalls, access control lists, network segmentation, virtual private networks)? 3. How does the organization ensure that access to networks and environments is granted only to authorized users, devices, and services? 4. Are there processes in place to monitor and detect unauthorized or suspicious network and environment access attempts or activities? 5. Does the organization maintain logs or records of network and environment access activities for auditing and forensic purposes? 6. How does the organization ensure that the network and environment access controls are consistently applied across different locations, systems, and infrastructure components? 7. Are there defined procedures for reviewing and updating the network and environment access	

NIST CSF 2.0 AUDIT CHECKLIST

	controls to address evolving threats and changes in the organization's risk landscape? 8. Does the organization provide training or guidance to personnel on the proper use and protection of networks and environments? 9. Are there clear roles and responsibilities assigned for the management and oversight of network and environment access controls?	
PR.IR-02: The organization's technology assets are protected from environmental threats	17. Does the organization have measures in place to protect its technology assets from environmental threats (e.g., power outages, natural disasters, extreme temperatures, humidity)? 18. What types of environmental controls or safeguards are implemented (e.g., uninterruptible power supplies, backup generators, climate control systems, fire suppression systems)? 19. How does the organization assess and mitigate the potential impact of environmental threats on its technology assets and operations? 20. Are there processes in place to monitor and detect environmental conditions that may pose a threat to technology assets? 21. Does the organization maintain contingency plans or procedures for responding to environmental incidents or disruptions? 22. How does the organization ensure that the environmental controls and safeguards are consistently applied across different locations and facilities? 23. Are there defined procedures for testing, maintaining, and updating the environmental controls and safeguards? 24. Does the organization provide training or guidance to personnel on the proper handling and protection of technology assets from environmental threats? 25. Are there clear roles and responsibilities assigned for the management and oversight of environmental controls and safeguards?	
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	18. Does the organization have mechanisms implemented to achieve resilience requirements in normal and adverse situations? 19. What types of resilience mechanisms are implemented (e.g., redundancy, failover, load balancing, backup and recovery, incident response planning)? 20. How does the organization determine the appropriate resilience requirements based on its risk assessment and business continuity objectives? 21. Are there processes in place to monitor and	

	validate the effectiveness of the implemented resilience mechanisms? 22. Does the organization maintain documentation or records of the resilience mechanisms and their associated requirements? 23. How does the organization ensure that the resilience mechanisms are consistently applied across different systems, applications, and infrastructure components? 24. Are there defined procedures for testing and validating the resilience mechanisms in simulated or controlled environments? 25. Does the organization provide training or guidance to personnel on the proper implementation and use of resilience mechanisms? 26. Are there clear roles and responsibilities assigned for the management and oversight of resilience mechanisms?	
PR.IR-04: Adequate resource capacity to ensure availability is maintained	19. Does the organization have processes in place to maintain adequate resource capacity to ensure availability of its systems and services? 20. What types of resources are considered in the capacity planning process (e.g., computing power, storage, network bandwidth, software licenses, personnel)? 21. How does the organization assess and determine the required resource capacity based on current and projected workloads, usage patterns, and growth expectations? 22. Are there mechanisms in place to monitor and track resource utilization and capacity levels? 23. Does the organization maintain contingency plans or procedures for responding to resource capacity shortages or spikes in demand? 24. How does the organization ensure that resource capacity is consistently managed across different systems, applications, and infrastructure components? 25. Are there defined procedures for provisioning, scaling, and decommissioning resources to maintain adequate capacity levels? 26. Does the organization provide training or guidance to personnel on the proper management and optimization of resource capacity? 27. Are there clear roles and responsibilities assigned for the management and oversight of resource capacity planning and maintenance?	

NIST CSF 2.0 AUDIT CHECKLIST

Function	**DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed**	
Category	**Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	
Subcategory	**Audit Questionnaire**	**Compliance Status**
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	27. Does the organization have systems and processes in place to continuously monitor networks and network services for potentially adverse events? 28. What tools or technologies are used for network monitoring (e.g., intrusion detection systems, network traffic analyzers, log management tools)? 29. How does the organization define and identify potentially adverse events in the context of network monitoring? 30. Are there established baselines for normal network behaviour, and how are deviations from these baselines detected and investigated? 31. How frequently are network monitoring tools and processes reviewed and updated to address new threats or technologies? 32. Are there documented procedures for responding to and investigating potentially adverse events detected through network monitoring? 33. How are the results of network monitoring communicated to relevant stakeholders within the organization? 34. Does the organization monitor both internal and external network traffic? 35. Are there mechanisms in place to correlate data from different network monitoring tools to improve threat detection capabilities? 36. How does the organization ensure that network monitoring activities comply with relevant privacy and data protection regulations?	
DE.CM-02: The physical environment is monitored to find potentially adverse events	23. Does the organization have systems and processes in place to monitor the physical environment for potentially adverse events? 24. What types of physical security controls are monitored (e.g., access control systems, surveillance cameras, environmental sensors)? 25. How does the organization define and identify potentially adverse events in the context of physical environment monitoring? 26. Are there established baselines for normal physical environment conditions, and how are deviations from these baselines detected and investigated? 27. How frequently are physical monitoring systems	

	and processes reviewed and updated? 28. Are there documented procedures for responding to and investigating potentially adverse events detected through physical environment monitoring? 29. How are the results of physical environment monitoring communicated to relevant stakeholders within the organization? 30. Does the organization integrate physical security monitoring with cybersecurity monitoring efforts? 31. Are there mechanisms in place to ensure continuous monitoring of critical physical areas, even during power outages or other disruptions? 32. How does the organization ensure that physical environment monitoring activities comply with relevant privacy and labor regulations?	
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	24. Does the organization have systems and processes in place to monitor personnel activity and technology usage for potentially adverse events? 25. What types of personnel activities and technology usage are monitored (e.g., login attempts, file access, email usage, application usage)? 26. How does the organization define and identify potentially adverse events in the context of personnel activity and technology usage? 27. Are there established baselines for normal personnel activity and technology usage, and how are deviations from these baselines detected and investigated? 28. How frequently are personnel activity and technology usage monitoring systems and processes reviewed and updated? 29. Are there documented procedures for responding to and investigating potentially adverse events detected through personnel and technology usage monitoring? 30. How are the results of personnel activity and technology usage monitoring communicated to relevant stakeholders within the organization? 31. Does the organization have policies in place to inform employees about monitoring activities and ensure compliance with privacy regulations? 32. Are there mechanisms in place to detect and investigate potential insider threats? **33.** How does the organization balance the need for monitoring with employee privacy concerns?	

NIST CSF 2.0 AUDIT CHECKLIST

DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	20. Does the organization have systems and processes in place to monitor the activities and services of external service providers for potentially adverse events? 21. What types of external service provider activities and services are monitored? 22. How does the organization define and identify potentially adverse events in the context of external service provider activities? 23. Are there established baselines for normal external service provider activities, and how are deviations from these baselines detected and investigated? 24. How frequently are external service provider monitoring systems and processes reviewed and updated? 25. Are there documented procedures for responding to and investigating potentially adverse events detected through external service provider monitoring? 26. How are the results of external service provider monitoring communicated to relevant stakeholders within the organization? 27. Does the organization have agreements in place with external service providers that allow for monitoring of their activities? 28. Are there mechanisms in place to ensure that external service providers comply with the organization's security policies and standards? 29. How does the organization ensure that its monitoring of external service providers complies with relevant contractual and legal requirements?	
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	1. Does the organization have systems and processes in place to monitor computing hardware, software, runtime environments, and their data for potentially adverse events? 2. What specific aspects of computing hardware, software, runtime environments, and data are monitored (e.g., system logs, application logs, configuration changes, data access patterns)? 3. How does the organization define and identify potentially adverse events in the context of these IT assets? 4. Are there established baselines for normal behaviour of computing hardware, software, runtime environments, and data, and how are deviations from these baselines detected and investigated? 5. How frequently are monitoring systems and processes for these IT assets reviewed and updated?	

NIST CSF 2.0 AUDIT CHECKLIST

	6. Are there documented procedures for responding to and investigating potentially adverse events detected through monitoring of these IT assets? 7. How are the results of this monitoring communicated to relevant stakeholders within the organization? 8. Does the organization use automated tools for monitoring and analyzing the behavior of computing hardware, software, runtime environments, and data? 9. Are there mechanisms in place to detect and investigate potential malware infections, unauthorized software installations, or unauthorized changes to runtime environments? 10. How does the organization ensure that its monitoring of computing hardware, software, runtime environments, and data complies with relevant privacy and data protection regulations?	
Category	**Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	
Subcategory	**Audit Questionnaire**	**Compliance Status**
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	24. Does the organization have a defined process for analyzing potentially adverse events? 25. What criteria are used to identify and prioritize potentially adverse events for analysis? 26. How does the organization ensure that the analysis of potentially adverse events is thorough and timely? 27. What tools or technologies are used to support the analysis of potentially adverse events? 28. Are there documented procedures for conducting the analysis of potentially adverse events? 29. How does the organization capture and document the findings from the analysis of potentially adverse events? 30. Are there mechanisms in place to identify patterns or trends across multiple potentially adverse events? 31. How does the organization use the results of the analysis to improve its overall security posture? 32. Are there clear roles and responsibilities assigned for the analysis of potentially adverse events? 33. How does the organization's leadership ensure the effectiveness of the analysis process for potentially adverse events?	
DE.AE-03: Information is correlated from multiple sources	17. Does the organization have processes in place to correlate information from multiple sources when analyzing cybersecurity events?	

NIST CSF 2.0 AUDIT CHECKLIST

	18. What types of information sources are used in the correlation process (e.g., log files, network traffic data, threat intelligence feeds)? 19. How does the organization ensure that the information from different sources is accurately and effectively correlated? 20. What tools or technologies are used to support the correlation of information from multiple sources? 21. Are there documented procedures for correlating and analyzing information from multiple sources? 22. How does the organization handle discrepancies or conflicts in information from different sources? 23. Are there mechanisms in place to identify complex or sophisticated attacks that may only be visible when correlating multiple data sources? 24. How does the organization use the correlated information to improve its detection and response capabilities? 25. Are there clear roles and responsibilities assigned for the correlation and analysis of information from multiple sources?	
DE.AE-04: The estimated impact and scope of adverse events are understood	6. Does the organization have a process for estimating the impact and scope of adverse events? 7. What criteria or metrics are used to assess the impact of adverse events (e.g., financial loss, operational disruption, data compromise)? 8. How does the organization determine the scope of adverse events, including affected systems, data, and users? 9. Are there documented procedures for assessing and documenting the impact and scope of adverse events? 10. What tools or methodologies are used to support the impact and scope assessment process? 11. How does the organization ensure that the impact and scope assessments are accurate and consistent across different types of adverse events? 12. Are there mechanisms in place to update the impact and scope assessments as new information becomes available? 13. How does the organization use the impact and scope assessments to prioritize its response and recovery efforts? 14. Are there clear roles and responsibilities assigned for assessing the impact and scope of adverse events?	

NIST CSF 2.0 AUDIT CHECKLIST

DE.AE-06: Information on adverse events is provided to authorized staff and tools	7. Does the organization have a process for providing information on adverse events to authorized staff and tools? 8. How does the organization determine which staff members and tools are authorized to receive information on adverse events? 9. What types of information about adverse events are shared with authorized staff and tools? 10. Are there mechanisms in place to ensure that sensitive information about adverse events is appropriately protected and shared only with authorized parties? 11. How quickly is information about adverse events made available to authorized staff and tools after detection? 12. What communication channels or platforms are used to share information about adverse events with authorized staff and tools? 13. Are there procedures in place for escalating information about critical or high-impact adverse events to appropriate stakeholders? 14. How does the organization ensure that the information provided about adverse events is accurate, timely, and actionable? 15. Are there clear roles and responsibilities assigned for managing and distributing information about adverse events?	
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	6. Does the organization integrate cyber threat intelligence and other contextual information into its analysis of adverse events? 7. What sources of cyber threat intelligence and contextual information does the organization use? 8. How does the organization ensure the reliability and relevance of the threat intelligence and contextual information it uses? 9. Are there processes in place to correlate threat intelligence and contextual information with observed adverse events? 10. How does the organization use threat intelligence and contextual information to enhance its understanding of potential threats and attack patterns? 11. What tools or technologies are used to support the integration of threat intelligence and contextual information into the analysis process? 12. Are there mechanisms in place to update and refine detection and analysis processes based on new threat intelligence and contextual information? 13. How does the organization measure the effectiveness of integrating threat intelligence and	

	contextual information into its analysis processes? 14. Are there clear roles and responsibilities assigned for managing and integrating threat intelligence and contextual information?	
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	7. Does the organization have defined criteria for declaring an incident based on adverse events? 8. What factors are considered in the incident declaration criteria (e.g., impact, scope, severity, type of assets affected)? 9. How are the incident declaration criteria communicated to relevant staff members? 10. Are there documented procedures for evaluating adverse events against the incident declaration criteria? 11. How does the organization ensure consistency in applying the incident declaration criteria across different types of adverse events? 12. What is the process for declaring an incident once the defined criteria are met? 13. Are there mechanisms in place to escalate potential incidents to appropriate decision-makers for declaration? 14. How quickly are incidents typically declared after the criteria are met? 15. Are there clear roles and responsibilities assigned for evaluating adverse events and declaring incidents?	

Function	**RESPOND (RS): Actions regarding a detected cybersecurity incident are taken**	
Category	**Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	37. Does the organization have a documented incident response plan that includes coordination with relevant third parties? 38. How does the organization identify and maintain a list of relevant third parties to be involved in incident response? 39. Are there clear procedures for notifying and engaging relevant third parties once an incident is declared? 40. How does the organization ensure that third parties understand their roles and responsibilities in the incident response process? 41. Are there mechanisms in place to securely share necessary information with third parties during incident response?	

NIST CSF 2.0 AUDIT CHECKLIST

	42. How does the organization coordinate and communicate with third parties throughout the incident response process? 43. Are there procedures for documenting the actions taken by third parties during incident response? 44. How does the organization evaluate the effectiveness of third-party involvement in incident response? 45. Are there processes in place to review and update the incident response plan based on lessons learned from third-party coordination?	
RS.MA-02: Incident reports are triaged and validated	1. Does the organization have a defined process for triaging and validating incident reports? 2. What criteria are used to assess the validity and severity of reported incidents? 3. How does the organization ensure that incident reports are triaged and validated in a timely manner? 4. Are there documented procedures for collecting and preserving evidence during the triage and validation process? 5. What tools or technologies are used to support the triage and validation of incident reports? 6. How does the organization handle false positives or duplicate incident reports? 7. Are there clear roles and responsibilities assigned for triaging and validating incident reports? 8. How does the organization ensure consistency in the triage and validation process across different types of incidents? 9. Are there mechanisms in place to escalate high-priority or complex incidents during the triage process? 10. How does the organization use the results of the triage and validation process to inform its incident response strategies?	
RS.MA-03: Incidents are categorized and prioritized	34. Does the organization have a defined system for categorizing and prioritizing incidents? 35. What criteria are used to categorize incidents (e.g., type of attack, affected systems, potential impact)? 36. How does the organization determine the priority of incidents? 37. Are there documented procedures for assigning categories and priorities to incidents? 38. How does the organization ensure consistency in the categorization and prioritization process across different incidents? 39. Are there mechanisms in place to adjust incident categories and priorities as new information	

	becomes available? 40. How does the categorization and prioritization of incidents inform the allocation of resources and response efforts? 41. Are there clear roles and responsibilities assigned for categorizing and prioritizing incidents? 42. How does the organization communicate incident categories and priorities to relevant stakeholders? 43. How does the organization's leadership use incident categorization and prioritization information to make strategic decisions about cybersecurity investments and improvements?	
RS.MA-04: Incidents are escalated or elevated as needed	30. Does the organization have defined criteria for escalating or elevating incidents? 31. What factors are considered when determining whether an incident should be escalated or elevated? 32. Are there clear procedures for the escalation or elevation process, including who to notify and how? 33. How does the organization ensure that incidents are escalated or elevated in a timely manner when necessary? 34. Are there different levels of escalation, and how are they defined? 35. How does the organization communicate escalated or elevated incidents to appropriate stakeholders, including senior management? 36. Are there mechanisms in place to track and monitor the status of escalated or elevated incidents? 37. How does the escalation or elevation process affect the allocation of resources and response efforts? 38. Are there clear roles and responsibilities assigned for making escalation or elevation decisions?	

RS.MA-05: The criteria for initiating incident recovery are applied	28. Does the organization have defined criteria for initiating incident recovery? 29. What factors are considered in the criteria for initiating incident recovery (e.g., containment status, impact assessment, business continuity needs)? 30. How are the criteria for initiating incident recovery documented and communicated to relevant personnel? 31. Are there clear procedures for assessing whether an incident meets the criteria for initiating recovery? 32. How does the organization ensure consistency in applying the criteria for initiating incident recovery across different types of incidents? 33. Are there mechanisms in place to initiate recovery processes once the criteria are met? 34. How does the organization balance the need for thorough investigation with the urgency of initiating recovery? 35. Are there clear roles and responsibilities assigned for assessing incidents against the recovery initiation criteria and making recovery decisions? 36. How does the organization document the decision-making process for initiating incident recovery?	
Category	**Incident Analysis (RS.AN):** Investigations are conducted to ensure effective response and support forensics and recovery activities	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	34. Does the organization have a defined process for analysing cybersecurity incidents to determine what has taken place and identify the root cause? 35. What methodologies or frameworks does the organization use for incident analysis and root cause determination? 36. How does the organization ensure that the incident analysis is comprehensive and covers all affected systems and data? 37. Are there tools or technologies in place to support the incident analysis and root cause determination process? 38. How does the organization document the findings of the incident analysis and root cause determination? 39. Are there procedures in place to involve relevant stakeholders (e.g., IT, security, business units) in the incident analysis process? 40. How does the organization use the results of	

NIST CSF 2.0 AUDIT CHECKLIST

	incident analysis and root cause determination to improve its overall security posture? 41. Are there mechanisms in place to ensure that lessons learned from incident analysis are incorporated into future incident response plans and procedures? 42. How does the organization handle situations where the root cause of an incident is not immediately apparent or involves complex factors? 43. Are there clear roles and responsibilities assigned for conducting incident analysis and root cause determination?	
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	26. Does the organization have a process for recording all actions performed during a cybersecurity incident investigation? 27. What types of information are captured in the investigation records (e.g., timestamps, actions taken, personnel involved, systems accessed)? 28. How does the organization ensure the integrity of the investigation records throughout the incident response process? 29. What methods or technologies are used to preserve the provenance of investigation records? 30. Are there documented procedures for maintaining chain of custody for investigation records and evidence? 31. How does the organization control access to investigation records to ensure they are only accessible to authorized personnel? 32. Are there mechanisms in place to protect investigation records from tampering or unauthorized modification? 33. How long are investigation records retained, and what is the process for securely disposing of them when no longer needed? 34. Are there clear roles and responsibilities assigned for recording and preserving investigation actions?	
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	15. Does the organization have a defined process for collecting incident data and metadata during a cybersecurity incident? 16. What types of incident data and metadata are collected (e.g., log files, network traffic data, system state information)? 17. How does the organization ensure the integrity of the collected incident data and metadata? 18. What tools or technologies are used to collect and preserve incident data and metadata? 19. Are there documented procedures for maintaining chain of custody for collected incident data and metadata?	

	20. How does the organization ensure that the collection of incident data and metadata does not interfere with ongoing business operations? 21. Are there mechanisms in place to protect collected incident data and metadata from tampering or unauthorized access? 22. How long is incident data and metadata retained, and what is the process for securely disposing of it when no longer needed? 23. Are there clear roles and responsibilities assigned for collecting and preserving incident data and metadata?	
RS.AN-08: An incident's magnitude is estimated and validated	15. Does the organization have a defined process for estimating and validating the magnitude of a cybersecurity incident? 16. What criteria or metrics are used to assess the magnitude of an incident (e.g., number of affected systems, data sensitivity, operational impact)? 17. How does the organization ensure that the initial magnitude estimate is based on accurate and up-to-date information? 18. Are there procedures in place for validating and refining the incident magnitude estimate as more information becomes available? 19. How does the organization communicate incident magnitude information to relevant stakeholders and decision-makers? 20. Are there defined thresholds or categories for incident magnitude that trigger different levels of response or escalation? 21. How does the organization use incident magnitude information to prioritize response efforts and allocate resources? 22. Are there mechanisms in place to review and learn from past incidents to improve the accuracy of future magnitude estimations? 23. Are there clear roles and responsibilities assigned for estimating and validating incident magnitude?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RS.CO-02: Internal and external stakeholders are notified of incidents	25. Does the organization have a documented process for notifying internal and external stakeholders about cybersecurity incidents? 26. How does the organization determine which internal stakeholders should be notified of an incident? (e.g., executive leadership, legal team, affected departments) 27. What criteria are used to determine when external stakeholders (e.g., customers, partners, regulators) should be notified of an incident? 28. Are there predefined templates or scripts for incident notifications to ensure consistency and completeness of information? 29. How does the organization ensure that incident notifications comply with relevant laws, regulations, and contractual obligations? 30. What is the typical timeframe for notifying stakeholders after an incident has been confirmed? 31. Are there different notification processes or timelines based on the severity or type of incident? 32. How does the organization maintain a record of incident notifications, including who was notified, when, and what information was shared? 33. Are there mechanisms in place to update stakeholders as new information about an incident becomes available? 34. How does the organization's leadership oversee and ensure the effectiveness of the incident notification process?	
RS.CO-03: Information is shared with designated internal and external stakeholders	25. Does the organization have a documented policy for sharing incident-related information with designated internal and external stakeholders? 26. How does the organization determine which internal and external stakeholders should receive specific types of incident-related information? 27. What types of incident-related information are typically shared with stakeholders? (e.g., incident details, impact assessments, remediation steps) 28. Are there processes in place to ensure that sensitive or confidential information is appropriately protected when shared with stakeholders? 29. How does the organization ensure that information sharing complies with relevant laws, regulations,	

	and contractual obligations? 30. What methods or platforms are used for sharing incident-related information with stakeholders? (e.g., secure portals, encrypted emails, phone calls) 31. Are there different levels or categories of information shared based on the stakeholder's role or need-to-know? 32. How does the organization verify that the right information is reaching the correct stakeholders in a timely manner? 33. Are there mechanisms in place for stakeholders to request additional information or clarification about shared incident details? 34. How does the organization measure and improve the effectiveness of its information sharing processes with stakeholders? 35. Are there clear roles and responsibilities assigned for managing the information sharing process during an incident? 36. How does the organization's leadership ensure that information sharing practices support effective incident response and stakeholder trust?	
Category	**Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RS.MI-01: Incidents are contained	28. Does the organization have a documented incident containment process? 29. How quickly are containment measures typically implemented after an incident is detected? 30. What tools and techniques are used for containing different types of incidents? 31. Are there predefined containment strategies for common incident types? 32. How does the organization ensure that containment actions don't destroy potential evidence? 33. Is there a process to verify the effectiveness of containment measures? 34. Who has the authority to make decisions about containment actions? 35. How are containment activities documented and reported? 36. Are containment drills or simulations conducted regularly? 37. How does the organization balance the need for containment with business continuity requirements?	

NIST CSF 2.0 AUDIT CHECKLIST

RS.MI-02: Incidents are eradicated	30. What is the organization's process for incident eradication? 31. How does the organization determine when an incident has been fully eradicated? 32. What tools and techniques are used in the eradication process? 33. How does the organization ensure that all components of the incident (e.g., malware, backdoors) are completely removed? 34. Is there a process to verify systems are clean after eradication efforts? 35. How are eradication activities documented and reported? 36. Who is responsible for declaring an incident officially eradicated? 37. What measures are taken to prevent reoccurrence of eradicated incidents? 38. How does the organization handle situations where full eradication may not be immediately possible? 39. Are post-incident reviews conducted to improve eradication processes?	
Function	**RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored**	
Category	**Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	20. Is there a documented process for transitioning from incident response to recovery? 21. How is the decision to initiate the recovery plan communicated to relevant stakeholders? 22. Who has the authority to initiate the recovery portion of the incident response plan? 23. Are there clear triggers or criteria for when the recovery plan should be executed? 24. How is the initiation of the recovery plan documented? 25. Is there a checklist or procedure to ensure all necessary steps are taken when initiating recovery? 26. How quickly is the recovery plan typically initiated after an incident is identified? 27. Are there regular drills or exercises to practice the initiation of the recovery plan? 28. How is the effectiveness of the recovery plan initiation process evaluated? 29. What metrics are used to measure the timeliness and efficiency of recovery plan initiation? 30. Is there a process to review and update the	

	recovery plan initiation procedure based on lessons learned? 31. How are dependencies between incident response and recovery processes managed?	
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	21. What process is in place for selecting appropriate recovery actions? 22. How are recovery actions prioritized? Is there a formal methodology? 23. What criteria are used to determine the scope of recovery actions? 24. Who is responsible for approving the selected recovery actions? 25. How are recovery actions documented and tracked during execution? 26. Is there a system in place to manage and coordinate multiple recovery actions simultaneously? 27. How are the interdependencies between different recovery actions considered? 28. What tools or technologies are used to support the execution of recovery actions? 29. How is the progress of recovery actions monitored and reported? 30. Is there a process for adjusting recovery actions if initial efforts are not effective? 31. How are resource allocations determined for each recovery action? 32. What measures are in place to ensure the continuity of critical operations during recovery?	
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	1. What methods are used to verify the integrity of backups before restoration? 2. How frequently are integrity checks performed on backup data? 3. Is there a documented procedure for verifying restoration assets? 4. Who is responsible for performing integrity checks on backups and restoration assets? 5. What tools or technologies are used to support the verification process? 6. How are the results of integrity checks documented and stored? 7. Is there a process in place to address situations where backup integrity is compromised? 8. How quickly can the integrity of backups be verified in an emergency situation? 9. Are there different verification processes for different types of backup data or systems?	

NIST CSF 2.0 AUDIT CHECKLIST

	10. How is the chain of custody maintained for backups and restoration assets? 11. Is there a process for regularly testing the restoration process using verified backups? 12. How are integrity verification failures investigated and resolved?	
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	19. How are critical mission functions identified and prioritized during recovery planning? 20. What process is used to assess cybersecurity risks when establishing post-incident operational norms? 21. How are stakeholders involved in defining post-incident operational norms? 22. Is there a documented methodology for balancing operational needs with security requirements? 23. How are changes to operational norms communicated and implemented across the organization? 24. What metrics are used to evaluate the effectiveness of post-incident operational norms? 25. Is there a process for regularly reviewing and updating post-incident operational norms? 26. How are lessons learned from previous incidents incorporated into operational norm planning? 27. What considerations are given to regulatory compliance when establishing post-incident norms? 28. How is the impact on business continuity assessed when defining new operational norms? 29. What role does the cybersecurity team play in establishing post-incident operational norms? 30. How are trade-offs between security and functionality documented and approved?	
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is	25. What methods are used to verify the integrity of restored assets? 26. How is the restoration of systems and services validated? 27. What criteria are used to confirm normal operating	

confirmed 	status? 28. Who is responsible for declaring that systems and services have been fully restored? 29. Is there a formal sign-off process for each restored system or service? 30. How are discrepancies or issues during the restoration process addressed? 31. What tools or technologies are used to support the verification of restored assets? 32. How is the performance of restored systems compared to pre-incident baselines? 33. Is there a process for conducting post-restoration security assessments? 34. How are stakeholders notified about the status of system and service restoration? 35. What documentation is maintained throughout the restoration and verification process? 36. How are partial restorations or phased recovery approaches managed and communicated?	
RC.RP-06: The end of incident recovery is declared based on criteria, and incident related documentation is completed	26. What specific criteria are used to declare the end of incident recovery? 27. Who has the authority to officially declare the end of incident recovery? 28. How is the declaration of recovery completion communicated to all relevant stakeholders? 29. What incident-related documentation is required to be completed? 30. Is there a checklist or template for ensuring all necessary documentation is completed? 31. Who is responsible for reviewing and approving the final incident documentation? 32. How is the completion of all recovery actions verified before declaring the end of recovery? 33. Is there a formal process for transitioning from recovery mode to normal operations? 34. How are lessons learned captured and incorporated into future incident response and recovery plans? 35. What metrics are used to evaluate the overall effectiveness of the recovery process? 36. Is there a post-incident review process to identify areas for improvement? 37. How long after the incident is the documentation typically completed and filed?	

NIST CSF 2.0 AUDIT CHECKLIST

Category	**Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties	
Subcategory	**Audit Questionnaire**	**Compliance Status**
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	27. Is there a documented process for communicating recovery activities and progress to designated stakeholders? 28. How are internal stakeholders identified and categorized for recovery communications? 29. How are external stakeholders identified and categorized for recovery communications? 30. What methods are used to communicate recovery progress to internal stakeholders? 31. What methods are used to communicate recovery progress to external stakeholders? 32. How frequently are updates on recovery activities and progress communicated to stakeholders? 33. Is there a system in place to track which stakeholders have been informed of recovery progress? 34. How is the effectiveness of recovery communications measured and evaluated? 35. Who is responsible for coordinating and overseeing recovery communications? 36. How are recovery communications tailored to different stakeholder groups?	
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	28. Is there a documented policy for sharing public updates on incident recovery? 29. What are the approved methods for sharing public updates on incident recovery? 30. Who is responsible for drafting and approving public messages about incident recovery? 31. Is there a pre-approved messaging template or framework for public incident recovery updates? 32. How is the timing of public updates determined? 33. What measures are in place to ensure consistency between public messaging and internal/stakeholder communications? 34. How is the effectiveness and reach of public updates measured? 35. What protocols are in place to handle media inquiries about incident recovery? 36. How are public updates coordinated with legal, PR, and other relevant departments? 37. Is there a process for reviewing and updating public communication strategies based on lessons learned from previous incidents?	

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO