NIST CSF 2.0

AUDIT CHECKLIST

PART 1
GOVERN(GV)

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?	

	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?	
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	

NIST CSF 2.0 AUDIT CHECKLIST

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?	
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?	
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**

NIST CSF 2.0 AUDIT CHECKLIST

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?	
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?	
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**

NIST CSF 2.0 AUDIT CHECKLIST

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? 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?	

NIST CSF 2.0 AUDIT CHECKLIST

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	

NIST CSF 2.0 AUDIT CHECKLIST

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?	
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)? 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? 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?	

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?	

FOLLOW FOR MORE SUCH INFOSEC CHECKLIST, TEMPLATES AND DOCUMENTS

PLAYBOOK MADE WITH ❤

MINISTRY OF MOS SECURITY