

NIST CSF 2.0


AUDIT CHECKLIST

PART 2 IDENTIFY (ID)




NIST CSF 2.0 AUDIT CHECKLIST


NIST CSF 2.0 Audit Checklist

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 	<ol style="list-style-type: none"> Does the organization maintain a comprehensive inventory of all hardware assets under its management? What types of hardware assets are included in the inventory (e.g., servers, workstations, network devices, mobile devices, IoT devices)? How does the organization ensure that the hardware inventory is accurate and up-to-date? Is there a defined process for adding new hardware assets to the inventory and removing decommissioned or retired assets? Does the hardware inventory include relevant details such as asset owner, location, configuration, and security controls? How is the hardware inventory information used to support cybersecurity risk management activities? Are there mechanisms in place to monitor and detect unauthorized or unmanaged hardware assets within the organization's environment? Does the organization have a centralized system or database for maintaining and managing the hardware inventory? Are there clear roles and responsibilities assigned for maintaining the hardware inventory? 	
ID.AM-02: Inventories of Software, Services, and Systems Managed by the Organization	<ol style="list-style-type: none"> Does the organization maintain inventories of all software, services, and systems under its management? What types of software, services, and systems are included in the inventories (e.g., applications, databases, cloud services, operating systems, network services)? How does the organization ensure that the software, services, and systems inventories are accurate and up-to-date? Is there a defined process for adding new software, services, and systems to the inventories and removing decommissioned or retired items? Do the inventories include relevant details such as software versions, licenses, configurations, and associated hardware assets? How are the software, services, and systems inventories used to support cybersecurity risk management activities? 	


NIST CSF 2.0 AUDIT CHECKLIST

	<ol style="list-style-type: none"> 7. Are there mechanisms in place to monitor and detect unauthorized or unmanaged software, services, and systems within the organization's environment? 8. Does the organization have a centralized system or database for maintaining and managing the software, services, and systems inventories? 9. Are there clear roles and responsibilities assigned for maintaining the software, services, and systems inventories? 	
<p>ID.AM-03: Representations of Authorized Network Communication and Data Flows</p> 	<ol style="list-style-type: none"> 1. Does the organization maintain representations of its authorized network communication and data flows, both internal and external? 2. What types of network communication and data flows are represented (e.g., application traffic, remote access, cloud services, partner connections)? 3. How does the organization ensure that the network communication and data flow representations are accurate and up-to-date? 4. Is there a defined process for updating the network communication and data flow representations when changes occur? 5. Do the network communication and data flow representations include relevant details such as source, destination, protocols, ports, and security controls? 6. How are the network communication and data flow representations used to support cybersecurity risk management activities? 7. Are there mechanisms in place to monitor and detect unauthorized or unmanaged network communication and data flows? 8. Does the organization have a centralized system or database for maintaining and managing the network communication and data flow representations? 9. Are there clear roles and responsibilities assigned for maintaining the network communication and data flow representations? 	


NIST CSF 2.0 AUDIT CHECKLIST

<p>ID.AM-04: Inventories of Services Provided by Suppliers</p>	<ol style="list-style-type: none"> 1. Does the organization maintain an inventory of services provided by its suppliers and third-party service providers? 2. What types of services provided by suppliers are included in the inventory (e.g., cloud services, managed services, outsourced services, software-as-a-service)? 3. How does the organization ensure that the inventory of supplier-provided services is accurate and up-to-date? 4. Is there a defined process for adding new supplier-provided services to the inventory and removing discontinued services? 5. Does the inventory of supplier-provided services include relevant details such as service descriptions, service level agreements, security controls, and risk assessments? 6. Are there mechanisms in place to monitor and detect unauthorized or unmanaged services provided by suppliers? 	
<p>ID.AM-05: Asset Prioritization Based on Classification, Criticality, Resources, and Impact</p> 	<ol style="list-style-type: none"> 1. Does the organization have a defined process for prioritizing its assets based on classification, criticality, resources, and impact on the mission? 2. What criteria or factors are used to determine the classification and criticality of assets (e.g., confidentiality, integrity, availability, regulatory requirements, business impact)? 3. How does the organization assess the resources required to protect and maintain different types of assets? 4. How does the organization evaluate the potential impact on its mission and objectives if specific assets are compromised or unavailable? 5. 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? 6. How is the asset prioritization information used to support cybersecurity risk management activities and resource allocation decisions? 7. Are there clear roles and responsibilities assigned for conducting asset prioritization activities? 8. Does the organization provide training or guidance to personnel involved in asset prioritization processes? 9. How does the organization's leadership oversee and ensure the effectiveness of the asset prioritization process? 10. Are there mechanisms in place to validate and audit the asset prioritization results for accuracy and consistency? 	


NIST CSF 2.0 AUDIT CHECKLIST

<p>ID.AM-07: Inventories of Data and Corresponding Metadata</p> 	<ol style="list-style-type: none"> 1. Does the organization maintain inventories of its data and corresponding metadata for designated data types? 2. What types of data are included in the inventories (e.g., sensitive data, proprietary data, customer data, intellectual property)? 3. What types of metadata are captured and maintained for the data inventories (e.g., data classification, data owners, access controls, retention policies)? 4. How does the organization ensure that the data and metadata inventories are accurate and up-to-date? 5. Is there a defined process for adding new data and metadata to the inventories and removing obsolete or decommissioned data? 6. Are there clear roles and responsibilities assigned for maintaining the data and metadata inventories? 	
<p>ID.AM-08: Life Cycle Management of Systems, Hardware, Software, Services, and Data</p>	<ol style="list-style-type: none"> 1. Does the organization have defined processes for managing systems, hardware, software, services, and data throughout their life cycles? 2. What stages of the life cycle are covered by the organization's management processes (e.g., acquisition, deployment, configuration, maintenance, disposal)? 3. How does the organization ensure that cybersecurity requirements and controls are integrated into the life cycle management processes? 4. Are there mechanisms in place to monitor and enforce compliance with the life cycle management processes? 5. 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? 6. Are there processes in place to address and mitigate any risks or vulnerabilities identified during the life cycle management activities? 7. Does the organization provide training or guidance to personnel involved in the life cycle management processes? 8. Are there mechanisms in place to measure and report on the performance of the life cycle management processes? 9. How does the organization incorporate lessons learned and best practices into the continuous improvement of its life cycle management processes? 	

NIST CSF 2.0 AUDIT CHECKLIST

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 	<ol style="list-style-type: none"> 1. Does the organization have a process in place to identify vulnerabilities in its assets (e.g., systems, applications, hardware, software)? 2. What sources of vulnerability information does the organization utilize (e.g., vendor advisories, threat intelligence feeds, vulnerability databases)? 3. How does the organization validate the identified vulnerabilities to ensure their relevance and applicability? 4. Is there a centralized repository or system for recording and tracking identified vulnerabilities? 5. Does the vulnerability information include details such as severity, impact, affected assets, and potential mitigations? 6. How does the organization ensure that vulnerability information is kept up-to-date and reflects the current state of its assets? 7. Are there clear roles and responsibilities assigned for the identification, validation, and recording of vulnerabilities? 8. Does the organization provide training or guidance to personnel involved in vulnerability management activities? 9. How does the organization's leadership oversee and monitor the effectiveness of the vulnerability identification and management processes? 10. Are there mechanisms in place to prioritize and address identified vulnerabilities based on risk assessments? 	
ID.RA-02: Receiving Cyber Threat Intelligence from Information Sharing Forums and Sources	<ol style="list-style-type: none"> 1. Does the organization have processes in place to receive and leverage cyber threat intelligence from information sharing forums and sources? 2. 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)? 3. How does the organization evaluate the reliability and credibility of the threat intelligence sources? 4. Is there a centralized system or database for collecting, storing, and analyzing the received threat intelligence? 5. How is the threat intelligence integrated into the organization's risk assessment and decision-making processes? 6. Are there mechanisms in place to analyze and 	


NIST CSF 2.0 AUDIT CHECKLIST

	<p>prioritize the threat intelligence based on its relevance and potential impact?</p> <ol style="list-style-type: none"> 7. Does the organization share relevant threat intelligence with its partners, suppliers, or other stakeholders as appropriate? 8. Are there clear roles and responsibilities assigned for the management and utilization of cyber threat intelligence? 9. Does the organization provide training or guidance to personnel involved in threat intelligence activities? 	
<p>ID.RA-03: Identification and Recording of Internal and External Threats</p> 	<ol style="list-style-type: none"> 1. Does the organization have a process in place to identify and record internal and external threats? 2. What sources of information does the organization utilize to identify internal threats (e.g., employee monitoring, data loss prevention, insider threat program)? 3. What sources of information does the organization utilize to identify external threats (e.g., threat intelligence feeds, security advisories, industry reports)? 4. Is there a centralized repository or system for recording and tracking identified internal and external threats? 5. Does the threat information include details such as threat actors, motivations, tactics, techniques, and potential impacts? 6. How does the organization ensure that threat information is kept up-to-date and reflects the current threat landscape? 7. Are there clear roles and responsibilities assigned for the identification and recording of internal and external threats? 8. Does the organization provide training or guidance to personnel involved in threat identification and management activities? 9. How does the organization's leadership oversee and monitor the effectiveness of the threat identification and management processes? 10. Are there mechanisms in place to prioritize and address identified threats based on risk assessments? 	


NIST CSF 2.0 AUDIT CHECKLIST

<p>ID.RA-04: Identification and Recording of Potential Threat Impacts and Likelihoods</p>	<ol style="list-style-type: none"> 1. Does the organization have a process in place to identify and record the potential impacts and likelihoods of threats exploiting vulnerabilities? 2. What methodologies or frameworks does the organization use to assess the potential impacts of threats (e.g., business impact analysis, risk assessment frameworks)? 3. How does the organization determine the likelihood of threats being realized or vulnerabilities being exploited? 4. Is there a centralized repository or system for recording the assessed impacts and likelihoods of threats and vulnerabilities? 5. Does the impact and likelihood information include details such as risk scores, risk levels, and potential consequences? 6. How does the organization ensure that the impact and likelihood assessments are kept up-to-date and reflect changes in the risk landscape? 7. Are there clear roles and responsibilities assigned for the assessment and recording of threat impacts and likelihoods? 8. Does the organization provide training or guidance to personnel involved in risk assessment activities? 9. How does the organization's leadership oversee and monitor the effectiveness of the impact and likelihood assessment processes? 10. Are there mechanisms in place to prioritize and address identified risks based on their assessed impacts and likelihoods? 	
<p>ID.RA-05: Utilization of Threats, Vulnerabilities, Likelihoods, and Impacts for Risk Understanding and Response Prioritization</p> 	<ol style="list-style-type: none"> 1. Does the organization utilize the information on threats, vulnerabilities, likelihoods, and impacts to understand its inherent cybersecurity risk? 2. How does the organization integrate and correlate the information on threats, vulnerabilities, likelihoods, and impacts to develop a comprehensive risk picture? 3. Are there methodologies or frameworks in place to analyze and prioritize risks based on the assessed threats, vulnerabilities, likelihoods, and impacts? 4. How does the organization determine its risk tolerance and appetite levels, and how are these factored into the risk analysis and prioritization? 5. Is there a centralized system or dashboard for presenting and reporting the organization's overall cybersecurity risk posture? 6. How does the organization utilize the risk analysis and prioritization to inform its risk response strategies and decision-making? 	


NIST CSF 2.0 AUDIT CHECKLIST

	<ol style="list-style-type: none"> 7. Are there clear roles and responsibilities assigned for the analysis and prioritization of cybersecurity risks? 8. Does the organization provide training or guidance to personnel involved in risk analysis and decision-making activities? 9. How does the organization's leadership oversee and monitor the effectiveness of the risk analysis and prioritization processes? 10. 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? 	
<p>ID.RA-06: Selection, Prioritization, Planning, Tracking, and Communication of Risk Responses</p> 	<ol style="list-style-type: none"> 1. Does the organization have a process in place for selecting, prioritizing, planning, tracking, and communicating risk responses? 2. What types of risk responses does the organization consider (e.g., accept, avoid, mitigate, transfer)? 3. How does the organization prioritize and select appropriate risk responses based on the assessed risks and organizational objectives? 4. Are there mechanisms in place to develop and document risk response plans, including assigned responsibilities and timelines? 5. How does the organization track the implementation and effectiveness of the selected risk responses? 6. Are there processes in place to communicate the selected risk responses and associated plans to relevant stakeholders within the organization? 7. Does the organization involve external stakeholders (e.g., partners, suppliers) in the risk response planning and communication processes, as appropriate? 8. Are there clear roles and responsibilities assigned for the selection, prioritization, planning, tracking, and communication of risk responses? 9. Does the organization provide training or guidance to personnel involved in risk response activities? 10. How does the organization's leadership oversee and monitor the effectiveness of the risk response processes? 	


NIST CSF 2.0 AUDIT CHECKLIST

<p>ID.RA-07: Management, Assessment, Recording, and Tracking of Changes and Exceptions</p> 	<ol style="list-style-type: none"> 1. Does the organization have a process in place for managing, assessing, recording, and tracking changes and exceptions? 2. What types of changes and exceptions are subject to this process (e.g., changes to systems, configurations, policies, processes)? 3. How does the organization assess the potential risk impact of proposed changes or exceptions? 4. Is there a centralized repository or system for recording and tracking changes and exceptions, along with their associated risk assessments? 5. Does the change and exception management process include mechanisms for approving, rejecting, or deferring proposed changes or exceptions based on their risk impact? 6. How does the organization ensure that approved changes or exceptions are implemented and tracked according to established procedures? 7. Are there clear roles and responsibilities assigned for the management, assessment, recording, and tracking of changes and exceptions? 8. Does the organization provide training or guidance to personnel involved in change and exception management activities? 9. How does the organization's leadership oversee and monitor the effectiveness of the change and exception management processes? 10. Are there mechanisms in place to continuously monitor and assess the risk impact of implemented changes or exceptions over time? 	
<p>ID.RA-08: Processes for Receiving, Analyzing, and Responding to Vulnerability Disclosures</p>	<ol style="list-style-type: none"> 1. Does the organization have established processes for receiving, analyzing, and responding to vulnerability disclosures? 2. What channels or mechanisms are in place for receiving vulnerability disclosures (e.g., vendor notifications, security researchers, public disclosures)? 3. How does the organization analyze and validate the credibility and severity of received vulnerability disclosures? 4. Does the organization have a centralized system or database for recording and tracking vulnerability disclosures? 5. What information is captured and maintained for each vulnerability disclosure (e.g., description, affected assets, severity, mitigation guidance)? 6. Are there defined criteria or processes for prioritizing the analysis and response to vulnerability disclosures? 7. How does the organization determine and implement appropriate mitigation or remediation 	


NIST CSF 2.0 AUDIT CHECKLIST

	<p>actions in response to validated vulnerability disclosures?</p> <ol style="list-style-type: none"> 8. Are there mechanisms in place to communicate relevant vulnerability information and mitigation guidance to stakeholders and affected parties? 9. Are there clear roles and responsibilities assigned for receiving, analyzing, and responding to vulnerability disclosures? 10. How does the organization's leadership oversee and ensure the effectiveness of the vulnerability disclosure management processes? 	
<p>ID.RA-09: Assessing the Authenticity and Integrity of Hardware and Software</p> 	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Does the organization have processes in place to assess critical suppliers prior to acquisition or engagement? 2. 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)? 3. How does the organization gather and evaluate information about potential critical suppliers (e.g., reputation, financial stability, security posture, compliance certifications)? 4. Are there defined risk assessment methodologies or frameworks used to assess the potential risks associated with critical suppliers? 5. Does the organization maintain records or documentation of the critical supplier assessments performed? 6. How does the organization handle situations where the risk assessment of a critical supplier reveals significant concerns or issues? 7. Are there mechanisms in place to monitor and periodically reassess the risks associated with critical suppliers during the course of the engagement? 8. 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 	<ol style="list-style-type: none"> 1. Does the organization have a process for conducting evaluations of its cybersecurity risk management program and related activities? 2. What types of evaluations are performed (e.g., internal audits, external assessments, maturity assessments, compliance reviews)? 3. How does the organization ensure that the evaluations are comprehensive, objective, and aligned with industry standards and best practices? 4. Does the organization maintain documentation or reports from the conducted evaluations? 5. Are there mechanisms in place to analyze the evaluation findings and identify opportunities for improvement? 6. How does the organization prioritize and select the improvements to be implemented based on the evaluation results? 7. Is there a defined process for planning, 	

NIST CSF 2.0 AUDIT CHECKLIST

	<p>implementing, and tracking the identified improvements?</p> <p>8. Are there clear roles and responsibilities assigned for conducting evaluations and identifying improvements?</p>	
<p>ID.IM-02: Identifying Improvements from Security Tests and Exercises</p> 	<ol style="list-style-type: none"> 1. Does the organization conduct security tests and exercises to identify potential improvements in its cybersecurity posture? 2. What types of security tests and exercises are performed (e.g., penetration testing, vulnerability assessments, tabletop exercises, incident response simulations)? 3. How does the organization ensure that the security tests and exercises are realistic, comprehensive, and aligned with its risk profile? 4. Are relevant suppliers and third parties involved in the planning and execution of security tests and exercises, where appropriate? 5. Does the organization maintain documentation or reports from the conducted security tests and exercises? 6. Are there mechanisms in place to analyze the results of security tests and exercises and identify opportunities for improvement? 7. How does the organization prioritize and select the improvements to be implemented based on the security test and exercise results? 8. Is there a defined process for planning, implementing, and tracking the identified improvements? 9. Are there clear roles and responsibilities assigned for conducting security tests and exercises, and identifying improvements? 	
<p>ID.IM-03: Identifying Improvements from Operational Processes, Procedures, and Activities</p>	<ol style="list-style-type: none"> 1. Does the organization have a process for identifying potential improvements during the execution of operational processes, procedures, and activities? 2. What types of operational processes, procedures, and activities are assessed for improvement opportunities (e.g., incident response, change management, access control, backup and recovery)? 3. How does the organization gather feedback and input from personnel involved in the execution of operational processes, procedures, and activities? 4. Are there mechanisms in place to analyze the feedback and identify potential areas for improvement or optimization? 5. How does the organization prioritize and select the improvements to be implemented based on the feedback and analysis? 	

NIST CSF 2.0 AUDIT CHECKLIST

	<ol style="list-style-type: none"> 6. Is there a defined process for planning, implementing, and tracking the identified improvements? 7. Are there clear roles and responsibilities assigned for identifying and implementing improvements to operational processes, procedures, and activities? 	
<p>ID.IM-04: Establishing, Communicating, Maintaining, and Improving Incident Response and Other Cybersecurity Plans</p> 	<ol style="list-style-type: none"> 1. Does the organization have established incident response plans and other cybersecurity plans that affect operations? 2. 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? 3. Are the incident response and other cybersecurity plans communicated to all relevant stakeholders, including personnel, suppliers, and relevant third parties? 4. 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? 5. 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? 6. Does the organization conduct tests or exercises to validate the effectiveness of the incident response and other cybersecurity plans? 7. Are there mechanisms in place to gather feedback and identify potential improvements to the incident response and other cybersecurity plans? 8. How does the organization prioritize and implement identified improvements to the incident response and other cybersecurity plans? 9. Are there clear roles and responsibilities assigned for establishing, maintaining, and improving the incident response and other cybersecurity plans? 	

DID YOU FIND THIS CHECKLIST USEFUL

**FOLLOW FOR FREE INFOSEC
CHECKLISTS | PLAYBOOKS
TRAININGS | VIDEOS**



WWW.MINISTRYOFSECURITY.CO