Cybersecurity

Topical Requirement

User Guide

The Institute of
Internal Auditors

Contents

Overview of Topical Requirements

Topical Requirements are an essential component of the International Professional Practices Framework®, along with the Global Internal Audit Standards™ and Global Guidance. The Institute of Internal Auditors requires the Topical Requirements to be used in conjunction with the Global Internal Audit Standards, which provide the authoritative basis of the required practices. References to the Standards appear throughout this guide as a source of more detailed information.

Topical Requirements formalize how internal auditors address prevalent risk areas to promote quality and consistency within the profession. Topical Requirements establish a baseline and provide relevant criteria for performing assurance services related to the subject of a Topical Requirement (Standard 13.4 Evaluation Criteria). Conformance with Topical Requirements is mandatory for assurance services and recommended for evaluation during advisory services. Topical Requirements are not intended to cover all potential aspects that should be considered when performing assurance engagements; rather, they are intended to provide a minimum set of requirements to enable a consistent, reliable assessment of the topic.

Topical Requirements clearly link to The IIA's Three Lines Model and the Global Internal Audit Standards. Governance, risk management, and control processes are the main components of Topical Requirements aligning with Standard 9.1 Understanding Governance, Risk Management, and Control Processes. In reference to the Three Lines Model, governance links to the board/governing body, risk management links to the second line, and controls or control processes link to the first line. While management is represented in both the first and second lines, the internal audit function is depicted in the third line as an independent and objective assurance provider, reporting to the board/governing body (Principle 8 Overseen by the Board).

Applicability, Risk, and Professional Judgment

Topical Requirements must be followed when internal audit functions perform assurance engagements on subjects for which a Topical Requirement exists or when aspects of the Topical Requirement are identified within other assurance engagements.

As described in the Standards, assessing risk is an important part of the chief audit executive's planning. Determining the assurance engagements to include in the internal audit plan requires assessing the organization's strategies, objectives, and risks at least annually (Standard 9.4 Internal Audit Plan). When planning individual assurance engagements,

internal auditors must assess risks relevant to the engagement (Standard 13.2 Engagement Risk Assessment).

When the subject of a Topical Requirement is identified during the risk-based internal audit planning process and is included in the audit plan, then the requirements outlined in the Topical Requirement must be used to assess the topic within the applicable engagements. In addition, when internal auditors perform an engagement (either included or not included in the plan) and elements of a Topical Requirement emerge, the Topical Requirement must be assessed for applicability as part of the engagement. Lastly, if an engagement is requested that was not originally in the plan and includes the topic, the Topical Requirement must be assessed for applicability.

Professional judgment plays a key role in the application of the Topical Requirement. Risk assessments drive chief audit executives' decisions about which engagements to include in the internal audit plan (Standard 9.4 Internal Audit Plan). Additionally, internal auditors use professional judgment to determine what aspects will be covered within each engagement (Standards 13.3 Engagement Objectives and Scope, 13.4 Evaluation Criteria, and 13.6 Work Program). Appendix A "Practical Application Examples" describes how internal auditors determine whether the Topical Requirement applies.

Evidence that each requirement in the Topical Requirement was assessed for applicability must be retained, including a rationale explaining the exclusion of any requirements. Conformance with the Topical Requirement must be documented using auditor professional judgment as described in Standard 14.6 Engagement Documentation.

While the Cybersecurity Topical Requirement provides a baseline of control processes to consider, organizations that evaluate cyber risk as very high may need to assess additional aspects.

If a chief audit executive determines that the internal audit function does not have the required knowledge to perform audit engagements on a Topical Requirement subject, the engagement work may be outsourced (Standards 3.1 Competency, 7.2 Chief Audit Executive Qualifications,10.2 Human Resources Management). Even then, outsourcing does not release the internal audit function from its responsibility for conforming with the Topical Requirements. The chief audit executive retains the ultimate responsibility for ensuring conformance. In addition, if the chief audit executive determines internal audit resources are insufficient, the chief audit executive must inform the board about the impact of insufficient resources and how any resource shortfalls will be addressed (Standard 8.2 Resources).

Performance, Documentation, and Reporting

When applying Topical Requirements, internal auditors also must conform with the Standards, conducting their work in alignment with Domain V: Performing Internal Audit Services. The standards in Domain V describe planning engagements (Principle 13 Plan Engagements Effectively), conducting engagements (Principle 14 Conduct Engagement Work), and communicating engagement results (Principle 15 Communicate Engagement Results and Monitor Action Plans).

Coverage of the Topical Requirement can be documented in either the internal audit plan or the engagement workpapers based on auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions.

The optional tool in Appendix C can be used as a reference and to document the work internal auditors perform.

Quality Assurance

The Standards require the chief audit executive to develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the internal audit function (Standard 8.3 Quality). The results must be communicated to the board and senior management. Communications must report on the internal audit function's conformance with the Standards and achievement of performance objectives.

Conformance with Topical Requirements will be evaluated in quality assessments. To prepare for a quality review, internal auditors may use the tool provided as Appendix C.

Cybersecurity

Cybersecurity is a broad topic related to most technological aspects of any organization. In addition to information technology, cybersecurity is commonly part of business processes, necessitating that internal auditors assess cyber-related risks when planning, scoping, and performing assurance engagements.

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, defines cybersecurity simply as "The ability to protect or defend the use of cyberspace from cyber attacks." The Cybersecurity Topical Requirement focuses on the external perimeter that organizations secure to mitigate risks from unauthorized users and malicious cyber threats. Cybersecurity is a subset of overarching information security, which NIST defines as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Requirements of the Cybersecurity Topical Requirement include:

- Governance – clearly defined baseline cybersecurity objectives and strategies that support organizational goals, policies, and procedures.
- Risk Management – processes to identify, analyze, manage, and monitor cyber threats, including a process to escalate cyber risks promptly.
- Controls – management-established, periodically evaluated control processes to mitigate cyber risk.

Considerations

Internal auditors may use the following considerations to aid their assessment of the requirements in the Cybersecurity Topical Requirement. These considerations, which cross-reference to the requirements, are illustrative but not mandatory. Internal auditors should rely on professional judgment when determining what to include in their assessments.

Governance Considerations

To assess how the governance processes are applied to cybersecurity objectives, internal auditors may review:

A. Formalized, documented cybersecurity strategic plan and objectives, including evidence that the board periodically (generally quarterly) reviews the cybersecurity updates provided by the head of the information security function, such as the chief information security officer (CISO). Evidence may include reporting on:
   - Monitoring the achievement of strategic objectives.
   - Budgetary needs to support cybersecurity goals and objectives.
   - Focus on risks and internal controls, including remediation progress.
   - Key performance indicators (KPIs) to measure success.
   - Human resources needed to hire, train, and develop cybersecurity personnel.

B. Policies, procedures, and other relevant documentation used to manage cybersecurity processes, including:
   - Policies that are reviewed and updated at least annually. Emerging cyber risks may necessitate that reviews and updates occur more frequently.
   - A process to determine whether policies and procedures are sufficient to support cybersecurity operations.
   - Widely adopted frameworks (NIST, COBIT, and others) to strengthen cybersecurity processes and internal controls.

C. Roles and responsibilities that support the achievement of cybersecurity objectives, including a structure that ensures that the cybersecurity function reports to a level in the organization that has sufficient visibility to achieve organizational support.
   - A process to periodically assess the knowledge, skills, and abilities of the personnel filling cybersecurity roles.

D. Evidence of engagement with relevant stakeholders (for example, senior management, operations, risk management, human resources, legal, compliance, strategic vendors, and others), including communication about existing and emerging cyber risks and known potential vulnerabilities. Evidence of communication may include meeting minutes, reports, or emails.

Risk Management Considerations

To assess how risk management processes are applied to cybersecurity objectives, internal auditors may review:

A. How the organization assesses and manages cybersecurity risk, including how threats and vulnerabilities are:
   - Initially identified and reported.
   - Analyzed to evaluate the risk to achieving organizational objectives.
   - Mitigated, including action plans to reduce risk to an acceptable level.
   - Monitored, including a plan for ongoing reporting until threats are fully resolved.

B. How the organization obtains periodic input regarding cybersecurity risk management from functional areas, such as information technology, enterprise risk management, human resources, legal, compliance, operations, accounting, and finance. A cross-functional cybersecurity team or IT steering committee may be used to obtain information.

C. How the organization has assigned the accountability and responsibility for cybersecurity risk management to an individual or team.
   - The person(s) responsible should communicate ongoing cybersecurity risk updates throughout the organization periodically (quarterly, monthly, or as needed) and may also include resource requirements for risk mitigation strategies.

D. The escalation processes for cybersecurity risks, including how the level of threat or risk is evaluated, assigned, and prioritized. The review may include identifying the:
   - Organization's defined risk levels – such as high, moderate, and low – with detailed explanations of each risk level and escalation procedures for each risk category.
   - List of cybersecurity risks currently identified and the mitigation status of each risk event.
   - Applicable legal, regulatory, and compliance requirements.
   - Both financial and nonfinancial (for example, reputation) risk impacts.

E. The process for communicating cybersecurity risks to management and employees, which includes:
   - Periodic (at least annually) employee cybersecurity training, such as unannounced, simulated phishing campaigns to test and track organizational awareness.
   - Updates on the remediation of existing cybersecurity issues, with anticipated completion dates.

- Monitoring noncompliance that includes updates to the board and senior management.
- Reassessing threats when the organization's risk appetite and risk tolerance changes.

F. Processes the organization has implemented regarding incident response and recovery, which include:

- A documented plan that is reviewed and updated as the organization's operations change over time. The plan should include:
  - How incidents are detected and reported.
  - How incidents are contained to prevent further damage.
  - How the organization will recover and respond to resume operations.
  - How the incident will be analyzed to identify lessons learned and how to prevent similar future events.
- Periodic (at least annually) testing (tabletop exercise) and reporting the results to senior management and relevant stakeholders. Action plans may result from the testing.

Control Process Considerations

To assess how control processes are applied to cybersecurity objectives, internal auditors may review:

A. Management's approach for building an effective cybersecurity internal control environment, including:

- Assessing and implementing the internal controls required to both mitigate elevated risks and protect sensitive, critical, personal, or confidential data, informed by the organizational risk assessment process.
- Determining resource requirements to maintain key cybersecurity controls.
- Considering vendor-based controls as part of the control environment, which includes reviewing service organization controls (SOC) reports from vendors before commencing the business relationship and throughout the term of the relationship.
- Periodic testing that cybersecurity controls are functioning in a manner that mitigates risks and supports achievement of cybersecurity objectives.
- Process for remediating internal control deficiencies or addressing findings from assessments performed by the internal audit function or other assurance providers (for example, penetration testing).

B. The organization's talent management process for recruiting and training cybersecurity professionals, including how the organization identifies opportunities to

increase cybersecurity professionals' capabilities to support technical knowledge and improve organizational awareness of emerging issues.

- Examples include participation in training, involvement with knowledge-sharing groups, and continuing professional education that includes achievement of cyber-related certifications.

C. Management's process for identifying, prioritizing, monitoring, and reporting emerging cybersecurity threats and vulnerabilities on a continuous basis that is focused on daily operations. The review may include that processes are established to assess threats and vulnerabilities related to new or emerging technologies such as the use of artificial intelligence.

D. Management's processes and controls established to manage and protect IT assets throughout the life cycle including the selection, usage, maintenance, and decommissioning of hardware, software, and vendor services. Hardware includes servers, networking equipment (such as routers or firewalls), desktops, laptops, cell phones, tablets, and peripherals. Software includes operating systems (such as Windows), enterprise resource planning software, applications, antivirus programs, and others. Hardware and software considerations may include:

- The organization's use of encryption, antivirus software, mobile device management, complex password requirements, virtual private network (VPN)/ zero trust networking (ZTN) for authentication, and periodic updating of firmware.
- An asset management process that ensures that company-issued hardware has an appropriate security configuration upon issuance and proper disposal when assets are retired.
- Database-related controls that include limiting user and administrator access, ensuring the use of encryption, the backup and testing of databases, and the presence of strong network security controls.
- How cybersecurity threats or vulnerabilities are considered in the system development life cycle (SDLC).
- The approach used by development, security, and operations (DevSecOps) to ensure the software development process includes cybersecurity to identify vulnerabilities proactively.

E. Processes used to strengthen cybersecurity, including:

- Configuration of security settings to minimize cybersecurity risk.
- Mobile device administration (including use of email and applications) is configured to mitigate cybersecurity risks and be remotely managed if a user's device is compromised.
- The use of encryption for data "at rest," such as information stored on a hard drive, or data "in transit," such as encrypting emails.
- Patching servers or software (such as an operating system) with the latest security releases.

- User access management such as the use of multifactor authentication (MFA) and unique user IDs with complex passwords that periodically expire.
- Monitoring controls in place to determine whether availability and resource utilization are performing adequately, allowing the review and analysis of potential cybersecurity issues that threaten performance.
- Integration of cybersecurity into the SDLC to identify and address cybersecurity vulnerabilities before software is moved into production.

F. Network-related controls that secure the organization's perimeter, including how the organization utilizes:
   - Network segmentation.
   - Firewalls.
   - User-access controls.
   - Limitations to both external and internal connections.
   - Controls surrounding the Internet of Things (IoT) for interconnected networks.
   - Intrusion detection/prevention systems to prevent, detect, and recover from cybersecurity attacks.

G. Controls surrounding endpoint-communication security controls applicable to services such as email, internet browsers, video conferencing, messaging (Zoom, MS Teams, and others), social media, cloud, and file-sharing protocols. Controls may include restricting the use of certain file extensions (such as .exe files) and multifactor authentication for file sharing.

Appendix A. Practical Application Examples

The following examples describe scenarios in which the Cybersecurity Topical Requirement would be applicable:

Example 1: Cybersecurity is identified for an internal audit engagement included in the internal audit plan.

When the internal audit function completes its risk-based planning process and includes one or more engagements on cybersecurity in the internal audit plan, the Topical Requirement is mandated when conducting such engagements. Conformance may be achieved by including the requirements across one or more engagements in the internal audit plan.

Cybersecurity is a broad topic, and not every requirement in the Topical Requirement may apply in every engagement. When internal auditors apply professional judgment and determine that one or more requirements of the Cybersecurity Topical Requirement are not applicable and therefore should be excluded from an engagement, internal auditors must document and retain the rationale for excluding those requirements. For example, the rationale for excluding some requirements could be that the internal audit function performs various cybersecurity engagements on a rotational basis or has determined that the risk's significance in the engagement is low.

Example 2: Cybersecurity risks are identified during an audit engagement that is not focused on cybersecurity.

Internal auditors may identify cybersecurity risks while assessing a process not directly related to cybersecurity. For example, internal auditors may be assessing the accounts payable process in an engagement not focused on cybersecurity and do not identify cybersecurity risks as within the scope when planning the engagement. However, after performing the initial walkthrough, internal auditors determine that such risks should be in scope; for example, they identify cybersecurity risks related to the web-based submission of an initial purchase order request (Standard 13.2 Engagement Risk Assessment).

Once relevant risks have been identified, internal auditors must review the Cybersecurity Topical Requirement and determine which requirements are applicable. In this example, they might exclude the cybersecurity governance process or the cybersecurity risk management process. They must document in the engagement workpapers the rationale for excluding the other requirements of the Cybersecurity Topical Requirement and retain the documentation.

Example 3: A cybersecurity engagement that was not originally included in the internal audit plan is requested.

Stakeholders such as the board, management, or a regulator may ask internal auditors to perform cybersecurity assessments outside the original audit plan. For example, when organizations are the target of a cyberattack, the board may request an internal audit engagement to assess cybersecurity controls. The Topical Requirement is applicable, the requirements must be assessed, and any exclusions documented.

Appendix B. Mapping to Frameworks

The organization may have its own cybersecurity efforts, using risk management and governance frameworks such as COBIT or NIST. Internal auditors may have already developed audit programs and testing procedures based on these frameworks. Internal auditors should reconcile their intended cybersecurity control testing to the Topical Requirement to ensure adequate coverage. The chart below maps the Cybersecurity Topical Requirement to three commonly used frameworks: NIST Cybersecurity Framework 2.0, COBIT 2019, and NIST 800-53. These frameworks have been mapped as they are readily available at no cost.

Governance Requirements	Framework References		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. A formal cybersecurity strategy and objectives are established and periodically updated. Updates on the achievement of cybersecurity objectives are periodically communicated and reviewed by the board, including resources and budgetary considerations to support the cybersecurity strategy.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Policies and procedures related to cybersecurity are established, periodically updated, and strengthen the control environment.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Roles and responsibilities that support cybersecurity objectives are established, and a process exists to periodically assess the knowledge, skills, and abilities of those filling those roles.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Relevant stakeholders are engaged to discuss and act on existing vulnerabilities and emerging threats in the cybersecurity environment. Stakeholders include senior management, operations, risk management, human resources, legal, compliance, vendors, and others.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Risk Management Requirements	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. The organization's risk assessment and risk management processes include the identification, analysis, mitigation, and monitoring of cybersecurity threats and their effect on achievement of strategic objectives.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Cybersecurity risk management is conducted across the organization, which may include the following areas: information technology, enterprise risk management, human resources, legal, compliance, operations, supply chain, accounting, finance, and others.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Accountability and responsibility for cybersecurity risk management is established and an individual or team is identified to periodically monitor and report how cybersecurity risks are being managed, including the resources required to mitigate risk and identify emerging cybersecurity threats.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. A process is established to quickly escalate any cybersecurity risk (emerging or previously identified) that rises to an unacceptable level based on the organization's established risk management guidelines or to comply with applicable legal and regulatory requirements. Both the financial and nonfinancial impacts of cybersecurity risk should be considered.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. A process is established to communicate cybersecurity risk awareness to management and employees, and for the periodic review by management of issues, gaps, deficiencies, or control failures with reporting and remediation.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. The organization has implemented a cybersecurity incident response and recovery process that includes detection, containment, recovery, and post-incident analysis. The incident response and recovery process is periodically tested.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Control Process Requirements	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. A process is established that ensures both internal controls and vendor-based controls are in place to protect the confidentiality, integrity, and availability of the organization's systems and data. Controls are periodically evaluated to determine they are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and timely resolution of issues.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. A talent management process is established and periodically reviewed for cybersecurity operations that includes training opportunities to develop and maintain technical competencies.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. A process is established to continuously monitor and report emerging cybersecurity threats and vulnerabilities and to identify, prioritize, and implement opportunities to improve cybersecurity operations.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Cybersecurity is included in the life cycle management (selection, usage, maintenance, and decommissioning) of all IT assets, including hardware, software, and vendor services.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Processes are established to promote cybersecurity including configuration, end-user device administration, encryption, patching, user-access management, and monitoring availability and performance. Cybersecurity considerations are included in software development (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Network-related controls are established, such as network access controls and segmentation; the use and placement of firewalls; limited connections from and to external networks; virtual private network (VPN)/zero trust network access (ZTNA), inclusion of Internet of Things (IoT) network controls, and intrusion detection/prevention systems (IDS and IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. Endpoint communication security controls are established regarding services such as email, internet browsers, videoconferencing, messaging, social media, cloud, and file-sharing protocols.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Appendix C. Optional Documentation Tool

Internal auditors are expected to exercise professional judgment in determining the applicability of the requirements based on the risk assessment and appropriately document the exclusions of certain requirements. The Topical Requirement can be documented in the internal audit plan or in the engagement workpapers based on the auditor's professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. The printable form below provides one option for documenting conformance with the Cybersecurity Topical Requirement, but its use is not mandatory.

Cybersecurity – Governance

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
A. A formal cybersecurity strategy and objectives are established and periodically updated. Updates on the achievement of cybersecurity objectives are periodically communicated and reviewed by the board, including resources and budgetary considerations to support the cybersecurity strategy.		
B. Policies and procedures related to cybersecurity are established, periodically updated, and strengthen the control environment.		
C. Roles and responsibilities that support cybersecurity objectives are established, and a process exists to periodically assess the knowledge, skills, and abilities of those filling the roles.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
D. Relevant stakeholders are engaged to discuss and act on existing vulnerabilities and emerging threats in the cybersecurity environment. Stakeholders include senior management, operations, risk management, human resources, legal, compliance, vendors, and others.		

Cybersecurity – Risk Management

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
A. The organization's risk assessment and risk management processes include identifying, analyzing, mitigating, and monitoring cybersecurity threats and their effect on achievement of strategic objectives.		
B. Cybersecurity risk management is conducted across the organization and may include the following areas: information technology, enterprise risk management, human resources, legal, compliance, operations, supply chain, accounting, finance, and others.		
C. Accountability and responsibility for cybersecurity risk management are established. An individual or team is identified to periodically monitor and report how cybersecurity risks are being managed, including the resources required to mitigate risks and identify emerging cybersecurity threats.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
D. A process is established to quickly escalate any cybersecurity risk (emerging or previously identified) that reaches an unacceptable level according to the organization's established risk management guidelines or applicable legal and regulatory requirements. Financial and nonfinancial impacts of cybersecurity risk should be considered.		
E. A process is established to communicate cybersecurity risk awareness to management and employees and for management to periodically review issues, gaps, deficiencies, or control failures with timely reporting and remediation.		
F. The organization has implemented a cybersecurity incident response and recovery process, including detection, containment, recovery, and post-incident analysis. The incident response and recovery process is periodically tested.		

Cybersecurity – Control Processes

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
A. A process is established to ensure both internal controls and vendor-based controls are in place to protect the confidentiality, integrity, and availability of the organization's systems and data. Evaluations are performed periodically to determine whether the controls are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and prompt resolution of issues.		
B. A talent management process is established that includes training to develop and maintain technical competencies related to cybersecurity operations. The process is periodically reviewed.		
C. A process is established to continuously monitor and report emerging cybersecurity threats and vulnerabilities and to identify, prioritize, and implement opportunities to improve cybersecurity operations.		
D. Cybersecurity is included in the life cycle management (selection, usage, maintenance, and decommissioning) of all IT assets, including hardware, software, and vendor services.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
E. Processes are established to promote cybersecurity, including configuration, end-user device administration, encryption, patching, user-access management, and monitoring availability and performance. Cybersecurity considerations are included in software development (DevSecOps).		
F. Network-related controls are established, such as network access controls and segmentation; the use and placement of firewalls; limited connections from and to external networks; virtual private network (VPN)/zero trust network access (ZTNA), Internet of Things (IoT) network controls, and intrusion detection/prevention systems (IDS and IPS).		
G. Endpoint communication security controls are established for services such as email, internet browsers, videoconferencing, messaging, social media, cloud, and file-sharing protocols.		

About The Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information www.theiia.org.

Disclaimer

Copyright

February 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101