Cybersecurity

Topical Requirement

The Institute of
Internal Auditors

Cybersecurity Topical Requirement

The International Professional Practices Framework® comprises the Global Internal Audit Standards™, Topical Requirements, and Global Guidance. Topical Requirements are mandatory and must be used in conjunction with the Standards, which provide the authoritative basis for the required practices.

Topical Requirements provide clear expectations for internal auditors by setting a minimum baseline for auditing specified risk topics. The organization's risk profile may require internal auditors to consider additional aspects of the topic.

Conformance with Topical Requirements will increase the consistency with which internal audit services are performed and improve the quality and reliability of internal audit services and results. Ultimately, Topical Requirements elevate the internal audit profession.

Internal auditors must apply Topical Requirements in conformance with the Global Internal Audit Standards. Conformance with Topical Requirements is mandatory for assurance services and recommended for advisory services.

The Topical Requirement is applicable when the topic is one of the following:

A. The subject of an engagement in the internal audit plan.
B. Identified while performing an engagement.
C. The subject of an engagement request not on the original internal audit plan.

Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented and retained. Not all individual requirements may apply in every engagement; if requirements are excluded, a rationale must be documented and retained. Conformance with the Topical Requirement is mandatory and will be evaluated during quality assessments.

For more information, see the Cybersecurity Topical Requirement User Guide.

Cybersecurity

The National Institute of Standards and Technology (NIST) defines cybersecurity simply as, “The ability to protect or defend the use of cyberspace from cyberattacks.” 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.”

Cybersecurity reduces risk by strengthening the overall control environment and protecting an organization's information assets from unauthorized access, disruption, alteration, or destruction. Cyberattacks can lead to direct and indirect impacts that are often significant, as computers, networks, programs, data, and sensitive information are critical components of most organizations.

Evaluating and Assessing Cybersecurity Governance, Risk Management, and Control Processes

This Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes. The requirements represent a minimum baseline for assessing cybersecurity in an organization.

GOVERNANCE: Evaluating and Assessing Cybersecurity Governance

Requirements:

Internal auditors must assess the following in relation to the organization's cybersecurity governance:

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 and periodically updated to 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 the individuals filling the roles.
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.

RISK MANAGEMENT: Evaluating and Assessing Cybersecurity Risk Management

Requirements:

Internal auditors must assess the following in relation to the organization's cybersecurity risk management:

A. The organization's risk assessment and risk management processes include identifying, analyzing, mitigating, and monitoring cybersecurity threats and their effect on achieving 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.

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 that includes detection, containment, recovery, and post-incident analysis. The incident response and recovery process is periodically tested.

CONTROLS: Evaluating and Assessing Cybersecurity Control Processes

Requirements:

Internal auditors must assess the following in relation to the organization's cybersecurity control processes:

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.

E. Processes are established to strengthen 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, visit www.theiia.org.

Copyright

February 2025

The Institute of Internal Auditors

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