Cybersecurity Topical Requirement

What are Topical Requirements?

Topical Requirements are an essential component of the International Professional Practices Framework®, which also includes the Global Internal Audit Standards™ and Global Guidance. The Institute of Internal Auditors as the standard-setter for the profession of internal auditing requires these mandatory Topical Requirements as a supplement to the Global Internal Audit Standards, which serve as the authority for the required practices described and cross-referenced in the Topical Requirements.

Topical Requirements provide structure for frequently audited global topics that are typically higher risk and pervasive in nature. While the Standards apply to all internal audit services performed, a Topical Requirement must be considered as additional mandatory requirements to be followed when that subject is the focus of an internal audit engagement.

Topical Requirements are to be applied at the entity or organizational level to topics that have an impact across the organization. Internal auditors must be familiar with Topical Requirements and be ready to apply them when the topic is included in their annual audit plans or if that specific topic is the focus of an internal audit engagement. The elements of the Topical Requirement must be assessed when scoping the engagement. Evidence that the assessment and treatment of the subject occurred must be documented and retained. Engagements that include any aspect of the topic must assess the requirements relevant to the engagement or document why specific requirements are not applicable. A tool to assist internal auditors with explaining the rationale for including or excluding requirements is provided as Appendix B.

Why are Topical Requirements necessary?

The application of Topical Requirements is designed to strengthen the ongoing relevance of an internal audit function to the evolving global risk landscape and enhance the value of internal audit services across industries and sectors. Conforming with Topical Requirements will help internal auditors raise the quality and consistency of engagements.

Topical Requirements are structured to provide guidance for performing internal audit services in three areas: governance, risk management, and control processes. Each area includes:

- Requirements, which are mandatory and cover essential organizational objectives.
- Considerations, which are not mandatory but serve as best practices for evaluating the design and implementation of organizational objectives. Considerations, provided in Appendix A, should be utilized simply as examples to validate the requirements.

Conformance with Topical Requirements will be evaluated in quality assessments. To demonstrate conformance in preparation for a quality review, internal auditors should use the tool provided as Appendix B to indicate conformance with each requirement or to explain why conformance was not achieved.

Cybersecurity Topical Requirement

Evaluating and Assessing the Effectiveness of Cybersecurity Governance, Risk Management, and Control Processes

Cybersecurity protects an organization's information assets from unauthorized users, disruption, alteration, or destruction, and strengthens the overall control environment to reduce risk. 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. Since organizations rely heavily on information technology resources, having clearly defined a cybersecurity plan, objectives, inherent risks, and effective controls should be a priority for management.

This Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes.

GOVERNANCE: Evaluating and Assessing Cybersecurity Governance

Requirements:

When performing an internal audit engagement that includes cybersecurity objectives in its scope, internal auditors must assess whether the organization's governance processes adequately address cybersecurity. Internal auditors must assess whether:

A. Policies and procedures related to cybersecurity risk management processes are established and periodically updated, including promotion of practices that strengthen the control environment based on widely adopted frameworks (NIST, COBIT, and others).

B. Roles and responsibilities that support the organization's cybersecurity objectives are clearly established and those roles are filled by individuals with the required knowledge, skills, and abilities.

C. Updates to cybersecurity objectives, strategies, risks, and mitigating controls are periodically communicated to the board.

D. Relevant stakeholders (for example, leadership, operations, strategic vendors, and others) are engaged to discuss how to best establish and improve cybersecurity risk management processes.

E. Required resources (such as leadership, funding, talent, hardware, software, and training) necessary to effectively execute cybersecurity risk management processes are communicated to the board.

RISK MANAGEMENT: Evaluating and Assessing Cybersecurity Risk Management

Requirements:

When performing an internal audit engagement that includes cybersecurity objectives in its scope, internal auditors must assess whether the organization's risk management processes adequately address cybersecurity. Internal auditors must assess whether:

A. An organizationwide risk management process is established that includes the identification, analysis, and management of risks related to information technology and security, with a specific focus on cybersecurity risks and how those risks may affect the ability to achieve organizational objectives.

B. Cybersecurity risk management processes are conducted by a cross-functional team that includes information technology leadership, organizationwide risk management, legal, compliance, other management (operations,

accounting, finance, and others) and engages external parties (vendors, outsourced service providers, suppliers, customers, and others) as applicable.

C. Cybersecurity risk management policies and procedures have been established and are periodically updated, including promotion of practices that strengthen cybersecurity risk management processes based on widely adopted risk management frameworks, authoritative guidance, or other best practices.

D. Accountability and responsibility regarding the management of cybersecurity risks is established and an individual or team has been identified that periodically monitors and communicates how cybersecurity risks are being managed, including resource requirements to mitigate risks and the identification of emerging cybersecurity risks that had previously not been identified.

E. A process is established to quickly escalate any cybersecurity risks (emerging or previously identified) that rise to unacceptable levels based on the organization's established risk management guidelines or to comply with applicable legal and/or regulatory requirements.

F. Cybersecurity risk management includes the coordination between information security, legal, compliance, and other management to identify and comply with all legal and contractual obligations, such as laws and regulations. The status of both compliance and noncompliance with applicable requirements is communicated within the organization periodically.

G. A process is established to identify and manage cybersecurity risks related to third parties. Vendors, suppliers, and other providers of outsourced processes and/or services are contractually required to implement effective cybersecurity controls that adequately protect the confidentiality, integrity, and availability of the organization's systems and data to which third parties have access.

H. Policies and processes related to data classification, retention, destruction, and encryption are adequately designed and effectively deployed to provide a systematic approach that ensures complete and accurate recording of data and protects the confidentiality and privacy of sensitive information.

I. A process is established for communicating cybersecurity operational risks to ensure awareness by management and employees. Any issues, gaps, deficiencies, or control failures are communicated to the board and management, and the status of remediation is closely monitored and reported. Noncompliance with cybersecurity policies is identified, investigated, reported, and remediated in a timely manner.

CONTROLS: Evaluating and Assessing Cybersecurity Control Processes

Requirements:

When performing an internal audit engagement that includes cybersecurity objectives in its scope, internal auditors must assess whether the organization's control processes adequately address cybersecurity. Internal auditors must assess if the organization:

A. Prioritizes cybersecurity controls and ensures the related budget and resources (such as personnel, software, tools, and others) are allocated to maximize expected benefits.

B. Ensures that cybersecurity controls are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and timely resolution of issues.

C. Provides sufficient training to personnel responsible for cybersecurity operations.

D. Has developed sufficient policies and procedures to manage all aspects of cybersecurity operations and related controls.

E. Ensures that management has the resources necessary to stay informed about emerging cybersecurity issues from new technologies, identify opportunities to improve operations, and understand how cybersecurity efforts can best be deployed to impact broader organizational goals and objectives.

F. Adequately integrates cybersecurity into the system development life cycle for business applications, including software and acquired or custom-developed applications.

G. Has included cybersecurity in the management of hardware (such as laptops, desktops, mobile devices).

H. Has implemented effective controls regarding production hardware support, such as configuring, patching, supporting user access management, and monitoring availability and performance. The organization has evaluated both the design adequacy and operational effectiveness of these controls.

I. Optimizes network-related controls regarding network segmentation, the use and placement of firewalls, limited connections to external networks and/or systems, and the use of preventive and detective technologies such as intrusion detection/prevention systems.

J. Has implemented effective controls surrounding common desktop communication services such as email, internet browsers, videoconferencing, messaging, and file-sharing protocols.

K. Has implemented appropriate service delivery controls to ensure the following areas are integrated with cybersecurity monitoring: change management, service/help desk, and end-user device administration.

L. Has implemented appropriate physical security controls to protect high-risk information centers (such as data centers, network operations centers, and security operations centers) from attacks.

M. Has implemented incident response and recovery controls.

Related Standards:

3.1 Competency
4.2 Due Professional Care
9.1 Understanding Governance, Risk Management, and Control Processes
9.4 Internal Audit Plan
12.3 Oversee and Improve Engagement Performance
13.1 Engagement Communication
13.2 Engagement Risk Assessment
13.3 Engagement Objectives and Scope
13.4 Evaluation Criteria
13.5 Engagement Resources
13.6 Work Program
14.1 Gathering Information for Analyses and Evaluation
14.2 Analyses and Potential Engagement Findings
14.3 Evaluation of Findings
14.4 Recommendations and Action Plans
14.5 Engagement Conclusions
14.6 Engagement Documentation
15.1 Final Engagement Communication
15.2 Confirming the Implementation of Recommendations or Action Plans

Related Global Technology Audit Guides (GTAGs):

Assessing Cybersecurity Risk: The Three Lines Model
Auditing Business Applications
Auditing Cyber Incident Response and Recovery
Auditing Cybersecurity Operations: Prevention and Detection
Auditing Identity and Access Management
Auditing IT Governance
Auditing Mobile Computing
Auditing Network and Communications Management

Appendix A. Considerations

Considerations for Each Governance Requirement:

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

A. Policies, procedures, and other relevant documentation utilized by the organization to manage daily cybersecurity responsibilities, including:
   1. Documentation that is clear, concise, consistent, and updated periodically, ideally as emerging cybersecurity risks are identified and at least annually.
   2. Procedures related to identifying, analyzing, resolving, and reporting breaches or other loss of sensitive data.
   3. Documentation of how management ensures policies and procedures are sufficient to support cybersecurity operations.

B. Roles and responsibilities created by the board to support the achievement of the cybersecurity strategy, including a reporting structure that ensures cybersecurity reports to a level in the organization that has sufficient visibility to achieve organizational support.

C. Materials presented to the board about cybersecurity strategy, objectives, risks, and controls, including analyzing whether:
   1. Communication frequency is adequate, ideally occurring quarterly and presented by the head of the information security function, such as a chief information systems officer.
   2. The information presented is clear, concise, and consistent; risks and controls are communicated in a manner that would be easily understood by the board.
   3. Key performance indicators or other important cybersecurity metrics/statistics are included.
   4. Where appropriate, board input is received by management and implemented, with status updates of changes communicated back to the board.

D. Evidence of management's cybersecurity-related communications with relevant stakeholders (for example, leadership, operations, strategic vendors, and others), including that information communicated is clear, concise, consistent, and tailored to the stakeholder audience:
   1. Employees.
   2. Vendors, suppliers, outsourced service providers, and third parties.
   3. Customers.
   4. Strategic partners.

E. The analysis and communication of resource requirements by management, including:
   1. Understanding how gaps are identified and what key metrics are utilized to anticipate changes in requirements.
   2. How management works with human resources to analyze cybersecurity talent needs.
   3. How management analyzes current hardware and software inventories and determines whether additional investment is needed to support cybersecurity initiatives.
   4. Whether internal auditors review how management establishes and updates cybersecurity training materials and identifies gaps, including ensuring that training covers emerging cybersecurity objectives, risks, and controls.

Considerations for Each Risk Management Requirement:

To assess the required aspects of cybersecurity risk management, internal auditors may review:

A. How management initially identifies cybersecurity risks, including:
   1. Understanding which personnel are responsible for both daily threats the organization faces and emerging risks with the information security community.
      a. Determine whether these individuals have the related professional experience and training required to effectively recognize and escalate threats to the broader risk management team.
   2. Identifying the software applications or vendors that management relies upon to identify cybersecurity risks.
   3. Documentation related to the cybersecurity risk management process, including:
      a. Meeting minutes.
      b. Action items.
      c. Lists of attendees or team members.
      d. Post-incident investigation/root cause analysis.

B. How management identifies or nominates risk management team members and the related business rationale or qualifications utilized to evaluate membership. Review evidence of periodic engagement of cybersecurity risk discussions with relevant external parties.

C. The process the organization uses to establish and periodically update policies and procedures related to cybersecurity risk management, which may include:
   1. An annual review and approval of policies and procedures.
   2. An understanding of how the organization ensures compliance with its risk management policies and procedures and the way personnel are trained on the execution of policies and procedures.
      a. An understanding of which frameworks or authoritative guidance management uses to manage cybersecurity risks (NIST, COBIT, and others) and the way the organization confirms adherence to chosen framework(s).

D. The individual(s) responsible for executing cybersecurity risk management, including ensuring their professional background, experience, qualifications, and credentials are appropriate for managing information security risks and threats. Verify that the responsible individual is positioned at a level within the organization to bring visibility to cybersecurity risks and communicate those risks effectively .

E. The escalation processes the organization utilizes for communicating cybersecurity risks, including how threat or risk level is evaluated, assigned, and prioritized. Verify that the organization has defined risk levels, such as high, moderate, low, including a detailed explanation for each risk level and escalation procedures for each category of risk. Review listing of current cybersecurity risks identified and the mitigation status of each event.

F. The process the organization utilizes to ensure conformance with all applicable cybersecurity regulations, including:
   1. How proposed or recently adopted regulations affect the organization.
   2. If there is an inventory of applicable regulations that is monitored, updated, and reported upon periodically to ensure organizational awareness.
      a. For any noncompliance items, verify that management is aware of the associated risks, including through periodic reporting.

G. The organization's process for managing third-party cybersecurity risks. Verify that vendor cybersecurity controls are reviewed prior to commencing a business relationship and that contracts build in the right to periodic reviews throughout the relationship. Include obtaining and analyzing the third party's service organization controls report and verifying the organization has documented its SOC report review, which should include ensuring user control

considerations have been implemented. Gain an understanding of management's approach to determine if third parties have an appropriate control environment that is commensurate with the organization's controls.

a. If third-party control weaknesses are found, understand the process management uses to gain comfort that the weaknesses do not compromise cybersecurity related to operations, or understand how the organization communicates that changes are required to maintain the applicable vendor relationship or that potentially a replacement vendor should be found.

H. The policies and processes the organization has established related to:
   1. Data classification.
   2. Data retention.
   3. Data destruction.
   4. Encryption.
   5. Access/identity management.
   6. Who prepares, reviews, and updates the documentation, which ideally should include legal and compliance personnel to ensure conformance with applicable regulations.
   7. How the organization performs data classification to ensure confidential and private data have been identified and have the appropriate level of protection, such as limiting user access.
   8. How the organization periodically reviews the process used to classify data and whether the process continues to support organizational cybersecurity objectives and comply with organizational policies and applicable regulations.

I. The process for communicating cybersecurity operational risks to management and employees. Ideally, such communication should be included with periodic cybersecurity training (at least annually). Understand management's process for communicating updates on existing remediation of cybersecurity issues along with anticipated completion dates. Verify that noncompliance is monitored closely, and updates are provided to the board and senior management.

Considerations for Each Control Process Requirement:

To assess the required aspects of cybersecurity controls, internal auditors may review:

A. Management's process for determining how to deploy budgeted resources to support the cybersecurity control environment, which should include strategic planning annually to ensure an appropriate level of organizational resources are available to fulfill cybersecurity objectives. Formal, documented results of annual planning and periodic monitoring of resource management should be reviewed.

B. Management's process for periodically evaluating that cybersecurity controls are functioning in a manner that promotes achievement of organizational cybersecurity objectives. Verify that management monitors control effectiveness and evaluates whether existing controls are designed appropriately or new controls are required. In many organizations, the internal audit function plays a significant role in this process by providing assurance on the design of controls and whether controls are operating effectively through periodic (quarterly, annual) testing. Verify management's processes for remediating control deficiencies or addressing findings from assessments performed by the internal audit function or other assurance providers (for example, penetration testing).

C. Management's process to evaluate training needs for cybersecurity personnel within the organization and how resources are assigned to deliver appropriate education and ensure that emerging cybersecurity threats are understood and managed. Understand how management ensures that employees have sufficient cybersecurity training, which may include live training events, recorded instruction, or completion of training modules.

D. The organization's process for creating and updating cybersecurity policies and procedures and how management evaluates whether said policies and procedures are adequate. Understand how personnel responsible for

cybersecurity operations and controls are trained in complying with policies and procedures and how they are evaluated for internal compliance.

E. The organization's process for appropriately training the management team responsible for cybersecurity operations and controls to recognize emerging trends and provide their teams and the organization with strategic leadership. Understand how the organization identifies opportunities to increase management's capabilities to support awareness of emerging issues, such as participation in training and continuing professional education.

F. How the organization addresses cybersecurity within their system development life cycle, including the following control aspects
   1. Planning: Cybersecurity has been identified as a key component when assessing risks and analyzing potential vulnerabilities. The scope and objectives of the software implementation should be included as the organization evaluates cybersecurity controls during the planning phase.
   2. Gathering requirements: Cybersecurity requirements are a component when defining functional requirements, which should also include complying with all applicable legal and regulatory requirements.
   3. Design: Cybersecurity considerations are included as an integral piece of the detailed processing requirements. Controls should be identified in all design aspects as the organization more formally defines the needs of the system architecture design (such as platforms, user interfaces, databases, and others).
   4. Development: The organization has established a secure environment and formally defined a development process that minimizes cyber vulnerabilities (for example, limited user access to development code, appropriate segregation from production environment, the use of approved tools, the existence of audit trails to track development activities, specific cybersecurity requirements for vendor-developed software, and others).
   5. Testing: The organization includes the review and assessment of cybersecurity during the testing phase (for example, automated testing, penetration testing, and vulnerability assessment). The organization should be able to quickly be alerted to and address any cyber vulnerabilities identified through testing, which includes a detailed description of the vulnerability and what code changes or mitigating controls were established in response.
   6. Deployment: As new software is moved into production, the organization should carefully monitor potential cybersecurity threats, including ensuring end-users have been trained to use the software in a way that minimizes cybersecurity risks. The organization should ensure that events and errors are logged and analyzed related to potential cybersecurity events.
   7. Maintenance: The organization should ensure that all security-related software releases are applied in a timely manner and should have open communication with software vendors to ensure emerging risks and threats are properly controlled and that end-users are informed of any known vulnerabilities.

G. Controls the organization has established to protect hardware (such as desktops, laptops, mobile devices, and others) from cybersecurity risks, which includes the use of encryption, antivirus software, complex password requirements, virtual private network or zero trust networking for authentication, periodic updating of firmware, and an asset management process that ensures that company-issued hardware has an appropriate security configuration upon issuance and proper disposal when assets are retired.

H. Controls the organization has deployed to ensure production support provides protection from cybersecurity risks, which should include that servers are patched with security releases in a timely manner to mitigate emerging risks. Review the monitoring controls in place to determine whether availability and resource utilization are performing adequately, allowing potential cybersecurity issues that threaten performance to be reviewed and analyzed. Review 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.

I. Network-related controls that provide for segmentation to limit cybersecurity risks from unauthorized access. Review how the organization utilizes firewalls, including where the firewalls are located and the process used to review, analyze, and restrict network access, preventing unauthorized access. Review how the organization utilizes intrusion detection/prevention systems to prevent, detect, and recover from cybersecurity attacks.

J. Controls the organization has established surrounding common desktop communication services, such as use of email encryption, ensuring internet browser security updates are applied in a timely manner, videoconferencing/messaging (for example, MS Teams, Zoom, and others) security settings are configured to restrict the use of certain file extensions (such as .exe files), and the use of multifactor authentication for file sharing.

K. Controls the organization has deployed to mitigate cybersecurity risks related to service delivery, including:
   1. Ensuring the change management process includes consideration of cybersecurity risks when evaluating and approving changes and timely cyber incident response.
   2. The user help desk logs all cybersecurity events communicated by the organization, ensures timely resolution, and escalates to the appropriate member of management.
   3. The administration of mobile devices (such as email, applications, and others) is configured to mitigate cybersecurity risks and can be remotely managed if a user's device is compromised.

L. Physical security controls to protect high-risk information including from cybersecurity risks. Examples include ensuring third party/vendor access is appropriate and limiting physical user access data centers, network operations centers, and security operations centers to authorized personnel .

M. Controls the organization has implemented regarding incident response and recovery, which should include:
   1. A documented plan that is reviewed and updated as the organization's operations change over time.
   2. Periodic testing and reporting the results to management.
   3. Determining whether any issues identified by testing are remediated in a timely manner.

Appendix B. Tool to Document Conformance with Topical Requirement

Cybersecurity – Governance

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
A. Policies and procedures related to cybersecurity risk management processes are established and periodically updated, including promotion of practices based on widely adopted frameworks (NIST, COBIT, and others) that strengthen the control environment.		
B. Roles and responsibilities that support the organization's cybersecurity objectives are clearly established, and the roles are properly filled.		
C. Updates to cybersecurity objectives, strategies, risks, and mitigating controls are periodically communicated to the board.		
D. Relevant stakeholders are engaged to discuss how to best establish and improve cybersecurity risk management processes.		
E. Required resources (leadership, funding, talent, hardware, software, training, and others) necessary to effectively execute cybersecurity risk management processes are communicated to the board.		

Cybersecurity – Risk Management

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
A. Establishment of an organizationwide risk management process that includes the identification, analysis, and management of risks related to information technology and security, with a specific focus on cybersecurity risks and how those risks may affect the organization's ability to achieve its objectives.		
B. Cybersecurity risk management processes are conducted by a cross-functional team that includes information technology leadership, organizationwide risk management, legal, compliance, and other management (for example, operations, accounting/finance) and engages external parties (vendors, suppliers, customers, and others) as applicable.		
C. Policies and procedures related to cybersecurity risk management have been established and are periodically updated, including promotion of practices that		

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
strengthen cybersecurity risk management processes based on widely adopted risk management frameworks, authoritative guidance, or best practices.		
D. Accountability and responsibility regarding the management of cybersecurity risks is established and an individual or team has been identified that periodically monitors and communicates how the cybersecurity risks are being managed, including resource requirements to mitigate risks and the identification of emerging cybersecurity risks that had previously not been identified.		
E. A process is established to quickly escalate cybersecurity risks (emerging or previously identified) that rise to unacceptable levels based on the organization's established risk management guidelines or to comply with applicable legal and/or regulatory requirements.		
F. Cybersecurity risk management includes the coordination between information security, legal, compliance, and other management to identify and comply with all legal and contractual obligations (laws, regulations). The status of compliance and noncompliance with applicable requirements is communicated to the organization periodically.		
G. A process is in place to identify and manage cybersecurity risks related to third parties. Vendors, suppliers, and other providers of outsourced processes and/or services are contractually required to implement effective cybersecurity controls that adequately protect the confidentiality, integrity, and availability of the organization's systems and data to which they have access.		
H. Policies and processes related to data classification, retention, destruction, and encryption are adequately designed and effectively deployed to provide a systematic approach that ensures complete and accurate recording of data and protects the confidentiality and privacy of sensitive information.		
I. A process is in place for communicating cybersecurity operational risks to ensure appropriate awareness by management and employees. Issues, gaps, deficiencies, and control failures are communicated to the board and management and the status of		

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
remediation is closely monitored and reported. Noncompliance with cybersecurity policies is identified, investigated, reported, and remediated in a timely manner.		

Cybersecurity – Control Processes

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
A. Prioritizes cybersecurity controls and ensures the related budget and resources (for example, personnel, software, tools) are allocated to maximize expected benefits.		
B. Ensures that cybersecurity controls are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and timely resolution as issues occur.		
C. Provides sufficient training to the personnel responsible for cybersecurity operations.		
D. Has developed sufficient policies and procedures to manage all aspects of cybersecurity operations and related controls.		
E. Ensures that management has the resources necessary to stay informed on emerging cybersecurity issues from new technologies, identify opportunities to improve operations, and understand how cybersecurity efforts can best be deployed to impact broader organizational goals and objectives.		
F. Adequately integrates cybersecurity into the system development life cycle for business applications, including software and acquired or custom-developed applications.		
G. Has included cybersecurity in the management of hardware (laptops, desktops, mobile devices).		
H. Has implemented effective controls regarding production hardware support, such as configuring, patching, supporting user access management, and monitoring availability and performance. The organization has evaluated both the design adequacy and operational effectiveness of these controls.		
I. Optimizes network-related controls regarding network segmentation, use and placement of firewalls, limited connections to external networks and/or systems, and the use		

Requirement	Conformance (Yes / No / Partial)	Evidence Obtained or Rationale for Exclusion
of preventive and detective technologies such as intrusion detection/prevention systems.		
J. Has implemented effective controls surrounding common desktop communication services such as email, internet browsers, videoconferencing, messaging, and file-sharing protocols.		
K. Has implemented appropriate service delivery controls to ensure the following areas are integrated with cybersecurity monitoring: change management, service/help desk, and end-user device administration.		
L. Has implemented appropriate physical security controls to protect high-risk information centers (such as data centers, network operations centers, and security operations centers) from attacks.		
M. Has implemented incident response and recovery controls.		

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is a professional association that serves more than 245,000 global members and has awarded more than 195,000 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.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

April 2024

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