# Cybersecurity Toolkit

## IIA Audit Tool

*Determining Risk Owners*

*Category:* Certified
*Purpose:* How To


The Institute of Internal Auditors

## Overview

Given the internal audit activity's role in providing independent assurance that an organization is managing risk in a way that is consistent with its risk appetite, the following components may comprise a useful framework for conducting an internal audit of cybersecurity risk. Test steps should be designed to address the organization's environment, policies, and procedures. Internal auditors may also need to consider risks and controls in related subjects, such as IT governance, insider threats, patch management, and IT outsourcing, to name a few, to design a comprehensive cybersecurity risk management audit.

### Component 1: Cybersecurity Governance

Cybersecurity governance consists of a number of processes coming together to make the program function. Elements of cybersecurity governance could include:

- *Board-level oversight*: Confirm that the board of directors sees regular reporting on cybersecurity risks and risk mitigation activities.
- *Policies and procedures*: Verify whether significant processes described below are adequately covered in policies and procedures, and whether the guidance has been reauthorized within a reasonable time period.
- *Risk management*: Determine whether management has conducted a comprehensive cyber risk assessment, covering all geographic areas of operation, business lines, etc.
- *Records and information management*: Verify whether system architecture and data flow documentation is complete, accurate, and consistently retained.
- *Compliance*: Determine whether IT and IS leaders have identified relevant external requirements and implemented controls to ensure the organization meets the standards
- *Data classification*: Confirm that a classification scheme has been defined and is recorded for all systems and databases.
- *Vendor management*: Verify whether third-party risks have been assessed, and whether vendors that store or process sensitive data are subject to sufficient contractual, oversight, and technical controls.
- *Management reporting*: Determine whether KPIs or KRIs have been defined for cybersecurity, and whether reporting is accurate and actionable.
- *Personnel*: Determine whether IT and IS staffing is sufficient and has the expertise to deploy security tools and enforce policies.

## Component 2: Inventory of Information Assets

IT should have complete inventories of hardware and software used by the organization, with sufficient metadata to enable administrative and operational processes.

- *Hardware*: Determine whether all servers, network devices, and end user devices are connected to a service management or operational support system, with custodial owners recorded. Processes for adding, moving or removing devices – including sanitization or destruction of memory – should also be evaluated.
- *Software*: Verify whether all applications in use by the business are recorded in a service management or specialized inventory application, including vendor-hosted or cloud-based applications that may not be managed by IT. Determine whether classification, ownership, and interface data is complete and accurate.

## Component 3: Standard Security Configurations

Obtain evidence that the organization secures the IT environment through the use of configuration best practices. An enterprise architecture planning process should evaluate and implement new technologies as appropriate to improve system performance and security. Vendor product guides may be useful sources of configuration best practices.

- *Servers*: Verify whether management has documented baseline configurations for dedicated and virtualized servers in accordance with external standards or best practices. Operating systems and component technologies should be running the latest approved versions. Confirm that changes to and variances from the approved baseline are prevented, detected or remediated as appropriate.
    - For outsourced infrastructure, like with cloud-based or vendor-managed applications, verify that connections to the organization's network are documented and configured according to best practices.
- *Databases*: Determine whether application databases and data warehouses are configured according to documented standards that are aligned with external standards or best practices. The use of encryption and middleware services, such as application programming interfaces, should be evaluated for conformance with internal standards.
- *Network devices*: Verify whether in-service devices meet enterprise architecture requirements, have default accounts or passwords changed, and have documented baseline configurations. Confirm that firmware patches are tested and implemented timely. Determine whether networks are adequately separated by data classification or other criteria, with sufficient access controls to prevent unfettered traversal.
- *Endpoint devices*: Confirm whether personal computers, printers, and other devices connected to the network are centrally managed to enforce security measures like preventing installation of unauthorized software, ensuring current anti-virus software, limiting communication protocols, and restricting the use of removable storage media. Determine whether non-managed devices, such as employees' personal cellphones or non-employees' laptops, are prevented from connecting to the network or at least meet minimum security requirements.

## Component 4: Information Access Management

Information access should be managed at every layer of technology to restrict users to only the permissions needed to perform authorized job functions. Identity and access management controls should be commensurate with the software or hardware data classification.

- *Administrator accounts*: Determine whether the creation and usage of administrative privileges is adequately restricted and logged. Confirm whether administrator account activity is monitored by automated tools managed by the IS team.
- *Developer accounts*: Confirm that software developers are not able to test their own code and do not have permission to access the production versions of applications they developed.
- *Application user accounts*: Verify whether applications are integrated with network identity and authentication controls, and if not, whether manual controls are adequately designed and implemented. Evaluate the use of role-based access controls to determine whether access rights are appropriately limited. Determine whether authorization, reauthorization, and deactivation processes are designed and implemented sufficiently.
- *User accountability*: Determine whether system administrators promote accountability by preventing the use of group accounts, self-approvals, or unattributed actions for sensitive operations.

## Component 5: Proactive and Preventive Controls

Controls to prevent, identify, or address vulnerabilities are important to an organization's cybersecurity.

- *Malware*: Determine whether anti-malware software is installed on servers and endpoint devices where appropriate, and whether anomalies detected by monitoring controls are investigated for undetected malware. Confirm that controls are in place to protect the network and end users from emails with suspicious attachments or links, and internet browser controls prevent access to specified types of sites and services.
- *Application security*: Verify whether security requirements are defined and implemented in the design and development of applications. For vendor-developed applications, confirm that the system is integrated with vulnerability scanning and cybersecurity monitoring controls.
- Network operations: Determine whether controls are in place to detect unauthorized wireless access points, undocumented middleware services, or anomalous traffic types or volumes. Evaluate the use of network segmentation and data flow controls, including authentication, to limit the impact of potential incidents.
- *Vulnerability scans*: Confirm that automated scans are used on applicable networks, applications, and technologies to identify known weaknesses in coding or configuration. Verify whether vulnerabilities are resolved within internal timeliness metrics, based on assigned criticalities.
- *Penetration tests*: Verify whether the IS department engages in approved attempts to infiltrate or compromise the technology resources, and uses the information gained to remediate identified vulnerabilities.
- *Monitoring*: Determine whether the organization uses intrusion detection or prevention systems, and system event log aggregators, to monitor network and application events for possible signs of internal misuse or external cyberattacks.
- *Data protection*: Verify whether processes and technology (e.g., encryption, data masking, use restrictions, and data loss prevention tools) are deployed to reduce the risks of misuse or exfiltration.

## Component 6: Response and Remediation

Incident detection and response controls are critical to limiting the damage from cyberattacks or breaches, and reporting processes may be required by regulation.

- *Incident response plan*: Determine whether the IS function has documented a plan for responding to various types of cybersecurity incidents, and verify whether the plans have been adequately tested.
- *Reporting and remediation requirements*: Determine whether management has documented regulatory

requirements for reporting and remediating cybersecurity incidents and breaches.

- *Past incidents*: Examine documentation of past incidents to determine whether the remediation and communication plans were invoked timely, and were effective at mitigating impacts.
- *Continuous improvement*: Verify whether the results of past incidents were used to identify opportunities for improving plans, processes, and technologies.

## IIA Audit Tool

*Category:* Certified
*Purpose:* Audit Program

### *Sample Audit Program*


The Institute of Internal Auditors

# Overview

Given the internal audit activity's role in providing independent assurance that an organization is managing risk in a way that is consistent with its risk appetite, the following components may comprise a useful framework for conducting an internal audit of cybersecurity risk. Test steps should be designed to address the organization's environment, policies, and procedures. Internal auditors may also need to consider risks and controls in related subjects, such as IT governance, insider threats, patch management, and IT outsourcing, to name a few, to design a comprehensive cybersecurity risk management audit.

## Component 1: Cybersecurity Governance

Cybersecurity governance consists of a number of processes coming together to make the program function. Elements of cybersecurity governance could include:

- *Board-level oversight*: Confirm that the board of directors sees regular reporting on cybersecurity risks and risk mitigation activities.
- *Policies and procedures*: Verify whether significant processes described below are adequately covered in policies and procedures, and whether the guidance has been reauthorized within a reasonable time period.
- *Risk management*: Determine whether management has conducted a comprehensive cyber risk assessment, covering all geographic areas of operation, business lines, etc.
- *Records and information management*: Verify whether system architecture and data flow documentation is complete, accurate, and consistently retained.
- *Compliance*: Determine whether IT and IS leaders have identified relevant external requirements and implemented controls to ensure the organization meets the standards
- *Data classification*: Confirm that a classification scheme has been defined and is recorded for all systems and databases.
- *Vendor management*: Verify whether third-party risks have been assessed, and whether vendors that store or process sensitive data are subject to sufficient contractual, oversight, and technical controls.
- *Management reporting*: Determine whether KPIs or KRIs have been defined for cybersecurity, and whether reporting is accurate and actionable.
- *Personnel*: Determine whether IT and IS staffing is sufficient and has the expertise to deploy security tools and enforce policies.

## Component 2: Inventory of Information Assets

IT should have complete inventories of hardware and software used by the organization, with sufficient metadata to enable administrative and operational processes.

- *Hardware*: Determine whether all servers, network devices, and end user devices are connected to a service management or operational support system, with custodial owners recorded. Processes for adding, moving or removing devices – including sanitization or destruction of memory – should also be evaluated.
- *Software*: Verify whether all applications in use by the business are recorded in a service management or specialized inventory application, including vendor-hosted or cloud-based applications that may not be managed by IT. Determine whether classification, ownership, and interface data is complete and accurate.

## Component 3: Standard Security Configurations

Obtain evidence that the organization secures the IT environment through the use of configuration best practices. An enterprise architecture planning process should evaluate and implement new technologies as appropriate to improve system performance and security. Vendor product guides may be useful sources of configuration best practices.

- *Servers*: Verify whether management has documented baseline configurations for dedicated and virtualized servers in accordance with external standards or best practices. Operating systems and component technologies should be running the latest approved versions. Confirm that changes to and variances from the approved baseline are prevented, detected or remediated as appropriate.
    - For outsourced infrastructure, like with cloud-based or vendor-managed applications, verify that connections to the organization's network are documented and configured according to best practices.
- *Databases*: Determine whether application databases and data warehouses are configured according to documented standards that are aligned with external standards or best practices. The use of encryption and middleware services, such as application programming interfaces, should be evaluated for conformance with internal standards.
- *Network devices*: Verify whether in-service devices meet enterprise architecture requirements, have default accounts or passwords changed, and have documented baseline configurations. Confirm that firmware patches are tested and implemented timely. Determine whether networks are adequately separated by data classification or other criteria, with sufficient access controls to prevent unfettered traversal.
- *Endpoint devices*: Confirm whether personal computers, printers, and other devices connected to the network are centrally managed to enforce security measures like preventing installation of unauthorized software, ensuring current anti-virus software, limiting communication protocols, and restricting the use of removable storage media. Determine whether non-managed devices, such as employees' personal cellphones or non-employees' laptops, are prevented from connecting to the network or at least meet minimum security requirements.

## Component 4: Information Access Management

Information access should be managed at every layer of technology to restrict users to only the permissions needed to perform authorized job functions. Identity and access management controls should be commensurate with the software or hardware data classification.

- *Administrator accounts*: Determine whether the creation and usage of administrative privileges is adequately restricted and logged. Confirm whether administrator account activity is monitored by automated tools managed by the IS team.
- *Developer accounts*: Confirm that software developers are not able to test their own code and do not have permission to access the production versions of applications they developed.
- *Application user accounts*: Verify whether applications are integrated with network identity and authentication controls, and if not, whether manual controls are adequately designed and implemented. Evaluate the use of role-based access controls to determine whether access rights are appropriately limited. Determine whether authorization, reauthorization, and deactivation processes are designed and implemented sufficiently.

- *User accountability*: Determine whether system administrators promote accountability by preventing the use of group accounts, self-approvals, or unattributed actions for sensitive operations.

## Component 5: Proactive and Preventive Controls

Controls to prevent, identify, or address vulnerabilities are important to an organization's cybersecurity.

- *Malware*: Determine whether anti-malware software is installed on servers and endpoint devices where appropriate, and whether anomalies detected by monitoring controls are investigated for undetected malware. Confirm that controls are in place to protect the network and end users from emails with suspicious attachments or links, and internet browser controls prevent access to specified types of sites and services.
- *Application security*: Verify whether security requirements are defined and implemented in the design and development of applications. For vendor-developed applications, confirm that the system is integrated with vulnerability scanning and cybersecurity monitoring controls.
- Network operations: Determine whether controls are in place to detect unauthorized wireless access points, undocumented middleware services, or anomalous traffic types or volumes. Evaluate the use of network segmentation and data flow controls, including authentication, to limit the impact of potential incidents.
- *Vulnerability scans*: Confirm that automated scans are used on applicable networks, applications, and technologies to identify known weaknesses in coding or configuration. Verify whether vulnerabilities are resolved within internal timeliness metrics, based on assigned criticalities.
- *Penetration tests*: Verify whether the IS department engages in approved attempts to infiltrate or compromise the technology resources, and uses the information gained to remediate identified vulnerabilities.
- *Monitoring*: Determine whether the organization uses intrusion detection or prevention systems, and system event log aggregators, to monitor network and application events for possible signs of internal misuse or external cyberattacks.
- *Data protection*: Verify whether processes and technology (e.g., encryption, data masking, use restrictions, and data loss prevention tools) are deployed to reduce the risks of misuse or exfiltration.

## Component 6: Response and Remediation

Incident detection and response controls are critical to limiting the damage from cyberattacks or breaches, and reporting processes may be required by regulation.

- *Incident response plan*: Determine whether the IS function has documented a plan for responding to various types of cybersecurity incidents, and verify whether the plans have been adequately tested.
- *Reporting and remediation requirements*: Determine whether management has documented regulatory requirements for reporting and remediating cybersecurity incidents and breaches.
- *Past incidents*: Examine documentation of past incidents to determine whether the remediation and communication plans were invoked timely, and were effective at mitigating impacts.
- *Continuous improvement*: Verify whether the results of past incidents were used to identify opportunities for improving plans, processes, and technologies.

## IIA Audit Tool

*Category:* Certified
*Purpose:* Planning

# *Sample Risk List*


The Institute of Internal Auditors

These are some main risk areas internal auditors should consider when performing a cybersecurity risk management engagement. The list is neither exhaustive nor meant to be used as an engagement work program or checklist.

- Disparate, fragmented government structure.
- Incomplete or unrealistic strategy.
- Delays of cybersecurity efforts/projects.
- Budget cuts and attrition in areas responsible for cybersecurity.
- Unclear resolve to enforce accountability for incidents.
- Lack of executive involvement and support of cybersecurity initiatives.
- Inadequate response and post-incident root cause analysis.
- Undefined protocols and responsibilities for responding to escalating incidents.
- Employees do not possess necessary skill sets and/or knowledge.
- Inability to proactively identify and address emerging risks.
- Inadequate allocation of money, time, and resources negatively impacting cybersecurity initiatives, including routine maintenance and patching.
- Inadequate and untimely identification and monitoring of cyber threats such as:
  - Nation-states.
  - Cyber criminals.
  - Hacktivists.
  - Insiders and service providers.
  - Developers of substandard products and services.

## About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.theiia.org.

## Disclaimer



## Copyright



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