Auditing Cybersecurity Operations: Prevention and Detection

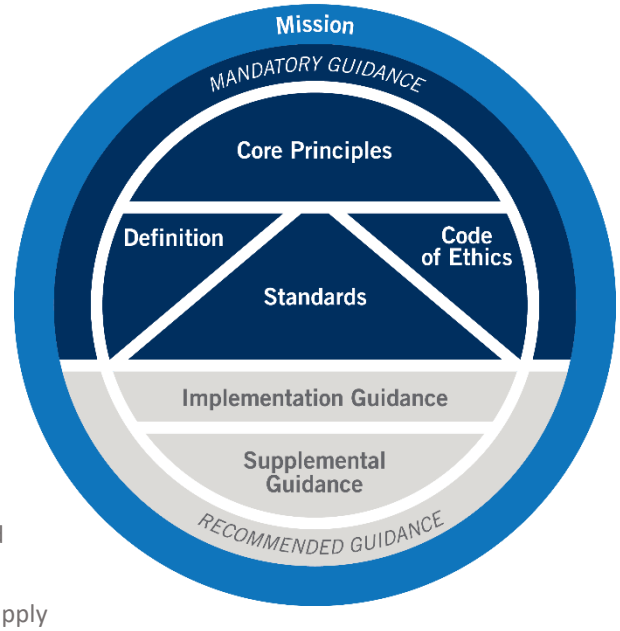
Supplemental Guidance | **Practice Guide**

GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of
Internal Auditors

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.



Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- International Standards for the Professional Practice of Internal Auditing.

Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.theiia.org.

About GTAGs

Within the IPPF's Supplemental Guidance, Global Technology Audit Guides (GTAGs) provide auditors with the knowledge to perform assurance or consulting services related to an organization's information technology (IT) and information security (IS) risks and controls. The *Standards* that give rise to the GTAGs are listed below.

- **1210.A3** – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.
- **2110.A2** – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **2120.A1** – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives.
    - Reliability and integrity of financial and operational information.
    - Effectiveness and efficiency of operations and programs.
    - Safeguarding of assets.
    - Compliance with laws, regulations, policies, procedures, and contracts.
- **2130.A1** – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives.
    - Reliability and integrity of financial and operational information.
    - Effectiveness and efficiency of operations and programs.
    - Safeguarding of assets.
    - Compliance with laws, regulations, policies, procedures, and contracts.
- **2220.A1** – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Contents

Executive Summary

Cybersecurity, also known as information security (IS), can be considered a subset of, or a complementary subject to, information technology (IT) risks and controls because of their interdependent operations yet often separate leadership. Cybersecurity controls include the policies, processes, tools, and personnel for ensuring an organization's information resources are adequately protected from many types of attacks, detecting when such attacks occur, and remediating deficiencies as effectively as possible – expressed in one significant framework as the following five functions: Identify, Protect, Detect, Respond, and Recover.

In the broadest sense, IT or IS teams may manage cybersecurity risks and controls, depending on the process under review and the organization's unique environment. For this document, "cybersecurity operations" will refer to controls that generally prevent or detect cyberattacks and are typically managed by IS rather than IT personnel. Nevertheless, cybersecurity operations controls are often embedded within systems planning, building, and monitoring processes managed by the IT department.

Cybersecurity operations can be broadly categorized according to three high-level control objectives:

1. Security in design: Operational contributions from the IS leader or function to governance, risk management, and IT-managed control processes ensure adequate protection of data and resources.
2. Prevention: Technologies like encryption, email and network filters, and antivirus and data loss prevention software aim to thwart attempts to misuse or disrupt information resources or communications. Cybersecurity awareness training also helps employees understand their role in protecting the organization's resources and reduces the likelihood that they will fall victim to social engineering or other malicious tactics.
3. Detection: Tools and processes such as cybersecurity monitoring — which includes event log monitoring and forensic analysis of system outages or anomalies, vulnerability management, and penetration testing — identify control weaknesses or the presence of entities or objects acting maliciously in the computing environment so that they can be addressed.

Stakeholders, primarily an organization's governing body and senior management, rely on independent, objective, and competent assurance services to verify whether cybersecurity operations controls are well-designed and effectively and efficiently implemented. The internal audit activity adds value to the organization when it provides such services in conformance with the *Standards* and with references to widely accepted control frameworks, particularly those expressly used by the organization's IT and IS functions.

Introduction

Cybersecurity refers to the technologies and processes designed to protect an organization's information resources — computers, network devices, software programs, and data — from unauthorized access, disruption, or destruction. Threats to information resources may come from inside or outside the organization. A wide range of **information technology** (IT) **controls**, including **information security** (IS) controls, collectively IT-IS controls, are available to prevent, detect, or mitigate the impact of **risk** events. For each organization, individualized assessments of cybersecurity risks help prioritize the allocation of control and assurance resources.

> **Note**
>
> Appendix A lists other IIA resources relevant to this guide. Terms in bold are defined in the Glossary in Appendix B.

According to The IIA's Three Lines Model[1], the IT and IS teams primarily responsible for information technology **governance**, **risk management**, and internal controls perform first and second line duties because they design and implement operational and oversight controls. Many organizations separate the responsibilities by designating a chief information officer (CIO) for IT and a chief information security officer (CISO) for IS. In many organizations, neither one of them reports to the other, though sometimes both will report to a chief technology officer or a similar executive, such as a chief operating officer. Of course, other titles may be used globally to describe or assign these responsibilities, but throughout this guide, the leader of the IT function may be referred to as the CIO, and likewise CISO for the IS function. Personnel in other business units may also be responsible for executing first-line controls related to cybersecurity, such as when a supervisor approves system access for a subordinate.

The **internal audit activity** — the third line — provides independent **assurance services** and **consulting services** regarding the adequacy and effectiveness of IT-IS processes, including cybersecurity operations. The internal audit activity **should** consider cybersecurity risks in planning and prioritizing its audit **engagements**. Some high-level questions for the organization and the internal audit activity to consider, with respect to the prevention and detection of cyberattacks, include:

- Which resources are the likeliest targets for cyberattacks?
- Who has access to the organization's most valuable information?

1. The Institute of Internal Auditors. *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. Lake Mary. The Institute of Internal Auditors, 2020. https://www.theiia.org/en/content/articles/-global-knowledge-brief/2020/july/the-iias-three-lines-model/.

- Which systems would cause the most significant disruption if compromised?
- Which data, if obtained by unauthorized parties, would cause financial or competitive loss, legal ramifications, or reputational damage to the organization?
- Would the organization know quickly if its defenses had been breached?

This guide discusses cybersecurity operations controls, which help design and embed security mechanisms into IT and communications resources and manage controls to prevent or detect cyberattacks. Coordination and collaboration between IT, IS, and the internal audit activity can provide the organization's governing body and management with a comprehensive, tailored view of the effectiveness and efficiency of cybersecurity operations controls, including **residual risks** that may require further mitigation.

Auditing cybersecurity operations involves an engagement-level risk assessment, a specified scope and **engagement objectives**, and tests to evaluate the design and implementation of relevant controls to determine whether any significant risk exposures exist. This approach helps internal auditors demonstrate conformance with Standard 1200 — Proficiency and Due Professional Care.

IT-IS Control Frameworks

This guide references four external IT-IS control frameworks of standards, guidance, and best practices, although many others are used worldwide. Each framework provides more information about specific controls than is discussed here. IT-IS personnel frequently benchmark operational and security controls against one or more of these frameworks. Internal auditors are encouraged to identify frameworks used by their organizations and review other widely adopted IT-IS control guidance to help them identify and understand common risks and controls. (Appendix C provides references to these sources.)

The four frameworks referenced are:

- COBIT 2019 Framework: Governance and Management Objectives from ISACA.
- NIST Special Publication (SP) 800-53, Revision 5: Security and **Privacy** Controls for Information Systems and Organizations from the National Institute of Standards and Technology (also referred to as NIST SP 800-53r5).
- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (also referred to as the NIST Cybersecurity Framework [or NIST CSF]).
- CIS Controls Version 8 from the Center for Internet Security.

Readers of this guide are assumed to have a general knowledge of IT-IS risks and controls, as described in the GTAG "IT Essentials for Internal Auditors." A basic understanding of technology processes and terms provides a foundation for reviewing the full texts of one or more IT-IS control frameworks as part of planning the audit and test program. Incorporating a review of external guidance into the engagement planning helps an internal auditor demonstrate the essence of Standard 1220 – Due Professional Care, which states: "Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility."

Cybersecurity GTAGs

Cybersecurity risks and controls are primarily covered in four GTAGs, with coverage of the relevant functions in the NIST CSF as follows:

- "Assessing Cybersecurity Risk – The Three Lines Model." Mainly corresponds to the Identify function, because it discusses how organizations apply governance and risk management approaches to determining effective and adequate cybersecurity controls.
- "Auditing Cybersecurity Operations – Prevention and Detection." Largely corresponds to the Protect and Detect functions, with an emphasis on controls likely to be managed by the CISO, or functionally considered part of IS, rather than IT.
- "Auditing Cyber Incident Response and Recovery." Maps to the Respond and Recover functions.
- "Auditing Insider Threat Programs." A topic of special emphasis that covers controls in all five NIST CSF functions.

Other GTAGs that cover risks and controls significant to a holistic view of cybersecurity include "Auditing Identity and Access Management" and "Auditing Mobile Computing." Additionally, controls to achieve the objectives of **confidentiality**, **integrity**, and data **availability** are embedded in the design and operations of IT processes, so all GTAGs have at least some useful guidance for assessing various aspects of cybersecurity.

Objectives

This guide will help the reader:

- Define cybersecurity operations and develop a working knowledge of relevant processes, including related governance and risk management controls.
- Identify components of cybersecurity operations, including contributions to system planning and development, as well as controls to prevent or detect cyberattacks.
- Consider relevant control guidance in widely used IT-IS control frameworks to increase the value of assurance and consulting services provided by the internal audit activity.
- Understand approaches to auditing cybersecurity operations, including specific controls that should be present and evaluated.

Cybersecurity Operations Controls

This guide will provide brief descriptions of cybersecurity operations controls categorized under three high-level objectives: security in design, prevention, and detection. It will include references to various IT-IS control frameworks. A review of one or more IT-IS control frameworks, such as the ISACA, NIST, and CIS frameworks discussed below, and many others, will allow an internal audit activity to supplement its collective knowledge of control best practices.

Security in Design

Several groups of IT-IS risks and controls may be categorized as contributing to security-in-design objectives. A systematic approach to analyzing an organization's cybersecurity operations controls in these groups may include a review of the IS team's involvement in the following areas:

- Governance and risk management: the establishment and management of IT-IS policies and budgets, and processes ensuring alignment among organizational and IT-IS strategies. It includes an organizationwide approach to risks and related responses, with an emphasis on the internal controls designed and implemented to reduce the likelihood and impact of cyberattacks.
- Technical planning and secure systems development: processes to identify, procure, build, test, and authorize sufficient technologies and practices to deliver services to various **user** groups while ensuring control objectives are met.
- Logical and physical access controls: ensuring that the usage of information resources is limited according to the **least privilege** principle. For cybersecurity operations, the focus is typically on **identity** and **authentication** management tools and processes. However, another common objective is to ensure physical control of — or proximity to — information resources is limited according to authorized **business rules**.

> The AICPA Trust Services Criteria categorize technology control objectives as including confidentiality, data integrity, availability, information security, and privacy.

The NIST CSF primarily includes such security-in-design controls in the Identify function, although some related controls appear in the Protect and Detect functions, as indicated below.

Governance and Risk Management

The organization's **board** and senior management exercise their governance responsibilities through establishing committees — for example, to oversee strategies, risk management, capital allocation, and assurance — and policies to set expectations and direct operations. Governance and risk management processes rely on timely, actionable data to inform decision-making, and audit services to provide independent insight. These processes, in general, are covered more extensively in the GTAGs "Auditing IT

Governance" and "Assessing Cybersecurity Risk: The Three Lines Model." However, relevant questions for an internal audit activity to consider when planning a cybersecurity operations engagement may include:

- Are IS policies and controls sufficiently deep and broad for the organization's current environment? Ideally, they should be modeled on a widely adopted IT-IS control framework.
- Is the designated head of cybersecurity (CISO) providing periodic updates and insightful reporting to the board and senior management regarding cybersecurity risks and the organization's responses?
- Does the IS team regularly review or implement security-related controls within significant business processes?

The organization's funding of IS objectives — for personnel, services, and tools — should be considered a significant constraining factor of control implementations. Similarly, staffing models and budgets for relevant IT-IS functions and the ability to fill open positions and retain skilled cybersecurity employees may also be evaluated in cybersecurity operations or IT governance audit engagements.

Other high-level objectives discussed in the NIST CSF Protect and Detect functions that are mainly related to performance reporting, human resources, vendor management, **compliance**, and change management are covered primarily in other GTAGs, including: "Auditing IT Governance"; "Assessing Cybersecurity Risk: The Three Lines Model"; "Information Technology Outsourcing"; and "IT Change Management: Critical for Organizational Success."

Controls over cybersecurity operations governance and risk management are primarily described in:

- COBIT 2019 Framework: Governance and Management Objectives, in practices:
    - EDM03.02 Direct Risk Management.
    - EDM04.02 Direct Resource Management.
    - APO01.05 Establish Roles and Responsibilities.
    - APO05.03 Monitor, Optimize and Report on Investment Portfolio Performance.
    - APO06.02 Prioritize Resource Allocation.
    - APO10.04 Manage Vendor Risk.
    - APO13.01 Establish and Maintain an Information Security Management System.
    - APO13.02 Define and Manage an Information Security Risk Treatment Plan.
    - APO13.03 Monitor and Review the Information Security Management System.
    - MEA01.03 Collect and Process Performance and Conformance Data.
    - MEA02.01 Monitor Internal Controls.
    - MEA03.02 Optimize Response to External Requirements.
- NIST SP 800-53r5, in controls:
    - PL-4 Rules of Behavior.
    - PM-1 Information Security Program Plan.
    - PM-3 Information Security and Privacy Resources.

    - PM-6 Measures of Performance.
    - PM-13 Security and Privacy Workforce.
    - PM-14 Testing, Training, and Monitoring.
    - PM-15 Security and Privacy Groups and Associations.
    - PM-31 Continuous Monitoring Strategy.
    - PS-9 Position Descriptions.
    - PT-2 Authority to Process Personally Identifiable Information.
    - RA-2 Security Categorization.
    - RA-7 Risk Response.
    - SA-2 Allocation of Resources.
    - SA-9 External System Services.
    - SC-43 Usage Restrictions.
- NIST CSF governance and risk management control objectives:
    - Effectiveness of protection technologies is shared (PR.IP-8).
    - Cybersecurity is included in human resources practices (PR.IP-11).
    - Roles and responsibilities for protection and detection are defined (PR.AT-3, PR.AT-4, PR.AT-5, DE.DP-1).
    - Configuration and change control processes are adequately managed (PR.IP-3).
    - Protection and detection processes are improved (PR.IP-7, DE.DP-5).
    - Detection activities comply with all applicable requirements (DE.DP-2).
- CIS Controls mainly in safeguards:
    - 4.6 Securely Manage Enterprise Assets and Software.
    - 15.4 Ensure Service Provider Contracts Include Security Requirements.
    - 15.6 Monitor Service Providers.

Technical Planning and Secure Systems Development

System architects and solution providers — which may include internal or external software developers, project managers, vendors, and others — work with senior management to identify, authorize, and deploy technology to meet business needs and objectives. Information security is generally among the significant objectives considered, so policies and practices typically cover:

- Secure systems development.
- Timely and effective support of purchased products.
- Private communications.
- The proper storage and usage of information resources.

While technical planning and system development risks and controls are covered more extensively in the GTAG "Auditing Business Applications," many of the same control objectives apply to cybersecurity operations solutions. Audits of cybersecurity operations should look for evidence of robust involvement from the IS function in enterprise architecture review processes, vendor or technology risk assessments, and testing of proposed and implemented solutions. For example, critical information resources – including hardware operating systems and business **applications** — usually can be programmed to log specified security events, such as when new user accounts are created or an existing account's privileges are escalated. So, determining which events to log and connecting the various system logs to the IS function's monitoring capability are key contributors to effective detective controls. Accordingly, an audit engagement could verify whether key applications or environments are integrated with the organization's protective and detective controls described in later sections (see below).

Other significant controls in systems planning, development, procurement, and implementation include applying common security engineering principles to technology solutions and protecting the communications links between resources. An audit in this area could look for evidence that the development and procurement processes for significant resources included reviews by the IS function for consideration of cybersecurity risk exposures and appropriate responses.

Controls over integrating cybersecurity into technical planning and systems development processes are primarily described in:

- COBIT 2019: Framework: Governance and Management Objectives, in the domains: Align, Plan and Organize; and Build, Acquire and Implement. The guidance is generally applicable to IT and IS solutions.
- NIST SP 800-53r5, in controls:
    - AU-2 Event Logging.
    - AU-3 Content of Audit Records.
    - AU-9 Protection of Audit Information.
    - CM-4 Impact Analyses.
    - CM-7 Least Functionality.
    - CM-11 User-Installed Software.
    - PL-2 System Security and Privacy Plans.
    - PM-32 Purposing.
    - SA-8 Security and Privacy Engineering Principles.
    - SA-17 Developer Security and Privacy Architecture and Design.
    - SA-22 Unsupported System Components.
    - SA-23 Specialization.
    - SC-3 Isolate Security Functions from Nonsecurity Functions.
    - SC-5 Denial-of-Service Protection.
    - SC-8 Transmission Confidentiality and Integrity.

    - SC-16 Transmission of Security and Privacy Attributes.
    - SC-25 Thin Nodes.
    - SC-30 Concealment and Misdirection.
    - SC-38 Operations Security.
    - SC-49 Hardware-Enforced Separation and Policy Enforcement.
    - SC-50 Software-Enforced Separation and Policy Enforcement.
    - SI-14 Non-Persistence.
- In the NIST CSF, related guidance covers the following objectives:
    - Incorporating security principles, including least functionality, into baseline configurations (PR.IP-1, PR.PT-3, DE.AE-1).
    - A system development life cycle to manage systems is implemented (PR.IP-2).
    - Data is destroyed according to policy (PR.IP-6).
    - Separating the development environment from production (PR.DS-7).
    - Audit/log records are determined, documented, and implemented (PR.PT-1).
- CIS Controls throughout control 16 Application Software Security, as well as safeguards:
    - 2.2 Ensure Authorized Software is Currently Supported.
    - 4.1 Establish and Maintain a Secure Configuration Process.
    - 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure.
    - 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software.
    - 8.1 Establish and Maintain an Audit Log Management Process.
    - 12.2 Establish and Maintain a Secure Network Architecture.

Logical and Physical Access Controls

Risks and controls related to establishing digital identities (IDs), granting system **access rights** to users, and authenticating the validity of system login attempts — collectively known as logical access controls — are covered primarily in the GTAGs "Auditing Identity and Access Management" and "Auditing Business Applications." Similarly, risks and controls related to remote access to a network are the primary focus of the GTAG "Auditing Mobile Computing." However, some aspects of logical access control that may be considered in an evaluation of cybersecurity operations include verifying whether standards for and reviews of non-employee IDs and authentication methods used throughout the enterprise have been formalized and implemented by the CISO.

Physical access controls, which are often designed and implemented by facility management personnel, rather than IT or IS teams, are not covered in detail in this guide. However, the CISO may be responsible for contributing to the design, review, or monitoring of physical security, especially relating to restrictions on the use of physical media. Therefore, an audit of cybersecurity operations could evaluate whether such efforts are mature and effective.

Relevant logical and physical access controls are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practice DSS05.05 Manage Physical Access to [Information and Technology] I&T Assets.
- NIST SP 800-53r5, in the Media Protection control family, especially control MP-2 Media Access, and controls:
    - AC-3 Access Enforcement.
    - AC-5 Separation of Duties.
    - AC-6 Least Privilege.
    - AU-10 Non-Repudiation.
    - CM-14 Signed Components.
    - IA-2 Identification and Authentication (Organizational Users).
    - IA-5 Authenticator Management.
    - IA-9 Identification and Authentication (Non-Organizational Users).
    - IA-10 Adaptive Authentication.
    - PE-4 Access Control for Transmission.
    - PS-6 Access Agreements.
    - PS-7 External Personnel Security.
    - SC-41 Port and I/O Device Access.
- In the NIST CSF, related guidance covers the following objectives:
    - Identities, credentials, and permissions are adequately managed (PR.AC-1, PR.AC-4, PR.AC-6).
    - Adequate, compliant physical security (PR.AC-2, PR.IP-5).
    - Remote access is adequately managed (PR.AC-3, PR.MA-2).
    - Authentication measures are commensurate with risks (PR.AC-7).
    - Removable media is protected and its use restricted (PR.PT-2).
- CIS Controls throughout Control 6 Access Control Management, and in safeguards:
    - 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts.
    - 10.3 Disable Autorun and Autoplay for Removable Media.
    - 10.5 Enable Anti-Exploitation Features.

Prevention

The processes for preventing cyberattacks employ technologies such as **encryption**, antivirus and data loss prevention software, and email and network filters that can thwart attempts to access or disrupt information resources or communications. Additionally, cybersecurity awareness training can help personnel avoid risks, such as phishing emails or other **social engineering** tactics.

A good argument could be made for including network administration and segmentation controls within the scope of a cybersecurity operations review; however, those risks and controls are usually managed by personnel under the CIO rather than the CISO, so are covered in other GTAGs.

Encryption

One common approach to improving the security of data is to encrypt it while it is in transit or wherever it is stored by converting **plaintext** to a coded message using a **cipher**. At a high level, an **encryption key** is used by the cipher to convert the text, then a **decryption key** is used to revert the message to its original form. Ciphers in widely used encryption technologies have varying strengths, so the IS team should review and authorize specific use cases, ideally as part of the organization's technical planning or system development controls. An audit of cybersecurity operations should determine whether the organization's encryption technologies are effectively managed to ensure sufficient strength in the ciphers and protection of the keys.

Controls over encryption are primarily described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practices:
    - DSS05.02 Manage Network and Connectivity Security.
    - DSS05.03 Manage Endpoint Security.
    - DSS05.06 Manage Sensitive Documents and Output Devices.
- NIST SP 800-53r5, primarily in controls:
    - IA-7 Cryptographic Module Authentication.
    - PL-8 Security and Privacy Architectures.
    - SC-12 Cryptographic Key Establishment and Management.
    - SC-13 Cryptographic Protection.
    - SC-17 Public Key Infrastructure Certificates.
    - SC-28 Protection of Information at Rest.
- In the NIST CSF, related guidance covers the following objectives:
    - Networks are managed appropriately (PR.AC-5).
    - Protect data at rest and in transit (PR.DS-1, PR.DS-2).
    - Communications and control networks are protected (PR.PT-4).

- CIS Controls safeguards:
    - 3.6 Encrypt Data on End-User Devices.
    - 3.9 Encrypt Data on Removable Media.
    - 3.10 Encrypt Sensitive Data in Transit.
    - 3.11 Encrypt Sensitive Data at Rest.

Antivirus Software

Organizations need to protect themselves from the threat of malicious software (**malware**) that can target nearly any resource in their technology environment. **Antivirus software** protects against multiple types of malware and suspicious file types, and can also include monitoring for anomalous or proscribed events. The deployment of antivirus software may be managed centrally or by teams responsible for specific technology layers or environments.

An audit of cybersecurity operations should determine whether antivirus software has been implemented to protect sensitive resources, ideally as directed in policy or procedure documents approved by the CISO. The risks and controls related to centralized device administration, which may be used to ensure adequate antivirus software on devices connecting to the organization's data network, are covered more broadly in the GTAG "Auditing Mobile Computing."

Controls over antivirus software are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practice DSS05.01 Protect Against Malicious Software.
- NIST SP 800-53r5, primarily in controls SC-35 External Malicious Code Identification and SI-3 Malicious Code Protection.
- The NIST CSF does not directly mention antivirus or malware protections.
- CIS Controls throughout Control 10 Malware Defenses, as well as safeguards:
    - 2.5 Allowlist Authorized Software.
    - 2.7 Allowlist Authorized Scripts.
    - 9.7 Deploy and Maintain Email Server Anti-Malware Protections. This safeguard also could be grouped with email protections listed below. However, the categorization of a control is usually less important than ensuring that it is included somewhere in the audit planning and scoping.
    - 13.7 Deploy a Host-Based Intrusion Prevention Solution.

Data Loss Prevention (DLP)

Controls over data protection, including data governance, management, and usage, are discussed more extensively in other GTAGs, mainly "Auditing Business Applications" and "Auditing Mobile Computing." However, one control that the CISO may be responsible for evaluating and potentially implementing is a DLP solution to reduce the risk of sensitive data being sent to an insecure environment. For example, if sensitive customer information is downloaded from a secure system and emailed to an external address,

or uploaded to a cloud-based storage site not managed by the organization, the data could be exposed to a greater risk of leakage, interception, or manipulation. Many commercial DLP solutions exist, so a cybersecurity operations audit can verify whether the CISO has established criteria for implementing such controls and whether environments or data types meeting the criteria have been protected.

Controls over DLP are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practice DSS06.06 Secure Information Assets, which includes activities that call for restricting the use of information, establishing data classification and related protection guidelines, and implementing processes, tools, and techniques to verify compliance.
- NIST SP 800-53r5, primarily in controls AU-13 Monitoring for Information Disclosure and PE-19 Information Leakage.
- The NIST CSF discusses DLP in control PR.DS-5: Protections against data leaks are implemented.
- CIS Controls in safeguard 3.13 Deploy a Data Loss Prevention Solution.

Email Protections

One of the most common collaboration tools is email, which is often provided automatically to new individual network accounts. Email addresses enable communications with accounts on external systems — an inherently risky capability, which is one reason they are a favorite **threat vector** for cyber attackers. Messages with embedded malware, or with links to websites that gather information from or about individuals for malicious purposes, are constantly bombarding enterprise email systems in either a scattershot (**phishing**) or more targeted (**spear phishing**) approach.

One objective of these attacks is to trick recipients into divulging sensitive information — such as passwords or contact lists — that can be used for further exploits. Another is to activate malware designed to explore the user's connection to and permissions in the enterprise network for opportunities to establish a covert communication channel to external servers, which will direct further exploits.

Most commercially available email platforms provide protection from suspicious file types and links to prohibited, unauthorized, or potentially malicious websites or domains. Advanced capabilities, such as decryption and content analysis, may also be provided by the email platform or a compatible add-on service. While the CIO is usually responsible for managing the email platform, the CISO should be assessing risks in the environment and suggesting additional mitigation as needed. An audit of cybersecurity operations could determine whether protections available in the email platform have been configured appropriately, and whether additional capabilities have been evaluated and deployed as approved by the CISO.

Controls over email platforms are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practices DSS05.01 Protect Against Malicious Software, and DSS05.03 Manage Endpoint Security.
- NIST SP 800-53r5, primarily in controls:
    - CA-3 Information Exchange.

    - SC-44 Detonation Chambers.
    - SI-8 Spam Protection.
- The NIST CSF does not explicitly mention email, though it may be inferred to be included in control PR.PT-4, which primarily focuses on securing communications networks.
- CIS Controls in Control 9 Email and Web Browser Protections, especially in safeguards 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients and 9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions. Some safeguards are relevant to network management and email protections, such as 9.6 Block Unnecessary File Types.

Security Awareness Training

Security awareness training is often touted as one of the most important preventive controls because it addresses the weakest link in most organizations' cybersecurity defenses: the people with access to system resources. General security awareness training provides best practices for using standard workplace tools — such as email, the internet, cloud-based applications, and file storage — without falling victim to social engineering, phishing, or other types of cyberattacks. Targeted security training may also be offered to personnel with security-sensitive roles, like software developers, **system administrators**, and technical support staff.

The CISO is often responsible for developing, or advising on the selection of, general and targeted security awareness training. An audit of cybersecurity operations should evaluate whether all appropriate personnel complete general and targeted security training, and whether the CISO ensures participation through monitoring, reporting, and other management controls.

Training controls are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practices APO07.03 Maintain the Skills and Competencies of Personnel and APO07.06 Manage Contract Staff.
- NIST SP 800-53r5 in the Awareness and Training control family, especially controls AT-2 Literacy Training and Awareness and AT-3 Role-based Training.
- The NIST CSF discusses training in controls PR.AT-1: All users are informed and trained, and PR.AT-2: Privileged users understand roles and responsibilities.
- CIS Controls throughout control 14 Security Awareness and Skills Training, and in safeguard 16.9 Train Developers in Application Security Concepts and Secure Coding.

Detection

Sometimes, even with adequate protective controls, internal or external cyber attackers can disrupt, misappropriate, or infiltrate an organization's information resources. When such events, known as cyber **incidents**, occur, management needs to be able to detect and analyze the attack's impact before beginning a process of response and recovery. This section focuses on controls that detect instances of, or conditions that could lead to, unauthorized: access, changes, or communications with external systems.

In some organizations, it may be important to distinguish between IT monitoring and cybersecurity monitoring. IT monitoring is typically focused on service availability, capacity utilization, configuration and file integrity, and other primarily operational metrics. Cybersecurity monitoring looks for signs that may indicate a cyber incident has occurred or is ongoing. The impacts of a cyber incident may also be to disrupt system availability, capacity, or configurations, so there is often considerable overlap between IT and cybersecurity monitoring in the events they cover. Therefore, the IS team should examine the root causes of specific IT incidents to look for the common attributes of possible cyber incidents. The cybersecurity monitoring tools might even use artificial intelligence or machine learning technologies to assist in detecting cyber incident patterns.

Vulnerability scanning and penetration testing are additional controls usually managed by the CISO, though always in close collaboration with teams who support applications and other technology layers. The CISO may be responsible for managing some of these controls or overseeing those managed by IT or other departments. When planning a cybersecurity operations audit, it may be helpful to include only the detective controls managed by the CISO, with IT-managed controls designated to separate audit subjects. Such an approach may help keep the engagement to a more manageable size.

Cybersecurity Monitoring

Cybersecurity monitoring typically includes system event **log monitoring** and network traffic analysis to identify actions, services, or users needing further examination. Forensic analysis may then determine whether a cyber incident is the root cause of a system outage or operational anomaly. Many organizations establish a security operations center, usually managed by the CISO, to centralize and standardize the technologies and practices used to ensure adequate visibility into and control over enterprise assets.

One common technology, known as a **security information and event management** application, collects security **event logs** from other systems for the CISO team's analysis and reporting. The evidentiary trails of many types of cyber incidents can be found in logs tracking a variety of operations and processes, including:

- The establishment of connections to unknown or unauthorized external systems.
- The elevation of system permissions for certain IDs.
- The deactivation of certain logging functions.

Other types of controls combine elements of prediction, monitoring, and analysis to detect vulnerabilities or intrusions. For example, technologies designed to attract cyber attackers — such as **honeypots** — can help detect vulnerabilities by confirming the presence of malicious actors and analyzing their origins and actions. Similarly, the IS team may conduct targeted analyses, often called threat hunting, to detect compromised systems or **advanced persistent threats** that have evaded other prevention and detection controls.

Some related controls, often managed by a network operations team, include intrusion prevention and detection capabilities that are embedded in most network management devices. Such controls are covered more extensively in other GTAGs, notably "Auditing Mobile Computing."

An audit of cybersecurity operations would generally focus a considerable amount of its resources on examining monitoring controls. Engagement objectives may include verifying whether cybersecurity monitoring controls cover sensitive systems or environments, and whether tools are correctly configured to use available, beneficial capabilities.

Relevant cybersecurity monitoring controls are described in:

- COBIT 2019: Framework: Governance and Management Objectives, most directly in objective DSS05 Managed Security Services, but also as applicable to both IT and cybersecurity monitoring in practices:
    - DSS01.02 Manage Outsourced I&T Services.
    - DSS01.03 Monitor I&T Infrastructure.
    - DSS03.01 Identify and Classify Problems.
    - DSS03.02 Investigate and Diagnose Problems.
    - DSS03.03 Raise Known Errors.
    - DSS03.04 Resolve and Close Problems.
    - DSS03.05 Perform Proactive Problem Management.
- NIST SP 800-53r5, controls:
    - AU-5 Response to Audit Logging Process Failures.
    - AU-6 Audit Record Review, Analysis, and Reporting.
    - AU-14 Session Audit.
    - CA-7 Continuous Monitoring.
    - RA-10 Threat Hunting.
    - SC-26 Decoys.
    - SC-31 Covert Channel Analysis.
    - SI-4 System Monitoring.
    - SI-6 Security and Privacy Function Verification.
    - SI-7 Software, Firmware, and Information Integrity.
    - SI-15 Information Output Filtering.
- In the NIST CSF, related guidance covers the following objectives:
    - Event data is collected, analyzed to understand impact, and communicated (DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.DP-4).
    - Incident alert thresholds are established (DE.AE-5).
    - Malicious code, including mobile code, and unauthorized personnel, connections, devices, and software are detected (DE.CM-4, DE.CM-5, DE.CM-7).
    - Software, hardware, and information integrity checking mechanisms are implemented (PR.DS-6, PR.DS-8).

    - Detection processes are tested (DE.DP-3).
- CIS Controls throughout control 8 Audit Log Management, and in safeguards:
    - 1.2 Address Unauthorized Assets.
    - 2.3 Address Unauthorized Software.
    - 3.14 Log Sensitive Data Access.
    - 13.1 Centralize Security Event Alerting.
    - 13.2 Deploy a Host-Based Intrusion Detection Solution.
    - 16.3 Perform Root Cause Analysis on Security Vulnerabilities.
    - 16.14 Conduct Threat Modeling.

Vulnerability Management

Controls to identify and proactively remediate weaknesses in the code or configuration of information resources, which potentially could be exploited by cyber attackers, mainly consist of vulnerability scanning and penetration testing. The CISO usually establishes the policy for vulnerability management, though IT support teams often are responsible for testing and managing updates to their respective assets.

Vulnerability scanning applications compare a database of known weaknesses in commercial software coding or configurations to an organization's environment to identify whether such conditions are present. The weaknesses are typically assigned a score — for example, based on the **common vulnerability scoring system** — that many organizations use in their policies for prioritization and desired timeliness of resolution. A cybersecurity operations audit would typically verify whether identified weaknesses were effectively addressed within established timelines, and escalation processes invoked when appropriate.

Penetration testing consists of the organization employing security experts, sometimes called ethical **hackers**, to attempt to access the organization's information resources to identify weaknesses that should be addressed. Typically, the CISO manages penetration-testing engagements and works with technology support teams to remediate findings. A cybersecurity operations audit should verify whether the organization conducts penetration tests on high-risk environments, and whether identified weaknesses are dealt with effectively, similar to the expectations for issues identified by vulnerability scanning.

Software patch management and version release controls, which may be relevant to remediating identified weaknesses in application coding, are covered more extensively in the GTAG "Auditing Business Applications."

Controls over vulnerability scanning and penetration testing are described in:

- COBIT 2019: Framework: Governance and Management Objectives, in practices:
    - DSS05.07 Manage Vulnerabilities and Monitor the Infrastructure for Security-Related Events.
    - DSS05.02 Manage Network and Connectivity Security.
- NIST SP 800-53r5 controls:
    - RA-5 Vulnerability Monitoring and Scanning.

    - SI-2 Flaw Remediation.
    - SI-5 Security Alerts, Advisories, and Directives.
    - CA-8 Penetration Testing.
- In the NIST CSF, related guidance covers the following objectives:
    - A vulnerability management plan is developed and implemented (PR.IP-12).
    - Vulnerability scans are performed (DE.CM-8).
    - Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers) [RS.AN-5].
- CIS Controls, mainly in:
    - Control 7 Continuous Vulnerability Management.
    - Control 18 Penetration Testing.
    - Safeguard 16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities.
    - Safeguard 16.13 Conduct Application Penetration Testing.

Conclusion

Cybersecurity operations controls safeguard the confidentiality, integrity, and availability of systems and data by preventing and detecting cyberattacks. The CISO and IS team should be actively involved in system design and development processes to ensure that security mechanisms are embedded as core functionalities. The CISO also is responsible for working with IT support teams to implement or oversee preventive and detective controls to mitigate the likelihood or impact of cyber incidents. Audits of cybersecurity operations should identify risks and controls relevant to the organization's environment, then determine whether controls have been adequately designed and implemented to take advantage of common technological capabilities to thwart cyber attackers. In its assurance and advisory services, the internal audit activity can provide valued insight to all stakeholders by incorporating the control guidance found in widely used frameworks into a systematic evaluation of the organization’s policies and procedures.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency
Standards
Standard 1200 – Proficiency and Due Professional Care
Standard 1210 – Proficiency
Standard 1220 – Due Professional Care
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2220 – Engagement Scope
Guidance and Other Resources
GTAG "Assessing Cybersecurity Risk – The Three Lines Model," 2020
GTAG "Auditing Business Applications," 2021
GTAG "Auditing Identity and Access Management," 2021
GTAG "Auditing Insider Threat Programs," 2018
GTAG "Auditing IT Governance," 2018
GTAG "Auditing Mobile Computing," 2022
GTAG "Information Technology Outsourcing," 2012
GTAG "IT Change Management: Critical for Organizational Success, 3rd Edition," 2020
GTAG "IT Essentials for Internal Auditors," 2020
The Institute of Internal Auditors *The IIA's Three Lines Model: An Update of the Three Lines of Defense*

Appendix B. Glossary

Definitions of terms marked with an asterisk are taken from the "Glossary" contained in The IIA's publication, "*International Professional Practices Framework*®, 2017 edition" (also known as the Red Book), published by the Internal Audit Foundation. Other sources are either defined for the purposes of this document or derived from the following sources:

- ISACA, *"*Glossary"*,* Information technology terms and definitions, accessed May 20, 2022. https://www.isaca.org/resources/glossary.
- Joint Task Force, NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, "Glossary," accessed May 20, 2022. https://csrc.nist.gov/glossary.

access rights – The permission or privileges granted to users, programs, or workstations to create, change, delete, or view data and files within a system, as defined by rules established by data owners and the information security policy [ISACA Glossary].

advanced persistent threat – An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives [NIST Glossary].

antivirus software – An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected [ISACA Glossary].

application – A computer program or set of programs that performs the processing of records for a specific function**.** Contrasts with systems programs, such as an operating system or network control program, and with utility programs [ISACA Glossary].

assurance services* – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system [NIST SP 800-53r5 Glossary].

availability – Ensuring timely and reliable access to and use of information [NIST SP 800-53r5 Glossary].

board* – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

business rules – Representations of business processes and constraints that are encoded into applications to fulfill user requirements.

cipher – An algorithm to perform encryption [ISACA Glossary].

common vulnerability scoring system – A system for measuring the relative severity of software flaw vulnerabilities [NIST Glossary].

compliance* – Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

confidentiality [of systems or data] **–** Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information [ISACA Glossary].

consulting services* – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

control(s)* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient action to provide reasonable assurance that objectives and goals will be achieved.

decryption – A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader. The decryption is a reverse process of the encryption [ISACA Glossary].

decryption key – A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption [ISACA Glossary].

encryption – The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext) [ISACA Glossary].

encryption key – A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext [ISACA Glossary].

engagement* – A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

engagement objectives – broad statements developed by internal auditors that define intended engagement accomplishments.

event log – Chronological record of system activities, like access attempts, role creation, user account creation or deactivation, etc. (See "audit log" in NIST SP 800-53r5 Glossary).

governance* – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

hacker – An individual who attempts to gain unauthorized access to a computer system [ISACA Glossary].

honeypot – A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems. Scope Notes: Also known as "decoy server" [ISACA Glossary].

identity – A unique label used by a system to indicate a specific entity, object, or group [NIST SP 800-53r5 Glossary].

incidents – Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service [ISACA Glossary].

information security – Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability) [ISACA Glossary].

information technology controls* — Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

integrity [of systems or data] – The guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity [ISACA Glossary].

internal audit activity* - A department, division, team of consultants, or other practitioners(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

least privilege – The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function [NIST SP 800-53r5 Glossary].

log monitoring – Using specialized software to scan event logs for patterns or anomalies that may indicate unauthorized accounts, access, or activities.

malware – Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Scope Notes: Malware is commonly taken to include

computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes [ISACA Glossary].

plaintext – Digital information, such as cleartext, that is intelligible to the reader [ISACA Glossary].

phishing – A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Scope Notes: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack [ISACA Glossary].

privacy – The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. Scope Notes: What is appropriate depends on the associated circumstances, laws and the individual's reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use and disclosure of his or her associated personal and sensitive information [adapted from ISACA Glossary].

residual risk – The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk) [*Internal Auditing: Assurance & Advisory Services, 4th ed.*].

risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

risk management* – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

security information and event management – An application that is used to analyze security alerts and similar information generated by information resources, to help determine whether an incident has occurred.

should* – The *Standards* use the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

social engineering – An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information [ISACA Glossary].

spear phishing – A targeted attack where social engineering techniques are used to masquerade as a trusted party to obtain sensitive information (personal, financial, intellectual property, etc.) or install malware [ISACA Glossary].

system administrators – Personnel authorized to configure and support the operation of an IT resource.

system architects – Personnel responsible for designing or approving systems that meet internal requirements and integrate with current or planned infrastructure.

threat vector – The path or route used by the adversary to gain access to the target [ISACA Glossary].

user – Individual, or (system) process acting on behalf of an individual, authorized to access a system [NIST SP 800-53r5 Glossary].

Appendix C. References

Anderson, Urton L., Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, and Paul J. Sobel. *Internal Auditing: Assurance & Advisory Services, 4th edition.* Lake Mary, FL: The Internal Audit Foundation, 2017. https://www.theiia.org/en/products/bookstore/internal-auditing-assurance--advisory-services-fourth-edition/

Association of International Certified Professional Accountants. "TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," March 2020. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.

Center for Internet Security. "CIS Critical Security Controls Version 8." Accessed May 20, 2022. https://www.cisecurity.org/controls/v8/.

The Institute of Internal Auditors. *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. Lake Mary. The Institute of Internal Auditors, 2020. https://www.theiia.org/en/content/articles/-global-knowledge-brief/2020/july/the-iias-three-lines-model/.

ISACA. Control Objectives for Information Technologies (COBIT) 2019. Online framework and guidance. Accessed May 20, 2022. https://www.isaca.org/resources/cobit.

ISACA. "Glossary." Information technology terms and definitions. Accessed May 20, 2022, https://www.isaca.org/resources/glossary.

Joint Task Force. NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5. Gaithersburg, MD: NIST, September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST Computer Security Resource Center. "Glossary." Accessed May 20, 2022, https://csrc.nist.gov/glossary.

Acknowledgements

IT Guidance Development Team

Jim Enstrom, CIA, United States

Ruth Mueni Kioko, CIA, Kenya

Avin Mansookram, CISA, CGEIT, South Africa

Scott Moore, CIA, United States

Manoj Satnaliwala, CIA, CPA, CISA, United States

Terence Washington, CIA, CRMA, United States

Global Guidance Council Reviewers

Jose Esposito Li Carrillo, CIA, CRMA, Peru

Susan Haseley, CIA, United States

Larry Herzog-Butler, CIA, CRMA, Germany

Karem Obeid, CIA, United Arab Emirates

Elodie Sourou, CIA, Canada

International Internal Audit Standards Board Reviewers

Naji Fayad, CIA, Saudi Arabia

Hans Peter Lerchner, CIA, CRMA, Austria

IIA Global Standards and Guidance

David Petrisky, CIA, CRMA, CPA, CISA, Director, (Project Lead)

Dr. Lily Bi, CIA, QIAL, CRMA, CISA, Executive Vice President

Anne Mercer, CIA, CFSA, CFE, Senior Director

Shelli Browning, Associate Manager

Helen Nicholson, Content Writer and Technical Editor

Geoffrey Nordhoff, Content Writer and Technical Editor

The IIA thanks the following oversight bodies for their support: Information Technology Knowledge Group, Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 210,000 members and has awarded 180,000 Certified Internal Auditor (CIA) designations worldwide. The IIA is recognized as the internal audit profession's leader in standards, certification, advocacy, education, research, and technical guidance throughout the world. The IIA's global headquarters is located in Lake Mary, Fla. For more information, visit www.theiia.org.

Disclaimer

Copyright

May 2022

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