Auditing Cybersecurity Operations: Prevention and Detection

2nd Edition

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

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

2nd Edition Reviewers

Nur Hayati Baharuddin, CIA, CCSA, CFSA, CGAP, CRMA, Malaysia

Tichaona Zororo, CIA, CRMA, South Africa

International Internal Audit Standards Board Reviewers

Naji Fayad, CIA, Saudi Arabia

Hans Peter Lerchner, CIA, CRMA, Austria

2nd Edition Reviewers

Peter Elam, CIA, QIAL, CRMA, United Kingdom

Dominique Vincenti, CIA, CRMA, United States

IIA Standards and Guidance

Benito Ybarra, CIA, CFE, CISA, CCEP, Executive Vice President

Katleen Seeuws, CIA, CGAP, CRMA, CFE, Vice President

George Barham, CIA, CRMA, CISA, Director (Project Co-lead)

William Truett, CISA, Senior Manager (Project Co-lead)

The IIA would like to thank the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About the IPPF

A framework provides a structural blueprint and coherent system that facilitates the consistent development, interpretation, and application of a body of knowledge useful to a discipline or profession. The International Professional Practices Framework® (IPPF)® organizes the authoritative body of knowledge, promulgated by The Institute of Internal Auditors, for the professional practice of internal auditing. The IPPF includes Global Internal Audit Standards™, Topical Requirements, and Global Guidance.

International Professional Practices Framework® (IPPF)

The IPPF addresses current internal audit practices while enabling practitioners and stakeholders globally to be flexible and responsive to the ongoing needs for high-quality internal auditing in diverse environments and organizations of different purposes, sizes, and structures.

Global Guidance

Global Guidance supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.

Global Guidance provides detailed approaches, step-by-step processes, and examples on subjects including:

- Assurance and advisory services.
- Engagement planning, performance, and communication.
- Financial services.
- Fraud and other pervasive risks.
- Strategy and management of the internal audit function.
- Public sector.
- Sustainability.
- Global Technology Audit Guides® (GTAG®) provide auditors with the knowledge to perform assurance and advisory services related to an organization's information technology and information security risks and controls.

Global Guidance is available as a benefit of membership in The IIA.

Contents

Executive Summary

Cybersecurity, which focuses on protecting digital data and systems from cyber threats, is a subset of the broader topic of information security. 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. These are expressed in the *NIST Cybersecurity Framework (CSF) 2.0* as six functions: Identify, Protect, Detect, Respond, Recover, and Govern.

In the broadest sense, IT or IS teams may manage cybersecurity risks and controls, depending on the activity under review and the organization's unique environment. In this document, "cybersecurity operations" refers 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 such as encryption, email and network filters, and antivirus and data loss prevention (DLP) software aim to prevent 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 identify control weaknesses or the presence of entities or objects acting maliciously in the computing environment so they may be addressed. These tools and processes include event log monitoring and forensic analysis of system outages or anomalies, vulnerability management, and penetration testing.

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 function adds value to the organization when it provides such services in conformance with the Global Internal Audit Standards™ and with references to widely accepted control frameworks, particularly those 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.

According to The IIA's Three Lines Model, 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.[1] 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 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, CIO is used to refer to the leader of the IT function and CISO for the IS function's leader. 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 function** — the third line — provides independent **assurance services** and **advisory services** regarding the adequacy and effectiveness of IT-IS processes, including cybersecurity operations; therefore, it is important that internal auditors develop their understanding of cybersecurity governance, risk management, and control processes (Standard 9.1 Understanding Governance, Risk Management, and Control Processes). The internal audit function should consider cybersecurity risks in planning and prioritizing its audit **engagements**

Note

Terms in **bold** are defined in the glossary in Appendix B.

The Global Internal Audit Standards™ use certain terms as defined in the glossary. To understand and implement the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

The Standards use the word "must" in the "Requirements" sections and the words "should" and "may" to specify common and preferred practices in the "Considerations for Implementation" sections.

1. The Institute of Internal Auditors. The IIA's Three Lines Model: An Update of the Three Lines of Defense.

(Standard 9.4 Internal Audit Plan). To prevent and detect cyberattacks, the organization and internal audit function should consider high-level questions including:

- Which resources are the likeliest targets for cyberattacks?
- Who has access to the organization's most valuable information?
- 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 function can provide the organization's **board** and management with a comprehensive, tailored view of the effectiveness and efficiency of cybersecurity operations controls, including **residual risks** that may require further mitigation. The "Considerations for Implementation" section of Standard 8.1 Board Interaction advises the CAE to seek the board's perspectives and expectations related to its understanding and oversight of cybersecurity, among other issues not strictly financial.

Auditing cybersecurity operations involves an engagement-level **risk assessment** (Standard 13.2 Engagement Risk Assessment), a specified scope and **engagement objectives** (Standard 13.3 Engagement Objectives and Scope), and tests to evaluate the design and implementation of relevant controls (Standard 13.4 Evaluation Criteria) to determine whether any significant risk exposures exist. This approach helps internal auditors demonstrate conformance with Standards 3.1 Competency and 4.2 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

Cybersecurity Topical Requirement

The IIA's Topical Requirements are a mandatory element of the IPPF, required for assurance engagements and recommended for advisory engagements. To conform with the IPPF, internal auditors must apply Topical Requirements when the topic is the subject of an engagement in the internal audit plan, identified while performing an engagement, or the subject of an engagement request not on the original internal audit plan. The IIA's Cybersecurity Topical Requirement provides baseline criteria for assurance engagements assessing governance, risk management, and control processes related to cybersecurity. The Cybersecurity Topical Requirement is accompanied by a user guide that provides practical examples and considerations for determining when and how to conform with the cybersecurity requirements.

Learn more at theiia.org/TopicalRequirements.

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 the 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 lists these sources as references. 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 2.0* (also referred to as the *NIST Cybersecurity Framework 2.0* or *NIST CSF*).
- *CIS Controls Version 8.1* 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 IIA's Global Technology Audit Guide "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 developing the **engagement work program**.

Incorporating a review of external guidance into **engagement planning** helps an internal auditor demonstrate the essence of Principle 4 Exercise Due Professional Care, which states: "Internal auditors apply due professional care in planning and performing internal audit services." The principle's description wisely recognizes: "When exercising due professional care, internal auditors perform in the best interests of those receiving internal audit services but are not expected to be infallible."

Cybersecurity GTAGs

Cybersecurity risks and controls are primarily covered in three additional 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 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 *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 governance, risk management, and control processes.
- 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 advisory services provided by the internal audit function.
- Understand approaches to auditing cybersecurity operations, including specific controls that should be evaluated.

Cybersecurity Operations Controls

This guide provides brief descriptions of cybersecurity operations controls categorized under three high-level objectives: security in design, prevention, and detection. It includes references to the four IT-IS control frameworks listed previously. The internal audit function can supplement its collective knowledge of control best practices by reviewing one or more of these or other IT-IS control frameworks.

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: governance includes the establishment and management of IT-IS policies and budgets, and processes ensuring alignment among organizational and IT-IS strategies. Risk mangement 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 (representations of business processes and constraints that are encoded into **applications** to fulfill user requirements).

> **Note**
>
> The AICPA Trust Services Criteria categorizes technology control objectives as including security, availability, process integrity, confidentiality, 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 function to consider when planning a cybersecurity operations engagement include:

- Are IS policies and controls deep and broad enough 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 IT 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 in other GTAGs, including: "Auditing IT Governance"; "Assessing Cybersecurity Risk: The Three Lines Model"; and "IT Change Management: Critical for Organizational Success."

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

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
  - EDM01.02 Direct the Governance System.
  - EDM01.03 Monitor the Governance System.
  - 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.
  - APO12.02 Analyze 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.
- DSS05.07 Manage Vulnerabilities and Monitor the Infrastructure for Security-related Events.
- DSS06.01 Align Control Activities Embedded in Business Processes with Enterprise Objectives.
- 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:
  - Cybersecurity is included in human resources practices (GV.RR-04).
  - Roles and responsibilities for protection and detection are defined (PR.AT-01, PR.AT-02, GV.RR-01, GV.RR-02).
  - Configuration management practices are established and applied (PR.PS-01).
  - Protection and detection processes are improved (ID.IM-02, ID-IM-03).

- *CIS Controls* 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 work with senior management to identify, authorize, and deploy technology to meet business needs and objectives. System architects are responsible for designing or approving systems that meet internal requirements and integrate with current or planned infrastructure. Solution providers may include internal or external software developers, project managers, vendors, and others.

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 the 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 (creating an **event log**), such as when new user accounts are created or an existing account's privileges are escalated. 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 of this guide.

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 engagement in this area could look for evidence that the development and procurement processes for significant resources include 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; and Deliver, Service and Support. 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 these objectives:
  - Configuration management practices are established and applied (PR.PS-1, ID.AM-03).
  - Systems, hardware, software, services, and data are managed throughout their life cycles (ID.AM-08).
  - Networks and environments are protected from unauthorized logical access and usage (PR.IR-01).
  - Log records are generated and made available for continuous monitoring (PR.PS-04).
- *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 may be considered in an evaluation of cybersecurity operations. They include verifying whether the CISO has formalized and implemented standards for and reviews of nonemployee IDs and authentication methods used throughout the enterprise.

This guide does not detail physical access controls, which are often designed and implemented by facility management personnel, rather than IT or IS teams. 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 practices:
  - DSS05.04 Manage User Identity and Logical Access.
  - DSS05.05 Manage Physical Access to I&T Assets.
  - DSS06.03 Manage Roles, Responsibilities, Access Privileges and Levels of Authority.
  - DSS06.06 Secure Information 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 these objectives:
  - Identities and credentials for authorized users, services, and hardware are managed by the organization (PR.AA-01, PR.AA-02, PR.AA-05).
  - Physical access to assets is managed, monitored, and enforced (PR.AA-06).
  - Users, services, and hardware are authenticated (ID.AM-08, PR.AA-03, PR.AA-05, PR.IR-01, PR.PS-02).
  - The confidentiality, integrity, and availability of data-at-rest are protected (PR.DS-01, PR.PS-01).

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

Note

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 and 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* 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 these objectives:
  - Networks and environments are protected from unauthorized logical access and usage (PR.IR-01).
  - Protect data at rest and in transit (PR.DS-1, PR.DS-2).
  - Physical access to assets is managed, monitored, and enforced commensurate with risk (PR.AA-06, PR.IR-01).
- *CIS Controls* in 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 must protect themselves from the threat of malicious software (**malware**), which can target nearly any resource in their technology environment. **Antivirus software** protects against multiple types of malware and suspicious file types and can include monitoring for anomalous or restricted 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 policies and procedures 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* in controls SC-35 External Malicious Code Identification and SI-3 Malicious Code Protection.
- *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 the email protections listed below. However, the categorization of a control is usually less important than ensuring that it is included somewhere in the engagement planning and scoping.
  - 13.7 Deploy a Host-Based Intrusion Prevention Solution.

Data Loss Prevention

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 engagement may 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* in controls AU-13 Monitoring for Information Disclosure and PE-19 Information Leakage.
- *NIST CSF* discusses DLP in controls PR.DS-01, PR.DS-02, and PR.DS-10: The confidentiality, integrity, and availability of data-at-rest, data-in-transit, and data-in-use are protected.
- *CIS Controls* in Safeguard 3.13 Deploy a Data Loss Prevention Solution.

Email Protection

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 containing embedded malware or links to websites that gather information from or about individuals for malicious purposes are constantly bombarding enterprise email systems in either scattershot (phishing) or more targeted (**spear phishing or whaling**) approaches.

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

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 cyber controls available on the email platform have been configured appropriately and are adequate and whether additional capabilities have been evaluated and deployed.

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* in controls:
  - CA-3 Information Exchange.
  - SC-44 Detonation Chambers.
  - SI-8 Spam Protection.
- *NIST CSF* does not explicitly mention email, though it may be inferred to be included in Control PR.IR-01 on securing networks and environments from unauthorized logical access and usage.
- *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, including software developers, system administrators (personnel authorized to configure and support the operation of an IT resource), 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.
- *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 disrupt, misappropriate, or infiltrate an organization's information resources. When such events, known as cyber **incidents**, occur, management must 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 unauthorized access, changes, or communications with external systems or conditions that could lead to such incidents.

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. Cyber incidents may 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. Cybersecurity monitoring tools may 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 in close collaboration with teams that 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 engagement, 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 (using specialized software to scan event logs for patterns or anomalies that may indicate unauthorized accounts, access, or activities) 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, response, and reporting. The application is used to analyze security alerts and similar information generated by information resources to help determine whether an incident has occurred.

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.

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

Audits of cybersecurity operations generally focus considerable 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 these objectives:
  - Event data is collected, analyzed to understand impact, and communicated (DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.AE-06).
  - Incidents are declared when adverse events meet the defined criteria (DE.AE-08).
  - Malicious code, including mobile code, and unauthorized personnel, connections, devices, and software are detected (DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09).
  - Software, hardware, and information integrity checking mechanisms are implemented (PR.DS-01, PR.CM-09, ID.RA-09).
  - Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties (DE.IM-02).

- *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 engagement would typically verify whether identified weaknesses were effectively addressed within established timelines and whether escalation processes were 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. Typically, the CISO manages penetration-testing engagements and works with technology support teams to remediate **findings**. A cybersecurity operations audit engagement should verify whether the organization conducts penetration tests on high-risk environments and whether identified weaknesses are dealt with effectively, in a manner similar to the 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:
  - DSS05.02 Manage Network and Connectivity Security.
  - DSS05.07 Manage Vulnerabilities and Monitor the Infrastructure for Security-Related Events.
- *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 these objectives:
  - Vulnerabilities in assets are identified, validated, and recorded (ID.RA-01).
  - Processes for receiving, analyzing, and responding to vulnerability disclosures are established (ID.RA-08).

- *CIS Controls* 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 is also responsible for working with business and IT support teams to implement and oversee preventive and detective controls to mitigate the likelihood or impact of cyber incidents.

Audit engagements of cybersecurity operations should identify risks and controls relevant to the organization's environment and then determine whether controls have been adequately designed and implemented to take advantage of common technological capabilities that impede or prevent cyberattacks. In its assurance and advisory services, the internal audit function can provide valued insight to **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 in this guide.

Standards and Principles
3.1 Competency
Principle 4 Exercise Due Professional Care
4.2 Due Professional Care
8.1 Board Interaction
9.1 Understanding Governance, Risk Management, and Control Processes
9.4 Internal Audit Plan
13.2 Engagement Risk Assessment
13.3 Engagement Objectives and Scope
13.4 Evaluation Criteria
Topical Requirements, Global Guidance, and Other IIA Resources
The IIA's "Cybersecurity Topical Requirement"
GTAG "Assessing Cybersecurity Risk – The Three Lines Model"
GTAG "Auditing Business Applications"
GTAG "Auditing Cyber Incident Response and Recovery
GTAG "Auditing Identity and Access Management"
GTAG "Auditing Insider Threat Programs"
GTAG "Auditing IT Governance"
GTAG "Auditing Mobile Computing"
GTAG "IT Change Management: Critical for Organizational Success, 3rd Edition"
GTAG "IT Essentials for Internal Auditors"
The IIA's *Three Lines Model: An Update of the Three Lines of Defense*

Appendix B. Glossary

Definitions are taken from the "Glossary" within The IIA's publication, Global Internal Audit Standards, 2024 Edition, unless otherwise noted as being from these sources:

- ISACA, Glossary, accessed Jan. 17, 2025, https://www.isaca.org/resources/glossary.
- Joint Task Force, *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5*, Glossary, (National Institute of Standards and Technology, September 2020), https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, Glossary, accessed Jan. 17, 2025. 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].

activity under review – The subject of an internal audit engagement. Examples include an area, entity, operation, function, process, or system.

advanced persistent threat – An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (for example cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend its presence 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 CSRC Glossary].

advisory services – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."

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 – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.

assurance services – Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational or performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed.

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 – Highest-level body charged with governance, such as:

- A board of directors.
- An audit committee.
- A board of governors or trustees.
- A group of elected officials or political appointees.
- Another body that has authority over the relevant governance functions.

In an organization that has more than one governing body, "board" refers to the body or bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.

If none of the above exists, "board" should be read as referring to the group or person that acts as the organization's highest-level governing body. Examples include the head of the organization and senior management.

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

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

compliance – Adherence to laws, regulations, contracts, policies, procedures, and other requirements.

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

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.

control process – The policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

criteria – In an engagement, specifications of the desired state of the activity under review (also called "evaluation criteria").

cybersecurity – The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems [ISACA Glossary].

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 or project that includes multiple tasks or activities designed to accomplish a specific set of related objectives. See also "assurance services" and "advisory services."

engagement objectives – Statements that articulate the purpose of an engagement and describe the specific goals to be achieved.

engagement planning – Process during which internal auditors gather information, assess and prioritize risks relevant to the activity under review, establish engagement objectives and scope, identify evaluation criteria, and create a work program for an engagement.

engagement work program – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors assigned to perform the tasks. The work program is based on information obtained during engagement planning.

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

finding – In an engagement, the determination that a gap exists between the evaluation criteria and the condition of the activity under review. Other terms, such as "observations," may be used.

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 so that their actions do not affect production systems. [ISACA Glossary].

impact – The result or effect of an event. The event may have a positive or negative effect on the organization's strategy or business objectives.

incidents – A violation or imminent threat of violation of computer security policies, acceptable use policies, guidelines or standard security practices [ISACA Glossary].

information security – The assurance that information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and nonaccess when required (availability). Information security deals with all formats of information — paper documents, digital assets, intellectual property in people's minds and verbal and visual communications [ISACA Glossary].

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

internal audit function - A professional individual or group responsible for providing an organization with assurance and advisory services.

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].

likelihood – The probability that a given event will occur.

malware – Malicious software designed to infiltrate or damage a computer system or obtain information from it without the owner's consent. Examples of malware include computer viruses, worms, Trojan horses, spyware, and adware. [ISACA Glossary].

phishing – A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine with the intention of obtaining information for use in social engineering. Scope Notes: For example, phishing attacks may take the form of an attacker 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 can be used in another form of active attack [ISACA Glossary].

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

privacy – The right 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. [ISACA Glossary].

residual risk– The portion of inherent risk that remains after management actions are implemented.

risk – The positive or negative effect of uncertainty on objectives.

risk assessment – The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed 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.

root cause – Core issue or underlying reason for the difference between the criteria and the condition of an activity under review.

senior management – The highest level of executive management of an organization that is ultimately accountable to the board for executing the organization's strategic decisions, typically a group of persons that includes the chief executive officer or head of the organization.

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

spear phishing – An attack designed to entice specific individuals or groups to reveal important information. Social engineering techniques are used to masquerade as a trusted party to obtain important information, such as passwords from the victim [ISACA Glossary].

stakeholder – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers, vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.

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].

whaling – A specific kind of phishing that targets high-ranking members of organizations [NIST CSRC Glossary].

Appendix C. References and Additional Reading

Association of International Certified Professional Accountants. “2017 Trust Services Criteria (With Revised Points of Focus – 2022)," September 2023. https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022.

Center for Internet Security. *CIS Critical Security Controls Version 8.1.* Accessed Feb. 11, 2025. https://www.cisecurity.org/controls/v8-1.

The Institute of Internal Auditors. *The IIA’s Three Lines Model: An Update of the Three Lines of Defense*. 2020. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/.

ISACA®. *COBIT® 2019 Framework*. Accessed Feb. 11, 2025. https://www.isaca.org/resources/cobit.

ISACA®. “Glossary.” Accessed Jan. 17, 2025. https://www.isaca.org/resources/glossary.

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

NIST Computer Security Resource Center. “Glossary.” Accessed Feb. 11, 2025. https://csrc.nist.gov/glossary.

About The Institute of Internal Auditors

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

Disclaimer

Copyright

Feb. 2025 (This version supersedes “Auditing Cybersecurity Operations: Prevention and Detection,” published in 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