IPPF
International Professional Practices Framework

Auditing Cyber Incident Response and Recovery

Supplemental Guidance | **Practice Guide**

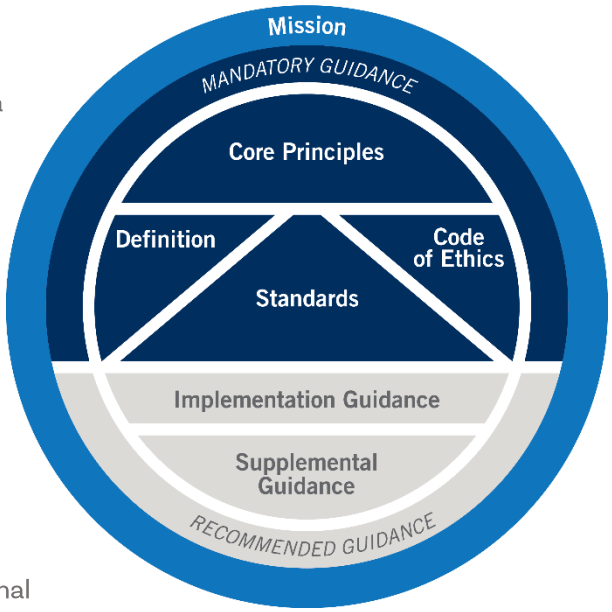
GLOBAL TECHNOLOGY AUDIT GUIDE

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.

IPPF | International Professional Practices Framework



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 attacks are increasing as the tools for detecting and exploiting vulnerabilities in networked systems and devices become increasingly sophisticated or commoditized. Threatening technologies and methods are advanced by criminal enterprises, state-sponsored hackers, and other individuals with malicious intentions. Nearly all organizations have some degree of risk exposure, and the potential impacts include a breach of customer data, direct financial loss, and physical manipulation of resources. Organizations employ governance and risk management techniques to protect against such risks, leading to the development of incident response plans for various types of attacks. However, even with a defense-in-depth strategy, sometimes a flaw in design, implementation, or human nature can be exploited. Controls are needed so that when a cyberattack is confirmed and an incident declared, an optimal response and recovery are ensured.

The primary controls for cyber incident response and recovery consist of planning for various cyberattack scenarios, then executing the plans as needed. Significant controls can be grouped into the following high-level business objectives:

1. Incident Response Planning – Policies and procedures should be established to guide the determination of whether an incident has occurred and what to do about it. The planning should involve key stakeholders, define roles and responsibilities, and be tested as appropriate to promote awareness and execution.
2. Incident Identification – Processes to analyze data from detective controls lead to the determination of the existence of a cyber incident, which typically is the trigger for the execution of one or more response plans.
3. Communications – There are many potential stakeholders in cyber incidents, so each response plan should incorporate a communications strategy for appropriate and timely notification of impacts and resolution efforts.
4. Technical Response and Recovery – The nature of the incident largely determines the necessary technical remediation and restoration controls, often involving coordination of efforts internally and externally.

Stakeholders, primarily an organization's governing body and senior management, rely on independent, objective, and competent assurance services to verify whether cyber incident response and recovery 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 information technology and information security 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. The terms cybersecurity and **information security** (IS) can essentially be used interchangeably, mainly due to the ubiquity of combining computing and communications technologies to enable business operations or products and services offered to customers. Threats to information resources may come from inside or outside the organization, and a wide range of **information technology (IT) controls**, including IS **controls**, collectively IT-IS controls, are available to prevent, detect, or mitigate the impact from **cyberattacks** (alternately referred to as **cyber incidents**).

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

A significant part of planning a cybersecurity defense strategy includes preparing for the possibility of a successful attack and having a plan in place to neutralize and eliminate the threat, remediate any damage inflicted on customers or operations, and resume operations in a strengthened state. Ideally, when a cyberattack is detected and confirmed by the IS function, a designated person — often a member of senior management — declares that a cyber incident has occurred (or is occurring) and invokes an appropriate planned response. Cyber incident response plans typically include protocols for communicating the issues and resolution efforts to stakeholders with a need to know or role to perform, as well as technical response plans that examine where vulnerabilities may have been exploited and determine appropriate fixes. In many organizations, cyber incident response and recovery plans are integrated with other organizational resilience planning efforts, including those that ensure **compliance** with external reporting requirements.

Unfortunately, incident response and recovery controls will probably be challenged regularly, due to the ease with which **bad actors** can automate some exploitation tools, and the endless virtual competition between attackers and defenders. Hence, most organizations employ a **defense-in-depth** strategy, where controls are tailored to various environments and **inherent risks**, creating overlapping or complementary protections to reduce the likelihood or impact of cyberattacks.

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. Many organizations separate the responsibilities by designating a chief information officer (CIO) for IT and a chief information security officer (CISO) for IS. Often, 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, many 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 cyber incident response and recovery controls. The internal audit activity **should** consider cyber incident response and recovery **risks** in its planning and prioritization of its audit **engagements**. Some high-level questions for the organization and the internal audit activity to consider include:

- Does the organization take a systematic approach to identifying, planning for, and responding to likely cyber incidents?
- Are incident response team member roles and responsibilities defined?
- Are the IS function's security event analysis controls adequately designed and reasonably mature?
- Have key stakeholders — including, perhaps, vendors and customers — been engaged in the design and testing of incident response plans?
- Have communication protocols with key stakeholders been incorporated into response plans?
- Would the organization be capable of responding quickly and effectively to eliminate a threat and resume strengthened operations?
- Is a continuous improvement process, with lessons learned from testing and actual cyber incidents, in place to update response and recovery plans?

Standard 2030 – Resource Management

The **chief audit executive** must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation:

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

By working closely with IT and IS, the internal audit activity can ensure senior management and the **board** get a clear and comprehensive view of the organization's preparedness for cyber incidents. Such a view would include an assessment of the adequacy and effectiveness of response and recovery controls, and identification of **residual risks** that may require further mitigation. Auditing cyber incident response and recovery controls 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. Following this approach helps internal auditors demonstrate conformance to 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 there are many others widely used around the world. 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 to 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.)

> **Note:** This guide cites control frameworks from NIST, ISACA and the Center for Internet Security (CIS). There are many other frameworks in use globally that can be compared to the ones cited here.

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* (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." Having a basic understanding of technology processes and terms provides a foundation for a review of 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."

> **Note:** The IIA's Code of Ethics states in Rule of Conduct 4.3, related to Competency, that internal auditors "shall continually improve their proficiency and the effectiveness and quality of their services."

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 availability of data are embedded in the design and operations of IT processes, so essentially all GTAGs have at least some useful guidance for assessing various aspects of cybersecurity.

Objectives

This guide will help the reader:

- Define cyber incident response and recovery.
- Develop a working knowledge of relevant processes, including related governance and risk management controls.
- Identify components of cyber incident response and recovery, including contributions from governance, risk management, and planning processes, as well as controls to test and execute response and recovery plans.
- Consider relevant control guidance in widely used IT-IS frameworks, to increase the value of assurance and consulting services provided by the internal audit activity.
- Understand approaches to auditing cyber incident response and recovery, including specific controls to be evaluated.

Cyber Incident Response and Recovery Controls

This section describes the context in which a cyber incident response and recovery audit engagement is planned. This is followed by brief descriptions of controls for responding to and recovering from identified cyber incidents, categorized under four high-level objectives:

- Incident Response Planning
- Incident Identification
- Communications
- Technical Response and Recovery

The discussion of each objective will include references to specific controls in various IT-IS control frameworks. A review of one or more IT-IS control frameworks, such as the ISACA, NIST, and CIS frameworks that are discussed below, as well as many others, will allow an internal audit activity to supplement its collective knowledge of control best practices.

Engagement Planning

Cyber incident response and recovery processes establish plans for various attack scenarios, to ensure impacts are mitigated and normal operations resumed as quickly as possible with minimum disruption. The plans include specified communications with stakeholders, and technical means to identify, neutralize, and eliminate **vulnerabilities** and cyberattacks from the organization's environment. Cyber incident recovery processes – which are often incorporated into the organization's business continuity, disaster recovery, and resiliency processes – restore the operating environment to a normal, preferably strengthened, state. Internal audit activities can provide assurance and advisory services over cyber incident response and recovery processes by leveraging an understanding of established control guidance with evidence obtained of the maturity and effectiveness of relevant practices in their respective environments.

Standard 2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

To start assessments of cyber incident response and recovery controls, internal auditors usually begin with a top-down assessment of how related objectives and risks are handled in the organization's governance and risk management processes. They then develop an understanding of the significant technology systems and their level of participation in controls applied broadly across the enterprise. Cyber incident response and recovery controls are usually planned and applied organizationwide, so during engagement planning an auditor could verify whether all significant business **applications** and other key information resources are included in formalized plans.

A review of prior audits or reports from other assurance providers covering related risks and controls may also contribute valuable context to engagement planning. An engagement-level risk assessment is then performed to further refine the fieldwork program. For example, in accordance with Standard 2050 – Coordination and Reliance, controls that were not recently tested by other assurance providers might be reviewed more extensively than controls found to be adequate by other assurance providers whose work was performed with sufficient proficiency and due professional care. Similarly, if an internal auditor determines that management has tested or recently invoked cyber incident response and recovery plans, thereby raising awareness among key stakeholders and improving the performance of restoration activities, then the control environment may be considered mature and residual risks generally lower. Response and recovery controls applied to any IT resource should be commensurate with the system's **security category**, as well as relevant risks of **fraud** or regulatory compliance. During planning and fieldwork, internal auditors may advise on how the organization can increase the effectiveness of cyber incident response and recovery controls, thereby reducing various types of residual risks.

> **Standard 2050 – Coordination and Reliance**
>
> The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Incident Response Planning

Policies and procedures guide how a cyber incident is determined and what to do about it. Ideally, the plans are developed with input from key stakeholders and tested as appropriate to promote awareness and execution. Many of the relevant planning controls are discussed in greater detail in other GTAGs as follows:

- The GTAG "Assessing Cybersecurity Risk – The Three Lines Model" primarily covers the *NIST CSF* Identify function, which includes high-level control objectives (called categories) that it identifies as:
    - Asset Management.
    - Business Environment.
    - Governance.
    - Risk Assessment.

    - Risk Management Strategy.
    - Supply Chain Risk Management.
- The GTAG "Auditing Cybersecurity Operations" primarily covers the *NIST CSF* Protect and Detect functions, which include the categories:
    - Awareness and Training.
    - Data Security.
    - Information Protection Processes and Procedures.
    - Maintenance.
    - Protective Technology.
    - Anomalies and Events.
    - Security Continuous Monitoring.
    - Detection Processes.

However, there are a few subcategories of Identify and Protect that are particularly relevant to cyber incident response and recovery planning, as discussed in the following sections:

- Governance and Risk Management.
- Incident Plans.
- Lessons Learned.

Governance and Risk Management

The processes to oversee and direct an organization's cyber incident response and recovery controls generally follow a risk-prioritized approach that identifies minimum operating requirements for IT resources. The approach also includes contingency plans for various types of attacks, and the procurement of sufficient reserve capacity to implement recovery plans when necessary. These contingency plans are usually created by the IS function with inputs from business units that are the major beneficiaries of significant IT systems and from production support leaders.

Guidance in other GTAGs

Relevant governance and risk management processes are described in other GTAGs. This GTAG will focus on aspects of controls specific to response and recovery.

An internal audit engagement of risks and controls for cyber incident response and recovery may examine the maturity of the organization's control environment. This may include determining whether sufficient requirements, plans, and contingent operating capacity have been documented for significant business applications, infrastructure, or data. Indicators of a reasonably mature environment may include such evidence as early warning systems and risk analytics, and organizationwide planning efforts to establish response and recovery criteria, with periodic evaluations of the effectiveness and efficiency of those efforts.

Information technology governance and risk management controls related most specifically to cyber incident response and recovery risks are described in:

- *COBIT 2019 Framework: Governance and Management Objectives*, in practices:
    - APO12.06 Respond to Risk.
    - APO14.10 Manage Data Backup and Restore Arrangements.
    - BAI04.02 Assess Business Impact.
    - DSS01.02 Manage Outsourced I&T Services.
    - DSS04.01 Define the Business Continuity Policy, Objectives and Scope.
    - DSS04.02 Maintain Business Resilience.
    - MEA01.02 Set Performance and Conformance Targets.
- *NIST SP 800-53r5* in:
    - The Contingency Planning control family, starting with control CP-1 Contingency Planning Policy and Procedures.
    - The Incident Response control family, starting with control IR-1 Incident Response Policy and Procedures.
    - Control PM-6 Measures of Performance.
    - Control RA-9 Criticality Analysis.
    - Control SA-5 System Documentation.
- *NIST CSF* in subcategories:
    - ID.BE-5 Resilience Requirements to Support Delivery of Critical Services are Established for all Operating States (for example, Under Duress/Attack, During Recovery, Normal Operations).
    - PR.DS-4 Adequate Capacity to Ensure Availability is Maintained.
    - PR.IP-9 Response Plans (Incident Response and Business Continuity) and Recovery Plans (Incident Recovery and Disaster Recovery) are In Place and Managed.
- *CIS Controls* in safeguards:
    - 11.1 Establish and Maintain a Data Recovery Process.
    - 11.4 Establish and Maintain an Isolated Instance of Recovery Data.
    - 17.1 Designate Personnel to Manage Incident Handling.
    - 17.5 Assign Key Roles and Responsibilities.

Incident Plans

Incident response and recovery plans are the typical output of governance and risk management processes, and such plans are tested and practiced by management to improve their content and execution. These plans typically anticipate various attack scenarios and establish processes to identify the impacted resources, neutralize the threat, and restore operations.

The Mitre Corporation (MITRE) — a non-profit dedicated to cybersecurity research — publishes a cyberattack framework (called MITRE ATT&CK) that identifies 14 categories of incidents, each with several associated attack techniques. An audit in this area could compare the organization's incident response plans to this list, to see whether all major types of attacks have been considered. The MITRE ATT&CK framework's categories are:

- Reconnaissance – Includes 10 techniques.
- Resource Development – 7 techniques.
- Initial Access – 9 techniques.
- Execution – 12 techniques.
- Persistence – 19 techniques.
- Privilege Escalation – 13 techniques.
- Defense Evasion – 40 techniques.
- **Credential** Access – 15 techniques.
- Discovery – 29 techniques.
- Lateral Movement – 9 techniques.
- Collection – 17 techniques.
- Command and Control – 16 techniques.
- Exfiltration – 9 techniques.
- Impact – 13 techniques.

An internal audit engagement may review the extent and quality of the documentation within the incident response plans, to determine whether the organization's important systems and resources are described, rather than containing generic or high-level objective statements. Incident response plans generally identify key stakeholders and set expectations for effective, timely communication of potential impacts and resolution efforts. An audit could verify whether management has tested its plans on high-risk systems and with key stakeholders whose roles and responsibilities have been clearly defined. An internal audit engagement may also verify whether any issues identified during management's testing of incident response plans were subsequently resolved to reduce the residual risks.

So-called "tabletop" exercises, which allow key stakeholders to discuss response and recovery plans, and possibly even practice some routines, may provide useful evidence of the promotion of awareness and the adequacy of the design of plans. However, full-scale simulations are also necessary to produce evidence that systems are properly configured and resourced to provide expected levels of service.

Controls related to developing and testing cyber incident plans are described in:

- *COBIT 2019: Framework: Governance and Management Objectives* in practices:
    - DSS04.03 Develop and Implement a Business Continuity Response.
    - DSS04.04 Exercise, Test, and Review the Business Continuity Plan (BCP) and Disaster Response Plan (DRP).
    - DSS04.06 Conduct Continuity Plan Training.
    - MEA02.04 Identify and Report Control Deficiencies.
- *NIST SP 800-53r5* in controls:
    - CP-2 Contingency Plan.
    - CP-3 Contingency Training.

    - CP-4 Contingency Plan Testing.
    - IR-2 Incident Response Training.
    - IR-3 Incident Response Testing.
    - IR-9 Information Spillage Response.
    - PL-2 System Security and Privacy Plans.
- *NIST CSF* subcategories:
    - PR.IP-9 Response Plans (Incident Response and Business Continuity) and Recovery Plans (Incident Recovery and Disaster Recovery) are In Place and Managed.
    - PR.IP-10 Response and Recovery Plans are Tested.
    - ID.SC-5 Response and Recovery Planning and Testing are Conducted with Suppliers and Third-party Providers.
    - RS.CO-1 Personnel Know Their Roles and Order of Operations when a Response is Needed.
- *CIS Controls* in safeguards:
    - 7.2 Establish and Maintain a Remediation Process.
    - 11.3 Protect Recovery Data.
    - 11.5 Test Data Recovery.
    - 17.4 Establish and Maintain an Incident Response Process.
    - 17.7 Conduct Routine Incident Response Exercises.

Lessons Learned

Another important response and recovery planning control is the feedback loop of analyzing cyber incidents to determine how attacks occurred, for the purpose of strengthening controls where appropriate. Documenting and applying the lessons learned from cyber incidents can help an organization improve its protective defenses, detection of cyber incidents, and resilience. Members of the IS function typically perform a forensic (including root cause) analysis to determine whether a confirmed cyberattack's method of infiltration was detected by the organization's defensive controls. Alternatively, if the attack was not detected, the IS function will usually determine whether controls can be improved to strengthen defenses.

An audit engagement in this subject area could verify whether recent cyber incidents declared by the organization were analyzed to identify the vulnerabilities that were exploited. An auditor would also usually verify whether the analysis led to the implementation of corrective actions that addressed the vulnerabilities or otherwise improved communications and collaboration among key stakeholders.

Controls over the incorporation of lessons learned into improvements in cyber incident response and recovery plans include:

- *COBIT 2019: Framework: Governance and Management Objectives* practices:
    - APO12.01 Collect Data.
    - BAI09.02 Manage Critical Assets.
    - DSS02.07 Track Status and Produce Reports.
    - DSS04.05 Review, Maintain, and Improve the Continuity Plans.

    - DSS04.08 Conduct Post-resumption Review.
    - MEA02.01 Monitor Internal Controls.
- *NIST SP 800-53r5* controls:
    - AT-3 Role-based Training.
    - CA-2 Control Assessments.
    - SA-15 Development Process, Standards, and Tools.
    - SI-4 System Monitoring.
- The *NIST CSF* subcategories:
    - RS.AN-3 Forensics are Performed.
    - RS.IM-1 Response Plans Incorporate Lessons Learned.
    - RS.IM-2 Response Strategies are Updated.
    - RC.IM-1 Recovery Plans Incorporate Lessons Learned.
    - RC.IM-2 Recovery Strategies are Updated.
- *CIS Controls* safeguard 17.8 Conduct Post-Incident Reviews.

Incident Identification

The processes for determining whether a cyber incident has occurred — or is occurring — are closely linked to the cybersecurity monitoring controls discussed more extensively in the GTAG "Auditing Cybersecurity Operations: Prevention and Detection." While the detective controls typically look for indicators that a system or **user** is exhibiting suspicious behavior, identified anomalies usually require an analysis before a decision is made to invoke response and recovery plans. Such analyses are typically performed by people. However, artificial intelligence (AI) programs are increasing in sophistication and may be adopted by management to accelerate the identification of likely cyber incidents.

Another source of potential incident identification is external notifications of widespread threats, which an organization can use to assess whether its environment may be at risk. For example, when a vulnerability is discovered in a widely used operating system, an organization's IT and IS teams may determine whether that operating system is used in the organization's technology infrastructure and whether any further analysis or remedial actions need to be taken. Additionally, the IS function may analyze user reports of compromised credentials or unusual system performance to determine whether response and recovery plans — and which ones — should be invoked. An audit engagement will usually include evaluating the design and implementation of controls whose objectives are to identify cyber incidents in a timely fashion and invoke appropriate responses.

Determining and Declaring an Incident

A key part of incident identification is determining and then declaring that an incident has taken place. One of the challenges of cybersecurity defense is separating the signals of incidents from the noise of false-positive alerts. A security incident and event management (SIEM) application, or tools with similar capabilities, may be used by the IS function to receive, interpret, and assign data for analysis. Controls may be designed to automate some responses to specified patterns —

or use AI to identify suspicious actions — though manual processes will probably also be needed to provide specialized oversight and judgment.

When a decision is made to declare a cyber incident, the appropriate response and recovery plans need to be invoked, according to the incident's type. The planning controls described earlier typically result in formalized, tested courses of action that can be applied to a variety of attack scenarios.

An audit engagement in this area could assess whether the documented plans, sometimes referred to as playbooks, cover the common types of incidents for the organization's significant environments and resources. The most frequent or impactful types of attack scenarios may include **ransomware** or viruses delivered in emails or downloaded from the internet. Other possible **attack vectors** include third-party software or interfaces with external systems. The MITRE ATT&CK framework is a widely used, freely available benchmark for categorizing common cyberattack types, so if the organization does not already explicitly align its response and recovery playbooks to an established IT-IS control framework, recommending the use of such sources could be a well-received advisory recommendation.

Controls over declaring an incident and invoking a response and recovery plan are discussed in:

- *COBIT 2019: Framework: Governance and Management Objectives* in practices:
    - DSS02.01 Define Classification Schemes for Incidents and Service Requests.
    - DSS02.02 Record, Classify, and Prioritize Requests and Incidents.
    - DSS02.04 Investigate, Diagnose, and Allocate Incidents.
    - DSS03.01 Identify and Classify Problems.
    - DSS04.02 Maintain Business Resilience.
    - DSS05.07 Manage Vulnerabilities and Monitor the Infrastructure for Security-related Events.
- *NIST SP 800-53r5* controls:
    - IR-4 Incident Handling.
    - IR-5 Incident Monitoring.
    - IR-8 Incident Response Plan.
- *NIST CSF* subcategories:
    - DE.AE-5 Incident Alert Thresholds are Established.
    - RS.AN-1 Notifications from Detection Systems are Investigated.
    - RS.AN-2 The Impact of the Incident is Understood.
    - RS.AN-4 Incidents are Categorized Consistent with Response Plans.
    - RS.AN-5 Processes are Established to Receive, Analyze and Respond to Vulnerabilities Disclosed to the Organization from Internal and External Sources (for example, Internal Testing, Security Bulletins, or Security Researchers).
    - RS.MI-3 Newly Identified Vulnerabilities are Mitigated or Documented as Accepted Risks.
    - RS.RP-1 Response Plan is Executed During or After an Incident.
    - RC.RP-1 Recovery Plan is Executed During or After a Cybersecurity Incident.

- *CIS Controls* safeguards:
    - 13.11 Tune Security Event Alerting Thresholds.
    - 14.6 Train Workforce Members on Recognizing and Reporting Security Incidents.
    - 17.3 Establish and Maintain an Enterprise Process for Reporting Incidents.
    - 17.9 Establish and Maintain Security Incident Thresholds.

Processes to address the risks of incidents arising from properly authorized internal accounts are covered more extensively in the GTAG "Auditing Insider Threat Programs."

Communications

When a cyber incident is declared and a response plan invoked, the subsequent communications among IT, IS, and various other groups should follow established protocols determined in the governance and risk management processes described earlier. Such processes are often integrated with general crisis management and organizational resilience programs. The affected systems may support business processes owned by functions other than IT or IS, so the **business owners**, internal client or account managers, and production support teams are typically included in communication protocols, along with key personnel in the legal, public relations, executive, and other functions. Communication escalation triggers should be defined based on incident impact and severity, to ensure that decisions and actions are taken promptly.

Cyber Incident Communications

Many governments, globally, have established requirements for reporting cyber incidents to security, regulatory, or public constituencies, to facilitate identification of the perpetrators or enabling technologies, or for other public objectives. Compliance with any particular reporting requirement is beyond the scope of this GTAG.

Communications may need to move to alternate or personal platforms, especially if the organization's phone, email, or internet services are compromised or unavailable. Ideally, key stakeholders would be notified timely that a response plan has been invoked, and they would have previously practiced – or at least reviewed and understood – their respective roles.

Reporting cyber incidents — as well as remediation efforts — to external bodies, such as law enforcement or regulatory agencies, may be required in some cases. The compliance processes in an organization should ensure that such obligations are reflected in its procedures. An organization may also choose to participate in cyber incident information sharing groups, publicly or privately managed, to mitigate the spread of cyberattacks and improve common defense awareness and effectiveness.

Additional communications typically also need to be made to customers, investors, or other key stakeholders, potentially including the general public. The organization will usually designate personnel to manage the various lines of communication, ideally with a centralized, approved message for each constituency. Management usually tests communication plans along with technical response and recovery plans, to establish contacts and a shared understanding of the roles, procedures, and sources of information among the designated participants.

An audit of this group of risks and controls typically includes a review of compliance with external reporting requirements, as well as the maturity and value of the organization's voluntary participation in cyber defense initiatives. Additionally, documentation related to declared incidents may be reviewed to determine whether communication plans were properly executed, and the processes were effective at providing key stakeholders with timely, accurate, and relevant information about the incident and mitigation efforts.

Controls over cyber incident communications are discussed in:

- *COBIT 2019: Framework: Governance and Management Objectives* in practices:
    - EDM05.01 Evaluate Stakeholder Engagement and Reporting Requirements.
    - EDM05.02 Direct Stakeholder Engagement, Communication and Reporting.
    - EDM05.03 Monitor Stakeholder Engagement.
    - APO01.02 Communicate Management Objectives, Direction and Decisions Made.
    - APO08.04 Coordinate and Communicate.
- *NIST SP 800-53r5* controls:
    - IR-6 Incident Reporting.
    - IR-7 Incident Response Assistance.
    - PM-15 Security and Privacy Groups and Associations.
    - SC-37 Out-of-band Channels.
    - SC-47 Alternate Communications Paths
    - SR-8 Notification Agreements.
- *NIST CSF* subcategories:
    - RS.CO-2 Incidents are Reported Consistent with Established Criteria.
    - RS.CO-3 Information is Shared Consistent with Response Plans.
    - RS.CO-4 Coordination with Stakeholders Occurs Consistent with Response Plans.
    - RS.CO-5 Voluntary Information Sharing Occurs with External Stakeholders to Achieve Broader Cybersecurity Situational Awareness.
    - RC.CO-1 Public Relations are Managed.
    - RC.CO-2 Reputation is Repaired After an Incident.
    - RC.CO-3 Recovery Activities are Communicated to Internal and External Stakeholders as well as Executive and Management Teams.
- *CIS Controls* in safeguards:
    - 15.4 Ensure Service Provider Contracts Include Security Requirements.
    - 17.2 Establish and Maintain Contact Information for Reporting Security Incidents.
    - 17.6 Define Mechanisms for Communicating During Incident Response.

Technical Response and Recovery

Processes for neutralizing cyberattacks and restoring the computing environment to a normal, strengthened operating state typically start with a determination of the nature and extent of the incident. Understanding data flows and dependencies between systems — ideally documented in an operations management system — helps determine the scope of containment and restoration efforts. The incident analysis and forensic controls discussed previously, as well as playbooks — if established — guide the IS and IT teams to appropriate countermeasures and restoration processes.

Risk management processes establish recovery time and point objectives for information resources — essentially how long the organization will tolerate the loss of a system's availability and how frequently data is backed-up to enable recovery from a set point in time. Such parameters are generally aligned with the security category each resource is given, with systems of greater importance usually provisioned for shorter recovery times and more frequent backups. Typically, there is a cost-benefit tradeoff for shorter recovery times and more frequent backups, which management considers when establishing standards and procedures.

Unlike operational service continuity and restoration processes, which generally revert a system to a previously established baseline, a cyber incident response and recovery plan may involve fixing the vulnerabilities that were exploited before restoring a system to service. Efforts to identify, test, and install fixes may involve coordination with vendors, law enforcement agencies, or internal development teams. Additionally, personnel and systems should retain documentation of incident indicators, communications, and technical responses to enable later analysis or investigation of the events and steps taken. Forensic investigation procedures are typically established to ensure the handling of evidence, often referred to as the **chain of custody**, follows legal requirements. Due to the uncertainty around the amount of time needed to assess the extent of — and the availability of a fix for — some types of cyberattacks, specified cyber incident response and recovery timeliness expectations may be different than normal service recovery time and point objectives.

Patch management controls are described more extensively in the GTAGs "Auditing Business Applications" and "Auditing Cybersecurity Operations: Prevention and Detection." While such controls offer preventive protection during the normal course of operations, they are also often key contributors to cyber incident responses because patches may be issued by vendors to eliminate the vulnerabilities in a program's code that were exploited.

Cyber incident response and recovery processes require sufficient — and adequately trained — resources to execute the plans and react effectively to rapidly unfolding threats. Specialized training, interaction with cyber defense organizations, and periodic testing of incident response and recovery controls can provide the technical skills necessary to mitigate the risks of cyberattacks.

An audit engagement in this area would usually examine evidence from recent incidents to determine whether response and recovery plans – as well as other controls that facilitate technical responses, like **event logging** — were designed and implemented effectively to enable timely service restoration. The timeliness of response and recovery processes may be examined

qualitatively, even if normal system recovery time and point objectives do not apply. The availability and technical capability of resources, including personnel, may also be assessed. For incident plans without recent invocations, an auditor may look for evidence of full-scale testing by production support teams and other key stakeholders, to verify whether recovery plans are at least formalized, aligned with best practices, and tested by management to promote awareness and efficiency.

Controls over technical responses to and recovery from cyber incidents are discussed in:

- *COBIT 2019: Framework: Governance and Management Objectives* in practices:
    - APO12.02 Analyze Risk.
    - DSS02.05 Resolve and Recover from Incidents.
    - DSS03.05 Perform Proactive Problem Management.
- *NIST SP 800-53r5* controls:
    - AC-12 Session Termination.
    - AU-6 Audit Record Review, Analysis, and Reporting.
    - AU-11 Audit Record Retention.
    - SC-24 Fail in Known State.
    - SI-2 Flaw Remediation.
    - SI-17 Fail-safe Procedures.
- *NIST CSF* subcategories:
    - ID.AM-5 Resources (Hardware, Devices, Data, Time, Personnel, and Software) are Prioritized Based on their Classification, Criticality, and Business Value.
    - ID.BE-4 Dependencies and Critical Functions for Delivery of Critical Services are Established.
    - ID.RA-2 Cyber Threat Intelligence is Received from Information Sharing Forums and Sources.
    - PR.IP-4 Backups of Information are Conducted, Maintained, and Tested.
    - PR.IP-7 Protection Processes are Improved.
    - DE.AE-1 A Baseline of Network Operations and Expected Data Flows for Users and Systems is Established and Managed.
    - DE.DP-5 Detection Processes are Continuously Improved.
    - PR.PT-5 Mechanisms (Failsafe, Load Balancing, Hot Swap) are Implemented to Achieve Resilience Requirements in Normal and Adverse Situations.
    - RS.MI-1 Incidents are Contained.
    - RS.MI-2 Incidents are Mitigated.
- *CIS Controls* safeguards:
    - 1.2 Address Unauthorized Assets.
    - 2.3 Address Unauthorized Software.

- 4.10 Enforce Automatic Device Lockout on Portable End-User Devices.
- 7.7 Remediate Detected Vulnerabilities

Conclusion

Cyber incident response and recovery controls safeguard the confidentiality, integrity, and availability of systems and data by providing critical layers to a defense-in-depth strategy. Despite an organization's best efforts at preventing cyber incidents, eventually some attackers will get into the environment and start executing their nefarious plans. Once a cyber incident is declared, technical responses and communications to key stakeholders are required to neutralize the threats, restore operations, and maintain trust with customers, vendors, and others.

Ideally, these response and recovery efforts will have been formalized and tested before invoking them; however, it may not be feasible or possible to plan for every possible attack scenario. In all cases, an effective defense depends on having well-trained personnel capable of following a plan or improvising based on an understanding of best practices, as well as sufficient resources to support the business needs before, during, and after an incident.

Additionally, processes that analyze past incidents and their response and recovery efforts for opportunities to improve controls in all areas can be important contributors to an organization's resilience. Internal audit activities that perform engagements in this subject area can add value to the organization through assurance and consulting services that leverage an understanding of internal policies and procedures, as well as widely used external control frameworks, such as those referenced in this guide.

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 2030 – Resource Management
Standard 2050 – Coordination and Reliance
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2220 – Engagement Scope
Standard 2201 – Planning Considerations
Guidance
GTAG "IT Essentials for Internal Auditors," 2020
GTAG "Assessing Cybersecurity Risk – The Three Lines Model," 2020
GTAG "Auditing Business Applications," 2021
GTAG "Auditing Cybersecurity Operations: Prevention and Detection," 2022
GTAG "Auditing Identity and Access Management," 2021
GTAG "Auditing Insider Threat Programs," 2018
GTAG "Auditing Mobile Computing," 2022

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 identified in footnotes.

- ISACA, Glossary, information technology terms, and definitions, accessed November 21, 2021, 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 (Gaithersburg, MD: NIST, September 2020), https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, Glossary, accessed March 18, 2022, https://csrc.nist.gov/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, such as copy and sort [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.

attack vector – A path or route used by the adversary to gain access to the target (asset). Scope Notes: There are two types of attack vectors: ingress and egress (also known as data exfiltration) [ISACA Glossary].

bad actors – a generic term for the people who plan or launch cyberattacks.

board* — The highest level governing body (for example, 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 (for example, an audit committee).

business owner – The leader of the business unit that receives the primary benefit from an IT resource. The business owner determines business requirements and authorizes acceptance of the resource (see "authorizing official" in NIST SP 800-53, Rev. 5).

chain of custody – A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Scope Notes: Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering [ISACA Glossary].

chief audit executive* — Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

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

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* – 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.

control framework – A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise [ISACA Glossary].

credential – An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber [NIST SP 800-53, Revision 5, Glossary].

cyber incident – Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. See incident. See also event, security-relevant event, and intrusion [NIST Glossary].

cyberattack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information [see "cyber attack" in NIST Glossary].

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

defense-in-depth – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization [NIST 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 logging – Chronologically recording system activities, such as access attempts, role creation, user account creation or deactivation. (see "audit log" in NIST SP 800-53, Rev. 5).

fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

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.

information security – Technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis [adapted from "information security program" in 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.

information technology (IT) governance* – Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

inherent risk – The risk level or exposure without taking into account the actions that management has taken or might take (for example, implementing controls) [ISACA Glossary].

internal audit activity* – A department, division, team of consultants, or other practitioner(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.

ransomware – Malware that restricts access to the compromised systems until a ransom demand is satisfied [ISACA Glossary]

residual risk – The remaining risk after management has implemented a risk response [ISACA Glossary].

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 category – The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals [NIST CSRC Glossary].

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

user – Individual, or (system) process acting on behalf of an individual, authorized to access a system [NIST SP 800-53, Revision 5, Glossary].

vulnerability – A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events [ISACA Glossary].

Appendix C. References

References

Center for Internet Security. "The 18 CIS Controls," interactive guide to CIS Controls, Version 8. Accessed June 24, 2022, https://www.cisecurity.org/controls/cis-controls-list/.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. NIST SP 800-61 Revision 2 Computer Security Incident Handling Guide. Gaithersburg, MD: NIST, August 2012. http://dx.doi.org/10.6028/NIST.SP.800-61r2.

Cybersecurity and Infrastructure Security Agency. "Cybersecurity Incident & Vulnerability Response Playbooks." November 2021. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

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

ISACA. Glossary. Information technology terms and definitions. Accessed June 14, 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.

MITRE. "ATT&CK Matrix for Enterprise." Accessed June 14, 2022, MITRE ATT&CK®.

NIST Computer Security Resource Center. Glossary. Accessed June 14, 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

Susan Haseley, CIA, United States

Emmanuel Johannes, CIA, CCSA, CGAP, Tanzania

Klaus Rapp, CIA, CRMA, Switzerland

Ana Cristina Zambrano Preciado, CIA, CRMA, CCSA, Colombia

Tichaona Zororo, CIA, CRMA, South Africa

International Internal Audit Standards Board Reviewers

Stephen Coates, CIA, CGAP, CRMA, CISA, United Kingdom

Naji Fayad, CIA, Saudi Arabia

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

Jill Austin, Senior Manager

Patricia Miller, Content Writer and Technical Editor

Helen Nicholson, Content Writer and Technical Editor

Geoffrey Nordhoff, Content Writer and Technical Editor

The IIA thanks 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 Institute of Internal Auditors

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

June 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