Auditing Mobile Computing

Supplemental Guidance | Practice Guide

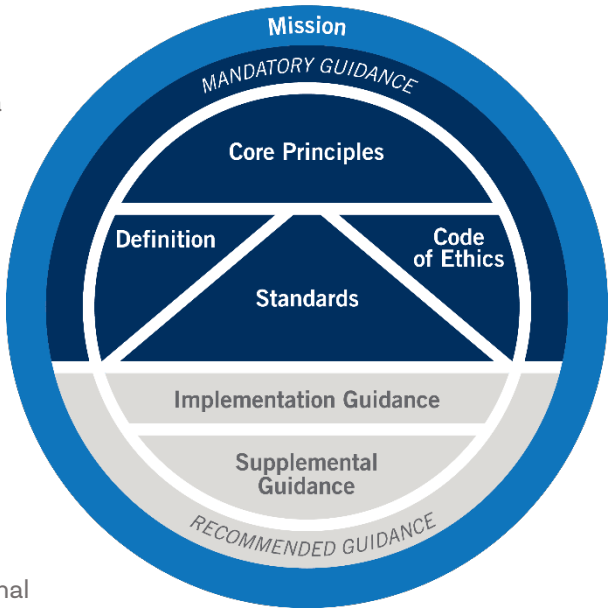
Global Technology Audit Guide

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 and 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 Proficiency – 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 Governance – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

2120.A1 Risk Management – 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 Control – 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 Engagement Scope – 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

The COVID-19 pandemic accelerated the adoption of remote work and may have permanently altered attitudes about whether or how often workers should be in the office. The rapid rise in remote connections to enterprise networks and the continued adoption of cloud-based services have increased the risks of accessing company data and applications over potentially less-secure networks and devices.

Internal auditors need to understand common technologies that enable remote work, the significant risks arising from remote access, and standard controls that prevent, detect, or remediate unauthorized access or sharing of information.

The primary control objectives for mobile computing include:

1. **Remote access –** Which users are authorized to access portions of the enterprise network remotely, and which security measures are in place to protect the transmission?
2. **Centralized device administration –** Which devices are authorized to access the enterprise network remotely, and how are secure configurations managed?
3. **Endpoint security –** How are on-device security measures, such as antivirus software and partitions of user-managed devices, ensured?
4. **Data protection –** How is sensitive data protected from transmission to a less secure environment, including being shared in collaboration tools?
5. **Cybersecurity monitoring –** Are there anomalies or red flags in the use of remote access that could indicate a breach or misuse?
6. **Training –** Do personnel have the training on collaboration tools and security awareness to perform their jobs remotely and securely?

With the rise in remote work, many organizations may be motivated to assess the risks and opportunities posed by mobile computing. Internal audit activities may have opportunities to deliver valuable assurance and consulting services related to the design and implementation of mobile computing controls — which, in turn, can help the organization achieve innovation and security objectives.

Introduction

Mobile computing evolved from an earlier workplace model, one in which office workers all log on to terminals that are physically connected to the enterprise **network**. The physically connected model still exists in many workplaces, but technological innovations have reduced dependence on physical connections since the internet was widely adopted in the 1990s. For instance, laptops have replaced desktop computers for many workers.

Note

Terms in bold are defined in the glossary.

Virtual private network (VPN) technology gave employees secure access to the enterprise network via an internet connection, allowing many employees to work remotely. The deployment of Wi-Fi has further freed the user from a physical connection, and as the processing power of cellphones and other wireless devices has expanded, employees increasingly are using their own smart devices to conduct some job functions. These changes have brought risks related to the use of personal devices (often called "bring-your-own-device" **risks**). Similar risks arise from the Internet of Things, a common term for the proliferation of devices that connect to the internet to receive and send data. Furthermore, the migration of business **applications** from the enterprise data network to the cloud — an internet-based access model — has continued the long process of de-emphasizing physical connections or **controls** in many IT processes while increasing the relevance of **information technology controls**.

IIA Standard 1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

An internal audit **engagement** to examine whether any significant **risk** exposures exist in an organization's mobile computing environment involves a risk assessment, a specified engagement scope, and tests to evaluate the design and implementation of relevant **control processes**. Ideally, the **internal audit activity**, **information technology** and **information security** (IT-IS) teams, and other personnel collaborate to provide valuable insight into inherent risks, the strength of controls, and residual risks. An audit engagement covering mobile computing risks and controls may help the internal audit activity provide assurance on whether the organization's **information technology governance** supports its strategies and objectives, as required by **Standard** 2110.A2. This approach helps internal auditors demonstrate conformance to Standard 1200 — Proficiency and Due Professional Care.

This guide supersedes the Global Technology Audit Guide (GTAG) "Auditing Smart Devices" and broadens the scope to focus on a wider range of risks and controls related to a mobile workforce. The COVID-19 pandemic increased the number and frequency of employees working from home, transforming previous notions of what was possible or desirable. At the same time, cybersecurity

risks are growing, along with the risks of workers using their personal networks or devices to connect to the enterprise network or access sensitive data via cloud-based applications. Additional, relevant internal audit guidance can be found in the GTAG "Assessing Cybersecurity Risk: The Three Lines Model."

IT-IS Control Frameworks

This guide references controls and guidance described in three external IT-IS **control frameworks** of standards, guidance, and best practices (although there are many others). Each framework provides more information about specific controls than is discussed here. Internal auditors are encouraged to identify frameworks used by their organizations and to review common IT-IS control guidance to understand common risks and controls in business processes relevant to their environment. Several resources are listed at the end of this guide.

This GTAG refers to controls described in the following publications:

- *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* (*NIST SP 800-53r5*) from the National Institute of Standards and Technology.
- *CIS Controls Version 8* from the Center for Internet Security.

IT-IS personnel frequently benchmark operational and security controls against one or more of these frameworks. Although each framework names and categorizes controls uniquely, the frameworks still share substantial commonalities in terminology and categorization.

This guide begins with the assumption that its readers have a general knowledge of IT-IS risks and controls, as described in the GTAG "IT Essentials for Internal Auditors." Furthermore, readers are encouraged to review the full texts of one or more IT-IS **control frameworks** while planning engagements and developing test programs. Additionally, when planning a mobile computing engagement, internal auditors should review relevant policies and procedures to understand control requirements established by the organization. These actions demonstrate the essence of Standard 2201 – Planning Considerations, which states that internal auditors planning an engagement 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.

This guide helps readers:

- Define mobile computing hardware, software, and communications tools.
- Understand risks and opportunities associated with mobile computing.
- Understand components of **remote access** processes and related security controls.
- Understand the basics of auditing mobile computing, including specific controls to evaluate.

Mobile Computing Control Groups

This section describes significant components of a mobile computing **ecosystem** as well as typical risks and related controls.

Certain controls in specific IT-IS control frameworks are referenced so that readers may pursue additional detailed guidance. Just as each framework has a distinct way of grouping controls, this guide categorizes controls to facilitate discussion and learning. This section generally associates controls within a process or control objective typically managed by a team in either IT or IS. However, this categorization scheme is not meant to replace or override those used in the cited frameworks or elsewhere. The way controls are organized varies from one organization to the next, so internal auditors are encouraged to customize their approach as appropriate.

Ecosystem

In IT, the term ecosystem often refers to the interdependent and evolving nature of hardware, software, and communications elements. This differs from the use of "digital ecosystem" to describe an organization's use of a core technology platform to offer multiple services, as Amazon and Facebook have done.

Remote Access

In the old model of physically connecting a computing device to a network, the data transmissions were secured by controls over the wired network. Mobile computing requires a secure method for establishing a trusted wireless connection. Many organizations use a VPN connection to secure remote access. A VPN not only establishes an encrypted transmission path between the user and the enterprise network, but also it can provide **multi-factor authentication**, for example, if the software is linked to a specific device.

Controls over remote access are described more fully as follows:

- In the *COBIT 2019 Framework: Governance and Management Objectives* in objectives:
    - BAI09 Managed Assets, especially in practice BAI09.02 Manage Critical Assets.
    - DSS05 Managed Security Services, particularly DSS05.02 Manage Network and Connectivity Security.
- *NIST SP 800-53r5* covers similar guidance in control AC-17 Remote Access.
- *CIS Controls* provides relevant coverage in subcontrols called "safeguards," specifically:
    - 12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure.
    - 13.5 Manage Access Control for Remote Assets.

Wireless Access

When wireless devices connect to a company-managed Wi-Fi router — also known as a wireless access point — the router typically uses a sufficient **encryption** method, such as Wi-Fi Protected Access 2 (WPA2). Additionally, company-managed routers generally allow only authorized devices to access the data network; however, a public network option may be set up for customers, authorized guests, or employees' personal devices. Unencrypted or weakly encrypted connections at work or home may be susceptible to eavesdropping, leading to additional problems.

Relevant guidance is described in:

- *NIST SP 800-53r5* controls:
    - AC-18 Wireless Access.
    - SC-40 Wireless Link Protection.
- *CIS Controls* safeguard 12.6 Use of Secure Network Management and Communication Protocols.

Access via the Internet

To help manage access to sensitive resources, network administrators **configure** devices and software to define network segments, sometimes called virtual local area networks. Within these segments, network administrators deploy controls of commensurate strength — such as requiring multi-factor authentication or preventing remote access to environments with personally identifiable information. The **subnetworks** and systems that are available to remote access may require online **authentication** or a VPN connection, or they may be open to the public. Internal auditors typically focus on assessing applications or environments in which the highest risks to the organization exist. These high-risk areas likely have some method of authentication in place. Internal auditors may verify whether remote access controls are sufficient for subnetworks and applications in the highest risk or criticality categories.

Controls that enable secure access to an organization's network or applications via the internet are described in more detail in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practice DSS05.02 Manage Network and Connectivity Security.
- *NIST SP 800-53r5* in controls:
    - SC-7 Boundary Protection.
    - SC-32 System Partitioning.
- *CIS Controls* in safeguards:
    - 4.4 Implement and Manage a Firewall on Servers.
    - 13.10 Perform Application Layer Filtering.

Centralized Device Administration

A team in IT operations usually centrally administers the processes to manage those organizational assets that connect to the company network and the processes that restrict or deny nonmanaged devices. Asset life cycle management and inventory **metadata** controls are relevant to mobile computing, especially in their contribution to identity and authentication controls. Internal audits of mobile computing typically include an assessment of risks and controls related to ensuring that only authorized devices are allowed to connect to the network.

Controls over **centralized device administration** are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* in the BAI09 Managed Assets and BAI10 Managed Configuration objectives.
- *NIST SP 800-53r5* control families:
    - Configuration Management.
    - Identification and Authentication.
    - Physical and Environmental Protection.
    - System and Communications Protection.
- *CIS Controls* — Control 1 Inventory and Control of Enterprise Assets, as well as safeguards:
    - 4.5 Implement and Manage a Firewall on End-User Devices.
    - 4.12 Separate Enterprise Workspaces on Mobile End-User Devices.

Asset Management

Controls over hardware procurement and end-of-life decommissioning are typically outside the scope of a mobile computing audit. However, devices in service may be recorded in a physical inventory system with a custodial owner, **media access control** number, manufacturer serial number, device operating system, and other metadata systematically captured. Controls in place to enforce approved operating system versions and **patch** implementation in a timely way may include standard configuration, monitoring, and maintenance controls as well as limited **administrator privileges**. An audit engagement in this area may involve determining whether controls implemented to monitor assets or update related records are consistent with established security requirements.

Relevant **asset management** controls are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - BAI09.01 Identify and Record Current Assets.
    - BAI10.05 Verify and Review Integrity of the Configuration Repository.
- *NIST SP 800-53r5* controls:
    - CM-8 System Component Inventory.
    - PM-5 System Inventory.

- *CIS Controls* safeguards:
    - 1.1 Establish and Maintain Detailed Enterprise Asset Inventory.
    - 1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory.
    - 1.5 Use a Passive Asset Discovery Tool.

Identity and Authentication

As part of the remote access controls, some environments may simply require a remote user to authenticate to the general enterprise network, while others require additional authentication steps for greater security. Some applications — particularly those that are cloud-based and not **federated** — may be accessible from any device, including nonmanaged personal ones. Alternatively, applications may be highly restricted, only accessible on specified devices and with the added requirement of a separate account identifier, password, or other factors.

While identity and authentication controls are covered more extensively in the GTAG "Auditing Identity and Access Management," an internal audit engagement of mobile computing may verify:

- Whether identity and authentication controls for remote users are sufficient for higher-risk systems.
- Whether any nonmanaged devices with remote access — such as contractor- or vendor-owned devices — are appropriately authorized and have a documented business purpose.

Controls over identity and authentication of remote users can be found in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - DSS05.04 Manage User Identity and Logical Access.
    - APO07.06 Manage Contract Staff.
- *NIST SP 800-53r5* mainly in controls:
    - AC-13 Supervision and Review — Access Control.
    - IA-3 Device Identification and Authentication.
    - IA-9 Identification and Authentication (Non-organizational Users).
    - SC-23 Session Authenticity.
- *CIS Controls* safeguards:
    - 6.3 Require MFA for Externally Exposed Applications.
    - 6.4 Require MFA for Remote Network Access.

Endpoint Security

Devices that are authorized to connect remotely to the organization's network should meet specific minimum security requirements to mitigate the risk of spreading malware from the device to the network. Controls to manage operating systems, patches, antivirus software, and

other on-device configurations may be necessary to protect the network. Such controls often involve coordination between IT and IS teams to ensure their people, processes, and technologies are aligned to sufficiently mitigate risks. In organizations without centralized administration, policies still generally require local controls to meet internal security requirements.

When evaluating controls over **endpoint security**, internal auditors may examine whether secure configurations for remote access are established using a formalized configuration management process, with sufficient policies, technologies, and personnel deployed to implement effective and, ideally, largely automated controls.

Controls over establishing secure **baseline configurations** for remote devices are primarily found in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - DSS05.03 Manage Endpoint Security.
    - BAI10.01 Establish and Maintain a Configuration Model.
- *NIST SP 800-53r5* controls:
    - CM-2 Baseline Configuration.
    - SC-18 Mobile Code.
- *CIS Controls* safeguards:
    - 4.10 Enforce Automatic Device Lockout on Portable End-User Devices.
    - 4.11 Enforce Remote Wipe Capability on Portable End-User Devices.

Device Scanning

When a device attempts to connect to the organization's network, automated controls may be in place to scan and determine whether the device has sufficient protections for the system that it is trying to access. As mentioned in the Centralized Device Administration section above, security requirements often lead to configuration standards for operating systems, patches, applications, services, and ports. When noncompliant technologies are detected, remediation is typically required before the device is allowed to access the environment. For nonmanaged devices, partitions or similar on-device protection may be required.

An internal audit engagement of mobile computing may seek to determine:

- Whether noncompliant devices are remediated before they are allowed to connect to the network remotely.
- Whether nonmanaged devices are allowed to connect if security requirements are met.

Controls over device scanning, enforcement of security requirements, and **authorization** of nonmanaged devices are found mainly in *NIST SP 800-53r5* controls AC-19 Access Control for Mobile Devices and MA-4 Nonlocal Maintenance.

Anti-Malware

An assessment of risks at each layer in the technology ecosystem generally provides the basis for decisions about where to apply anti-malware programs and which solutions to implement.

Advanced malware attacks often involve remote access capability, so the enabling hardware and software are typically protected with anti-malware controls that are preventive or detective. An example of a preventive control is blocking certain types of files or protocols from running. In contrast, a detective control may monitor the hardware and software for file types or actions that could indicate the presence of unauthorized code or users. Where deployed, anti-malware software updates generally are automated and pushed from a central source to ensure the latest approved version is installed on all devices connected to the network. In addition, most anti-malware products use databases of known malware characteristics, which are updated continually to improve defensive capabilities.

Anti-malware controls are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* practice DSS05.01 Protect Against Malicious Software.
- *NIST SP 800-53r5* controls:
    - SC-35 External Malicious Code Identification.
    - SI-3 Malicious Code Protection.
- *CIS Controls* safeguards:
    - 10.1 Deploy and Maintain Anti-Malware Software.
    - 10.5 Enable Anti-Exploitation Features.
    - 10.7 Use Behavior-Based Anti-Malware Software.

Email and Internet Protection

To reduce the impact of email-initiated threats, specialized applications or tools may scan incoming emails for risk-based criteria, including likely spam or phishing attempts. Internet browsers and website access controls also are usually centrally administered, with preventive controls blocking certain site categories and communication protocols. An internal audit engagement of mobile computing risks and controls could include verifying whether the protections from tools such as email and browser filters extend to personal devices that connect to the organization's network.

Controls relevant to remote email and internet browser security are described in:

- *NIST SP 800-53r5* control CA-3 Information Exchange.
- *CIS Controls* safeguards:
    - 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients.
    - 9.3 Maintain and Enforce Network-based URL Filters.
    - 9.6 Block Unnecessary File Types.

Data Protection

Controls that protect the security and **privacy** of sensitive data can be put in place at the physical, transmission, and storage layers. Decisions about where to implement such controls are determined in governance, risk management, and **compliance** processes. For example, data

types are typically classified according to internally defined standards and managed throughout their life cycle, with more stringent controls applied to types that are more sensitive. Such controls ensure that data has **integrity**, is available to the right users, and is protected from unauthorized access or misuse. Organizations also may have a formalized privacy program, with a data privacy officer designated to oversee risks and controls related to **data protection**.

Especially pertinent to mobile computing is the risk of sensitive data being exposed over the internet or to devices and environments not controlled by the organization. An example is a user having the ability to access a web-based version of their organization's email, file storage, or collaboration tool from a personal mobile device. Encryption technologies are often critical to protecting data transmissions, reducing the risk of intercepted messages, and safeguarding databases from unauthorized access. However, it may be equally important to prevent users from copying certain files or data types from one environment to another of lesser security — for example, onto the device's onboard memory or a different web-based storage service. **Data loss prevention** programs are often used to detect and prevent attempts to move or copy specified data to an insufficiently secure environment.

When providing **assurance** or **consulting services** over mobile computing, internal auditors may consider a range of data governance and protection risks in the engagement scoping process; however, focusing on the aspects particular to mobile computing, as described above, may be most efficient.

Controls over **data protection** primarily are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* in objectives:
    - APO14 Managed Data.
    - DSS05 Managed Security Services.
- *NIST SP 800-53r5* controls:
    - SC-35 External Malicious Code Identification.
    - SI-3 Malicious Code Protection.
- *CIS Controls* safeguard 10.1 Deploy and Maintain Anti-Malware Software.

Data Classification

Internal audit engagements of mobile computing risks may verify:

- Whether data classification policies and procedures establish categories of sensitivity to which security and operational objectives can be linked.
- Whether restrictions have been placed on remote access to the most sensitive data classifications.
- How such controls are implemented.

Data privacy concerns are usually considered during **technology planning** efforts, with input and participation from the IS team. If an application or resource can be accessed remotely, internal auditors may verify whether it has been appropriately classified and protected.

Data classification controls are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* practice APO01.07 Define Information (Data) and System Ownership.
- *NIST SP 800-53r5* control AC-16 Security and Privacy Attributes.
- *CIS Controls* safeguard *3.7* Establish and Maintain a Data Classification Scheme.

Data Loss Prevention

Some of the biggest risks to mobile data include leakage and interception. Leakage (also called data loss) occurs when sensitive data is moved from a sufficiently secured environment to a less secure one — for example, saving a file with personally identifiable information to a storage application that is cloud-based and accessible from any device. Interception occurs when a transmission's contents are scanned, redirected, or altered. A mobile computing audit typically considers risks and controls related to data loss prevention in planning and scoping decisions.

For a mobile device, controls over information storage or processing may include:

- Only allowing registered devices to access cloud-based applications.
- Deploying data loss prevention tools to mitigate the risk of leakage.
- Requiring a minimum level of security for mobile connections, as with a VPN connection.

Relevant guidance not previously mentioned includes:

- *COBIT 2019 Framework: Governance and Management Objectives* practice DSS06.06 Secure Information Assets.
- *NIST SP 800-53r5* control PE-19 Information Leakage.
- *CIS Controls* safeguard 3.13 Deploy a Data Loss Prevention Solution.

Encryption

One of the most widely applicable control types for mobile computing risk is encryption, which can be used to protect transmissions, device hard drives, shared files, and application databases. During the planning, design, development, and **production support** phases of the **system development life cycle**, the IS team usually determines where to deploy encryption and what technologies to use. Internal auditors may want to verify whether IT and IS teams have assessed the risks of mobile access to various systems and developed appropriate encryption strategies.

Relevant encryption guidance in controls not previously mentioned can be found in:

- *NIST SP 800-53r5* control SC-8 Transmission Confidentiality and Integrity.
- *CIS Controls* safeguards:
    - 3.6 Encrypt Data on End-user Devices.
    - 3.9 Encrypt Data on Removable Media.

Cybersecurity Monitoring

The chief information security officer, or someone similarly designated, usually designs and manages controls that monitor remote access and attempts at remote access to see whether any anomalies have occurred that may indicate a cyberattack. Additionally, the tools used to monitor security **event logs** across networks and applications may be configurable to prevent some attacks by integrating with **firewalls** and other network administration tools, which helps to enforce security-related **business rules**. An internal audit engagement to examine controls over **cybersecurity monitoring** of mobile computing may verify:

- Whether all high-risk systems that are exposed to the internet or other remote access methods are integrated with the IS team's monitoring tools.
- Whether monitoring processes make use of advanced technologies, such as artificial intelligence or machine learning, to improve risk awareness or resiliency.

Controls over cybersecurity monitoring of mobile computing can be found in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - APO13.02 Define and Manage an Information Security and Privacy Risk Treatment Plan.
    - DSS06.01 Align Control Activities Embedded in Business Processes with Enterprise Objectives.
- *NIST SP 800-53r5* controls:
    - IR-4 Incident Handling.
    - IR-5 Incident Monitoring.
- *CIS Controls* safeguards:
    - 2.3 Address Unauthorized Software.
    - 13.2 Deploy a Host-Based Intrusion Detection Solution.
    - 13.3 Deploy a Network Intrusion Detection Solution.

Network Monitoring

Often, organizations have a network monitoring team — frequently in a network operations center (NOC) — that is responsible for detecting and resolving operating issues. The issues managed by the NOC teams typically relate to service **availability**, asset utilization, power supply, and similar concerns, though they may also include network traffic monitoring and analysis, including remote access. Controls that monitor access to the organization's network are usually programmed to detect unauthorized or anomalous accounts attempting to access sensitive environments or systems remotely. If the organization uses an **intrusion detection system**, it is typically configured to analyze connections to external networks, looking for signs of cyberattacks or **advanced persistent threats**. Examples of such signs include connections that are activated and deactivated frequently or have their security event logging deactivated.

Controls over network monitoring not previously mentioned include:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - DSS01.03 Monitor I&T Infrastructure.
    - DSS02.04 Investigate, Diagnose and Allocate Incidents.

- *NIST SP 800-53r5* control CA-7 Continuous Monitoring.
- *CIS Controls* safeguard 13.6 Collect Network Traffic Flow Logs.

Account Usage Monitoring

One of the ways to detect anomalous remote access is to monitor usage patterns for inherently suspect activity — such as downloading, copying, or sending sensitive files — or for activity that is unusual for the account. For example, an account accessing the system outside of normal working hours or from an unusual location could be an indicator of compromised **credentials**. An internal audit engagement of mobile computing may assess whether remote user activity is monitored for cyberattack characteristics.

Controls relevant to user account monitoring not previously mentioned include:

- *COBIT 2019 Framework: Governance and Management Objectives* practice DSS06.05 Ensure Traceability and Accountability for Information Events.
- *NIST SP 800-53r5* control AU-2 Event Logging.
- *CIS Controls* safeguard 8.5 Collect Detailed Audit Logs.

Training

Security-related training is one of the most effective preventive controls, because users are often the weakest link in an organization's security chain. Such training is usually designed to help users protect their credentials, devices, and networks and to responsibly use collaboration tools, such as email, video conferencing, and cloud-based file storage.

An internal audit engagement of mobile computing scoped to include training risks and controls typically verifies whether the entity's cybersecurity awareness training includes risks, responsibilities, and expectations relating to remote access and handling of sensitive data. An advisory recommendation might be to create separate training courses that specifically cover the organization's mobile computing risks, policies, and procedures with guidance for protecting personal networks.

Another potential area of concern for a mobile computing engagement is whether employees know how to use online collaboration tools securely, without exposing the organization to data leakage or interception. The personnel responsible for supporting the organization's online and networked information sharing functions, both public and internal, may need specialized training to help ensure they understand and follow appropriate policies, procedures, best practices, and documented standards.

Controls over training can be found in:

- *COBIT 2019 Framework: Governance and Management Objectives* objective APO07 Managed Human Resources.
- *NIST SP 800-53r5* control families:
    - Program Management.
    - Awareness and Training.
- *CIS Controls* — Control 14 Security Awareness and Skills Training.

Conclusion

Mobile computing risks increased dramatically in 2020 due to the impact of COVID-19, which changed where and how employees conduct work. However, a remote workforce can offer significant benefits to the organization. Therefore, internal audit engagements are necessary to provide assurance services to the **board** and senior management on the effectiveness of the design and use of mobile computing controls.

For a mobile computing engagement, the audit team typically considers the organization's circumstances and use of remote access or web-based tools to determine the scope of key risks and related controls. There are many IT-IS control frameworks to use as reference guides, which can help internal auditors provide more than just assurance of compliance with internal policies. **Engagement objectives** and test plans generally aim to verify whether the organization has designed controls to prevent, detect, or remediate significant risk occurrences and whether the controls are implemented consistently and efficiently. A well-planned and professionally executed internal audit engagement of mobile computing can **add value** to the organization by providing insight to management and the board on mobile computing governance and risk management, including the strength of internal controls, which may enable the organization to take advantage of the many benefits mobile computing offers.

Relevant IIA Standards and Guidance

The following IIA resources were referenced directly or indirectly 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 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2220 – Engagement Scope
Standard 2201 – Planning Considerations
Guidance
GTAG "Assessing Cybersecurity Risk: The Three Lines Model," 2020.
GTAG "IT Essentials for Internal Auditors," 2020.
GTAG "Auditing Identity and Access Management," 2021.

Glossary

Definitions of terms marked with an asterisk are taken from the Glossary of The IIA's *International Professional Practices Framework®*, 2017 edition. Other definitions are either defined for the purposes of this document or derived from the following sources:

- ISACA, Online Glossary, accessed January 12, 2022, https://www.isaca.org/resources/glossary.
- NIST Computer Security Resource Center (CRSC), Online Glossary, accessed December 2, 2021, https://csrc.nist.gov/glossary.
- *NIST SP 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*, "Appendix A: Glossary," https://doi.org/10.6028/NIST.SP.800-53r5 (PDF).
- *NIST SP 800-63-3: Digital Identity Guidelines*, "Appendix A: Definitions and Abbreviations," https://doi.org/10.6028/NIST.SP.800-63-3 (PDF).
- Techopedia.com, "IT Dictionary for Computer Terms and Tech Definitions," https://www.techopedia.com/dictionary.

add value* – The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.

administrator privileges – The authorized ability to perform security-relevant functions that ordinary users are not authorized to perform, such as creating system user accounts or roles, changing configurations, managing event logs, etc.

advanced persistent threat – An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives [*NIST SP 800-53r5* 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 or sort [ISACA Online Glossary].

asset management – A set of processes to record, safeguard, and optimize the use of resources.

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

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

authorization – Access privileges granted to a user, program, or process or the act of granting those privileges [*NIST SP 800-53r5* Glossary].

availability – Ensuring timely and reliable access to and use of information. [NIST CSRC Online Glossary].

baseline configuration – An approved set of components, system settings, and connections to other systems. [See also *NIST SP 800-53r5* Glossary].

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

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

centralized device administration – A set of processes and tools to manage end-user devices, typically employing an inventory of managed devices, standardized configurations, and restrictions preventing end-users from having administrator rights on the device.

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

configure – Programming the settings and connections necessary to make hardware and software operational to desired specifications.

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 Online Glossary].

control processes* – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

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 800-53r5* Glossary].

cybersecurity monitoring – A set of processes and tools to analyze system logs, transmissions, account usage, and other security-relevant data to detect and initiate a response to cyberthreats.

data loss prevention – A system's ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information [NIST CSRC Online Glossary].

data protection – A set of processes and tools to protect the confidentiality, integrity, security, and privacy of data at rest and in transmission.

ecosystem – The hardware, firmware, software, and connections that make up a business application's environment.

encrypted – 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) [adapted from "encryption," ISACA Online Glossary].

endpoint security – A set of processes and tools to strengthen security over device configurations and component technologies, including operating systems and applications.

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

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

event log – A chronological record of system activities, like access attempts, role creation, user account creation or deactivation, etc. [See also "audit log" entry in *NIST SP 800-53r5* Glossary].

federated – using a process that allows the conveyance of identity and authentication information across a set of networked systems [adapted from "federation," *NIST SP 800-63-3* Glossary].

firewall – A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the internet [ISACA Online Glossary].

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

information security – Ensures that, within the enterprise, 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 Online Glossary].

information technology – Information technology (IT)
The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form [ISACA Online 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 governance* – Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

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

intrusion detection system – Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack [ISACA Online Glossary].

media access control (MAC) – Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card [ISACA Online Glossary].

metadata – Information that describes the characteristics of data, including data format, syntax, semantics, and contents [adapted from *NIST SP 800-53r5* Glossary].

multi-factor authentication – An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are [adapted from *NIST SP 800-53r5* Glossary].

network – A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices [*NIST SP 800-53r5* Glossary].

patch – Fixes to software programming errors and vulnerabilities [ISACA Online Glossary].

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

production support – Processes to configure, administer, and troubleshoot applications. (See also "system administration," Techopedia.com).

remote access – Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network [*NIST SP 800-53r5* 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.

Standard* – A professional pronouncement promulgated by the International Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities and for evaluating internal audit performance.

subnetworks – Engineered partitions of an enterprise network that help control access to specified sets of resources. Subnetworks are often aligned with security categories, to enable commensurate access control mechanisms. (See also "subnetwork (subnet)," Techopedia.com Dictionary).

system development life cycle (SDLC) – The phases deployed in the development or acquisition of a software system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation, and post-implementation review, but not the service delivery or benefits realization activities [adapted from ISACA Glossary].

technology planning – Activities to align IT-IS resources with business needs, ensuring objectives of confidentiality, integrity, availability, privacy, and security are met. (See also ISACA's definition for "strategic planning" and *NIST SP 800-53r5*'s definition of "enterprise architecture").

virtual private network (VPN) – A secure private network that uses the public telecommunications infrastructure to transmit data. Scope notes: In contrast to a much more expensive system of owned or leased lines that can only be used by one enterprise, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two internet points, maintaining privacy and security [ISACA Glossary].

Resources

Center for Internet Security. "The 18 CIS Controls," interactive guide to *CIS Controls, Version 8*. Accessed August 13, 2021, https://www.cisecurity.org/controls/cis-controls-list/.

Grassi, Paul A., Michael E. Garcia, and James L. Fenton. *NIST SP 800-63-3: Digital Identity Guidelines*. Gaithersburg, MD: NIST, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3.

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

Joint Task Force. *NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

The Institute of Internal Auditors. *International Professional Practices Framework*. 2017 ed. Lake Mary, Florida: The Institute of Internal Auditors, 2017.

Acknowledgments

IT Guidance Development Team

Ruth Mueni Kioko, CIA, Kenya (Team Lead)

Jim Enstrom, CIA, United States

Avin Mansookram, CISA, CGEIT, South Africa

Scott Moore, CIA, CISA, CRISC, United States

Manoj Satnaliwala, CIA, CPA, CISA United States

Terence Washington, CIA, CRMA, United States

Global Guidance Council Reviewers

Larry Herzog Butler, CIA, CRMA, Germany

Lesedi Lesetedi, CIA, QIAL, CRMA, Botswana

Karem Obeid, CIA, CCSA, CRMA, United Arab Emirates

Klaus Rapp, CIA, CRMA, Switzerland

Carolyn Saint, CIA, CRMA, CPA, United States

International Internal Audit Standards Board Reviewers

Naji Fayad, CIA, Saudi Arabia

Hans-Peter Lerchner, CIA, CRMA, Austria

IIA Global Standards and Guidance

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

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

Anne Mercer, CIA, CFSA, CFE, Senior Director

Shelli Browning, Associate Manager

Christine Janesko, Associate Manager

Lauressa Nelson, Associate Manager

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

About The IIA

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

Disclaimer

Copyright

First edition, "Auditing Smart Devices," published 2016

Second edition January 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