Auditing Mobile Computing

2nd Edition

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

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, CPA, 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

2nd Edition Reviewers

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

Eileen Iles, CIA, CCSA, CFSA, CRMA, United States

Jose Carlos Penaloza Rojas, CIA, Peru

International Internal Audit Standards Board Reviewers

Naji Fayad, CIA, Saudi Arabia

Hans-Peter Lerchner, CIA, CRMA, Austria

2nd Edition Reviewers

Maciej Piołunowicz, CIA, Poland

Angela Simatupang, CIA, CRMA, Indonesia

IIA Global Standards and Guidance

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

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

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

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

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

About the IPPF

International Professional Practices Framework® (IPPF)

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

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

Global Guidance

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

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

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

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

Contents

Executive Summary

The COVID-19 pandemic accelerated the adoption of remote work and may have permanently altered views 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 warnings 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, organizations may be motivated to assess the risks and opportunities posed by mobile computing. Internal audit functions may have opportunities to deliver valuable assurance and advisory services related to the design and implementation of mobile computing controls, helping the organization achieve innovation and security objectives.

Introduction

Mobile computing evolved from an earlier workplace model, one in which office workers logged on to terminals that were 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.

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 perform 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.

An internal audit **engagement** to examine whether any significant **risk** exposures exist in an organization's mobile computing environment involves a **risk assessment** (Standard 13.2 Engagement Risk Assessment), a specified engagement scope (Standard 13.3 Engagement Objectives and Scope), and tests (Standard 13.6 Work Program) to evaluate the design and implementation of relevant **control processes**. Ideally, the **internal audit function**, **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 function provide **assurance** on whether the organization's information technology governance supports

Note

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

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

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

its strategies and objectives. Such assurance contributes to the understanding required to conform with Standards 9.1 Understanding Governance, Risk Management, and Control Processes and 9.4 Internal Audit Plan.

This guide supersedes the Global Technology Audit Guides "Auditing Smart Devices" and the first version of "Auditing Mobile Computing" issued in January 2022, broadening 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. The GTAG "Assessing Cybersecurity Risk: The Three Lines Model" provides additional, relevant guidance.

IT-IS Control Frameworks

This guide references controls and guidance described in several 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.

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.
- *NIST Special Publication (SP) 800-124, Revision 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST SP 800-124r2)* from the National Institute of Standards and Technology.
- CIS Critical Security Controls® Version 8.1 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 both a general knowledge of IT-IS risks and controls (Standard 3.1 Competency), as described in the GTAG "IT Essentials for Internal Auditors" and an understanding of the importance of assessing the nature, circumstances, and requirements of the services to be provided (Standard 4.2 Due Professional Care). Furthermore, readers are encouraged to review the full texts of one or more IT-IS control frameworks while planning engagements (Standards 13.2 and 13.3) and developing work programs (Standard 13.6). 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 13.2, which states that internal auditors planning an engagement must identify and gather reliable, relevant, and sufficient information regarding:

- The organization's strategies, objectives, and risks relevant to the **activity under review.**
- The **governance**, **risk management**, and control processes of the activity under review.
- The organization's **risk tolerance,** if established.
- The risk assessment supporting the **internal audit plan**.
- Applicable frameworks, guidance, and other **criteria** that can be used to evaluate the effectiveness of those processes.

Internal auditors must review the gathered information to understand how processes are intended to operate.

Internal auditors must identify the risks to review by:

- Identifying potentially significant risks to the objectives of the activity under review.
- Considering specific risks related to **fraud**.
- Evaluating the significance of the risks and prioritizing them for review.

This guide helps readers:

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

Mobile Computing Internal Controls

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 to provide additional detailed information. 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 using the term "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. Increasingly, organizations are implementing **zero trust network access (ZTNA)** for securing remote access. A ZTNA model denies access by default and only allows access to resources when explicitly granted.

Controls over remote access are described more fully within these resources:

- *COBIT 2019 Framework*:
    - 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.

- *NIST SP 800-124r2* sections:
    - 4.1.4 VPN Support.
    - 4.3.5 Use Secure Connections to Resources.
- CIS Controls safeguards:
    - 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 risks.

Relevant guidance is described in:

- *NIST SP 800-53r5* controls:
    - AC-18 Wireless Access.
    - SC-40 Wireless Link Protection.
- *NIST SP 800-124r2* sections:
    - 2.4 Mobile Communication Mechanisms and Other Common Mobile Components.
    - 4.3.5 Use Secure Connections to Resources.
- 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*: DSS05.02 Manage Network and Connectivity Security.
- *NIST SP 800-53r5* controls:
    - SC-7 Boundary Protection.
    - SC-32 System Partitioning.
- CIS Controls safeguards:
    - 4.4 Implement and Manage a Firewall on Servers.
    - 13.10 Perform Application Layer Filtering.

Centralized Device Administration

An IT operations team usually centrally administers the processes to manage 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*:
    - BAI09 Managed Assets.
    - BAI10 Managed Configuration Objectives.
- *NIST SP 800-53r5* control families:
    - Configuration Management.
    - Identification and Authentication.
    - Physical and Environmental Protection.
    - System and Communications Protection.
- *NIST SP 800-124r2* sections:
    - 4.2.1 Enterprise Mobility Management.
    - 4.2.2 Mobile Application Management.
- CIS Controls 1 Inventory and Control of Enterprise Assets and 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 mobile computing audit engagements. 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.

Controls relevant to **asset management,** including processes to record, safeguard, and optimize the use of resources, are described in:

- *COBIT 2019 Framework*:
    - 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.
- *NIST SP 800-124r2* offers processes for mobile asset management life cycle in section 5 Enterprise Mobile Device Deployment Life Cycle and in particular sections:
    - 5.1 Identify Mobile Requirements.
    - 5.3 Implement Enterprise Mobile Strategy.
    - 5.5 Dispose and/or Reuse Device.
- 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 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 may be found in:

- *COBIT 2019 Framework*:
    - DSS05.04 Manage User Identity and Logical Access.
    - APO07.06 Manage Contract Staff.
- *NIST SP 800-53r5* 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.
- *NIST SP 800-124r2* sections:
    - 4.2.13 Strong Authentication.
    - 4.3.4 Security Focuses Device Selection.
- 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.

Controls over **endpoint security** are processes and tools to strengthen security over device configurations and component technologies, including operating systems and applications. When evaluating these controls, 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 may be found in:

- *COBIT 2019 Framework*:
    - 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.
- *NIST SP 800-124r2* sections:
    - 4.2.1 Enterprise Mobility Management.
    - 4.2.2 Mobile Application Management.
- 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 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 may be found in *NIST SP 800-53r5* controls AC-19 Access Control for Mobile Devices and MA-4 Nonlocal Maintenance.

Anti-malware

Assessing 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 preventive or detective anti-malware controls.

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*: DSS05.01 Protect Against Malicious Software.
- *NIST SP 800-53r5* controls:
    - SC-35 External Malicious Code Identification.
    - SI-3 Malicious Code Protection.
- *NIST SP 800-124r2* sections:
    - 3.1.9 Mobile Malware.
    - 3.1.13 Exploitation of Supply Chain Vulnerabilities.
    - 4.3.4 Security Focused Device Selection.
- 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 may 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.
- *NIST SP 800-124r2* sections:
    - 3.1.5 Credential Theft via Phishing.
    - 3.1.10 Information Loss via Insecure Lockscreen Configuration.
    - 4.2.7 Secure Containers.
- 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 may be implemented 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**, including processes and tools to protect the confidentiality, integrity, security, and privacy of data at rest and in transmission.

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. For example, a user may have 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 may be used to detect and prevent attempts to move or copy specified data to an insufficiently secure environment.

When providing **assurance** or **advisory services** over mobile computing, internal auditors may consider a range of data governance and protection risks when establishing the engagement scope. However, focusing on the aspects particular to mobile computing may be most efficient.

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

- *COBIT 2019 Framework:*
    - APO14 Managed Data.
    - DSS05 Managed Security Services.
- *NIST SP 800-53r5* controls:
    - SC-35 External Malicious Code Identification.
    - SI-3 Malicious Code Protection.
- *NIST 800-124r2* sections:
    - 4.1.2 Data Isolation Mechanisms.
    - 4.2.3 Mobile Threat Defense.
    - 4.2.7 Secure Containers.
    - 4.3.6 Rapid Adoption of Software Updates.
    - 4.3.7 OS and Application Isolation.
- 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 relevant 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*: 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 cloud-based storage application accessible from any device. Interception occurs when a transmission's contents are scanned, redirected, or altered. When planning and scoping a mobile computing audit engagement, risks and controls related to data loss prevention should be considered.

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*: DSS06.06 Secure Information Assets.
- *NIST SP 800-53r5* control PE-19 Information Leakage.
- *NIST SP 800-124r2* section 3.1.12 Data Loss via Synchronization.
- 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 information may be found in:

- *NIST SP 800-53r5* control SC-8 Transmission Confidentiality and Integrity.
- *NIST SP 800-124r2* sections:
    - 4.1.1 Hardware Backed Processing and Storage.
    - 4.1.2 Data Isolation.
    - 4.2.1.3 Data Communication and Storage.
    - 4.3.5 Use Secure Connections to Resources.
- 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 determine 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**, which are business processes and constraints encoded into applications to fulfill user requirements.

Cybersecurity monitoring includes the processes and tools for analyzing system logs, transmissions, account usage, and other security-relevant data to detect and initiate responses to cyberthreats. Audit engagements to assess cybersecurity monitoring may verify:

- Whether all high-risk systems 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 may be found in:

- *COBIT 2019 Framework*:
    - 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.
- *NIST SP 800-124r2* sections:
    - 4.2.3 Mobile Threat Defense.
    - 4.3.2 Cybersecurity Recommended Practices.
    - 5.2 Perform Risk Assessment.
    - 5.4.2 Device Usage.
- 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

Organizations may have a network monitoring team, frequently in a network operations center (NOC), responsible for detecting and resolving operating issues. Issues managed by 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 include:

- *COBIT 2019 Framework*:
    - DSS01.03 Monitor I&T Infrastructure.
    - DSS02.04 Investigate, Diagnose and Allocate Incidents.
- *NIST SP 800-53r5* control CA-7 Continuous Monitoring.
- *NIST SP 800-124r2* sections:
    - 4.2.3 Mobile Threat Defense.
    - 5.4.2 Device Usage.
- CIS Controls safeguard 13.6 Collect Network Traffic Flow Logs.

Account Usage Monitoring

One way to detect anomalous remote access is to monitor usage patterns for inherently suspect activity, such as downloading, copying, or sending sensitive files, or for unusual or atypical account activity. 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* DSS06.05 Ensure Traceability and Accountability for Information Events.
- *NIST SP 800-53r5* control AU-2 Event Logging.
- *NIST SP 800-124r2* section 5.4.2 Device Usage.
- 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 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. If an internal audit engagement is open to advisory recommendations, suggesting the creation of separate training courses specifically covering the organization's mobile computing risks, policies, and procedures with guidance for protecting personal networks may be appropriate.

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 may be found in:

- *COBIT 2019 Framework*: APO07 Managed Human Resources.
- *NIST SP 800-53r5* controls :
    - 3.2 Awareness and Training.
    - 3.13 Program Management.
- *NIST SP 800-124r2* section 4.3.10 User Education.
- 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 may offer significant organizational 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. Internal auditors may refer to one or more of the many available IT-IS control frameworks for information that will allow them to provide more than just assurance of compliance with internal policies.

Engagement objectives and **engagement work programs** 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 may be valuable by providing the board and management with insights 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.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced in this guide.

Standards
Standard 3.1 Competency
Standard 4.2 Due Professional Care
Standard 9.1 Understanding Governance, Risk Management, and Control Processes
Standard 9.4 Internal Audit Plan
Standard 13.2 Engagement Risk Assessment
Standard 13.3 Engagement Objectives and Scope
Standard 13.6 Work Program
Global Guidance
GTAG “Assessing Cybersecurity Risk: The Three Lines Model”
GTAG “IT Essentials for Internal Auditors”
GTAG “Auditing Identity and Access Management”

Appendix B. Glossary

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

- ISACA, Glossary, https://www.isaca.org/resources/glossary.
- IBM.com, "What is Zero Trust?" Accessed Sept. 10, 2024. https://www.ibm.com/topics/zero-trust.
- NIST Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary.
- *NIST SP 800-53r5: Security and Privacy Controls for Information Systems and Organizations,* Appendix A: Glossary. Sept. 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
- *NIST SP 800-63.3* Digital Identity Guidelines, Appendix A: Definitions and Abbreviations, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3.
- Technopedia.com, "IT Dictionary for Computer Terms and Tech Definitions," https://www.technopedia.com/dictionary.

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

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, and others [defined by authors].

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].

advisory services – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes,

systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."

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].

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

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

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

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 – A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures [*NIST SP 800-53r5* Glossary].

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

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

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

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

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 [defined by authors].

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

configure – Programming the settings and connections necessary to make hardware and software operational to desired specifications [defined by authors].

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.

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, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

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].

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

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

ecosystem – The hardware, firmware, software, and connections that make up a business application's environment [defined by authors].

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].

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

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

engagement work program – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors

assigned to perform the tasks. The work program is based on information obtained during engagement planning.

event log – A chronological record of system activities, like access attempts, role creation, user account creation or deactivation, and others [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].

fraud – Any intentional act characterized by deceit, concealment, dishonesty, misappropriation of assets or information, forgery, or violation of trust perpetrated by individuals or organizations to secure unjust or illegal 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.

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

Inherent risk – The combination of internal and external risk factors that exists in the absence of any management actions.

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 – The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form [ISACA Online Glossary].

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

internal audit plan – A document, developed by the chief audit executive, that identifies the engagements and other internal audit services anticipated to be provided during a given period. The plan should be risk-based and dynamic, reflecting timely adjustments in response to changes affecting the organization.

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].

mobile device – A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device [NIST CSRC Online 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 [adapted from "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].

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

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

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

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

risk tolerance – Acceptable variations in performance related to achieving objectives.

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

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 [adapted from "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 Online 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 Online Glossary].

zero trust network access (ZTNA) – This access model denies access by default and only allows access to resources when explicitly granted. ZTNA establishes secure access after the user authenticates through a secure, encrypted tunnel. It allows users to see only applications and services they have permission to access and prevents lateral movement from unauthorized users [IBM].

Appendix C. References

Center for Internet Security. "The 18 CIS Critical Security Controls," interactive guide to CIS Controls, Version 8.1. Accessed Sept. 10, 2024, 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.

Howell, Gema, Joshua M. Franklin, Vincent Sritapan, Murugiah Souppaya, Karen Scarfone. *NIST SP 800-124-r2: Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Gaithersburg, MD: NIST, May 2023. https://doi.org/10.6028/NIST.SP.800-123r2.

IBM.com, "What is Zero Trust," https://www.ibm.com/topics/zero-trust.

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

Joint Task Force. *NIST Special Publication 800-53r5, 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.

Techopedia.com, "IT Dictionary for Computer Terms and Tech Definitions," https://www.techopedia.com/dictionary.

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 245,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance.

For more information, visit theiia.org.

Disclaimer

Copyright

Sept. 2024 (This version supersedes “Auditing Mobile Computing,” published in 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