International Professional Practices Framework

Supplemental Guidance

GTAG®

Global Technology Audit Guide

Auditing Smart Devices

An Internal Auditor's Guide to Understanding and Auditing Smart Devices

The Institute of Internal Auditors | Global

Contents

Executive Summary

Smart devices, such as cell phones and tablets, offer truly mobile and convenient options for working remotely. Like any new or expanding technology, smart devices also introduce additional risks for organizations.

Internal auditing's approach to assessing risks and controls related to smart devices is evolving as new technologies emerge and the variety of devices increases. To meet these challenges, internal auditors are tasked with:

- Understanding the organization's smart device strategy.
- Evaluating the effect of smart device technology on the organization.
- Providing assurance over the smart device environment by:
  - Identifying and assessing risks to the organization arising from the use of such devices.
  - Determining the adequacy of applicable governance, risk management, and controls related to such devices.
  - Reviewing the design and effectiveness of related controls.

Chief audit executives (CAEs) should have a thorough understanding of the opportunities and threats that smart devices present to the organization and the internal audit activity. The internal audit activity can support management's efforts to mitigate risks associated with the use of smart devices.

This guidance should help internal auditors better understand the technology, risks, and controls associated with smart devices. Appendix C provides an engagement work program, including a risk assessment, designed specifically to evaluate risk management and controls related to smart devices.

Introduction

Smart devices — electronics programmed and controlled through computer technology — have revolutionized the workforce and given new meaning to the concept of the "mobile worker." Whereas working remotely was once limited to connecting to the organization's network via a laptop provided by the organization, today's options include phones and tablets that utilize specially designed applications (*apps*) and features to conduct business in a truly mobile way.

Smart devices provide organizational users with portable computing power, internet connectivity wherever there is Wi-Fi or cellular service, and the possibility of having one convenient device for personal and business use. Types of smart devices vary widely, as do their operating systems, security mechanisms, apps, and networks. Examples include smartphones, tablets, portable digital assistants (known as *PDAs*), wearable devices (e.g., watches and glasses), and handheld gaming devices.

Some characteristics associated with smart devices include:

- Form factor (e.g., tablet, clamshell, wearable).
- Operating system (e.g., Apple iOS, Android, Windows Mobile, Blackberry OS).
- Voice and data networking.
- Video and photograph.
- Data storage (removable and nonremovable).
- Global Positioning System (GPS), which enables location services.
- Consumer and enterprise applications (pre-installed or downloaded).

In some organizations, employees may be required to use their own devices to conduct business, or they may request to do so, a circumstance known as *bring your own device* (*BYOD*). Whether owned by the organization or the employee, smart devices, like any new or expanding technology, introduce myriad risks that challenge an IT department's traditional approach to risk management.

The internal audit activity can support management's efforts to manage the risks associated with the use of smart devices. According to Standard 2120.A1 and Standard 2130.A1, the internal audit activity must evaluate the risk exposures relating to the organization's governance, operations, and *information systems*, as well as the adequacy and effectiveness of controls in responding to such risks.[1] This GTAG offers a thorough description of the risks related to the use of smart devices, the controls that can be used to mitigate those risks to an acceptable level, and an engagement work program that can be used to effectively assess the organization's governance, risk management and controls related to smart devices.

[1] Emphasis added. See Appendix A for the complete text of these and other relevant IIA standards.

Related Risks

Risks related to smart devices can be categorized as either compliance, privacy, physical security, or information security.

Compliance Risks

In BYOD situations, organizations may rely heavily on users to comply with applicable policies and procedures, such as guidelines for updating software or operating systems. Users who consider updates overly intrusive or degrading to the performance of the device might choose to bypass controls or not install the updates. A BYOD environment requires the organization's IT support services to expand its skills and capabilities. Growth in the variety and number of devices compounds the organization's exposure to a range of vulnerabilities. Managing the various versions of hardware and software that have the ability to access and hold proprietary data can be difficult, especially in the absence of prescriptive policies, procedures, and protocols.

Privacy Risks

BYOD practices may raise privacy concerns from the perspectives of the organization and the employee. For example, it may be difficult for an organization to protect a stakeholder's privacy when personally identifiable information (PII) is accessed or stored on a smart device, an increasingly common occurrence. Equally, employees may have privacy concerns that their smart device enables intrusive monitoring by the organization or that the organization might inadvertently *wipe*, or remove, personal information (e.g., pictures and contact information) from their devices when organizational data is deleted. Additional risk is introduced when third parties (e.g., vendors, guests, or visitors) access organizational networks and systems using their own smart devices.

Security Risks

Information stored on smart devices may include personal and organizational data. The information may be compromised if the smart device is physically lost or stolen, if the device user leaves the organization without deleting proprietary data from the device, or if appropriate security controls are not in place and operating as intended. Before designing a smart device audit program, auditors should understand the details of several categories of security risks.

Physical Security Risks

Smart devices are continuously exposed to physical security risks. Due to their mobile nature, smart devices are used in multiple locations and are susceptible to being lost or stolen. The organization's sensitive data may be at risk if the device is used to store or access such information. Organizations should have established protocols for reporting loss or theft and

responding to security incidents; for example, by remotely wiping data stored on smart devices.

Information Security Risks

Data storage and backup

Personal and organizational data stored on smart devices may be compromised if appropriate security measures, such as encryption, are not deployed. Recovery of data from device or system failure also may be a concern if devices are not backed up properly.

Operating systems

Each of the various smart device operating systems (OSs) presents unique security features and risks that may need to be managed, configured, and secured differently. When users bypass OS administrative restrictions through the processes of *jailbreaking* (Apple OS) or *rooting* (Android OS), factory-installed security controls are disabled and additional security vulnerabilities may be introduced. Additionally, the variation in platforms makes it more complicated for organizations to wipe data when an employee replaces a device or changes service providers.

Network connections

Smart devices connect to the internet via wireless or cellular networks, which may be untrusted. Untrusted networks (e.g., unsecure wireless networks or Bluetooth) are susceptible to various security risks that could compromise data in transit, such as *session hijacking* (an exploitation of a valid network session for unauthorized purposes), *eavesdropping*, and *man-in-the-middle attacks (*an attack strategy in which the attacker intercepts the communication stream between two parts of the victim's system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication).

Applications

An extensive number and variety of apps available from mobile app stores can be downloaded directly to the smart device. These apps are generally developed by third-party vendors, ranging from large software development companies to individuals working from their homes. Viruses, Trojan horses, and other malware may infect the smart device if mobile device platforms and app stores do not place security restrictions or other limitations on third-party app publishing.

Location

A GPS, which enables location services, could be used to track smart devices, monitor user behavior, and plan cyberattacks. The location and personal characteristics of an individual can potentially be determined by comparing data from various sources such as social media, web browsers, and navigation apps. Additional location leaks can occur from GPS embedded photos.

Related Controls

Smart Device Security Controls

Smart devices offer a number of security features that organizations can use to reduce risks.

Authentication – Authentication, the first step in securing a smart device, prevents unauthorized users from accessing the device's apps and data. Smart devices typically employ one or more of the following authentication methods: passcode, swipe pattern, biometrics, security questions, or a personal identification number (PIN). A PIN is a numeric code, the simplest form of authentication. A passcode uses a combination of numbers, letters, and other symbols. Another authentication method is the *swipe pattern*, which requires the user to swipe a chosen matrix of dots on the initial screen. Finally, security questions require users to answer one or more preset personal security questions. These methods are subject to user discretion; the user chooses the code or pattern.

To mitigate the risk that users will select weak PINs or passcodes, an organization's IT function can enforce strong parameters through mobile device management (MDM) software or require a second authentication to access the organization's apps. Security questions are often used for secondary authentication in smart devices (e.g., when the user forgets the passcode, the security questions option can be used to authenticate). Perhaps the most secure authentication method is *biometrics*, the use of technology such as facial recognition and fingerprint readers.

Remote Wipe – Remote wipe is the ability of the user or an IT administrator to wipe data and applications via the network, without having physical possession of the device. Remote wipe can also restore default settings and lock encrypted data from further access. For organization-owned smart devices, IT administrators should deploy MDM software or an alternative solution such as Microsoft Exchange ActiveSync to remotely wipe a smart device.

It is important to note that remote wipe does not completely remove all data from a smart device. Some MDM software does not enable remote wipe of Secure Digital (SD) cards. Remote wipe does not delete data backed up to a desktop or via cloud computing. Jailbreaking and rooting can also interfere with remote wipe.

Hardware or Device Encryption – Smart devices commonly support hardware encryption. When enabled, the data and apps remain encrypted until a passcode is entered. Encryption keys are typically generated using a factory-assigned unique code and a user-defined passcode. Hardware encryption is a key control for protecting data on smart devices.

Software Encryption – Software encryption is a must for all organizational apps, especially email. For smart devices that do not support hardware encryption, software encryption, which requires a second passcode to access an app, can be used to protect the organization's apps and data. Unlike hardware encryption, which encrypts all the data on the device, software encryption only encrypts data related to the app that invokes the encryption algorithm. The encryption level utilized by the app developer should be assessed to ensure it meets the organization's minimum standards.

Encryption of Data in Transit – Many smart devices support Transport Layer Security (TLS) for encrypting email, web traffic, and virtual private networks (VPN).

IT Policy Control Considerations

In addition to instituting controls at the device level, management may put security features in place at the policy and procedural levels.

Anti-malware Software – This software detects and removes malicious software that negatively impacts smart devices and may allow access to private data. To protect against malware, smart device policy should require users to:

a. Install anti-malware software, and make sure that all smart devices remain currently protected.
b. Keep operating systems updated. Smart device manufacturers update their operating systems quite frequently to enhance security features or defense mechanisms that combat known malware and security vulnerabilities.
c. Download apps only from reputable mobile app stores. Organizations also can develop their own secure enterprise app stores for employee use.
d. Update apps timely because app developers enhance security features often.
e. Refrain from jailbreaking/rooting. Altering the smart device's operating system and removing the manufacturer's native restrictions and controls bypasses important security features rendering the device vulnerable to threats. While such processes may be legal in some countries, they could infringe upon local copyright laws and may void the manufacturer's warranty of the device. Organizations should prohibit the use of smart devices that have been jailbroken or rooted.

BYOD Policy – If employees are permitted to use personal smart devices to conduct business, then a comprehensive BYOD policy should be implemented. The policy should cover, among other things:

a. Approved devices and possibly operating systems (e.g., iOS, Android) and responsibilities for maintenance.
b. Expectations and responsibilities related to organizational and personal information stored on the smart device. For example, the organization may be responsible for restricting data downloads or transfers, and the employee may be responsible for not sharing the device with other family members if confidential data resides on the device.
c. Minimum security requirements, such as strong passwords and up-to-date operating systems.
d. Timely reporting of a security breach and lost or stolen devices.
e. Accessing the organization's data, apps, and network resources, including who can access what apps and by what means (e.g., web, VPN, or app-based).
f. Backups and transfers, specifically how and where to back up the organization's data and what can be transferred to other devices. For example, can an employee transfer or back up organizational data to a home computer or a public data hosting service? These decisions may impact data security and compliance with certain privacy, regulatory, or contractual obligations (e.g., U.S. Health Insurance Portability and Accountability Act (HIPAA), U.S. Sarbanes-Oxley Act of 2002, Payment Card Industry Data Security Standard (PCI DSS), and Personally Identifiable Information (PII)).
g. Remote wiping. Users should enable the remote wipe option and identify specific applications to be remotely wiped. One concern is that a remote wipe could impact PII, as well as organizational data. It is important to establish whether the organization can access or delete all the data or just organizational data. Organizations with BYOD policies should involve their legal departments when developing and implementing appropriate remote wipe policies and procedures.
h. Process for retiring smart devices, including options for selling, exchanging, swapping, donating, or otherwise disposing of a smart device.
i. Employee acknowledgement and sign-off of all appropriate policies and procedures.

Data/Attachment Download – Downloading sensitive data to a smart device should be discouraged. Restrictive apps provide users the ability to view sensitive attachments on smart devices without downloading them to an SD card. Similarly, it is important to consider controlling the ability to take screenshots.

Data Backup – Implementing secure backup for data on smart devices enables data from a lost, damaged, or remotely wiped device to be restored to a new device. Most smart devices provide native data backup to a desktop, laptop, or cloud service. Organizational data and apps should be backed up at the organization's data center, which is controlled by the IT administrator, instead of native backup storage, which is controlled by the user. Backup systems should be properly secured.

Mobile Application Management (MAM) – MAM software aims to manage and protect data on specific applications. MAM addresses how an application is developed, managed, used,

modified, and transferred to the smart device, as well as the security controls deployed to protect the data used by the application.

Mobile Device Management (MDM) – MDM software is more effective when MDM software solutions are implemented. Such software can protect critical data by interfacing with security controls embedded in the smart device operating system.

MDM software can:

- Deploy and centrally manage the IT controls, such as strong passwords, encryption levels, remote wiping, and other device security.
- Inventory, deliver, install, update, and remove applications.
- Monitor devices, notify the user and management when a control policy is violated, and even disable smart devices that do not comply with policies.

Wi-Fi Restrictions – These restrict the use of Wi-Fi networks, which are secured according to industry best practices. Virtual private network solutions are preferred when accessing an organization's applications and data on smart devices.

The development of policies, procedures, and technology to manage smart devices is only effective if users understand the associated risks and how to take protective measures. All employees using organizational or personal smart devices to access the organization's data and applications should receive periodic training applicable to their roles in the organization and on appropriate smart device usage.

Smart Device Audit Engagement

An audit engagement work program should outline the engagement's objectives and scope, as well as the relevant risks and controls related to smart devices and audit procedures that will be used.

Internal audit's involvement in assessing the control environment enables an organization to be more aware of the risks associated with the use of smart devices, which should lead to strengthened security controls. As part of providing assurance over information systems, as described in Standard 2120.A1 and Standard 2130.A1, it is prudent that the internal audit activity evaluate risk exposures and consider the adequacy and effectiveness of risk management and controls related to storing and running an organization's critical data on smart devices, operating systems, and mobile apps.

Engagement Planning

Standard 2200 states that for each engagement, internal auditors must develop and document a plan, which must include the engagement's objectives, scope, timing, and resource allocations. One of the most important things an internal audit activity needs to determine in planning the engagement is whether the organization has a unified and cohesive governance structure in place, including policies and procedures, from which clear and consistent guidance can be distributed across the organization. A strong governance model will provide the necessary policies, processes, and tools to consistently manage the environment and control the risks related to smart devices and mobile apps, which is essential for adequate protection of the organization's information. While multiple organizational functions may own part of the smart device strategy, (e.g., IT may own security and legal may own privacy), the key to a successful governance program is to designate a single owner. This single owner should ensure consistent standards and procedures, collaboration across functions, connection to business goals, and optimization of resources.

Engagement Objective

In a highly competitive business market, quick access to an organization's data and resources is crucial. However, associated risks and their potential impacts on the organization should be well understood by management, and the internal audit activity should contribute to this understanding.

Internal auditors should establish engagement objectives to address the risks associated with the activity under review. A risk assessment should be performed to assist in defining initial objectives and identify other significant areas of concern.

Engagement Scope and Resource Allocation

Procedures to be performed and the scope (nature, timing, and extent) of the engagement should be determined after the risks have been identified. According to Standard 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."

Smart device utilization exposes organizations to myriad risks that require controls in several layers of the IT architecture. The audit engagement should encompass strategy and governance, including smart device policies, standards, and procedures; employee awareness and training; smart device and app management; and data protection.

The internal audit activity must determine the skills necessary to complete the audit engagement and the total number of resources required. The internal audit staff must have the

appropriate level of expertise, knowledge, and skills to successfully perform the audit engagement, or external resources with the competencies required should be utilized.

Engagement Work Program

Before commencing an audit of smart devices, the internal audit activity should understand the organization's deployment and use of smart devices. In accordance with Standard 2240.A1 Engagement Work Program, "Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement."

A smart device engagement work program may include inquiries such as:

- Is the organization's network accessible via smart devices?
- Is access limited to messaging, or does it include the organization's data?
- Does the organization provide employees with smart devices?
- Are employees permitted to use their own smart devices to conduct business?
- How does smart device technology integrate with the organization and user base?
- Who owns the smart device strategy and enforces the organization's smart device policies and procedures?
- How is back-end information stored and maintained?
- How does the organization protect itself against data loss, data corruption, security breaches, network downtime, and lost or stolen devices?
- Are smart devices supported and protected as assets or tools for the organization to help accomplish business goals?
- Does the organization continue to conform to legal and regulatory policies?

Appendix C provides an example of a smart device security audit engagement work program, including a risk assessment.

Appendix A. Related IIA Standards and Guidance

Standard 2110: Governance
The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

Standard 2120: Risk Management
The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

Standard 2130: Control
The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

Standard 2200: Engagement Planning
Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

Standard 2201: Planning Considerations
In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its 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; and
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

Standard 2210: Engagement Objectives
Objectives must be established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A3 – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management and/or the board to develop appropriate evaluation criteria.

Standard 2220: Engagement Scope
The established scope must be sufficient to achieve the objectives of the engagement.

2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Standard 2230: Engagement Resource Allocation
Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Standard 2240: Engagement Work Program
Internal auditors must develop and document work programs that achieve the engagement objectives.

2240.A1 – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

Standard 2310: Identifying Information
Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Related IIA Recommended Guidance

Practice Guide "Auditing Privacy Risks, 2nd Edition"
"GTAG: Information Technology Risk and Controls"
"GTAG: Information Security Governance"

Appendix B. Definitions of Key Concepts

Back-end — the server side of a client/server system[2].

Bring your own device (BYOD) — an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Typically, it spans smartphones and tablets, but the strategy may also be used for PCs. It may include a subsidy.[3]

Cloud computing — a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.[4]

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.[5]

Jailbreak — the process of removing software restrictions imposed by iOS, Apple's operating system, on devices running it through the use of software exploits. Jailbreaking permits root access to the iOS file system and manager, allowing the download of additional applications, extensions and themes that are unavailable through the official Apple App Store.[6]

Malware — short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.[7]

Mobile application management (MAM) — describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and BYOD. Provides granular controls at the application level that enable administrators to manage and secure app data.[8]

Mobile application stores — offer downloadable applications to mobile users via a storefront that is either embedded in the device or found on the Web. Application categories in public application stores include games, travel, productivity, entertainment, books, utilities, education,

---

[2] *Gartner IT Glossary*, http://www.gartner.com/it-glossary (accessed March 9, 2016).
[3] Ibid.
[4] Ibid.
[5] The Institute of Internal Auditors, *International Professional Practices Framework (IPPF)* (Altamonte Springs: The Institute of Internal Auditors, Inc., 2013), 43.
[6] "IOS Jailbreaking." *Wikipedia*. Accessed March 9, 2016. https://en.wikipedia.org/wiki/IOS_jailbreaking.
[7] ISACA, "ISACA Glossary of Terms," 59. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (accessed March 9, 2016). All rights reserved. Used by permission.
[8] "IOS Jailbreaking." *Wikipedia,* https://en.wikipedia.org/wiki/IOS_jailbreaking (accessed March 9, 2016).

travel etc., and can be free or charged-for. Private application stores can be created by enterprises for mobile workers.[9]

Mobile device management (MDM) — includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets. MDM functionality is similar to that of PC configuration life cycle management (PCCLM) tools; however, mobile-platform-specific requirements are often part of MDM suites.[10]

Personally identifiable information (PII) — any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements (e.g., indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.[11]

Rooted or Rooting — the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems. As Android uses the Linux kernel, rooting an Android device gives similar access to administrative superuser permissions as on Linux or any other Unix-like operating system such as FreeBSD or OSX.[12]

SD storage — refers to a Secure Digital storage card in a smart device. Secure Digital refers to a standard that was introduced in 1999 and is maintained by the SD Association.[13]

Smartphone — a mobile communications device that uses an identifiable open OS. An open OS is supported by third-party applications written by a notable developer community. Third-party applications can be installed and removed, and they can be created for the device's OS and application programming interfaces (APIs). Developers may be able to access APIs through a discrete layer such as Java. The OS supports a multitasking environment and user interface that can handle multiple applications simultaneously. For example, it can display email while playing music.[14]

[9] *Gartner IT Glossary* (2012), http://www.gartner.com/it-glossary (accessed March 9, 2016).
[10] *Gartner IT Glossary* (2012), http://www.gartner.com/it-glossary (accessed March 9, 2016).
[11] "Guidance on the Protection of Personal Identifiable Information," United States Department of Labor, http://www.dol.gov/dol/ppii.htm (accessed March 9, 2016).
[12] "Rooting," *Wikipedia*, https://en.wikipedia.org/wiki/Rooting_(Android_OS) (accessed March 9, 2016).
[13] "Fact Sheet," *SD Association*, ttps://www.sdcard.org/about_sda/fact_sheet/ (accessed March 9, 2016).
[14] *Gartner IT Glossary* (2012), http://www.gartner.com/it-glossary (accessed March 9, 2016).

Appendix C. Smart Device Audit Program

Objective 1: Plan and Scope the Audit		
Review Activities		**Control**
1.1 Define the engagement objectives. (Standard 2210) The audit/assurance objectives are high level and describe the overall audit goals.		
1.2 Identify and assess risks. (Standard 2210.A1) The risk assessment is necessary to evaluate where the internal auditors should focus.		
1.2.1	Identify the business risks associated with mobile computing that are of concern to business owners and key stakeholders.	
1.2.2	Verify that the business risks are aligned with the IT risks under consideration.	
1.2.3	Evaluate the overall risk factor for performing the review.	
1.2.4	Based on the risk assessment, identify changes to the scope.	
1.2.5	Discuss the risks with management, and adjust the risk assessment.	
1.2.6	Based on the risk assessment, revise the scope.	
1.3 Define the engagement scope. (Standard 2220) The review must have a defined scope. The reviewer should understand the smart devices in use by the organization, the data passing through these devices, and the relative risk to the organization.		
1.3.1	Obtain a list of smart devices in use.	
1.3.2	Determine the scope of the review.	
1.4 Define assignment success. Success factors need to be identified and agreed upon.		
1.4.1	Identify the drivers for a successful audit.	
1.4.2	Communicate success attributes to the process owner or stakeholder and obtain agreement.	
1.5 Define resources required to perform the audit engagement. (Standard 2230) In most organizations, audit resources are not available for all processes.		
1.5.1	Determine the audit/assurance skills necessary for the review.	
1.5.2	Estimate the total audit/assurance resources (hours) and time frame (start and end dates) required for the review.	

1.6 Define deliverables. (Standard 2210.A3) The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner is essential to assignment success.		
1.6.1	Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses or meetings, and the final report.	
1.7 Communicate the process. (Standard 2201.C1) The audit/assurance process must be clearly communicated to the customer/client.		
1.7.1	Conduct an opening conference to: • Discuss the scope and objectives with the stakeholders. • Obtain documents and information security resources required to perform the review effectively. • Communicate timelines and deliverables.	

Objective 2: Identify and Obtain Supporting Documents (Standard 2310)	
Review Activities	**Control**
2.1 Review smart device (including BYOD) and security policies.	
2.2 Review IT infrastructure architecture documents.	
2.3 Review MAM and MDM procedures.	
2.4 Review reports produced from MAM and MDM.	

Objective 3: Understand the Smart Device Environment	
Review Activities	**Control**
3.1 Is the device owned by the organization or bring your own (BYOD)?	
3.2 Is organization-owned data separated from personal data?	
3.3 Is personal use of the device allowed (for games, social media, etc.)?	
3.4 Is an agreement in place whereby the employee abides by the corporate security policy?	
3.5 Has the employee agreed to remote wipe of the device?	
3.6 Has the employee agreed that a record of his or her phone calls may be viewed by the organization?	
3.7 Does confidential data reside on the device? If so, what are the procedures in place to monitor and control the confidential data?	
3.8 What type of smart devices and operating systems are allowed?	
3.9 Is there a backup strategy and procedure in place for smart devices?	

3.10 Is the smart device connecting to the organization's network? How is it being connected?
3.11 How are apps pushed to the device? Does the organization develop its own apps? Does it have its own app store or marketplace?

Objective 4: Understand the IT Architecture Supporting the Smart Device Environment	
Review Activities	**Control**
4.1 Is the MDM solution a cloud-based solution, or is it internally deployed?	
4.2 Is the solution hosted by a third-party, or is it self-supported?	
4.3 Is there a third-party agreement in place with the vendor?	

Objective 5: Understand Smart Device Security Features	
Review Activities	**Control**
5.1 Verify that the password policy meets industry standards.	
5.2 Review the encryption requirements (especially for confidential data) and how encryption is deployed.	
5.3 Is there a requirement for port controls on a device (camera usage, Bluetooth usage, Wi-Fi controls)?	
5.4 What procedure is in place for remote wipe/locking and unlocking of the device?	
5.5 What procedure is in place for reporting lost devices?	
5.6 How are the devices tracked and monitored?	
5.7 What device configuration is pushed to the device (VPN? Email? Etc.)?	
5.8 How is the delivery of applications to the device controlled? How are the features implemented?	
5.9 What audit and monitoring features are turned on? What reports are being generated?	

Objective 6: Understand How Smart Devices Are Enrolled in the MDM Software	
Review Activities	**Control**
6.1 Does the organization use self-registry? How do users register their device?	
6.2 How do users re-register when they purchase a new device or replace an existing device? What happens to the old device? Is the data wiped off the device?	

6.3 How is it verified that the appropriate security policy has been pushed to the device?

Objective 7: Understand How Smart Devices Are Provisioned for Email, Contacts, and Address Books	
Review Activities	**Control**
7.1 How is email synced with the organization's servers? Is the email encrypted?	
7.2 Where and how is virus checking performed?	

Objective 8: Understand How Applications Are Installed on Smart Devices	
Review Activities	**Control**
8.1 Review applications utilized and how the data is stored and encrypted on the device.	
8.2 Review application deployment.	
8.3 Review the authentication procedure for the applications. How are passwords authenticated? Is there an authorization process established for employee use of organizational data?	

Objective 9: Understand How Smart Devices Are Connected to the Organization's Network	
Review Activities	**Control**
9.1 What type of remote connection is used?	
9.2 What authentication is used prior to allowing access to the organization's network?	
9.3 What encryption protocols are in place for the remote connection?	

Objective 10: Understand Regulatory and Compliance Requirements Related to Smart Devices	
Review Activities	**Control**
10.1 What reports and controls are in place to support regulatory and compliance requirements (such as HIPAA, Sarbanes-Oxley, PCI, PII and others)?	

Objective 11: Understand Management Reports Produced Related to Smart Devices	
Review Activities	**Control**
11.1 What reports are reviewed by management?	
11.2 What key statistics are monitored and reviewed?	

Authors/Contributors

Brad Ames, CRMA, CISA
Frederick Brown, CISA, CRISC
John Bogert, CISA
Michelle Creer, CISA
Jacques Lourens, CIA, CISA, CGEIT, CRISC
Raj Patel, CISA, CISM, CRISC
Sajay Rai, CISM, CISSP
Steve Stein, CIA, CISA

About The IIA

The Institute of Internal Auditors (The 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 more than 180,000 members from more than 170 countries and territories. The association's global headquarters are in Altamonte Springs, Fla., USA. For more information, visit www.globaliia.org or www.theiia.org.

About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (non-mandatory) guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. As part of the IPPF Guidance, conformance with Practice Guides is recommended (nonmandatory). Practice Guides are endorsed by The IIA through formal review and approval processes.

A Global Technology Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to IT management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance or www.theiia.org/guidance.

Disclaimer

Copyright

August 16