Auditing Computing Infrastructure and IT Operations

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

Acknowledgements

IT Guidance Development Team

Jim Enstrom, CIA, CISA, United States

Avin Mansookram, CISA, CGEIT, South Africa

Scott Moore, CIA, United States

Terence Washington, CIA, CRMA, United States

Brittany Long, CIA, CRMA, CISA, CDPSE, United States

Uday Gulvadi, CIA, CPA, CAMS, CISA, United States

Global Guidance Council Reviewer

Joonas Värtinen, CIA, Finland

International Internal Audit Standards Board Reviewers

Laurent Philippe Berliner, CIA, CRMA, Luxembourg

Jessica Echenique Montero, CIA, United States

IIA Standards and Guidance

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

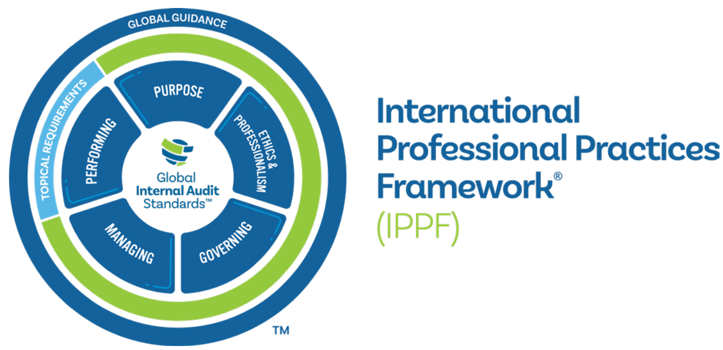
Katleen Seeuws, CIA, CGAP, CRMA, CFE, CISA, Vice President

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

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

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

About the IPPF



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

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

Global Guidance

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

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

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

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

Contents

Executive Summary

Computing infrastructure and IT operations are the fundamental technology assets and services required for organizations worldwide to perform their daily operations. Computing Infrastructure includes hardware, software, and network devices. IT operations are focused on helping ensure that the infrastructure runs reliably and effectively. Together, they form the technology foundation that organizations rely upon to conduct business operations and achieve operational objectives.

IT management should continuously monitor and assess the security of the organization's computing infrastructure and IT operations, including ensuring timely patching, logically and physically restricting access, and scanning for threats. Effective data backup and recovery protocols should also be in place as part of the organization's disaster recovery and response plan.

Internal audit engagements to assess the computing infrastructure and IT operations should identify risks and controls relevant to the organization's environment and determine whether controls have been adequately designed and effectively implemented to minimize downtime and restrict unauthorized users. In its assurance and advisory services, the internal audit function can provide valuable insights to all stakeholders by incorporating the control guidance from widely used frameworks into a systematic evaluation of the organization's policies and procedures.

Introduction

Computing infrastructure and IT operations provide the foundational resources that organizations use in most aspects of their daily processes and activities.

More specifically, computing infrastructure is the collection of technology that supports IT services. It includes the hardware, software, data storage, and network elements that support the management of an organization's information, data, and processing. Organizational computing infrastructure needs may be met using internal assets, external service providers, or a hybrid approach. Many organizations also use cloud-based computing infrastructure resources.

IT operations encompass the activities involved in managing, maintaining, and delivering services that support the technological aspects of the organization's computing infrastructure, enabling the performance of daily business functions.

An organization's computing infrastructure and IT operations should support achieving operational objectives, including **confidentiality**, **integrity**, and **availability** of data and information, while being closely aligned with strategic objectives. Computing infrastructure and IT operations should adapt to the organization's changing needs. Internal auditors should understand computing infrastructure and IT operations because these areas are exposed to **inherent risks** from external and internal threats and are critical to most technology-based audit **engagements**.

Note

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

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

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

Readers of this guide are assumed to have a general knowledge of information technology – information systems ("IT-IS") **risks** and **controls** (Standards 3.1 Competency and 13.5 Engagement Resources). This guide expands on the high-level descriptions found in the "IT Infrastructure" section of the GTAG "IT Essentials for Internal Auditors," which provides an in-depth look at risks and controls relevant to the hardware and software that support an organization's technology environment.

This GTAG covers processes that internal auditors should consider when planning an engagement to assess the organization's controls over IT infrastructure and operations. For the **internal audit function** to provide valuable **assurance** and **advisory services**, auditors should understand the risks and controls relevant to meeting an organization's needs for computing infrastructure and IT operations.

This guide refers to The IIA's Global Internal Audit Standards, including its principles and domains, as applicable. Appendix A lists IIA resources that offer information and cover additional topics in more detail. For example, the GTAG "Auditing Network and Communications Management" thoroughly explains network considerations, while this guide focuses on other key areas. Appendix C lists additional references and resources that readers may find helpful.

While individual organizations' needs are unique, the processes to establish and operate computing infrastructure and IT operations can be grouped into:

- Governance and risk management.
- Managing computing infrastructure.
- Managing IT operations.

The following sections describe these objectives and their respective risks and controls in greater detail. They refer to specific, relevant sections of widely used external control frameworks to help internal auditors plan engagements (Principle 13 Plan Engagements Effectively).

References to IT-IS Control Frameworks

This guide references four external IT-IS control frameworks of standards, guidance, and best practices, while recognizing that many others are used worldwide. Each framework provides more information about specific controls than is discussed here. IT-IS personnel frequently benchmark operational and security controls against one or more of these frameworks. Internal auditors are encouraged to identify the frameworks used by their organizations and review other widely adopted IT-IS control guidance to help them identify and understand common risks and controls. Appendix C provides links to these frameworks and more.

The four frameworks referenced are:

- *COBIT 2019 Framework: Governance and Management Objectives* from ISACA.
- *NIST Special Publication (SP) 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations* from the National Institute of Standards and Technology (also referred to as *NIST 800-53r5).*
- *NIST Framework for Improving Critical Infrastructure Cybersecurity Version 2.0* (also referred to as the *NIST Cybersecurity Framework Version 2.0* or *NIST CSF.*
- *CIS Controls Version 8.1* from the Center for Internet Security.

Incorporating a review of external guidance into **engagement planning** and performance helps an internal auditor demonstrate the essence of Principles 3 and 4 of the Global Internal Audit Standards. Principle 3 Demonstrate Competency states in part: "Demonstrating **competency** requires developing and applying the knowledge, skills, and abilities to provide internal audit services," and Principle 4 Exercise Due Professional Care includes: "Due professional care requires planning and performing internal audit services with the diligence, judgment, and skepticism possessed by prudent and competent internal auditors." Additionally, Standard 13.4 Evaluation Criteria states that, "Internal auditors must identify the most relevant **criteria** to be used to evaluate the aspects of the **activity under review** defined in the **engagement objectives** and scope."

Guidance Objectives

This GTAG provides a systematic approach that can be adopted by internal auditors of all backgrounds and adapted to their organizations. This guide helps the reader:

- Describe the importance of computing infrastructure and IT operations to achieving organizational objectives and understanding the risks that threaten the achievement of those objectives.
- Identify the typical components of computing infrastructure and IT operations processes, including common risks and controls.
- Identify the relevant **control processes** of external frameworks for further research into best practices.
- Plan and perform assurance and advisory services over computing infrastructure and IT operations.

While the guide provides common considerations for internal auditors performing audit engagements on computing infrastructure and IT operations, it is not intended to be an all-encompassing inventory of aspects that could be assessed. It is important that internal auditors develop an understanding of how their organization operates and use their professional judgment regarding what should be included in the scope of the engagement. Aspects not included in this guide may also be required.

Internal Audit Plan

Standard 9.4 Internal Audit Plan states: "The **chief audit executive** must create an **internal audit plan** that supports the achievement of the organization's objectives." As part of the planning process, the chief audit executive reviews the organizationwide risk assessment results and uses that assessment as the basis for the internal audit plan. The chief audit executive should stay informed of emerging risk information. Technology is critical to most organizations' processes and transactions, so it is vital to understand the risk environment related to computing infrastructure and IT operations. Additionally, some internal audit functions may rely upon the work of other **assurance** providers regarding computing infrastructure and IT operations. Standard 9.5 Coordination and Reliance applies, stating in part: "The chief audit executive must coordinate with internal and external providers of assurance services and consider relying upon their work."

Audit Resources

See The IIA's Global Practice Guides "Coordination and Reliance: Working with Other Assurance Providers" and "Developing a Risk-Based Internal Audit Plan" for more information.

Engagement Planning

An internal audit **engagement** that examines computing infrastructure and IT operations involves a **risk assessment** (Standard 13.2 Engagement Risk Assessment) and specified **engagement objectives** (Standard 13.3 Engagement Objectives and Scope). It also includes tests (Standard 13.6 Work Program) to evaluate the adequacy and effectiveness of relevant **control processes** to determine whether any significant risk exposures exist. Ideally, the internal audit function, technology management teams, and other personnel collaborate to provide valuable insight into inherent risks, the adequacy and effectiveness of controls, and **residual risks**.

An audit engagement covering the risks and controls relevant to computing infrastructure and IT operations contributes to providing assurance on whether the organization's information technology governance supports its strategies and objectives (Standard 9.1 Understanding Governance, Risk Management, and Control Processes).

Governance and Risk Management

Governance

As described in The IIA's Three Lines Model™, the governing body (referred to as the **board** in the Standards) is responsible for ensuring that organizational activities are aligned with the prioritized interests of **stakeholders**. An important aspect of governance is overseeing management's actions to achieve strategic objectives, including the application of resources.

Information technology resources are vital to organizations: daily transactions occur through deployed computing infrastructure supported by IT operations. Therefore, it is important that the governance process includes overseeing that the IT resources support the organization's goals, objectives, and strategies. Standard 8.1 Board Interaction states: "The chief audit executive must provide the board with the information needed to conduct its oversight responsibilities."

Risk Management

Numerous risks are associated with computing infrastructure and IT operations. Therefore, processes to manage risks that could threaten the achievement of strategic goals should include consideration of technology resources. For example, many organizations require infrastructure to be scalable and able to adjust to increasing capacity demands for their critical processes. Internal auditors should gain an understanding of business drivers that may require the organization's infrastructure to adapt. While reviewing how current risks are managed is important, understanding how IT management is prepared to support the organization's technology demands, which are increasing at an unprecedented pace, is also necessary.

Audit Resources

See The IIA's Global Technology Audit Guides "Auditing Cybersecurity Operations: Prevention and Detection" and "Auditing Cyber Incident Response and Recovery" for more information.

Risks may include:

- Resources related to computing infrastructure or IT operations do not support the organization's technological requirements for operations or do not achieve its operational objectives. Resources may include physical assets, services, third parties, or qualified staff.
- Computing infrastructure is not configured properly from a security standpoint to minimize vulnerabilities, causing slower-than-desired processing or unplanned downtime.
- Difficulty in tracking and managing the costs associated with computing infrastructure and IT operations as the organization's use of technological resources increases.
- Inability to source computing infrastructure assets due to supply chain disruption, such as political instability in countries where critical parts or hardware are produced.
- IT operations, including **incident** response, that are ineffective and fail to mitigate risks related to cyberattacks, data breaches, unauthorized access, software failure, or other issues.
- Inability to recover from a disaster.
- Untimely resolution of end-**user** issues.
- Non**compliance** with laws or regulations.

As stated in Standard 13.2 Engagement Risk Assessment: "Internal auditors must develop an understanding of the activity under review to assess the relevant risks." Understanding how the organization manages the risks related to computing infrastructure and IT operations is an important consideration. Internal auditors may review recently performed risk assessments or meet with the risk management team to understand how risks are identified, assessed, mitigated, and monitored.

Computing Infrastructure

Computing infrastructure includes the hardware, software, network devices, and peripherals that organizations use to perform operations. This section offers considerations for performing engagements on computing infrastructure components.

Hardware

Hardware includes the physical devices or equipment used to process transactions, including storing data and maintaining communication networks. Internal auditors should understand how data stored on hardware is protected. This includes protecting data on hardware currently in use, such as using **encryption**, and when hardware is decommissioned from service, which should include a process to permanently erase data. Internal auditors should also understand how data on hardware is backed up to ensure protection from loss.

An organization's hardware infrastructure may be hosted on-premises (also called on-site) or off-premises, in which an organization **outsources** its infrastructure to a vendor or third party. Organizations may utilize a vendor for on-demand cloud computing resources, such as data storage, which is known as "infrastructure as a service." Examples include Microsoft Azure, Amazon Web Services, and Google Compute Engine.

Data Centers

Data centers house the organization's servers and other computing hardware and may be located on the organization's premises. However, this function is increasingly outsourced to a third party that specializes in housing data centers for organizations.

Internal auditors should consider the following when reviewing on-premise data centers:

- Physical security of the data center, including:
    - Who can physically access computing hardware.
    - The process for granting, removing, and periodically reviewing access.
    - Video monitoring of facility entrances and exits and the equipment itself.
- Environmental controls in place, including:
    - Adequate cooling and ventilation for the equipment.
    - Temperature monitoring procedures.
    - Maintenance of the cooling equipment.
    - Procedures for monitoring facility water leakage.
    - Raised floors to further secure equipment from potential water damage.

    - Fire suppression.

- Other controls to consider, including:
    - Backup generators to ensure the data center has power in the event of a power outage or failure.
    - Uninterruptible power supplies to keep equipment operating temporarily if the power fails, giving time for the generators to be activated.
    - Procedures for monitoring the health of the generators and uninterruptible power supply systems, including periodically testing that they are operating as intended.

For outsourced data centers, internal auditors should review the appropriate system and organization controls (SOC) report to ensure that the complementary user entity controls are adequately addressed by the organization. Internal auditors should know the locations of the physical servers and consider whether there may be data compliance requirements related to location. Additionally, the engagement should verify that a disaster recovery plan is in place and tested periodically to minimize potential disruption.

Servers

Servers are powerful computers and critical components of the computing infrastructure. They provide other computers, also called clients, with functionality or services such as data storage, programs, or other resources. Common types of servers include **application**, database, file, email, print, and web.

When servers are included in an audit engagement's scope, obtaining an up-to-date network diagram and a detailed server inventory, including each server's function, helps internal auditors identify those in active use. After selecting a sample of servers based on the scope and objectives of the engagement, internal auditors may validate these attributes:

- On-premise servers are in a secure location with restricted physical access.
- Logical access to servers is limited to authorized users who have a legitimate business need and a level of access commensurate with their job duties, and access is periodically reviewed. Requirements to access servers includes complex passwords (complying with organizational policy) that expire periodically. Some organizations may use multifactor **authentication** as well.
- Administrator rights are commensurate with job duties (proper segregation of duties) and are periodically reviewed.
- Each sample server is reviewed for its purpose and criticality, applications in use, and the type of data being stored.
- The **operating system** is updated with the latest security patches and updates, including adherence to the organization's hardening policies. Patch management addresses vulnerabilities or issues with the code. An example is Windows Server Update Service for Microsoft-based servers. Emergency or zero-day patches are applied timely.

- **Antivirus software** has been installed and updated with the most recent releases.
- The server is backed up, tested periodically, and included in the disaster recovery plan.
- Servers comply with relevant regulations, such as the European Union's General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA), and other **privacy** laws.
- Data is encrypted.
- **Audit logs** record events such as who accessed a server, when it was accessed, what files were accessed, and what transactions and activities were performed. Audit logs are secured to prevent editing, ensuring reliability.
- Performance and utilization are monitored to identify operational issues.
- A configuration management database is established to track server attributes.
- A formal process is used to acquire new servers, deploy them into production, and retire existing servers after data has been backed up and erased.

End-User Devices

End-user devices include laptop and desktop computers and mobile devices such as tablets and mobile phones used by individuals within an organization to send and receive data, process transactions, and more. Internal auditors should understand how the organization configures end-user devices to determine compliance with the organization's security policies. Internal auditors should verify the following when auditing end-user devices:

> **Audit Resource**
>
> See The IIA's Global Technology Audit Guide "Auditing Mobile Computing" for more information.

- End-users have limited or no administrative **access rights** to their company-issued devices. Examples of administrative access rights include:
    - Installing unapproved software.
    - Disabling antivirus/anti**malware** software, operating system and application software updates, or screen lock.
    - Altering security settings, such as password requirements.
- Encryption is used to protect stored data and data in transit.
- Virtual private networks (VPNs) or zero-trust networking are used for remote-user access.
- The organization is able to determine when devices require updates or the latest security patches have not been applied.
- USB ports have been locked to prevent **data leakage**, malware infections, and the use of unauthorized personal devices.

- A formal process for disposing of end-user devices exists and includes erasing sensitive data.

Many organizations use a "bring your own device" (BYOD) approach for mobile phones and tablets, enabling employees to use their personal devices for work purposes, such as accessing an email application. Internal auditors should verify that the organization has a comprehensive BYOD policy that includes expectations for employees to adhere to established parameters. The policy also outlines basic security features that should be in place, such as locked screens, strong passwords, and the ability to apply updated security patches to address known vulnerabilities.

Auditors should verify the presence of a "remote wipe" capability and understand how the organization performs this security action on lost devices or the devices of terminated users. This capability minimizes the risk of losing sensitive data. Awareness and training should be in place to educate users on the organization's policies and the risks associated with using their personal devices to conduct business transactions.

Network Devices

Network devices enable communication and interaction (such as email, file sharing, and messaging) between internal computers and external devices and networks. In addition to providing network connectivity for an organization's technology assets, they may also provide protection from unauthorized external users. Common network devices include routers, hubs, switches, bridges, repeaters, firewalls, and intrusion detection/prevention systems.

Obtaining the organization's network topology and architecture documentation can help internal auditors understand the existing network. The "IT Network" section of the GTAG "IT Essentials for Internal Auditors" provides a detailed overview of different types of networks and approaches organizations may use to build their networks. The GTAG "Auditing Network and Communications Management" provides an in-depth look at network-related processes that internal auditors should consider when assessing an organization's communications ecosystem.

Additionally, internal auditors may review these control considerations related to network devices to assess whether the organization:

- Has identified all network devices and employs a process to update the devices with the most recent software and **firmware** releases and security patches.
- Has established a process for monitoring unusual activity (or access) and restricting unauthorized users and unnecessary traffic, such as blocking internet protocol (IP) addresses or IP address ranges within firewall configurations. The process should include procedures to review and potentially escalate concerning events, such as a cyberattack, in a timely manner. Organizations commonly utilize penetration, or "pen," testing to proactively identify vulnerabilities.
- Uses network segmentation to hinder or prevent unauthorized users from accessing sensitive data.

Uses an intrusion detection or prevention system to monitor, detect, and remove or block unauthorized users.

Peripherals

Peripheral devices enable users to enter and receive information from their computers. Input occurs through mice, keyboards, web cameras, microphones, and scanners. Output devices include monitors, speakers, and printers. Properly securing printers from unauthorized users is vital because these devices contain temporary memory files from which physical copies can be printed. Peripherals also include storage mechanisms and devices, such as USB flash drives and mobile hard drives. Internal auditors should verify that storage devices are encrypted and only company-issued storage devices are used.

Software

Operating Systems and Applications

An operating system (OS) is a "master control program that runs the computer and acts as a scheduler and traffic controller."[1] The most common operating systems are Microsoft Windows, Apple Mac OS, and Linux.

An application is "a computer program or set of programs that performs the processing of records for a specific function."[2] This section reviews the risks associated with operating systems and applications and the audit steps that may be performed to address the risks. Many risks associated with operating systems and applications are similar and select risks specific to each area are individually addressed.

Common Secure Configuration

Secure configuration of operating systems and applications is an important risk area. NIST defines it as "a recognized, standardized, and established benchmark that stipulates specific secure configuration settings for a given information technology platform."[3] Areas of secure configuration to address when assessing an operating system or application include:

- Devices locking after a defined number of unsuccessful logins.
- Password parameters, which should be configured based on the organization's policy. Ideally, the policy is reviewed periodically and updated as appropriate to ensure best practice standards.
- Default user IDs and passwords, which should be changed from the original settings to prevent unauthorized user access.

A device lock/unsuccessful login configuration is a setting that determines how many times an ID can unsuccessfully attempt to log in before that ID or device is disabled. Locking the ID and/or device after a predetermined number of unsuccessful login attempts helps prevent **brute force attacks** through which an unauthorized user tries to access the operating system or application and its resources.

1. ISACA glossary, https://www.isaca.org/resources/glossary.
2. ISACA glossary.
3. NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/Common_Secure_Configuration.

Evaluation of this setting should include:

- Obtaining the access management or other policy that defines how many unsuccessful login attempts are allowed before the account is disabled.
- Reviewing the policy and determining whether the settings appear reasonable.
- Obtaining evidence from the operating system that the parameters for unsuccessful login attempts align with the policy.

Password parameters for IDs on an operating system or application establish the acceptable quantity of characters and combination of uppercase and lowercase characters, numbers, and/or special characters. The parameters also define how often passwords expire and if passwords can be reused. Proper parameters are important to ensure that passwords are strong and not easily guessed. Evaluations of password parameters should include:

- Obtaining the access management or other policy that defines password parameters.
- Reviewing the policy and determining whether the settings appear reasonable based on leading practices. Complex passwords (passwords that contain uppercase and lowercase characters, numbers, and special characters, and total to a minimum number of characters) should be required at a minimum, and multifactor authentication should be enabled for any IDs that have elevated access, which may also include rotation of passwords for highly privileged accounts.
- Obtaining evidence from the operating system and applications that the password parameters are configured according to the policy.
- For shared service accounts accessed by multiple users, some organizations use a secure password vault to restrict access to authorized users and implement a key-based password rotation.

Additionally, many applications may be configured for single sign-on (SSO), a function that enables users to automatically log onto applications when logging on at the operating system level. For SSO-enabled applications, internal auditors should expect to see the SSO parameter enabled (turned on) within the application, and pointing to the correct area for authentication.

Some operating systems and applications come with preconfigured, or default, IDs and associated default passwords. Because these IDs often have known passwords and privileged levels of access, it is critical to ensure a process is in place to identify and secure them appropriately. Some Windows OS default IDs include administrator, guest, and help assistant. Some Linux default IDs include root, adm, and bin. The process for evaluating the treatment of default IDs includes:

- Obtaining a list of all operating system IDs.
- Identifying the default IDs and asking IT management about security procedures.
- Determining whether the accounts have been properly secured, such as by changing default passwords.

Operating systems also often come with services, ports, and features that should be disabled if they remain unused because they may provide an opportunity for **hackers** to gain unauthorized access. The process for evaluating the treatment of unused services, ports, and features includes:

- Obtaining a listing of all active services, ports, and features.
- Reviewing the listing with management to determine whether all active services, ports, and features have a valid purpose.

The IIA's GTAG "Auditing Identity and Access Management" provides more information on user access.

Privileged Access

Privileged access grants a user "greater than basic access privileges…with more rights than a standard user account."[4] **Privileged user** access may include performing functions such as:

- Adding or removing users.
- Modifying user system access.
- Modifying key configuration settings (password parameters and lockout duration, among others).
- Performing other key system administrative functions.

Evaluations of privileged access to the operating system and application software should include verifying whether:

- All accounts (or roles) with privileged access are identified and periodically recertified to ensure access is appropriate, including clearly defining processes and roles for those who are allowed to modify access rights.
- Accounts with privileged access require multifactor authentication.
- Activities performed by privileged access users are logged and monitored for appropriateness.
- Proper segregation of duties exists to assess permissions commensurate with user roles.

Virtualization

NIST defines virtualization as "the simulation of the software and/or hardware upon which other software runs."[5] Virtualization has gained popularity because it allows for fast scalability, improved performance, better disaster recovery, reduced costs, and other advantages. The main risks associated with virtualization are:

- Security of the hypervisor.
- Security of the virtualized components (operating systems, for example).

4. ISACA glossary.
5. NIST Computer Security Resource Center.

- Secure configuration of the virtualized environment.

Hypervisor is "the virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware."[6] The hypervisor is the software that allows multiple virtual machines to run on a single piece of hardware. Popular hypervisor software includes VMware vSphere, Microsoft Hyper-V, and Citrix XenServer. Securing the hypervisor is vital as unauthorized access may result in full control over the machines and data it manages. When assessing the security of the hypervisor, internal auditors should consider:

- Reviewing the policies that describe the process, including:
    - A policy for reducing the hypervisor's attack surface by ensuring only necessary software is installed (drivers, backup agents, virus/malware protection, and security tools, for example).
    - A policy describing the roles of those who should have hypervisor remote access.
- Inspecting the hypervisor configuration to assess compliance with policies.

The hypervisor manages the virtualized servers, but each virtualized server should be managed like a comparable physical server. The operating system and application software should be treated as described in the "Operating Systems and Applications" section.

As stated, one advantage of virtualization is its ease of scalability. The processes for configuring the virtualized environment must be secured to monitor, prevent, and detect risks such as:

- Unauthorized copying/cloning of the virtual environment and its data.
- The creation of virtual machines that are not securely configured.
- Unauthorized changes.

When assessing the processes and procedures implemented to control the copying of virtual environments, internal auditors should consider:

- Reviewing relevant policies and procedures, including:
    - Approval requirements before copies are made.
    - Segregation of duties between approvers and those with the ability to make copies.
    - Standardized process for copying environments.
    - Provisions for masking/anonymizing sensitive data in nonproduction environments.
- Testing procedures to assess whether they are followed.

6. NIST Computer Security Resource Center.

- Identifying processes intended to detect unauthorized copies of virtual environments.

The organization's procedures should ensure that all created virtual environments are configured securely. This may be accomplished by requiring all environments to adhere to approved templates that adequately address security issues. When assessing the configuration of virtual environments, internal auditors should consider:

- Reviewing relevant policies and procedures, including:
    - Security-hardened templates for configuring virtual environments.
    - Provisions for maintaining audit logs of all access and configuration changes for virtual environments and unusual activity.
    - Provisions for regularly patching the hypervisor.
- Reviewing the process for scanning virtual machine configurations before deployment to ensure alignment with the approved templates.
- Reviewing processes and procedures for monitoring virtual environment configuration.
- Verifying that access to virtual machine creation and configuration is restricted to appropriate users.
- Inspecting virtual environments to assess compliance with policies.

Organizations may outsource virtualization to third-party service providers. Popular solutions include V2 Cloud, AWS, Google Cloud, Oracle VM VirtualBox, and Microsoft Azure. When third-party service providers are used, internal auditors should consider:

- Obtaining and reviewing the relevant SOC reports to ensure that no control issues are noted and that the organization — not the service provider — addresses the complementary user entity controls, as stated in the SOC report. If significant control issues are identified, additional procedures may be necessary to rely on the service provider's controls.
- Identifying the locations of the physical servers to ensure that relevant regulatory requirements for data protection are followed (GDPR, for example).

Directory Services

Directory services are databases that store identity information and enable the authentication and identification of people and machines.[7] Popular directory services include Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). When assessing directory services, internal auditors should consider:

- Controls over privileged access.
- Audit policies to analyze activity, changes made to objects, and user logs.
- Configuration and key security features.

---

7. *NIST SP 1800-16*, Securing Web Transactions. https://doi.org/10.6028/NIST.SP.800-53r5.

Roles with privileged access to directory services are able to create and delete user accounts, reset passwords, change group memberships, and modify objects. Assessing controls over privileged access to directory services includes reviewing whether:

- Users and roles with privileged access are appropriately assigned.
- Specific authorization is required to grant users access to such roles.
- The appropriateness of privileged access for users with these roles is periodically checked.

Internal auditors should also review whether:

- The directory services' audit policies are configured to monitor privileged user activities, critical objects, and events (for example, creating/deleting accounts in a timely manner, resetting passwords, and changing group memberships).
- Change controls over these configurations and controls are present to ensure that logs are not altered or deleted.

Data Storage

Organizations store tremendous amounts of data in databases (such as SQL, IBM DB2, and Oracle) and in structures known as "data warehouses" (used for structured data) or "data lakes" (used for unstructured and structured data). Data storage may also be hosted in cloud environments. These options may present challenges for internal auditors. When auditing data storage, internal auditors should consider the following:

- Access controls, especially "write" and "modify" privileges.
- Authentication process.
- Change management processes, including logging and monitoring changes.
- Job monitoring, including scheduling.
- File monitoring and encryption.
- The type of data and its sensitivity with regard to privacy regulations.
- Compliance with regulations, especially related to privacy.
- Backup and recovery, including storage version control.

For data storage access controls, the primary risk to address is determining which users have permission to write and modify data. Internal auditors may review whether the organization has established and implemented adequate policies to govern which job roles are permitted to modify data. Additionally, internal auditors may obtain system-generated listings of users who can modify data and determine whether their access is appropriate. Internal auditors also may assess the process for periodically reviewing users who have access to write and modify content.

Internal auditors should evaluate the adequacy of the organization's procedures and tools for monitoring files to determine whether any changes were made. Processes should include determining whether changes were properly authorized and documented and monitoring data access logs for any unauthorized activity. This is particularly important related to artificial intelligence processes, due to the risk of manipulating input data to produce biased results. Internal auditors should determine whether the organization's data encryption processes are operating effectively.

Internal auditors should review whether the type of data stored and the data's physical storage location(s) present regulatory compliance concerns. Regulations vary depending on the organization's location(s) and the global regions in which it conducts business, including the collection of users' personal data.

Data backup is vital to ensure that critical data is not compromised or lost to disasters, equipment failures, or cyberattacks. Internal auditors should evaluate whether tools and procedures are in place to back up critical data. Auditors should also verify whether periodic data recovery tests are performed to ensure that backed-up data can be restored.

Messaging

Messaging includes email, text, messaging (Zoom, Teams, and similar apps), and the transfer of attachments through such technologies. As with applications and operating systems, internal auditors should verify that appropriate safeguards are in place regarding:

- Secure configuration.
- Patch management.
- Vulnerability management.
- Change management.
- Privileged access.

Internal auditors should evaluate the processes, procedures, and technologies used by the organization to detect and prevent viruses, **spam**, and phishing attempts from propagating through messaging systems. In particular, auditors may review:

- The configuration of filters.
- Processes for changing the configuration.
- Who has access to change the configuration.
- Monitoring procedures to detect changes to the configuration.
- Training activities to increase awareness of harmful activities.

Filters are the rules the messaging system uses to determine which emails it allows to be received. These rules can include approved senders, approved content, and approved attachments. Auditors should develop an understanding of the processes and controls over how changes are made to the configuration of filters.

File Sharing

File-sharing applications/services such as Google Drive, SharePoint, DropBox, and OneDrive are tools for collaborating and sharing information/files. Internal auditors should review the organization's policies to determine whether file-sharing options are specified and whether procedures have been implemented to monitor compliance with policies. Additionally, auditors should review whether the user authentication and access controls related to the file-sharing applications or service comply with the organization's access control policies and whether additional controls, such as multifactor authentication, are in place.

Mobile Devices and Mobile Device Management

Mobile devices and their management have increased in prevalence and importance over time. New technologies have enabled users to gain greater access to organizational computing resources through mobile connections. These risks and considerations are detailed in the GTAG "Auditing Mobile Computing."

Managing IT Operations and Service Delivery Management

IBM defines IT operations, or "ITOps," as "the process of implementing, managing, delivering and supporting IT services to meet the business needs of internal and external users."[8] IT operations play a critical role in organizational operations because they are responsible for keeping technology processes running and minimizing user downtime. In other words, IT operations help ensure the reliable performance of the various computing infrastructure elements described previously in this guide.

Service delivery management, or IT service management (ITSM), is "the practice of planning, implementing, managing and optimizing the end-to-end delivery of information technology services to meet user needs and business goals."[9]

The main risk of ineffective IT operations and service delivery management is that an organization is unable to perform the activities required to perform business transactions. This may include being unable to conduct business with customers or third parties. It is vital that IT operations and service delivery management act promptly when responding to organizational user needs and threats from outside the organization that could lead to downtime or disruption in service. While the previous section on "Computing Infrastructure" focuses on the assets that an organization needs to support operations, this section addresses the services or actions performed by IT to support the organization's computing infrastructure.

Patch Management

Patch management can be defined as "an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk."[10] Patch management is a critical process for ensuring that the operating system and application software are secure.

Two critical aspects of patch management are monitoring and implementation. It is vital to understand management's monitoring process for identifying available patches. This can be accomplished by subscribing to services or by periodically monitoring vendor websites of the operating system or application software vendors for security releases. Determining which patches should be applied (or whether an approval process is required), who should apply the patches, and that the patches are applied in a timely manner are vital for the implementation process. Additionally, having an updated inventory of assets that require patching is necessary

8. IBM, *What is ITOps*?, accessed July 23, 2025, https://www.ibm.com/think/topics/it-operations.
9. IBM, *What is ITSM (IT service management)?*, accessed July 23, 2025, https://www.ibm.com/think/topics/it-service-management.
10. ISACA glossary.

to ensure that clear ownership of patching responsibilities exists. Internal auditors should consider the following aspects related to implementing patch management:

- Obtaining the policy for implementing patches.
- Determining whether management has a timeline for implementing patches based on severity (for example, identifying a process for expediting critical patches).
- Determining whether patches are implemented in a test environment before being implemented in the production environment.

Vulnerability Management

Vulnerability management is the process of actively looking for security weaknesses in the network (or in software). NIST defines it as a "capability that identifies vulnerabilities on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network."[11] While this process generally applies more to operating system software, it can also apply to application software. A vulnerability management program should include processes for:

- Periodically scanning (such as pen testing) for vulnerabilities [*NIST 800-53r5,* RA5]. This includes scanning for vulnerabilities covered previously in this guide, such as those related to patches, ports, services, and privileged access.
- Addressing any identified vulnerabilities in a timely manner.
- Communicating vulnerabilities to those responsible to raise awareness.

Change Management

Change management is a methodical approach for controlling and implementing changes in a planned and structured manner.[12] Organizations should implement policies and procedures to manage changes to operating systems and application software. Evaluations of the change management function should include reviewing:

- The change management policy, including the approval process and documentation of changes.
- Whether patches are implemented in a test environment before being implemented in the production environment.
- Whether the duties (and corresponding logical access) of the individuals who implement the changes are segregated from those who migrate the change to the production environment.
- Whether the testing documentation related to the change is complete and the results are favorable.

11. *NIST SP 800-53r5.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
12. ISACA glossary.

The GTAG "IT Change Management: Critical for Organizational Success" provides more information.

Cybersecurity and Incident Response

Cybersecurity is a broad topic that requires organizations to implement effective control processes to restrict unauthorized users from gaining access to digital assets and sensitive data. The IIA's "Cybersecurity Topical Requirement and User Guide" outlines the minimum requirements the internal audit function should assess when performing an assurance assessment over cybersecurity. Additionally, these IIA Global Technology Audit Guides provide internal auditors with information to be used when performing cybersecurity engagements:

- "Auditing Cybersecurity Operations: Prevention and Detection."
- "Auditing Cyber Incident Response and Recovery"
- "Auditing Network and Communications Management."

Artificial Intelligence for IT Operations

Artificial Intelligence for IT Operations (AIOps) is the "the application of artificial intelligence (AI) capabilities — such as natural language processing and machine learning models — to automate, streamline and optimize IT service management and operational workflows."[13] An example of AIOps is the use of machine learning to analyze large data sets to identify trends or anomalies. Real-time analysis conducted by IT operations may enable predicting issues and automating or implementing resolutions promptly.

It is essential that internal auditors understand key aspects of AIOps' use within the organization, including:

- Identifying who is responsible for overseeing AIOps (for example, the board or a designated committee), specifically, the oversight to ensure use in an ethical and transparent manner.
- Understanding how AIOps are managed and organized.
- Determining who manages AIOps (for example, a member of executive management).
- Reviewing established policies and procedures related to AIOps.
- Assessing how AIOps contribute to achieving the organization's strategic goals and objectives.
- Evaluating the internal controls in place to manage risks associated with AIOps.
- Understanding how the organization assesses and scales the additional processing power required by AI.
- Examining the reporting mechanisms used to monitor and assess AIOps' performance.

13. IBM, *What is AIOps?*, accessed July 23, 2025, https://www.ibm.com/think/topics/aiops.

The IIA's "Artificial Intelligence Auditing Framework" is useful to an internal audit function providing assurance or advice on AI-related processes.

Access Management

Limiting access to authorized users is an important foundational element of an effective internal control environment. Access management, also known as identity and access management, has three main control objectives:

- *Identification* – Who is the user? Digital identifiers (IDs) may be created for people, groups, and system-defined processes. Each ID should be traceable to or owned by an employee to ensure accountability.
- *Authorization* – What can the user do in this system? This objective requires coordination between system administrators (usually in IT), the primary benefiting business unit (often called the "business owner"), and end users and their supervisors. It involves defining appropriate permissions for various job functions and ensuring that each ID requesting access rights is given an appropriate response. Account reauthorization and deactivation processes may require coordination between human resources, the business unit, and IT.
- *Authentication* – Is the user who they claim to be? Control mechanisms such as passwords, temporary access codes, or biometric data may be used to verify the identity of the person or process attempting to gain access to the permissions associated with an ID. Authentication factors are often defined as something one knows (like a password), something one has (like a mobile phone), or something one is (biometric data, such as a fingerprint).

The GTAG "Auditing Identity and Access Management" provides additional information to consider when performing assurance or advisory services over access management.

Disaster Recovery

ISACA defines disaster recovery as the "activities and programs designed to return the enterprise to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions."[14] A major focus of disaster recovery includes the IT components required to restore technological operations. Disaster recovery is part of the larger business continuity plan within the organizational resilience strategy, which covers all components of an organization that are necessary or required to resume normal business operations, including IT.

Key aspects of a disaster recovery include:

- Establishing a formal disaster recovery plan that is tested periodically and includes third parties.

14. ISACA glossary.

- Identifying a disaster recovery team with roles and responsibilities clearly defined regarding what important duties must be fulfilled when a disrupting event occurs.
- Identifying a key IT asset inventory, which is typically tied to a risk assessment or business **impact** analysis. IT assets should be prioritized according to their criticality and the order in which they should be restored to ensure continuity of operations.
- Regularly backing up key IT assets along with periodic testing of backups (such as testing a restore of a server or files).
- Identifying an alternate site for operations when a significantly disruptive event occurs, such as a temporary location that can be utilized until the organization's main site is suitable for return.

IT Project Management

IT project management is the process of implementing IT-related solutions. The phases of IT project management may include:

- Initiation, which includes creating a business case or establishing a need for the project. This may include identifying alternative options and assessing their cost-benefit aspects. Approvals are a critical internal control.
- Planning, including assessing risk, determining requirements, assigning IT staff, setting timing deadlines, and establishing success criteria, such as key performance indicators (KPIs) or other measurables that will be reported. Establishing a budget is often an important aspect of the planning phase. Another key consideration is an analysis of the internal control environment, including identifying required controls based on the risk assessment or how the project fits into the existing, established control processes.
- Performance, which includes activities related to achieving project goals, providing deliverables, and meeting timing deadlines. This is the phase in which the actual project is performed.
- Monitoring, which includes periodic reporting based on established success criteria, such as project completion status, KPIs, or closely tracking budgetary parameters. Managing issues regarding the identification of barriers or obstacles that may be preventing projects from progressing or achieving milestones is an important component of monitoring. Gantt charts or other project management software may be utilized.
- Communication with relevant stakeholders to ensure all parties are aware of a particular project's progress. This could be achieved by issuing status reports, emails, or in-person/virtual meetings. Effective communication is crucial during all project phases.
- Final deliverables or the completion of the project, which might include **hindsight analysis** or key learnings from the project (such as what worked well, what could have been improved, or other **findings**).

The following are examples of typical IT initiatives that may require project management:

- Installation of new software (at an organizational level, not on a single user's device).
- Software upgrades, including both operating, application software, and utility software such as antivirus software.
- Hardware upgrades, such as installing new servers or network equipment.
- Moving in-house functions to a cloud or outsourced environment.
- Cybersecurity-related projects, such as launching the use of an intrusion detection/prevention system.

Control objective BAI 11 Managed Projects in the *COBIT 2019 Framework* offers more information.

IT Program Management

Program management differs from project management as it is more strategic in nature, focusing on longer-term objectives and goals versus short-term, single projects. IT program management exists to ensure that technology-based initiatives are aligned with broader organizational strategic objectives. Program management may have flexible deadlines since it often includes multiple projects with interdependent contingencies that can last several months or even years. Because IT program management is more strategic in nature, the following aspects should be considered:

- The board (or subcommittee) provides strategic direction and oversight regarding how IT program management supports organizational goals and objectives.
- IT management has identified an individual to oversee program management, with KPI-based reporting provided to the board periodically.
- Relevant stakeholders are engaged to ensure that the IT programs support organizational expectations, which may include periodic meetings and reports.

More information is available in *NIST 800-53r5*, 3.13 Program Management, and BA1 01 Managed Programs in the *COBIT 2019 Framework*.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced in this guide.

Standards and Principles
Principle 3 Demonstrate Competency
Standard 3.1 Competency
Principle 4 Exercise Due Professional Care
Standard 8.1 Board Interaction
Standard 9.1 Understanding Governance, Risk Management, and Control Processes
Standard 9.4 Internal Audit Plan
Standard 9.5 Coordination and Reliance
Principle 13 Plan Engagements Effectively
Standard 13.2 Engagement Risk Assessment
Standard 13.3 Engagement Objectives and Scope
Standard 13.4 Evaluation Criteria
Standard 13.5 Engagement Resources
Standard 13.6 Work Program
Global Guidance and Other IIA Resources
“Cybersecurity Topical Requirement and User Guide”
GTAG “Auditing Cybersecurity Operations: Prevention and Detection”
GTAG “Auditing Cyber Incident Response and Recovery”
GTAG “Auditing Identity and Access Management”
GTAG “Auditing Mobile Computing”
GTAG “Auditing Network and Communications Management”
GTAG “IT Change Management: Critical for Organizational Success”
GTAG “IT Essentials for Internal Auditors”
The IIA’s *Three Lines Model: An Update of the Three Lines of Defense*
The IIA’s *Artificial Intelligence Auditing Framework*

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 or other footnoted sources:

- IBM, https://www.ibm.com/think/topics, accessed July 23, 2025.
- ISACA, "Glossary," Information technology terms and definitions, accessed July 23, 2025. https://www.isaca.org/resources/glossary.
- Joint Task Force, *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5.* Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, "Glossary," accessed July 23, 2025. https://csrc.nist.gov/glossary.

access rights – The permission or privileges granted to users, programs, or workstations to create, change, delete, or view data and files within a system, as defined by rules established by data owners and the information security policy [ISACA Glossary].

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

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

antivirus software – An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected [ISACA Glossary].

application – A computer program or set of programs that performs the processing of records for a specific function. *Scope Notes*: Applications contrast with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort [ISACA Glossary].

artificial intelligence for IT operations (AIOps) – The application of artificial intelligence (AI) capabilities—such as natural language processing and machine learning models—to automate, streamline and optimize IT service management and operational workflows [IBM].

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.

audit log – A chronological record of system activities, including records of system accesses and operations performed in a given period [ISACA Glossary].

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

availability – Ensuring timely and reliable access to and use of information [*NIST SP 800-53r5* Glossary].

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

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

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

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

brute force attack – A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords [*NIST SP 800-72*].

chief audit executive – The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

competency – Knowledge, skills, and abilities.

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

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

control(s) – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

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

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

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

data leakage – Unauthorized transmission of data from an organization, either electronically or physically [ISACA Glossary].

directory services – A database for storing and maintaining information about users and resources. Directory Services are often referred to as directories, user stores, Identity Stores, or LDAP Directory, and they store information such as usernames, passwords, user preferences, information about devices, and more. Network and system administrators use directory services to onboard users, manage access privileges and monitor and control access to applications and infrastructure resources.[15]

encryption – The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext) [ISACA Glossary].

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

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

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

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

15. CyberArk, CyberArk Glossary, *What is Directory Services?*, accessed July 23, 2025, https://www.cyberark.com/what-is/directory-services/.

firmware – Program code embedded in hardware devices that enables them and their features to function properly [IBM].

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

hacker – An individual who attempts to gain unauthorized access to a computer system [ISACA Glossary].

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.

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

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

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

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

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.

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

operating system - The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations [*NIST SP 800-44 Version 2*].

privacy – The rights of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of his/her associated personal and sensitive information within the context and according to the purposes for which it was collected or derived [ISACA Glossary].

privileged user - Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account [ISACA Glossary].

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

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

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

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

spam – The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. [*NIST 800-53r5*].

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

user – Any person, organization or functional unit that uses the services of an information processing system [ISACA Glossary].

Appendix C. References and Additional Reading

Center for Internet Security. *CIS Critical Security Controls Version 8.1.* Accessed July 23, 2025. https://www.cisecurity.org/controls/v8-1.

CyberArk. CyberArk Glossary. *What is Directory Services?* Accessed July 23, 2025. https://www.cyberark.com/what-is/directory-services/.

IBM. Explainers. Featured topics. Accessed July 23, 2025. https://www.ibm.com/think/topics.

IBM®, "z/OS Basic Skills Information Center Mainframe concepts" © Copyright IBM Corporation 1990, 2010. https://www.ibm.com/docs/en/zos-basic-skills?topic=vmt-who-uses-mainframes-why-do-they-do-it.

ISACA. COBIT, an ISACA Framework. Accessed July 23, 2025. https://www.isaca.org/resources/cobit.

ISACA. "Glossary." Information technology terms and definitions. Accessed July 23, 2025. https://www.isaca.org/resources/glossary.

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

NIST Computer Security Resource Center. "Glossary." Accessed July 23, 2025. https://csrc.nist.gov/glossary.

NIST SP 1800-16: Securing Web Transactions: TLS Server Certificate Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf.

Appendix D. Mapping to Frameworks

Information technology governance and risk management controls related most specifically to operating system risks can be mapped to these resources.

Topic	Framework Reference
Access Management	NIST 800-53: AC-2, AC-3, AC-17, AC-19, IA-2, SC-2 COBIT 2019: DSS05, DSS06 NIST CSF: PR.AA-01, PR.AA.03, PR.AA-01 CIS 8.1: Control 3, Control 5, Control 6
Change Management	NIST 800:53: CM-9, SA-10, SA-11 COBIT 2019: DSS03, BAI07 CIS 8.1: Control 5, Control 16
Common Secure Configuration	NIST 800:53: 3.5, CM-2, CM-5, CM-6, CM-9, SA-5, SA-10 COBIT 2019: BAI03, BAI10 NIST CSF: PR.PS-01, PR.PS-02 CIS 8.1: Control 4
Cybersecurity and Incident Response	NIST 800:53: IR-4, SI-4, SI-5 COBIT 2019: DSS05, DSS06 NIST CSF: Entire Framework CIS 8.1: Control 3, Control 7, Control 9, Control 10, Control 13, Control 14, Control 17
Data Centers	NIST 800-53: CP-9, PE-3, PE-6, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15
Data Storage	NIST 800:53: AC-23, SA-9 COBIT 2019: AP014, DSS01, DSS05 CIS 8.1: Control 3, Control 11
Directory Services	NIST 800:53: CM-6 COBIT 2019: DSS05 CIS 8.1: Control 5, Control 6
Disaster Recovery	NIST 800:53: 3.6, 3.8, CP-2, CP-6, CP-8, IR-3, SR-3 COBIT 2019: APO14, BAI03, BAI06, DSS01, DSS04 NIST CSF: RC-RP, RC.CO CIS 8.1: Control 11, Control 17
End-User Devices	NIST 800:53: AC-11, AC-17, AC-19, CA-9, IA-3, IA-6, SI-8, SC-8 COBIT 2019: DSS05 CIS 8.1: Control 1, Control 3, Control 4, Control 9, Control 10, Control 12, Control 14

Topic	Framework Reference
File Sharing	NIST 800:53: CM-10 CIS 8.1: Control 3, Control 4
Mobile Devices	NIST 800-53: AC-7, AC-11, AC-17, AC-19, CA-9, CM-6, IA-3, IA-6, SI-8, SC-8, SC-43 COBIT 2019: DSS05 CIS 8.1: Control 1, Control 3, Control 4, Control 9, Control 10, Control 12, Control 14
Network Devices	NIST 800:53: AC-3, AC-6, CP-10, IR-4, RA-5, SC-7, SC-28, SI-4, SR-12 COBIT 2019: BAI09, DSS05 NIST CSF: ID.AM-03, PR.IR-01, DE.CM-01 CIS 8.1: Control 1, Control 12, Control 13
Operating Systems and Applications	NIST 800:53: AC-6, AC-7, AC-11, AC-19, AC-25, AU-9, CA-8, CM-2, CP-9, SA-8, SA-11, SC-2, SC-27, SC-29, SI-3, SI-7 COBIT 2019: DSS05 NIST CSF: PR.PS-02, PR.PS-05, PR.PS-06, ID.AM-02, ID.AM-05, ID.AM-08 CIS 8.1: Control 2, Control 4, Control 16
Patch Management	NIST 800:53: CM-2, CM-11, CM-14, IA-3, MA-3, PL-2, RA-5, SA-17, SI-2 CIS 8.1: Control 1, Control 2, Control 4, Control 7, Control 9, Control 12
Peripherals	NIST 800:53: AC-3, AC-16, CA-9, MA-2, MP-6, PE-3, PE-5, PE-22, RA-5, SC-7, SC-8, SC-43 COBIT 2019: BAI09, DSS05 CIS 8.1: Control 1, Control 12, Control 13
Privileged Access	NIST 800:53: AC-2, AC-3, AC-6, AC-17, AU-9, IA-2, MA-5, RA-5, SC-2, SC-7 COBIT 2019: DSS05, DSS06 NIST CSF: PR.AA-05 CIS 8.1: Control 5, Control 6
Program Management	NIST 800:53: 3.13 COBIT 2019: BAI01
Project Management	COBIT 2019: BAI11
Servers	NIST 800:53: AC-4, AC-17, AC-20, AU-9, CA-9, CM-2, CM-6, CP-3, CP-9, PE-3, PE-6, SC-2, SC-7, SC-28, SI-4, SI-8, SR-12 COBIT 2019: BAI09, DSS05 NIST CSF: ID.RA-09 CIS 8.1: Control 1, Control 2, Control 3, Control 4, Control 8, Control 9
Virtualization	NIST 800:53: SC-2, SC-7, SC-29, SC-30, SC-34, SC-35, SC-39, SI-14 CIS 8.1: Control 1, Control 4, Control 8, Control 12
Vulnerability Management	NIST 800:53: CA-8, RA-5, SA-11, SI-2 COBIT 2019: MEA02 NIST CSF: ID.RA-01, ID.RA-08 CIS 8.1: Control 7, Control 16, Control 18

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 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

July 2025

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