IPPF

International Professional Practices Framework

Supplemental Guidance

GTAG®

Global Technology Audit Guide

Auditing Identity and Access Management

2nd Edition

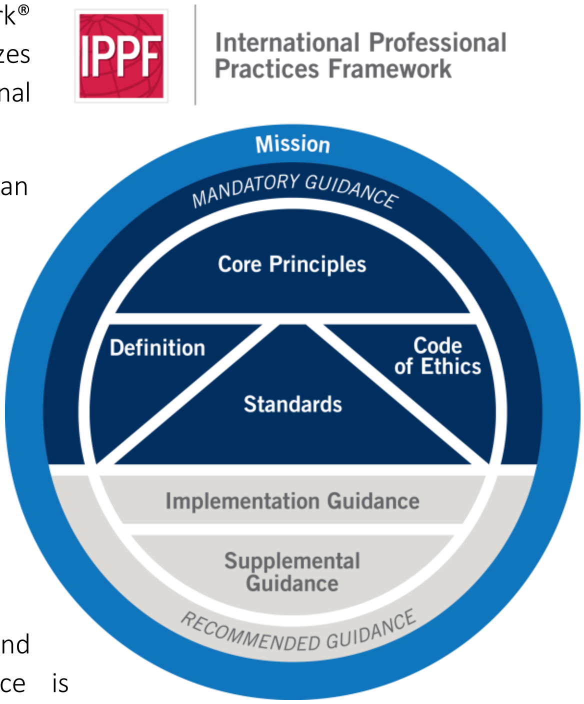
The Institute of Internal Auditors® | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.

Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.



Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

About GTAGs

Within the IPPF's Supplemental Guidance, Global Technology Audit Guides (GTAGs) provide auditors with the knowledge to perform assurance and advisory services related to an organization's information technology (IT) and information security (IS) risks and controls. The standards that give rise to the GTAGs are listed below.

- 1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.
- 2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- 2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives.
    - Reliability and integrity of financial and operational information.
    - Effectiveness and efficiency of operations and programs.
    - Safeguarding of assets.
    - Compliance with laws, regulations, policies, procedures, and contracts.
- 2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Table of Contents

Executive Summary

Identity and access management (IAM) covers the policies, processes, and tools for ensuring users have appropriate access to information technology (IT) resources. IAM controls are necessary wherever the use of hardware or software requires differentiated permissions or the ability to track actions taken. IAM processes may require coordination between personnel and systems in human resources, other business units, and IT.

Fundamentally, IAM consists of three **control** objectives:

1. *Identity – Who are you?* 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.
2. *Authorization – What can you do in this system?* This objective requires coordination between **system administrators** (usually in IT), the primary benefitting 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.
3. *Authentication – Are you who you 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 you know (like a password), something you have (like a mobile phone), or something you are (biometric data, such as a fingerprint).

Other significant control objectives related to IAM include, but are not limited to:

4. **Risk management** – *Are deployed IAM solutions commensurate with each system's criticality?*
5. **Event logging** – *Are the systems logging security events, such as account activation or deactivation, login attempts, and permission changes?*
6. **Log monitoring** – *Are the security event logs secured and monitored to detect anomalous activity?*

Note: While managing physical access is a key objective, this Guide will focus on **user** access to technology resources and information, sometimes referred to as logical access. For purposes of this Guide, "access" will be synonymous with logical access for users.

Stakeholders such as senior management and the **board** require **assurance** that **information technology controls**, including managing access to IT resources, are well designed and effectively implemented.

Introduction

Note: Appendix A lists other IIA resources that are relevant to this Guide. Terms in bold are defined in Appendix B.

There are many widely used frameworks that provide descriptions of IAM controls, including COBIT 2019 from ISACA, special publications from the National Institute of Standards and Technology (NIST), and the "Center for Internet Security Top 20 Controls & Resources" for cybersecurity, among others. This guide will reference some of the controls described in these frameworks to help readers grasp the concepts, but it will not reproduce the entirety of all control and subcontrol descriptions. Readers of this guide are assumed to have a general knowledge of IT and information security (IS) **risks** and controls, as described in the Global Technology Audit Guide (GTAG) "IT Essentials for Internal Auditors," and are encouraged to incorporate a review of the full texts of one or more IT-IS control frameworks in their audit planning and test programs.

IAM processes establish user IDs and related IT resource permissions and verify that requests for access to and actions within a system are made by the account owner and not an impostor. IDs may be created for employees, contractors, vendor personnel, customers, machinery, and programs – basically any entity that needs access to a system to perform a business function. The means by which the organization facilitates user access, yet restricts it to only what is necessary to perform authorized functions, forms the foundation of IAM.

Types of IDs

IAM control concepts are applicable to accounts used by humans, as well as programmed functions or services that may be assigned a **mechanized ID** (mech ID) to access IT resources. In this guide, the term ID applies to all kinds of IDs, unless otherwise noted.

Identity and access management controls are so fundamental to **IT governance** and the achievement of the organization's IT-IS strategies and objectives that the internal audit activity must examine how organizations control access, understanding that processes may be applied enterprisewide or be specific to a particular resource or environment. Not all IT resources require the same level of protection, so IAM controls are ideally designed to be commensurate with each system's **security category**, as well as relevant risks of **fraud** or regulatory **compliance**.

IAM controls are implemented in every layer of IT resources, including network infrastructure equipment (e.g., switches, routers, and network management systems), servers, databases, **middleware** services, and **applications**. Organizations of all sizes face IAM challenges, largely due to the proliferation and variety of IT resources and access methodologies. To design, implement, and execute effective IAM controls, system administrators, business units, and end users must coordinate and adhere to the **least privilege** principle, which states that system access is limited to only what is necessary to perform authorized business functions.

To start assessments of IAM controls, internal auditors usually identify the particular IT resources or the layer or group of resources to be examined, then develop an understanding of the business context for the assets. A risk assessment may then be performed on the in-scope systems to further refine the engagement work program. During planning and fieldwork, internal auditors may advise on how the organization can increase the effectiveness of IAM controls, thereby reducing security and regulatory risks. Following this approach, an internal auditor will demonstrate adherence to **Standard** 1220 – Due Professional Care.

Standard 1220 – Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

Objectives

This guide will help the reader:

- Define IAM and develop a working knowledge of relevant processes, including related **governance** and security controls.
- Understand risks and opportunities associated with IAM.
- Understand components of the IAM process, including provisioning IDs, administering and authorizing access rights, and maintaining enforcement through authentication, reauthorization reviews, and automated account deactivation processes.
- Understand some considerations and strategies for implementing IAM controls.
- Understand the basics of auditing IAM, including specific controls to be evaluated.

IAM Components

This section will provide brief descriptions of controls over identity, authorization, and authentication, with references to IAM control frameworks where appropriate. More thorough definitions of the controls are available in the source documents.

Identity

One of the better documents for understanding risks and control objectives relating to the establishment of system IDs is the *NIST Special Publication (SP) 800-63 Digital Identity Guidelines* (PDF). That document states "[a] digital identity is the unique representation of a subject," and "[t]he processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks."[1] Thus, the creation, management, and security of IDs are key control objectives for every IT resource that requires differentiated permissions.

The group of documents associated with *NIST SP 800-63* recognizes that not all system IDs may need to be traceable to a verified individual. However, for most IAM engagements, a risk-based scoping will focus on processes and controls that require verified individual IDs or mechanized IDs with documented owners to ensure accountability for actions taken within the system.

System architects determine the types of IDs necessary for each IT resource to fulfill its business purposes, while administrators create and manage system IDs according to the defined needs. System administrators typically work with the resource's business owners to implement processes that document individual identities or individuals responsible for mechanized IDs.

Network Identity

In an enterprise IT environment, the establishment of network IDs, which are required to access the organization's data network, is a fundamental control, typically executed for individuals during an onboarding process. Network administrators may also create mechanized IDs or special purpose IDs (e.g., administrator IDs to be used only when an individual is performing authorized administrator functions).

The network ID is often also used by applications running on the data network in a process known as **federation** (sometimes referred to as single sign-on), which allows the application to rely on the controls implemented to create and manage network IDs. Business applications that do not require an end user who is logged in to the entity's data network to also enter **credentials** to log in to the application — or that request the user's network ID and password to log in — are federated with the network ID and authentication processes to some extent.

Federation of IDs is especially helpful for automating the activation and deactivation of user accounts, since the network ID is usually associated with the human resources database of verified identities (employees and contractors) and their current status. For example, once an employee or contractor is officially terminated — and their employment status is changed in the database to inactive — the network ID status would also become inactive, and the state of the ID would immediately be inactive for all federated applications.

Device- or Application-specific Identity

IT resources that are not federated with the network ID will require the establishment of user IDs that usually have the same risks and control objectives as the network ID. Essentially, if accountability for actions performed in the system is a control objective, then unique, nonshared IDs must be created and associated with or owned by verified individuals. Nonfederated systems

[1] Paul Grassi, Michael Garcia, James Fenton, *NIST SP 800-63-3 Digital Identity Guidelines*,"NIST, iv, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

require an end user to log in with an ID and password that are not tied to the network ID. Cloud-based applications may be federated or not.

Nonfederated applications have inherently riskier IAM controls than federated ones because system administrators and end-user supervisors typically do not verify or manage IDs as robustly as human resources processes do. Additionally, user metadata — such as employment status and current job function — require manual updates in a nonfederated system. When auditing IAM for nonfederated devices or applications, auditors evaluate the strength of the processes used to verify individual identities associated with each system ID (including mechanized IDs) and examine whether processes to verify the current status of employee and nonemployee users are adequate.

Approval and Validation

Identity requests are typically subject to an approval and validation process, called "proofing" in *NIST SP 800-63.*[2] The ID request is approved by the requestor's supervisor or designated responsible employee. Adherence to the established proofing requirements may be validated either automatically — such as upon successful completion of an I-9 employment eligibility verification[3] to validate an individual's identity — or manually by someone other than the requestor's supervisor, to ensure adequate **separation of duties**.

Authorization

The processes for determining which systems an ID can access and what permissions the ID has in each system are known as authorization. Authorization processes are determined by **business rules** and may be automated in the onboarding process or require some degree of manual intervention. For instance, giving every human-associated network ID an email account during onboarding is an example of an automated authorization process. The *COBIT 2019 Framework: Governance and Management Objectives* describes authorization activities under DSS06.03 – Manage Roles, Responsibilities, Access Privileges, and Levels of Authority.

Determining a User's Applications

Individuals typically need access to one or more business applications to perform their job duties, so a process is needed to determine which applications are needed by each person. In a simple, primarily manual process, the person's supervisor is usually responsible for determining the necessary applications and approving the initial access requests. More generally, the applications needed for each job are documented, and if any of the applications are federated with the network ID, setting up new users with the applications can be automated.

[2] Grassi, Garcia, and Fenton, *NIST SP 800-63-3*, iv.

[3] "I-9, Employment Eligibility Verification," U.S. Citizenship and Immigration Services, accessed January-February 2021, https://www.uscis.gov/i-9.

Defining System Roles

An IT resource's business owner works with system administrators to establish permissions that correlate to the needs of job functions or titles. For example, designated personnel from the customer care department work with the administrators of the customer relationship management system to establish roles within that system that match the needs of customer service representatives, team leads, managers, and directors, with escalating privileges corresponding to the organizational hierarchy. Many systems, such as enterprise resource platforms, may have a default set of standardized roles based on common business practices.

Defining **superusers**, **database administrators**, and other administrative or privileged roles may require dual authorization — for example, from both the business owner and system administrator. Requiring dual authorization prohibits the system administrator from creating a new role unilaterally and requires approval for each role to come from the business owner or the administrator's supervisor. System roles, their related permissions, and their associated job functions or titles may be documented to formalize the agreement between the business owner and system administrator and to assist account provisioning processes, including automation.

Note: Applications that do not use system roles, requiring permissions to be granted manually to each account, are inherently riskier due to the possibility of errors or intentional overgranting of privileges.

An additional step often taken when defining system roles is for the business owner to identify permissions that would represent an insufficient separation of duties, such as the ability to submit and approve one's own purchase requisition or timecard.

Many applications, databases, and tools require the use of mechanized IDs to perform specific tasks or communicate with different system components. For example, a database management system may require the server on which it is hosted to have specific accounts created and active for the database system to operate. Therefore, the business owner or administrator's supervisor should document and approve system roles created for mechanized IDs.

Assigning System Roles

One common approach to providing users with access is called **role-based access control**, where subject matter experts determine which applications and system roles are needed for each job title or function in their organization, then work with network and system administrators to implement a provisioning process, which can be manual or automated to some extent. Alternatively, access provisioning can be manually determined on an individual basis if there are variations in access needs among members of the same job function.

Some system role requests, especially ones with relatively elevated permissions, may require dual authorization, where a supervisor and the designated business owner both need to approve user access to the role.

Controls to prevent separation of duty violations are implemented at the ID level to ensure a user does not have overly broad permissions. Checking for separation-of-duties violations may be automated or performed manually by designated business owners.

Privileged Account Management

Accounts with administrator privileges, such as the ability to create new roles or accounts or modify permissions of existing accounts, are normally assigned to designated IT personnel or non-IT superusers. Often, a **privileged user** is given a separate ID to be used solely for administrative functions. Privileged accounts are the prime target of cybercriminals because of their ability to create IDs and system accounts, elevate privileges, and access databases. To prevent inappropriate creation of or access to these privileged accounts, many organizations implement a privileged account management tool to facilitate provisioning, administration, monitoring, and enforcement.

Reauthorization Processes

Periodically, supervisors may be required to reauthorize the system access of their direct reports to mitigate the risk of unnecessary permissions. The frequency of reauthorization should be commensurate with the system's data classification, which means more sensitive systems should have their user accounts reauthorized more frequently. System administrators are generally expected to design and implement a process that provides the users' supervisors with enough information to make an informed reauthorization decision. Such information may include descriptions of the applications, roles associated with the user, and the job titles that are expected to receive each role.

When individuals change job functions, their system access requirements often change as well, so a best practice is to have a process in place for the former supervisor to deactivate unneeded access and the new supervisor to approve access for the new role. Ideally, this process is automated by integrating IAM tools with the human resources system and using role-based access control as much as possible. However, even without integration or facilitating tools, the least privilege principle should still be enforced.

An organization may employ one or more IAM tools to facilitate or automate reauthorization processes, though applications not integrated with the tools may require a manual reauthorization approach. Audits of IAM controls typically verify whether accounts not approved for reauthorization were deactivated. Additionally, auditors may look for job title or department anomalies in user account and system role lists to address the risk of supervisors reauthorizing users automatically without due consideration. Such a review might require comparing the user access list to data from human resources.

One benefit of automated IAM processes is that integrated applications inherit the strength of the controls (known as **control inheritance**), so if the automated process has been audited and found to be compliant with the organization’s policies and procedures, then it may not be necessary to retest that process when a federated resource is audited.

Account Deactivation

Sometimes it is necessary for a user account to be deactivated due to employment termination, a change in job function, or a period of inactivity. Rules for deactivating idle accounts should be commensurate with the system’s data classification. Where appropriate, system administrators set control parameters to automatically deactivate accounts that have not been accessed within a specified period. If necessary, users can request that their accounts be reactivated, subject to their supervisor’s approval.

Federated applications can inherit or receive automatic notifications of changes in an ID’s status, while nonfederated applications must rely on manual processes, which are inherently slower and riskier.

Authentication

Controls that verify an access request is coming from the entity authorized to use an account are called authentication. Passwords are an authentication factor that most people are familiar with, and while there are guidelines for enhancing the security that passwords provide, their shortcomings are also widely known. The design of adequate authentication controls is described at length in *NIST SP 800-53 Revision 5* (PDF), in the section on identification and authentication.

Authentication Factors

As stated previously, authentication factors are often defined as something you know (like a password), something you have (like a mobile phone), or something you are (biometric data, like a fingerprint). System architects and administrators determine authentication methods commensurate with the resource’s data classification and technical capabilities. Some lower-risk systems may rely solely on network authentication, inheriting the strength of network access controls, while higher-risk resources or processes — databases with personally identifiable information or system administrator functions, for instance — may require additional authentication steps to access.

Multi-factor authentication processes require an ID to provide more than one type of authentication. For instance, after verifying an ID and password, a system may send a temporary access code to a user’s registered email account or mobile phone that the user is required to enter before being granted access to the system. Frequently, system administrators integrate commercial, off-the-shelf tools to provide multi-factor authentication services. The organization’s data classification and related data protection policies ideally establish criteria for when multi-factor authentication is required and what methods are acceptable.

Password Controls

In most commercial, off-the-shelf applications, controls to enhance the security of passwords include:

- *Length* – The organization defines a minimum number of characters for passwords; many suggest using a passphrase to make it more memorable.
- *Complexity* – The use of lowercase and uppercase letters, numbers, and symbols (!, #, $, *, etc.) increases the set of possible values, thereby making the password harder to crack.
- *Expiry and reuse* – Passwords expire after a set amount of time, according to the resource's data classification, and are sufficiently different than some number of previous passwords to reduce the risk of compromised credentials.
- *Lockout* – IDs can be temporarily locked out of a system if there are more than a specified number of unsuccessful login attempts within a certain time period. This control mitigates the risk of password cracking attempts.
- *Storage and access* – Passwords are stored in encrypted files that administrators are only able to reset, not decrypt.

Since users may have dozens of frequently expiring passwords, credential maintenance can become a challenge, so the organization may have a tool for secure password storage and retrieval by the user, or a policy regarding the use of external password management tools.

Physical Factors

In multi-factor authentication, physical factors — something a user has — are often used in addition to passwords to provide an extra degree of security. Device identifiers, like a media access code, may be registered so that a user can only log in to an account on a particular machine, or a software token may be installed to allow an authentication service to uniquely identify the device. Users may also carry a separate device, like a physical token that is synchronized with a central code generator or a cell phone with a number that has previously been registered by the user.

Digital certificates are a quasi-physical factor used by automated services or programs in a public key infrastructure authentication methodology, in the sense that a digital certificate is something that the program has. The validity of a digital certificate must be verified with a trusted issuer or verification service.

Biometrics

A special type of physical factor is data derived from a person's unique physical characteristics, like the pattern of a fingerprint, retina, or voice. These factors must be registered with a verification service, which may be on a device, as in the case of a fingerprint scanner on a cell phone or laptop computer.

Related Risk and Control Groups

Some of the IT-IS control objectives most closely related to IAM risks are briefly discussed below.

Risk Management

There are potentially significant impacts from inadequate IAM controls from insiders, hackers, and automated "bots" attempting to gain access to IT resources. The organization's risk management processes ideally identify high-risk systems and data as part of a data classification and protection program and determine necessary safeguards — like role-based access control, multi-factor authentication, or privileged account management — for each category. The risk assessment process should identify areas where IAM solutions are insufficiently secure and document remediation plans or management's justification for accepting the risk.

Event Logging

It is a best practice to log security-related events that include attempts to access resources, the creation of IDs and system accounts, escalation of roles or privileges, and other system administrator activities. Logs of such events typically contain enough information to establish accountability and **nonrepudiation**, which facilitates monitoring and forensic processes.

Log Monitoring

Proactive monitoring of security event logs may be able to detect insider or external threats attempting to access IT resources. Indicators may include repeated unsuccessful login attempts, self-authorized ID creation or privilege escalation, or repeated activation and deactivation of accounts. Log monitoring controls are typically implemented by the information security organization. During planning of an IAM audit, internal auditors may identify whether log monitoring controls are in place for all high-risk systems and whether the controls are designed to detect likely IAM risk patterns.

Conclusion

IAM controls safeguard the confidentiality and integrity of systems and data by restricting users to only the rights needed to fulfill authorized actions. System architects and administrators are responsible for planning and implementing IAM controls that are strong enough to meet the security needs of each system. User IDs and their related system permissions are reviewed periodically, and processes automated where feasible, to ensure that privileges remain aligned with the users' current needs. Logging and monitoring IAM events and unsuccessful access attempts may enable security engineers to detect cyberattacks or insider threats.

Appendix A. Related IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency

Standards
Standard 1210 – Proficiency
Standard 1220 – Due Professional Care
Standard 2110 – Governance
Standard 2130 – Control
Standard 2220 – Engagement Scope

Guidance
"GTAG: IT Essentials for Internal Auditors," 2020

Appendix B. Glossary

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

- Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *NIST SP 800-63-3: Digital Identity Guidelines*, Glossary (Gaithersburg, MD: NIST, June 2017), https://doi.org/10.6028/NIST.SP.800-63-3.
- ISACA, Glossary, information technology terms, and definitions, accessed March 15, 2021, https://www.isaca.org/resources/glossary.
- Joint Task Force, *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations*, *Revision 5*, Glossary (Gaithersburg, MD: NIST, September 2020), https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, Glossary, accessed April 8, 2021, 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].

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

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

authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system [*NIST SP 800-53, Revision 5*, Glossary].

authorization – Access privileges granted to a user, program, or process or the act of granting those privileges [*NIST SP 800-53, Revision 5*, Glossary].

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

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

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

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

control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient action to provide reasonable assurance that objectives and goals will be achieved.

control inheritance – A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [*NIST SP 800-53, Revision 5*, Glossary].

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

database administrator – An individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition, and maintenance of the database [ISACA Glossary].

event logging – Chronologically recording system activities, like access attempts, role creation, user account creation or deactivation, etc. (see "audit log" in *NIST SP 800-53, Rev. 5*).

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

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

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

identity (or identifier) – A unique label used by a system to indicate a specific entity, object, or group [*NIST SP 800-53, Revision 5*, Glossary].

information technology controls* – Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

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

least privilege – The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function [*NIST SP 800-53, Revision 5*, Glossary].

log monitoring – Using specialized software to scan event logs for patterns or anomalies that may indicate unauthorized accounts, access, or activities.

mechanized ID – A system ID created for automated programs or services. A mechanized ID or "mech ID" should have a person identified as responsible for its configuration and operation.

middleware – Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services [ISACA Glossary].

multi-factor authentication – An authentication system that requires more than one authentication factor for successful authentication. The three authentication factors are something you know, something you have, and something you are [*NIST SP 800-53, Revision 5*, Glossary].

nonrepudiation – Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message [*NIST SP 800-53, Revision 5*, Glossary].

privileged user – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform [*NIST SP 800-53, Revision 5*, Glossary].

risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

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

role-based access control – Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals [*NIST SP 800-53, Revision 5*, Glossary].

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

segregation/separation of duties – A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets [ISACA Glossary].

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

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

superuser – A type of system administrator role that has all permissions, including root access to the operating system.

system administrators – Personnel authorized to configure and support the operation of an IT resource.

system architects – Personnel responsible for designing or approving systems that meet internal requirements and integrate with current or planned infrastructure.

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

Appendix C. References

Center for Internet Security. "The 20 CIS Controls & Resources." Interactive guide to CIS controls. Version 7.1. Accessed May 3, 2021, https://www.cisecurity.org/controls/cis-controls-list/.

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

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

ISACA. Glossary. Information technology terms and definitions. Accessed May 3, 2021, https://www.isaca.org/resources/glossary.

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

NIST Computer Security Resource Center. Glossary. Accessed May 3, 2021, https://csrc.nist.gov/glossary.

Acknowledgements

IT Guidance Development Team

Susan Haseley, CIA, United States (Chairman)
Terence Washington, CIA, CRMA United States (Project Lead)
Brad Ames, CISA, CPA, United States
Anand Balakrishnan, CIA, United States
Ruth Mueni Kioko, CIA, Kenya
Sajay Rai, CISM, CISSP, CPA, United States

IIA Global Standards and Professional Practices

David Petrisky, CIA, CRMA, CISA, CPA, Director (Project Lead)
Jim Pelletier, CIA, CGAP, Vice President
Harold Silverman, CIA, QIAL, CRMA, Managing Director
Anne Mercer, CIA, CFSA, CFE, Director
Pam Stroebel Powers, CIA, CRMA, Director
Daniel Walker, CIA, CISA, CISSP, CPA, Director
Tammy Wyche, Director
Shelli Browning, Manager
Logan Wamsley, Manager
Lauressa Nelson, Senior Editor
Christine Janesko, Content Writer and Technical Editor

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

About The IIA

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

Disclaimer

The IIA publishes this document for informational and educational purposes and, as such, is only intended to be used as a guide. This guidance material is not intended to provide definitive answers to specific individual circumstances. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

First edition published 2009
Second edition June 2021

The Institute of Internal Auditors | Global

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
www.theiia.org