# Auditing Identity and Access Management

## 2nd Edition

### Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

# 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

## Global Guidance Council Reviewers

Gally Amazan, Haiti

Lesedi Lesetedi, CIA, QIAL, CRMA, Botswana

## International Internal Audit Standards Board Reviewers

Jessica Echenique, CIA, United States

Maciej Piołunowicz, CIA, Poland

## IIA Global Standards and Guidance

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

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

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

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

The IIA 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


International Professional Practices Framework® (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** ..... **1**

**Introduction** ..... **2**

Objectives ..... 3

**IAM Components** ..... **4**

Identity ..... 4

Authorization ..... 5

Authentication ..... 8

**Related Risk and Control Groups** ..... **10**

Risk Management ..... 10

**Conclusion** ..... **11**

**Appendix A. Relevant IIA Standards and Guidance** ..... **12**

**Appendix B. Glossary** ..... **13**

**Appendix C. References** ..... **17**

# 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 cross-functional 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 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.
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:

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

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

### Note

While managing physical access is an 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.

# Introduction

There are many widely used frameworks that provide descriptions of **identity and access management (IAM)** controls, including *COBIT 2019 Framework: Governance and Management Objectives* (*COBIT 2019*) from ISACA, special publications and the *Cybersecurity Framework 2.0* (*NIST CSF*) from the National Institute of Standards and Technology (NIST), and the *CIS Critical Security Controls Version 8.1* (*CIS Controls v8.1*) among others. This guide references some of the **controls** described in these frameworks to help readers grasp the concepts, but it does not reproduce the entirety of all control and subcontrol descriptions. References to applicable Global Internal Audit Standards appear throughout this guide.

Readers of this guide are assumed to have a general knowledge of IT and information security (IS) **risks** and controls (Standards 3.1 Competency and 13.5 Engagement Resources), 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 when establishing the internal audit plan and **engagement work program**. (Standards 4.2 Due Professional Care, 9.4 Internal Audit Plan, and 13.6 Work Program).

### 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.

IAM processes establish **user** identities (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 — 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. This approach to granting necessary user access to perform authorized business functions is also commonly called **least privilege**. (*COBIT 2019*, DSS05.04; *NIST CSF*, PR.AA-05).

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 function** must examine how organizations control access, understanding that processes may be applied enterprisewide or be specific to a particular resource or environment (Standard 9.1

Understanding Governance, Risk Management, and Control Processes). 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 (for example, 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 methods. **System administrators**, business units, and end users must coordinate and adhere to the least privilege principle to design, implement, and execute effective IAM controls.

### 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 or "mech ID," which is a system ID created for automated programs or services. A mech ID should have a person identified as responsible for its configuration and operation to access IT resources. In this guide, the term ID applies to all kinds of IDs, unless otherwise noted.

To start assessments of IAM controls, internal auditors usually identify the particular IT resources or the layer or group of resources to be examined (Standard 13.3 Engagement Objectives and Scope) and then develop an understanding of the business context for the assets. During **engagement planning**, internal auditors must understand the in-scope systems and identify and assess the risks to review (Standard 13.2 Engagement Risk Assessment). Engagement planning also includes establishing and documenting the evaluation criteria, resources, and work program (Standards 13.4 Evaluation Criteria, 13.5 Engagement Resources, and 13.6 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 (Standard 13.1 Engagement Communication). At the end of the **engagement**, internal auditors must report findings, a conclusion, and recommendations and/or actions agreed upon with management (Standards 11.3 Communicating Results, 14.4 Recommendations and Actions Plans, and 15.1 Final Engagement Communication).

## 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 provides 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 *NIST Special Publication (SP) 800-63-3 Digital Identity Guidelines* (*NIST SP 800-63-3*). The 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 800-63-3* recognizes that not all system IDs may need to be traceable to a verified individual. However, for most IAM engagements, 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 are the personnel responsible for designing or approving systems that meet internal requirements and integrate with current or planned infrastructure. They determine the types of IDs necessary for each IT resource to fulfill its business purposes. System administrators create and manage system IDs according to the defined needs, typically working 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, establishing 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 (for example, 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**

1. NIST, NIST SP 800-63-3, iv.

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 also becomes inactive, and the state of the ID is immediately inactive for all federated applications.

### *Device or Application-specific Identity*

IT resources that are not federated with the network ID 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 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 the 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 800-63-3*.[2] The ID request is approved by the requestor's supervisor or a 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 to validate an individual's identity, or manually by someone other than the requestor's supervisor, to ensure adequate **separation of duties**.[3]

## 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 example, giving every human-associated network ID an email account during onboarding is an example of an automated authorization process. The *COBIT 2019* describes authorization activities under "DSS06.03 – Manage Roles, Responsibilities, Access Privileges, and Levels of Authority."

2. NIST, *SP 800-63-3,* iv.
3. U.S. Citizenship and Immigration Services, "I-9, Employment Eligibility Verification."

### *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 each person needs. 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.

### *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 (*COBIT 2019*, DSS06.03). 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 that business owner or the administrator's supervisor to approve each role. System roles, related permissions, and associated job functions or titles should 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 systems 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. "Control 6 Access Control Management, Safeguard 6.8: Define and Maintain Role-Based Access Control" from the *CIS Controls v8.1* provides additional information. 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. "Control 5 Account Management, Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts" from the *CIS Controls v8.1* provides additional information. 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. "Control 6 Access Control Management, Safeguard 6.2: Establish an Access Revoking Process" from the *CIS Controls v8.1* provides additional information. 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 lists of user accounts and system roles 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. System administrators set control parameters where appropriate to automatically deactivate accounts that have not been accessed within a specified period. "Control 5 Account Management, Safeguard 5.3: Disable Dormant Accounts" from the *CIS Controls v8.1* provides additional information. If necessary, users can request that their accounts be reactivated, subject to their supervisor's approval.

## Authentication

Controls that verify an access request is coming from the entity authorized to use an account are called authentication (*NIST CSF*, PR.AA-03; *COBIT 2019*, DSS05.04). 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 Special Publication (SP) 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53r5)* 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 (MFA)** 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 must enter before being granted access to the system. Frequently, system administrators integrate commercial, off-the-shelf tools to provide MFA 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. "Control 6 Access Control Management," Safeguards 6.3: Require MFA for Externally-exposed Applications, 6.4: Require MFA for Remote Network Access, and 6.5: Require MFA for Administrative Access from the *CIS Controls v8.1* provide additional information.

### *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 – Using lowercase and uppercase letters, numbers, and symbols (such as !, #, $, and *) increases the set of possible values, thereby making the password harder for an unauthorized user to discern.
- Expiration and reuse – Passwords expire after a set amount of time, according to the resource's data classification, and are sufficiently different from 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 period. This control mitigates the risk of password-cracking attempts.
- Storage and access – Passwords are stored in encrypted files that administrators can only reset, not decrypt.

Since users may have numerous 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. Control 5 Account Management, Safeguard 5.2: Use Unique Passwords from the *CIS Controls v8.1* provides additional information.

### *Physical Factors*

In MFA, using physical factors — something a user has — in addition to passwords provides 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. **Facial recognition technology** is an example of a biometric that is commonly utilized to verify users when attempting to unlock mobile devices. **Computer vision** is a form of **artificial intelligence** that is utilized for facial recognition in deciphering visual information.

# Related Risk and Control Groups

This section briefly covers some of the IT-IS control objectives most closely related to IAM risks.

## 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, referred to as **event logging**, including 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 enable the detection of 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. When planning an IAM engagement, 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. Control 8 Audit Log Management from the *CIS Controls v8.1* provides additional information.

# 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 related system permissions are reviewed periodically and processes are 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. Relevant IIA Standards and Guidance

The following IIA resources were referenced in this guide.

| Standards |
| --- |
| Standard 3.1 Competency |
| Standard 4.2 Due Professional Care |
| Standard 9.1 Understanding Governance, Risk Management, and Control Processes |
| Standard 9.4 Internal Audit Plan |
| Standard 11.3 Communicating Results |
| Standard 13.1 Engagement Communication |
| 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 Engagement Work Program |
| Standard 14.4 Recommendations and Action Plans |
| Standard 15.1 Final Engagement Communications |
| **Global Guidance** |
| GTAG “IT Essentials for Internal Auditors” |

# Appendix B. Glossary

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

- ISACA, Glossary. https://www.isaca.org/resources/glossary.
- IBM, "What are business rules?" https://www.ibm.com/topics/business-rules.
- Microsoft, "Event logging," January 7, 2021. https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging.
- NIST, Computer Security Resource Center (CSRC), Glossary. https://csrc.nist.gov/glossary.
- NIST, *NIST SP 800-53r5: Security and Privacy Controls for Information Systems and Organizations*, Appendix A: Glossary. Sept. 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
- United States Department of Homeland Security, "Highlight," April 2009. https://www.dhs.gov/publication/facial-recognition-technology.

**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].

**artificial intelligence –** An advanced computer system that can simulate human capabilities, such as analysis, based on a predetermined set of rules [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].

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

**biometric data –** Biological attribute of an individual from which distinctive and repeatable values can be extracted for the purpose of automated recognition. Fingerprint ridge structure and face topography are examples of biometric characteristics [NIST CSRC, Glossary].

**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 800-53r5*, Glossary].

**business rules** – Business rules guide the everyday decision-making within businesses by outlining the relationships between objects, such as customer names and their corresponding orders. Business rules provide the foundation for automation systems by taking documented or undocumented information and translating it into various conditional

statements. Business rules are used for a variety of use cases, which can be based on either internal or external constraints [IBM, "What are business rules?"].

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

**computer vision** – A subfield of artificial intelligence (AI) concerned with enabling computers to interpret and understand visual information such as images and videos [ISACA Glossary].

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

**control 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 800-53r5*, 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 800-53r5*, 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].

**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."

**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.

**engagement work program** – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors assigned to perform the tasks. The work program is based on information obtained during engagement planning.

**event logging** – Event logging provides a standard, centralized way for applications (and the operating system) to record important software and hardware events. The event logging service records events from various sources and stores them in a single collection called an event log [Microsoft, "Event logging"].

**facial recognition technology** – A contemporary security solution that automatically identifies and verifies the identity of an individual from a digital image or video frame. This technology can be compared to other biometric technologies and used for a number of activities [adapted from the United States DHS, "Highlight"].

**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 intentional act characterized by deceit, concealment, dishonesty, misappropriation of assets or information, forgery, or violation of trust perpetrated by individuals or organizations to secure unjust or illegal personal or business advantage.

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

**identity (or identifier)** – A unique label used by a system to indicate a specific entity, object, or group [*NIST SP 800-53r5*, Glossary].

**identity and access management (IAM)** – Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users [NIST CSRC, 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.

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

**least privilege** – A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks [NIST CSRC, Glossary].

**log monitoring** – Using specialized software to scan event logs for patterns or anomalies that may indicate unauthorized accounts, access, or activities [adapted from NIST CSRC, Glossary term "log analysis"].

**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 (MFA)** – 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 800-53r5*, 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 CSRC, 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 800-53r5*, Glossary].

**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.

**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 800-53r5*, 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].

**separation of duties/segregation** – 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].

**superuser** – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform [NIST CSRC, Glossary].

**system administrator** – Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures [NIST CSRC, Glossary].

**user** – Individual, or (system) process acting on behalf of an individual, authorized to access a system [*NIST SP 800-53r5*, Glossary].

# Appendix C. References


Center for Internet Security. *CIS Critical Security Controls Version 8.1*. CIS. August 2024. https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf.

Grassi, Paul A., Michael E. Garcia, and James L. Fenton. *NIST SP 800-63-3: Digital Identity Guidelines*. June 2017. NIST, June 2017, updated March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2018; also accessed online, November 12, 2024. https://www.isaca.org/resources/cobit.

ISACA. "Glossary." ISACA, accessed November. 12, 2024. https://www.isaca.org/resources/glossary.

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

NIST Computer Security Resource Center. "Glossary." NIST, accessed November 12, 2024, https://csrc.nist.gov/glossary.

NIST. *NIST Cybersecurity Framework 2.0*. NIST, February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

U.S. Citizenship and Immigration Services. "I-9, Employment Eligibility Verification.," https://www.uscis.gov/i-9.

## About The Institute of Internal Auditors

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

## Disclaimer



## Copyright



Dec. 2024 (This version supersedes “Auditing Identity and Access Management,” published in 2021.)

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