
# Auditing Business Applications

Supplemental Guidance | **Practice Guide**

GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of Internal Auditors

# About the IPPF

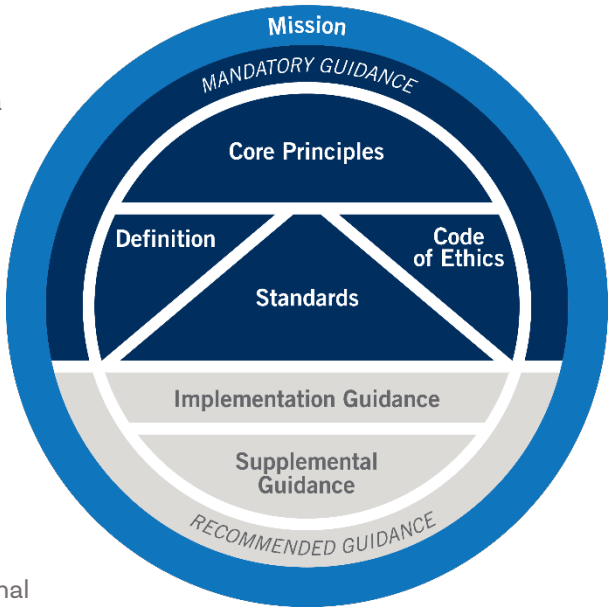
The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.

**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.

IPPF | International Professional Practices Framework




## 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.theiia.org.

# Contents

# Executive Summary

**Business applications may be** a single software program or a collection of hardware, firmware, and software applications operating as an integrated system to enable the organization's processes. Business applications are subject to common IT and information security (IS) control categories. Each category consists of standard control processes, which vary in relevance depending on the specificities of the organization and application. Stakeholders such as senior management and the governing body require assurance services to verify whether controls over business applications are well designed and effectively implemented.

### Note

The cover, logo, and references in this guide have been updated since its original publication. The content has not changed.

This guide categorizes control objectives over business applications as relating to:

1. **Technology planning —** IT-IS planners work with business unit leaders to design technology solutions to meet business needs. Enterprise and security engineers determine requirements for applications and component technologies, often documented in a technology roadmap. Planning for component obsolescence is a critical step in the roadmap.
2. **System development life cycle —** Applications require coding that adheres to functional and security requirements. The source code is written, tested, released into service, and revised as needed to fix errors, address security flaws, accommodate new technology, or add features.
3. **Production support —** System administrators, who are usually in IT, prepare business applications for service and provide ongoing support. System administrators work with the benefitting business units to create system roles for various job functions and implement account authorization, reauthorization, and deactivation processes.
4. **Application security —** Controls over secure design and coding, patch management, user access management, and event logging are part of planning, the system development life cycle, and support processes.

Other significant control objectives over business applications include but are not limited to:

5. **Records and information management (RIM) —** Maintaining documentation of application architecture, system interfaces, data flows, and source code.
6. **Vendor management —** Ensuring contracts provide sufficient terms for the performance and security of applications purchased from or significantly modified by vendors.

7. **Software asset management —** Maintaining an inventory of in-service applications and related metadata to support various governance and operational needs.
8. **Database administration and business intelligence —** Controlling access to and use of application data to support privacy and management reporting objectives.

# Introduction

**A business application may be** a single software program or a collection of hardware, firmware, and software applications operating as an integrated system to enable the organization's processes. Common examples of business applications include enterprise resource planning systems, point-of-sale systems, industrial control systems, and customer relationship management and billing systems. Key features that distinguish a business application from a simpler program — often called a tool — include (1) whether the software has been programmed to perform specific business processes and (2) whether user accounts have differentiated permissions.

### Note

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

Typically, the organization's IT department administers business applications; however, it is not uncommon for **shadow IT** functions to exist within other business units, especially as vendor-managed and cloud-based applications become more prevalent. Regardless of the department performing system administration and oversight, the business unit personnel that benefit from the applications have roles to play in defining business needs, executing authorization **controls**, and providing feedback on system performance.

As directed by a **risk**-based audit plan, internal auditors may evaluate how organizations develop or acquire business applications to facilitate significant business processes. A single internal audit **engagement** may assess whether management has implemented controls to ensure adequate **confidentiality**, **integrity**, and **availability** of systems and data. Some technology control frameworks, such as the AICPA's Trust Services Criteria, add security and **privacy** as additional objectives.

### Standard 1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

Auditing a business application involves a risk assessment, a specified engagement scope, and tests to evaluate the design and implementation of relevant controls to determine whether any significant risk exposures exist. Ideally, the **internal audit activity**, IT-IS teams, and the benefitting business unit personnel collaborate to provide valuable insight into **inherent risks**, the strength of controls, and **residual risks**. An audit engagement covering a business application may be one of a series of engagements that supports the internal audit activity's ability to provide assurance regarding whether the organization's **information technology governance** supports its strategies and objectives, as required by **Standard** 2110.A2. Following this approach helps

internal auditors demonstrate conformance with Standard 1200 — Proficiency and Due Professional Care.

## IT-IS Control Frameworks

This guide mentions three external IT-IS **control** frameworks of standards, guidance, and best practices (although there are many others). Each **framework** provides more information about specific controls than is discussed here. Internal auditors are encouraged to identify frameworks used by their organizations and to review common IT-IS control guidance to understand common risks and controls. Appendix C provides details on these sources.

This GTAG refers to controls described in the following publications:

- COBIT 2019 Framework: Governance and Management Objectives from ISACA.
- NIST Special Publication (SP) 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations from the National Institute of Standards and Technology (also referred to as NIST SP 800-53r5).
- *CIS Controls Version 8* from the Center for Internet Security.

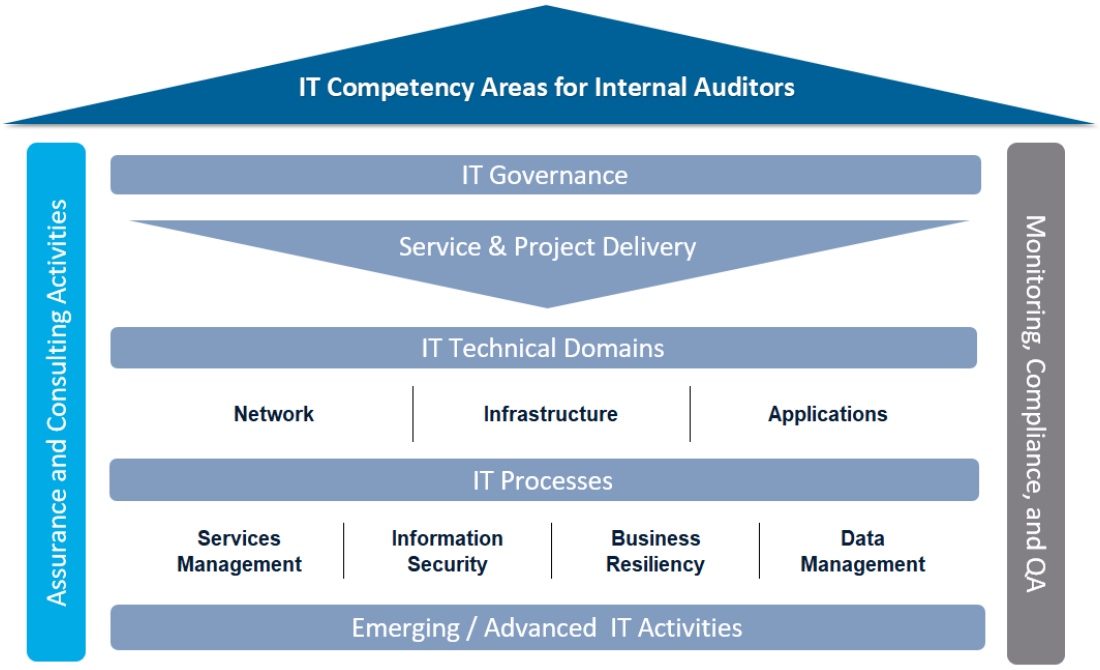
IT-IS personnel frequently benchmark operational and security controls against one or more of these frameworks. Although each framework uses its own groupings of controls, the categories and terminology share substantial commonalities.

This Global Technology Audit Guide (GTAG) references the guidance in these frameworks where doing so may be helpful to an auditor. Readers of this guide are assumed to have a general knowledge of IT-IS risks and controls, as described in the GTAG "IT Essentials for Internal Auditors." Additionally, readers are encouraged to incorporate a review of the full texts of one or more IT-IS control frameworks in their engagement planning and test programs.

## Previous GTAG and Terminology

This guide supersedes the GTAGs "Auditing Application Controls" and "Auditing User-developed Applications," which were published in 2009 and 2010 respectively. Some terminology has been revised and content rearranged to broaden the scope of the previous guides. The GTAG now includes risks and controls relevant to the "Applications" technical domain, as depicted in **Figure 1** below, which was introduced in the GTAG "IT Essentials."

Figure 1: The IIA's IT Competencies for Internal Auditors




Source: The Institute of Internal Auditors.

The previous definition of "application controls," which this guide refers to as "**application functionality controls,**" was primarily focused on transaction-level risks, while the term "IT general controls" was used to refer to everything else. Although these terms are still widely used among auditors, they are not used in *COBIT 2019*, *NIST SP 800-53r5*, or the *CIS Controls* and do not align with The IIA's IT Competencies for Internal Auditors construct depicted in **Figure 1**. They also do not align well with the IT infrastructure of a modern enterprise, which often includes vendor-managed, cloud-based, and on-premises solutions, with varying control responsibilities in each environment. Therefore, this guide does not use the terms "application controls" and "IT general controls," even though they may remain in use among audit practitioners.

In The IIA's *Standards*, "**information technology controls**" is used in the broadest sense to describe the **governance** and management of technology. However, this guide favors the phrase "IT-IS risks and controls" because it reflects the common practice of splitting information security responsibilities from information technology by establishing a chief information security officer (CISO) who does not report to the chief information officer, although both may report to a chief technology officer or similar executive. The phrase "IT-IS risks and controls" also better captures the notion that the technology management practices that are recommended in widely used IT-IS control frameworks have evolved to mitigate common universally applicable risks. Accordingly, this GTAG broadly covers risks and related controls in process-based groupings, as outlined in the Executive Summary.

## Objectives

This guide is intended to help the reader:

- Define business applications and obtain a working knowledge of relevant processes, including related administrative and operational controls.
- Understand risks and opportunities associated with business applications.
- Understand components of the **system development life cycle**, including:
    - Coding to meet operational and security requirements.
    - Testing for security and functionality.
    - Controlling the release and storage of **source code**.
    - Installing security **patches** and other updates.
- Understand components of **production support**, including:
    - Configuring the application and connections to external systems.
    - Administering **system roles** and accounts.
    - Responding to user and operational feedback, including errors and outages.
- Understand some related controls for documentation, **vendor management**, **asset management**, and reporting from application databases.
- Understand approaches to auditing business applications, including specific controls that should be present and evaluated.

# Business Application Engagement Planning

**Before setting an engagement's scope,** internal auditors can take a methodical approach to understand an application's context and delivery model by assessing relevant risks. Asking a series of questions about the application's use and administration may help internal auditors assess the inherent risks of a business application. Figure 2 shows potential questions and describes their relevance to an application risk assessment.

| Q# | Question | Relevance to Risk Assessment |
|---|---|---|
| 1. | Is the application a single software program or a platform that consists of multiple applications and products interfacing and operating together? | An application platform is inherently riskier than a single application due to security and performance risks with **component technologies** – on top of risks associated with the primary application. |
| 2. | What significant business processes does the application support, and who is/are the **business owner(s)**? | Unclear or disengaged ownership may lead to suboptimal management of strategy, governance, business requirements, service delivery, or the prioritization or funding of enhancements. |
| 3. | Does the application process financial transactions? Is the process a significant input to the financial statement accounts? | Applications that process financial transactions may be subject to external audits of financial statements, so coordination of **assurance services** should be considered (per Standard 2050 – Coordination and Reliance). **Fraud** is also a likely risk. |

| Q# | Question | Relevance to Risk Assessment |
|---|---|---|
| 4. | Does the application process or store personally identifiable information (PII) or other sensitive data? | Data privacy, **compliance**, and cybersecurity risks are heightened when an application handles or stores PII. |
| 5. | Is the application internet facing? | Controls over **encryption**, **firewalls**, secure coding, connections to external systems, and monitoring are typically more important for internet-facing applications. |
| 6. | To what extent are vendors involved in developing, administering, or **hosting** the application? | Nonemployees may execute controls related to the system development life cycle, system administration, database administration, and hosting, which heightens vendor risk and the importance of performance oversight as well as identity and access management. |
| 7. | To what extent is the application included in standardized **control processes**, such as identity and access management, patch management, monitoring for availability, and cybersecurity? | Due to **control inheritance**, an internal audit assessment may not need to retest the controls of an application covered by standardized controls that work in multiple systems and have been tested in a separate engagement. |
| 8. | Has the application been the subject of an internal audit engagement before? If so, what were the **engagement objectives**, scope, and results? Are there any open action plans? | Previously identified conclusions of design inadequacy or operating ineffectiveness can be retested, although a fresh risk assessment and scope determination are advisable. |
| 9. | Has the application been covered by a recent risk assessment performed by IT-IS or by an external assurance provider, such as for a Payment Card Industry Data Security Standards (PCI-DSS) or Service Organization Controls (SOC) audit? Have deficiencies or excessive risk exposures been noted? | Considerations are similar to #8, although internal auditors should evaluate the testing performed by other assurance providers (for example, external auditors) to reduce overlap and efficiently utilize resources. Furthermore, the internal audit activity may consider providing consulting services (advisory engagements) to reduce the client's audit fatigue while still promoting positive changes. |
| 10. | Is the application (and its component applications) included in the organization's software inventory, completely populated with key **metadata,** such as business owner; production support, development, and security contacts; system criticality and data classification ratings; and system **interfaces**? | If the organization does not have an inventory system integrated with governance, development, and support processes, there is a higher likelihood of manual processes, which are inherently riskier than automated ones. |
| 11. | Is there a significant risk or history of fraud or cybersecurity breaches? Have the root causes been identified and remediated? | Instances of fraud or cybersecurity breaches can highlight deficiencies in the design or implementation of controls. |
| 12. | Does there appear to be a robust **control environment**, including but not limited to policies, procedures, designated personnel for properly separated roles, management reporting, and training? | The existence of well-documented expectations, monitoring of outcomes, and corrective actions taken for variances typically indicates a well-controlled environment, and the opposite is true. |

## Scoping the Engagement

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

Business applications may enable, support, or monitor business processes, which themselves may be part of larger processes. Using and supporting business applications depends upon multiple controls that may be standardized throughout the enterprise or tailored to the specific circumstances of an application under review. Therefore, determining the scope of a business application engagement requires consideration of the context, risks, and engagement objectives, as required by Standard 2220 – Engagement Scope. Furthermore, Standard 2220.A1 requires the scope of the engagement to consider relevant systems, among other specific considerations, during an assurance engagement.

Engagement objectives typically drive decisions about which business processes or controls to include in the scope. An integrated audit of operational and technical controls may be desirable; however, this guide covers only the assessment of business application controls.

### *Business Process Scoping Method*

The business process scoping method evaluates all the systems that support a particular business process. The focus of such an engagement would likely be on the applications' functionalities and their ability to meet business needs. However, based on the engagement risk assessment, the scope could include other aspects, such as vendor management or identity and access management. As part of the scoping activity, the internal auditor identifies the input, processing, and output systems of the process or area under review, including connections to external systems. Sometimes, especially for complex business applications such as an enterprise resource planning system, different modules of the same **ecosystem** can be considered similar to external input or output applications, particularly for data flow mapping or data processing reconciliations. Therefore, it may be important to identify the application modules supporting the business process and the data that flows between them.

### *Single Application Scoping Method*

Single application engagements could comprise an end-to-end view of the application ecosystem, including **technology planning**, system development life cycle, production support, **application security**, record and information management, vendor management, asset management, and database administration controls. This approach might be preferred for business applications that support processes whose operational controls are likely to be covered in separate engagements, for example, an industrial control systems application.

### *Single Module Scoping Method*

Sometimes, an audit of functionality in a single module, such as the fixed assets module in an accounting application, may be desired. These engagements are narrow in scope, primarily focusing on whether **business rules** are documented and adequately implemented. As such, a single module engagement would likely focus on application functionality controls and the working relationship between the benefitting business units, production support, and database administration teams.

# Performing the Engagement

**Scoping decisions determine** which control types are relevant to the audit. The following sections describe common risks and controls for each type.

## Technology Planning

High-level planning controls enable the service relationship between IT-IS and other business units and ensure that business applications are compatible with existing and future technologies in the organization. Collaboration between technology and other business units typically results in a **technology roadmap**, which plots the timeline for introducing upgrades or new component technologies to a business application, together with plans for introducing other technologies in the enterprise architecture or hosting environment. An assessment of business applications should consider whether controls are documented and operating adequately to ensure alignment with and sufficient support of business strategies. An engagement could also determine whether the organization incorporates new technologies in a deliberate and coordinated way, for example, as evidenced with technology roadmaps.

- In *COBIT 2019 Framework: Governance and Management Objectives*, technology planning controls are primarily described in the Align, Plan, and Organize domain, especially in objectives:
    - APO02 Managed Strategy.
    - APO03 Managed Enterprise Architecture.
    - APO04 Managed Innovation.
- *NIST SP 800-53r5* covers planning processes throughout the following control families:
    - Planning.
    - Program Management.
    - Personally Identifiable Information Processing and Transparency.
    - Risk Assessment.
    - System and Services Acquisition.
    - System and Communications Protection.
- *CIS Controls* covers technical planning in subcontrols called “safeguards,” specifically:
    - 2.2 Ensure Authorized Software is Currently Supported.
    - 16.5 Use Up-to-Date and Trusted Third-Party Software Components.

### *Gathering Requirements and Build vs. Buy*

The business owners and benefitting business units are responsible for identifying the need for a business application, determining the capabilities needed to support business processes, and selecting an overall approach or solution. IT or IS leaders may also be business owners for applications that meet their department's needs, such as supporting an IT service desk or event **log monitoring**. Typically, IT leaders help business owners determine whether the organization should develop the software internally, engage external developers, purchase commercially available software, or seek vendor-provided solutions. Vendor-provided solutions may be cloud-based, on-premises, or hybrid hosting models.

If an organization decides to develop software internally, using employees or contractors, IT leaders typically engage with the benefitting business units to identify how the software needs to enable the business processes and where controls are needed to enforce business rules and implement automation. If the organization purchases an off-the-shelf or vendor-provided solution, the benefitting business unit should verify that the software provides the necessary capabilities. Otherwise, the business unit may decide to alter processes to match the software's functionalities.

- *COBIT 2019 Framework: Governance and Management Objectives* provides relevant control guidance for solution identification in the practices:
    - EDM02.02 Evaluate Value Optimization.
    - APO02.03 Define Target Digital Capabilities.
    - APO04.04 Assess the Potential of Emerging Technologies and Innovative Ideas.
    - APO08.02 Align I&T Strategy with Business Expectations and Identify Opportunities for IT to Enhance the Business.
- *NIST SP 800-53r5* covers planning processes in these control families:
    - Planning, particularly controls PL-7 Concept of Operations and PL-10 Baseline Selection.
    - Program Management, especially PM-7 Enterprise Architecture.
- *CIS Controls* indirectly addresses technical planning in safeguard 16.11 Leverage Vetted Modules or Services for Application Security Components, which presumes the organization has processes to vet technologies for use in its environment.

### *Security in Design*

When planning the system design, security-related attributes to be considered include the system's **security category**, whether and where to deploy encryption, the risks associated with potential vendors, cybersecurity risks, and more. If the application will be connected to the internet, the placement and configuration of **web application firewalls** need to be determined. Many of these IS controls are covered more extensively in the GTAG "Assessing Cybersecurity Risk: The Three Lines Model" and other GTAGs.

An internal audit of a business application could determine whether the CISO has assessed the information security risks and authorized the chosen mitigation approaches in the architecture,

operating systems, application software, and communications technologies for the application(s) under review. An audit could also verify whether the system architecture and data flow documentation include IS measures.

- In *COBIT 2019 Framework: Governance and Management Objectives*, secure design controls are covered mainly in practices:
    - APO01.07 Define Information (Data) and System Ownership.
    - BAI03.02 Design Detailed Solution Components.
    - BAI08.01 Identify and Classify Sources of Information for Governance and Management of I&T.
    - DSS06.06 Secure Information Assets.
- In *NIST SP 800-53r5*, relevant controls are primarily found in the following control families:
    - Risk Assessment, especially RA-2 Security Categorization.
    - System and Services Acquisition, particularly control SA-5 System Documentation.
    - System and Communications Protection, especially control SC-3 Security Function Isolation.
- *CIS Controls* includes guidance on security in design in safeguards:
    - 3.7 Establish and Maintain a Data Classification Scheme.
    - 16.10 Apply Secure Design Principles in Application Architectures.

## System Development Life Cycle

Application development is characterized as a life cycle because the process is usually circular: software is planned, developed, tested, and implemented, and then operational feedback is obtained, which informs further planning and development, and so on. There are many languages and development methods used to create software programs. The following sections focus on the generalized objectives and controls in creating integrated applications that meet business needs. The GTAG "Auditing IT Projects" more extensively covers controls over program and project management.

Guidance for system development life cycle controls primarily can be found in:

- COBIT 2019 Framework: Governance and Management Objectives in the Build, Acquire and Implement domain.
- *NIST SP 800-53r5* System and Services Acquisition and System and Communications Protection control families.
- *CIS Controls* — control 16 Application Software Security.

### *Software Development*

The processes to create a business application include coding and testing to meet business requirements and integrating with other systems to provide a complete solution. A common approach is a service management model, where the business owner and other benefitting

business units are the customers and authorizers. In such a model, the IT function performs client management, systems development, and service delivery functions; and the IS group reviews security mechanisms in the design, coding, and configuration of solutions.

When an organization develops a business application or has a vendor develop a customized solution, the IT team typically manages updates in the coding as different releases, also known as production versions. A **version control system** may be used to automate the release approval and implementation workflows and to ensure other documentation controls are enacted. An assessment of an internally developed application should determine whether controls exist to ensure that the requirements and approvals for each release have been documented.

Another essential consideration for development includes establishing a separate coding environment, which should not be directly connected to the production environment. Static and dynamic code testing tools are often used in a test environment to improve the quality, efficiency, and security of software code. Developers should not have access to code or systems that are currently operating because such access could allow them to insert unauthorized code or security bypass mechanisms or to otherwise subvert the authorized operations of the application. Restricting developers from testing their own code is part of maintaining a separation of duties, which is necessary to mitigate the risk of intentional or unintentional vulnerabilities. Internal audits of business applications should verify whether separate environments are maintained for developing, testing, and hosting applications and should determine whether duties have been separated appropriately for the testing of new coding or releases.

Business applications that are purchased as commercial, off-the-shelf programs or as cloud-based services (the software as a service, or SaaS, model) may limit the amount of input or direction the vendor takes from each customer. For example, enterprise resource platforms, industrial control systems, and other large-scale application platforms may be offered with automatic version updates; or they may allow the customer to control which version of the software runs in its environment but provide limited or no access to the application source code. Therefore, a review of software development risks and controls — on its own or within an audit of a business application — should consider the extent of the organization's control over the timing, quality, and security of the source code. Other guidance more extensively covers the IS controls that address risks related to purchased applications. These include vulnerability scans and other preventive and detective controls.

Controls over software development or procurement are described in:

- COBIT 2019 Framework: Governance and Management Objectives in objectives:
    - BAI03 Managed Solutions Identification and Build.
    - BAI07 Managed IT Change Acceptance and Transitioning.
- *NIST SP 800-53r5* control families that cover software development or procurement include:
    - System and Services Acquisition, most notably SA-3 System Development Life Cycle and SA-8 Security and Privacy Engineering Principles.

    - System and Communications Protection, especially SC-2 Separation of System and User Functionality.

- *CIS Controls* covers software development mainly in safeguard 16.1 Establish and Maintain a Secure Application Development Process.

### *Application Functionality Controls*

Organizations often manage operational risks using programmed or configurable controls, such as enabling a three-way match control and acceptable variance tolerances for invoices going through the accounts payable process. The IIA and others have historically referred to these types of controls as "application controls." However, "application functionality controls" is a more specific term because the control functions are programmed according to the business owner's documented requirements, known as business rules. These controls enable business processes through the validation of input data, separation of business functions, balancing of processing totals (for example, the count and dollar value of a batch of invoices approved for cash disbursement), transaction logging, and error reporting. The controls are usually preventive or detective, but they may also enable forensic analysis.

Types of application functionality controls include:

- **Input controls –** Used mainly to check the integrity of data entered into a business application to ensure that it remains within specified parameters, is limited to valid data types, and is properly authorized.
- **Processing controls –** Used to ensure processing is complete, accurate, authorized, and timely.
- **Output controls –** Used to ensure accuracy and completeness by comparing output results to inputs and properly recording output data.
- **Integrity controls –** Used to monitor data in process and at rest to ensure it remains consistent and **persistent**.
- **Interface controls –** Used to ensure proper connections to separate systems that provide inputs or receive outputs.
- **Transaction and event logging –** Used to assign unique **identifiers** (IDs) to transactions and events to enable forensic investigation and ensure accountability.

In engagements that include a review of application functionality controls, internal auditors evaluate whether these controls are documented and implemented appropriately due to their importance to operations. One way to do that is to compare business requirements to the design and results of **user acceptance testing**; another is to verify whether management analyzes the root causes of performance issues and determine whether frequent or high-impact events led to configuration or code changes.

- In *COBIT 2019 Framework: Governance and Management Objectives*, controls to ensure application functionality meets business requirements are covered mainly in practices:
    - APO08.04 Coordinate and Communicate.
    - BAI03.07 Prepare for Solution Testing.

- *NIST SP 800-53r5* guidance mainly focuses on security and privacy, rather than service management or meeting operational requirements; however, control PL-10 Baseline Selection establishes a relevant control objective: that system functionality requirements should be reflected in the control baseline.
- Similarly, *CIS Controls* primarily focuses on cybersecurity, not service management, so application functionality guidance is not directly covered.

### *User Acceptance Testing*

In addition to the static and dynamic code testing mentioned previously, the benefitting business units should test software to ensure application functionality controls meet documented business rules and that the application interacts with input and output systems as intended. The business owner may categorize issues identified in user acceptance testing as either:

1. Needing to be resolved before acceptance.
2. Authorized to be addressed in a subsequent release.

Procured business applications also go through user acceptance testing before being placed into service for the same reasons as developed software. Identified issues may need to be negotiated with the vendor to determine whether the delivered program meets contractual terms. Managing the documentation of requirements and plans for enhancements is an ongoing process for the benefitting business units and developers, whether in-house or external. An assessment of business applications may check whether user acceptance tests are designed to verify compliance with business requirements, whether results are documented, and whether the issues identified during testing are either resolved to the business owner's satisfaction or accepted, usually to be resolved in a subsequent release.

- *COBIT 2019 Framework: Governance and Management Objectives* describes controls over user acceptance testing in objective BAI07 Managed IT Change Acceptance and Transitioning, especially in practices:
    - BAI07.01 Establish an Implementation Plan.
    - BAI07.05 Perform Acceptance Tests.
- *NIST SP 800-53r5* controls related to establishing system requirements, testing, and acceptance criteria focus on security and privacy rather than functionality objectives; these are covered primarily in controls:
    - SA-4 Acquisition Process.
    - SA-11 Developer Testing and Evaluation.
- *CIS Controls* does not cover user acceptance testing directly.

### *Release Management and Software Escrow*

Code that has been tested and approved for use is compiled into an approved software version, which should be protected from unauthorized modification. Typically, a version control system is used to manage this process and enforce security objectives. Approved versions should be

stored off-site with a software escrow service to be used in the event that files or hardware are damaged or corrupted. An internal audit of business applications could verify whether management has ever tested the ability to recover operations from an escrowed version of production software and whether the in-service version has been escrowed.

- *COBIT 2019 Framework: Governance and Management Objectives* describes controls over approved versions of software in practices:
    - BAI07.06 Promote to Production and Manage Releases.
    - APO10.04 Manage Vendor Risk.
- In *NIST SP 800-53r5*, relevant guidance is found in controls:
    - CM-7 Least Functionality.
    - SA-10 Developer Configuration Management.
    - SC-34 Non-modifiable Executable Programs.
- *CIS Controls* does not directly address controls over the release or off-site storage of software versions.

### *Security in Development*

In addition to the security-related steps mentioned previously, a vulnerability scan should be performed on an application after launching it into the production environment (but before opening it to full service) to identify configuration or component weaknesses. IT-IS personnel and the business owner should evaluate the results of the scan to determine whether the residual risk is acceptable. Other GTAGs will cover controls over vulnerability scanning more extensively.

In a business application ecosystem, vendor-provided software, including firmware, is often updated to address security flaws in the code or interactions with component technologies in a new version called a patch. The controls over implementing patches are generally the same as for other new software versions, except there may be internal deadlines for patches that are not expected of other updates. The IS team typically has some responsibility for monitoring or enforcing those expectations.

Patch management controls are covered in:

- COBIT 2019 Framework: Governance and Management Objectives in objectives:
    - BAI03 Managed Solutions Identification and Build.
    - DSS05 Managed Security Services.
- *NIST SP 800-53r5* control SI-2 Flaw Remediation.
- *CIS Controls* safeguard 7.4 Perform Automated Application Patch Management.

## Production Support

Controls to manage an in-service application include several significant IT-IS processes, including:

- Working with IS to implement encryption, identity, and **authentication** technologies.
- Establishing system backup and recovery processes.
- Hosting an approved version on a server and putting new versions into service.
- Connecting the application to its databases.
- Connecting the system to internal or external interfaces, including **application programming interface** (API) **middleware**.
- Working with the benefitting business units to establish necessary system roles and authorization processes.
- Monitoring system performance and responding to errors and outages.

This guide and the GTAG "Auditing Identity and Access Management" cover certain aspects of identity and access management. This guide also covers other control types, such as configuration management and system performance monitoring, as they pertain to applications. Additionally, other GTAGs will detail processes including system hosting, database administration, middleware management, encryption, and system backup and recovery.

One aspect to consider when scoping a business application engagement is whether the standardized control processes that apply to other applications in the enterprise have been applied to the application under review. As stated in **Figure 2: Questions to Support Internal Audit's Risk Assessment**, question 7, due to control inheritance, an audit of a business application may exclude from its scope any controls effected by standardized processes that are audited separately. However, during planning, the internal audit team should verify the extent to which the business application is covered.

### *Configuration Management*

One step in designing a business application is establishing a **baseline configuration**, which documents the set of approved component technologies, interface settings, and other controls that make the application operational. A service management application may help coordinate and record changes and automatically update the baseline configuration. Configuration changes may cause or fix processing and output errors and other system performance issues.

An internal audit engagement focused on a particular business application may consider whether configuration management controls are applied generally, meaning that the application's configuration is centrally managed (through an enterprisewide tool, such as a service management application). If the application's configuration controls are not integrated and configuration is managed separately, internal auditors may have an opportunity to consult on feasible alternatives to strengthen controls by implementing enabling technology. For example, the configuration management controls of legacy systems and vendor-managed systems may not be integrated through the enterprisewide tool.

The GTAG "IT Change Management" further describes the controls over configuration management and changes to in-service systems. Configuration management controls are also covered in:

- The COBIT 2019 Framework: Governance and Management Objectives, mainly:
    - Practice BAI03.05 Build Solutions.
    - Objective BAI10 Managed Configuration, primarily practice BAI10.01 Establish and Maintain a Configuration Model.
- In *NIST SP 800-53r5*, mainly in the Change Management control family, especially controls:
    - CM-2 Baseline Configuration.
    - CM-3 Configuration Change Control.
- In *CIS Controls*, throughout the 12 safeguards in control 4 Secure Configuration of Enterprise Assets and Software.

### *User Access Management*

The GTAG "Auditing Identity and Access Management" discusses user access management controls at length, including the idea that if a business application is **federated** with standardized tools, then such controls may be excluded from the scope of an application audit. However, in certain higher-risk applications, internal auditors may desire an analysis of users with elevated privileges, even in federated applications, to determine whether users' supervisors are exercising meaningful, rather than perfunctory, oversight. In the context of a business application, elevated privileges may mean higher financial approval thresholds or the ability to unmask protected data. In contrast, a **privileged account** usually refers to a **system administrator**, **superuser,** or **database administrator** role.

If a business application is not federated with the human resources information system for user IDs, then the application's inherent risk is higher because user access management will have to rely more heavily on manual processes. Also, if nonemployees, especially individuals not issued a network ID, have access to a business application, there is a higher inherent risk because the process for role and employment status updates is probably manual and reliant on vendor personnel to notify the system administrator timely, which may not always happen. A business application audit should evaluate controls over nonemployee accounts, which could belong to contractors or temporary personnel managed by the organization, vendor, partner, or other individuals not recognized as employees in the human resources database of record.

System roles within business applications may be predefined and unalterable in some off-the-shelf or vendor-provided software but are more likely to be configurable by administrators to meet the needs of the benefitting business units. Administrators should document the roles, related permissions, and intended users based on input from the benefitting business units. During authorization processes, user supervisors should use this information to guide authorization decisions.

- *COBIT 2019 Framework: Governance and Management Objectives* describes user access management controls in the practice DSS06.03 Manage Roles, Responsibilities, Access Privileges and Levels of Authority.
- In *NIST SP 800-53r5*, relevant guidance is found in control families:
    - Access Control.
    - Identification and Authentication.
    - Personnel Security.
- *CIS Controls* covers similar measures in the following safeguards:
    - 4.7 Manage Default Accounts on Enterprise Assets and Software.
    - 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts.
    - 6.1 Establish an Access Granting Process.
    - 6.2 Establish an Access Revoking Process.
    - 6.8 Define and Maintain Role-Based Access Control.

### *Security in Production*

In business applications, one security-related control that is usually configurable is the recording in log files of transactions and other events, such as the creation of new roles or user accounts or the initiation and termination of user sessions. The IS and production support teams should work together to identify what types of events and information should be logged, undertake agreed-upon solutions, and connect application logs to organizationwide log monitoring tools. Logging event information provides data for other controls, such as those for monitoring and analyzing event logs. Such controls will be covered in other GTAGs.

Event logging and log monitoring controls are primarily described in:

- COBIT 2019 Framework: Governance and Management Objectives practices:
    - DSS06.05 Ensure Traceability and Accountability for Information Events.
    - DSS01.03 Monitor I&T Infrastructure.
- *NIST SP 800-53r5* provides excellent guidance for controls over logging in the Audit and Accountability control family, especially in controls:
    - AU-2 Event Logging.
    - AU-3 Content of Audit Records.
- *CIS Controls* primarily covers similar measures in safeguards:
    - 8.5 Collect Detailed Audit Logs.
    - 8.10 Retain Audit Logs.

## Other Relevant Control Types

Other control types that are relevant to, embedded in, or built on business application control processes include but are not limited to those described below.

### *Records and Information Management*

The organization's **records and information management** (RIM) program should recognize the following items as official records and establish requirements for their retention:

- Application architecture diagrams.
- Data flow diagrams.
- Quality assurance and user acceptance testing routines and results.
- Source code for approved versions.
- Baseline configurations.
- System roles and user account and permissions authorizations.
- Event logs.

A business application engagement should verify whether requirements for retaining the listed document types are established and whether the necessary documentation for the application(s) under review is retained properly.

Controls over record retention are mainly described in:

- COBIT 2019 Framework: Governance and Management Objectives in practices:
    - BAI08.01 Identify and Classify Sources of Information for Governance and Management of I&T.
    - DSS06.05 Ensure Traceability and Accountability for Information Events.
- NIST SP 800-53r5 in controls:
    - SI-12 Information Management and Retention.
    - SA-5 System Documentation.
- *CIS Controls* covers similar guidance in safeguards:
    - 3.4 Enforce Data Retention.
    - 12.4 Establish and Maintain Architecture Diagram(s).

### *Vendor Management*

Wherever external personnel or entities help develop or support business applications, contracts and related documents should explain security and performance requirements sufficiently. A business application engagement should verify whether contracts include service level agreements and whether ongoing oversight, communication, and remediation processes have been exercised, as appropriate. The GTAG "Information Technology Outsourcing" describes controls over vendors in detail.

- *COBIT 2019 Framework: Governance and Management Objectives* — controls over vendors are described throughout objectives:
    - APO08 Managed Relationships.
    - APO09 Managed Service Agreements.
    - APO10 Managed Vendors.
- *NIST SP 800-53r5* — similar guidance is found in several control families, primarily:
    - Program Management, especially control PM-30 Supply Chain Risk Management Strategy.
    - Personnel Security, such as control PS-6 Access Agreements.
    - System and Services Acquisition, especially control SA-9 External System Services.
    - System and Communications Protection; for example, control SC-8 Transmission Confidentiality and Integrity.
    - Supply Chain Risk Management, especially SR-3 Supply Chain Controls and Processes.
- *CIS Controls* — control 15 Service Provider Management offers relevant guidance in several safeguards, such as 15.2 Establish and Maintain a Service Provider Management Policy.

### *Asset Management*

Maintaining an inventory of business applications with sufficient metadata to support governance, security, and operational needs is a fundamental enabler of many IT-IS processes. In the absence of a specifically designated software inventory tool, a service management application may serve as a de facto inventory because it contains a good amount of configuration and management details. However, the service management application may not capture all cloud-based applications or have all the desired metadata. A business application engagement should determine whether a sufficient software inventory system is in place and whether the application(s) under review are fully integrated with the inventory system, with all required data present, accurate, and current.

With vendor-provided applications, the unauthorized use of software licenses or the underutilization of purchased licenses may also be relevant concerns. An audit test could reconcile license assignees against the human resources information system to evaluate compliance with contract terms and cost management objectives. This reconciliation could determine whether the number of licenses is managed properly, for example, by verifying whether licenses are sufficiently utilized and only assigned to organization-managed devices or personnel.

Controls over a system inventory are mainly described in:

- COBIT 2019 Framework: Governance and Management Objectives in the following practices:
    - APO09.02 Catalog I&T-enabled Services.
    - APO14.03 Establish the Processes and Infrastructure for Metadata Management.
    - BAI09.01 Identify and Record Current Assets.

- BAI09.05 Manage Licenses.
- BAI10.05 Verify and Review Integrity of the Configuration Repository.

- NIST SP 800-53r5 controls:
  - PM-5 System Inventory.
  - CM-8 System Component Inventory.
- *CIS Controls* safeguards:
  - 1.1 Establish and Maintain Detailed Enterprise Asset Inventory.
  - 1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory.
  - 1.5 Use a Passive Asset Discovery Tool.

### *Database Administration and Business Intelligence*

Application databases may store confidential information about transactions, customers, vendors, employees, or other sensitive data types critical to business operations. Many controls related to configuration management, identity and access management, and backup and recovery apply at the database layer. Additionally, personnel with database administrator roles may be in IT or the benefitting business units. Therefore, planning a business application audit typically includes assessing the design and implementation of the various data management controls.

Organizationwide processes often manage database administration controls, so a business application engagement might be primarily concerned with verifying the justifications for individual and system IDs, including APIs and middleware services, to have access to confidential records. Assessments may also verify the use of encryption on tables or specific fields or review who is authorized to view encrypted data in **plaintext**.

The usage of data, sometimes referred to as **business intelligence**, entails creating standardized and ad hoc reporting capabilities to support governance, **risk management**, monitoring, and other objectives. A business application engagement may determine whether the system(s) under review support critical management reporting processes or whether other financial or operational metrics are derived from the application's database. If so, internal auditors may verify whether reporting processes provide reliable, accurate, and timely data. Internal auditors with knowledge of advanced data analytics tools or techniques may find advisory opportunities when reviewing the organization's use of business intelligence. When such opportunities arise, it may be necessary to formalize an

**Standard 2220 – Engagement Scope**

**2220.A2** – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting

agreement between the internal audit activity and the engagement client on the nature of additional consulting services, as recommended in Standard 2220 – Engagement Scope.

The GTAG "Fraud Prevention and Detection in an Automated World more thoroughly covers controls to detect fraud. A separate GTAG on cybersecurity operations details controls that monitor cybersecurity, including those that monitor database administration actions.

Controls over database management and business intelligence are primarily covered in:

- COBIT 2019 Framework: Governance and Management Objectives practices:
    - APO14.06 Ensure a Data Quality Assessment Approach.
    - APO14.08 Manage the Life Cycle of Data Assets.
    - MEA01.03 Collect and Process Performance and Conformance Data.
    - MEA01.04 Analyze and Report Performance.
- *NIST SP 800-53r5* control families:
    - Change Management, especially control CM-12 Information Location.
    - Program Management, especially control PM-6 Measures of Performance.
    - System and Communications Protection, especially control SC-28 Protection of Information at Rest.
    - System and Information Integrity, especially control SI-12 Information Management and Retention.
- In the *CIS Controls* similar guidance is mainly found in safeguards:
    - 3.3 Configure Data Access Control Lists.
    - 3.12 Segment Data Processing and Storage Based on Sensitivity.
    - 3.14 Log Sensitive Data Access.

## Using Computer-assisted Audit Techniques

Many off-the-shelf applications and tools enable internal auditors to enhance the breadth and efficiency of the audit process with computer-assisted audit techniques (CAATs). In an assessment of business applications, CAATs can enable a review of an entire population of transactions or records in a given period, identify anomalies in user access management, or perform other possible audit tests. A well-designed and documented engagement supported by CAATs demonstrates conformance with the following standards:

Standard 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. (emphasis added)

Standard 1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

# Conclusion

Business application controls cover the full life cycle of the application, from planning and development to support and management reporting. When considering the risks and scope of an engagement to audit a business application, it is important to understand how the application supports business needs and the role of external parties in every control category. This understanding helps internal auditors provide value-added insight by focusing on the most significant risks. Given the critical role of applications as enablers of business processes, a risk-based audit plan should include engagements that evaluate standardized and system-specific controls to determine whether significant risks are adequately managed.

# Appendix A. Related IIA Standards and Guidance

The following IIA resources were referenced directly or indirectly 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 1200 – Proficiency and Due Professional Care |
| Standard 1210 – Proficiency |
| Standard 1220 – Due Professional Care |
| Standard 2050 – Coordination and Reliance |
| Standard 2110 – Governance |
| Standard 2120 – Risk Management |
| Standard 2130 – Control |
| Standard 2130 – Control |
| Standard 2220 – Engagement Scope |
| **Guidance** |
| TAG "IT Essentials for Internal Auditors," 2020 |
| GTAG "Assessing Cybersecurity Risk: The Three Lines Model," 2020 |
| GTAG "Auditing IT Projects," 2009 |
| GTAG "Auditing Identity and Access Management," 2021 |
| GTAG "IT Change Management," 2020 |
| GTAG "Information Technology Outsourcing, 2nd Edition," 2012 |
| GTAG "Fraud Prevention and Detection in an Automated World," 2009 |

# 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:

- *Internal Auditing: Assurance & Advisory Services, 4th edition,* https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition.
- ISACA, Glossary, accessed August 3, 2021, https://www.isaca.org/resources/glossary.
- *NIST SP 800-63-3: Digital Identity Guidelines*, Glossary, https://doi.org/10.6028/NIST.SP.800-63-3.
- *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations*, *Revision 5*, Glossary, https://doi.org/10.6028/NIST.SP.800-53r5.

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

**application functionality controls** — The programmed routines and related parameters that enable software to execute according to business rules.

**application programming interface (API)** — A set of routines, protocols and tools referred to as "building blocks" used in business application software development. A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system that applications need to specify, for example, when interfacing with the operating system. A programmer utilizes these APIs in developing applications that can operate effectively and efficiently on the platform chosen [ISACA Glossary].

**application security** — The set of system-specific and inherited IS controls applied to the development, operation, and usage of an application.

**asset management** — A set of processes to record, safeguard, and optimize the use of resources.

**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 800-53r5* Glossary].

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

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

**baseline configuration** — An approved set of components, system settings, and connections to other systems.

**business intelligence** — The use of data to present, analyze or predict business activities.

**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 also "authorizing official" in *NIST SP 800-53r5* Glossary).

**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.

**component technologies** — Discrete technology assets that represent a building block of a system and may include hardware, software, or firmware. (See also "system component" in *NIST SP 800-53r5* Glossary.)

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

**control environment*** — The discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

**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].

**control processes*** — The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

**customer relationship management** — A way to identify, acquire and retain customers. CRM is also an industry term for software solutions that help an enterprise manage customer relationships in an organized manner [ISACA Glossary].

**database administrator (or administration)** — 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].

**dynamic code testing** — Analysis of software in operation, by using specified test routines and observing the results.

**ecosystem** — The hardware, firmware, software and connections that make up a business application's environment.

**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, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

**engagement objectives*** — Broad statements developed by internal auditors that define intended engagement accomplishments.

**enterprise resource planning system** — A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes, share common data and practices across the entire enterprise, and produce and access information in a real-time environment [ISACA Glossary].

**event logging** — Chronologically recording system activities, like access attempts, role creation, user account creation or deactivation, etc. (See also "audit log" in *NIST SP 800-53r5* Glossary.)

**federated** — integrated with an identity and authentication information process across a set of networked systems [Adapted from "federation" in *NIST SP 800-63-3* Glossary].

**firewall** — A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the internet [ISACA Glossary].

**firmware** — Computer programs and data stored in hardware — typically in read-only memory or programmable read-only memory — such that the programs and data cannot be dynamically written or modified during execution of the programs [*NIST SP 800-53r5* Glossary].

**framework** — A body of guiding principles that form a template against which organizations can evaluate a multitude of business practices. These principles are comprised of various concepts, values, assumptions, and practices intended to provide a yardstick against which an organization can assess or evaluate a particular structure, process, or environment or a

group of practices or procedures. [*Internal Auditing: Assurance & Advisory Services*, 4th edition]

**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.

**hosting** — Providing the physical and logical infrastructure to run software applications that have distributed users.

**identifier** — Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group [*NIST SP 800-53r5* Glossary].

**industrial control system** — General term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as programmable logic controllers found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (like electrical, mechanical, hydraulic, and pneumatic) that act together to achieve an industrial objective (such as manufacturing, or the transportation of matter or energy) [*NIST SP 800-53r5* 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 governance*** — Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

**inherent risk** — The combination of internal and external risk factors in their pure, uncontrolled state, or, the gross risk that exists, assuming there are no internal controls in place [*Internal Auditing: Assurance & Advisory Services, 4th ed.*]

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

**interface** — Common boundary between independent systems or modules where interactions take place [*NIST SP 800-53r5* Glossary].

**internal audit activity*** — A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to

evaluate and improve the effectiveness of governance, risk management and control processes.

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

**metadata** — Information that describes the characteristics of data, including data format, syntax, semantics, and contents [*NIST SP 800-53r5* Glossary].

**middleware** — Another term for an 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].

**patch** — Fixes to software programming errors and vulnerabilities [ISACA Glossary].

**persistent** — A characteristic of stored data that keeps it the same, enabling later retrieval.

**plaintext** — Digital information, such as cleartext, that is intelligible to the reader [ISACA Glossary].

**point-of-sale system** — Enables the capture of data at the time and place of transaction; such terminals may include use of optical scanners for use with bar codes or magnetic card readers for use with credit cards. Point-of-sale systems may be connected online to a central computer, or used as stand-alone terminals that hold the transactions until the end of a specified period, then sending data to the main computer for batch processing [adapted from ISACA Glossary].

**privacy** — The rights of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of his or her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. Scope notes: What is appropriate depends on the associated circumstances, laws, and the individual's reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use, and disclosure of his or her associated personal and sensitive information [adapted from ISACA Glossary].

**privileged account** — A system account with the authorizations of a **privileged user** [*NIST SP 800-53r5* 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].

**production support** — Processes to configure, administer and troubleshoot applications. (See also "IT service," ISACA Glossary).

**records and information management** — An enterprisewide program to identify official record types and their storage locations, and establish retention and destruction requirements.

**residual risk** — The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk) [*Internal Auditing: Assurance & Advisory Services, 4th ed.*].

**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.

**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 [excerpted from *NIST SP 800-53r5* Glossary].

**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 [adapted from "segregation/separation of duties," ISACA Glossary].

**shadow IT** — Personnel or resources performing an IT function outside of the IT management hierarchy.

**source code** — The language in which a program is written. Source code is translated into object code by assemblers and compilers [adapted from ISACA Glossary].

**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.

**static code testing** — An automated analysis of code, usually in the development environment, to detect potential errors, vulnerabilities, or inefficient coding.

**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 development life cycle (SDLC)** — The phases deployed in the development or acquisition of a software system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities [adapted from ISACA Glossary].

**system roles** — Sets of permissions within an application that typically correspond to job functions.

**technology planning** — Activities to align IT-IS resources with business needs, ensuring objectives of confidentiality, integrity, availability, privacy, and security are met. (See also ISACA's definition for "strategic planning," and *NIST SP 800-53r5*'s definition of "enterprise architecture).

**technology roadmap** — A plan for a business application's version and component updates, aligned with the enterprise architecture plan. (See also ISACA's definitions for "IT strategic plan" and "IT tactical plan").

**technology-based audit techniques*** — Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and computer-assisted audit techniques (CAATs).

**user acceptance testing** — A phase of the SDLC where application users run a series of tests to verify whether the solution meets the business requirements.

**vendor management** — A set of processes to procure goods and services, ensure acceptable delivery or performance, and resolve disputes.

**version control system** — An application used in SDLC to manage changes to the source code and facilitate approvals to promote code from the development environment to the test environment, and then to the production environment.

**vulnerability scan** — Automated routine to detect known weaknesses in software code or configurations. The vulnerabilities may be assigned a score to facilitate prioritization of resolution efforts.

**web application firewall** — A firewall placed between the internet and an application server to filter traffic and prevent various types of cyberattacks.

# Appendix C. References

## References


Anderson, Urton L., Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, and Paul J. Sobel. *Internal Auditing: Assurance & Advisory Services, 4th edition.* Lake Mary, FL: The Internal Audit Foundation, 2017.

Association of International Certified Professional Accountants. "TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," March 2020. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf..

Center for Internet Security. "The 18 CIS Controls," interactive guide to *CIS Controls, Version 8*. Accessed August 13, 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 July 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*. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

The Institute of Internal Auditors. *International Professional Practices Framework*. 2017 ed. Lake Mary, Florida: The Institute of Internal Auditors, 2017.

# Acknowledgements


## IT Guidance Development Team

Susan Haseley, CIA, United States (Chairman)

Justin Pawlowski, CIA, CRMA, Germany (Team Lead)

Brad Ames, CISA, CPA, United States

Jim Enstrom, CIA, United States

Ruth Mueni Kioko, CIA, Kenya

Mike Lynn, CIA, CRMA, United States

Scott Moore, CIA, United States

Sajay Rai, CISM, CISSP, CISM, United States

Manoj Satnaliwala, CIA, CPA, CISA, United States

Terence Washington, CIA, CRMA, United States

## IIA Global Standards and Guidance

David Petrisky, CIA, CRMA, CISA, CPA, Director, (Project Lead)

Dr. Lily Bi, CIA, QIAL, CRMA, CISA, Executive Vice President

Anne Mercer, CIA, CFSA, CFE, Senior Director

Pam Stroebel Powers, CIA, CRMA, CPA, Director

Daniel Walker, CIA, CISA, CISSP, CPA, Director

Shelli Browning, 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, Professional Guidance Advisory Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight 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 200,000 members from nearly 200 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.theiia.org.**

## Disclaimer



## Copyright



First editions, "Auditing Application Controls," published 2009, and "Auditing User-developed Applications," published 2010

Second edition September 2021

Note: The cover, logo, and certain references were updated November 2021. There were no changes to the original content. Questions may be directed to guidance@theiia.org.

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