ISACA®

Trust in, and value from, information systems

Information Systems Auditing:

Tools and Techniques

Creating Audit Programs

Abstract

Information systems audits can provide a multitude of benefits to an enterprise by ensuring the effective, efficient, secure and reliable operation of the information systems so critical to organizational success. The effectiveness of the audit depends, in large part, on the quality of the audit program.

TABLE OF CONTENTS

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

INTRODUCTION

Organizations undertake audits for many reasons. An audit can help the enterprise ensure effective operations and attest to its compliance with administrative and legal regulations. It can confirm for management that the business is functioning well and is prepared to meet potential challenges. Perhaps most important, it can assure stakeholders of the financial, operational and ethical well-being of the organization. Information systems (IS) audits support all those outcomes, with a special focus on the information and related systems upon which most businesses and public institutions depend for competitive advantage.

Achievement of the many benefits that can accrue to an effective audit depends on proper and thorough planning of the audit engagement. The scope and the objective of the audit must be understood and accepted by both the auditor and the area being audited. Once the purpose for the audit is clearly defined, the audit plan can be created, which will encapsulate the agreed scope, objectives and procedures needed to obtain evidence that is relevant, reliable and sufficient to draw and support audit conclusions and opinions.

An important component of the audit plan is the audit program, also known as work program. The audit program is commonly used to document the specific procedures and steps that will be used to test and verify control effectiveness. The quality of the audit program has a significant impact on the consistency and quality of the audit results, so it is imperative that IS auditors understand how to develop comprehensive audit programs.

Purpose of This Publication

The purpose of this publication is to provide a basic understanding of the steps necessary to develop comprehensive audit programs that clearly and consistently document the procedures that will be used to test controls and gather supporting data. This guide is also intended to help audit/assurance professionals develop audit programs that comply with generally accepted audit standards, especially those issued by ISACA,[1] the Public Company Accounting Oversight Board (PCAOB),[2] the Institute of Internal Auditors (IIA),[3] and the American Institute of Certified Public Accountants (AICPA).[4]

This publication is not intended to provide technical guidance on how to audit specific technologies.

Audience

This guide is intended primarily for IS and non-IS audit/assurance professionals who need to gain an understanding about the process to develop audit programs for IS audit engagements. This guide is also beneficial for audit/assurance professionals who wish to enhance their skills in developing IS audit programs.

Scope and Approach

This publication is intended to provide practical guidance to develop audit programs from the ground up. The guide has been organized into three main areas:
- Audit process overview
- Steps to develop an audit program
- List of resources

In addition, other audit program resources are available from ISACA at *www.isaca.org/creating-audit-programs*, including a Sample Audit Program document and an Infographic—Step-by-Step Audit Plan Activities.

[1] ISACA, *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/default.aspx*
[2] PCAOB, *General Audit Standards, AS 2101: Audit Planning*, USA, 2015, *http://pcaobus.org/Standards/Auditing/Pages/AS2101.aspx*
[3] The IIA, *International Standards for the Professional Practice of Internal Auditing (Standards)*, USA, revised 2012, *https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf*
[4] AICPA, *Due Professional Care in the Performance of Work, AU-C Section 300, Planning an Audit*, USA, 2015, *www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00300.pdf*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Terminology

The terms “audit plan,” “audit program” and “work program” are frequently used interchangeably; however, they are different types of documents that serve different purposes within specific audit engagements. The main difference between audit plans and audit programs is the scope of the document, as described in the following terminology list:

- **Audit plan**—A high-level description of the audit work to be performed in a certain period of time by the auditor or a team of auditors. This document should contain details about the engagement, including the stakeholders, subject, objective, scope and deliverables of the engagement. Other critical details that should be documented in the audit plan include the budget, resource allocation, schedule dates, type of report and its intended audience, and the methodology that will be used to assess controls in scope.
- **Audit program**—A more granular description of the work to be performed to meet the engagement objectives. The audit program should be used to document step by step the set of audit procedures and instructions needed to test controls, evaluate results, obtain suitable evidence to form an opinion and report the findings to the stakeholders. Other details that should be included in the audit program include the areas to be audited, high-level objectives, and the tools and techniques that will be used to test controls.
- **Work program**—A list of procedures and tasks that should be performed to meet audit objectives
- **Internal controls questionnaire**—A document that auditors can use to inquire about the existence of internal controls before performing the audit. The questionnaire is useful to determine the areas on which the audit should focus.
- **Checklist**—A list of items that is used to verify the completeness of a task or goal
- **Test scripts**—A list of specific instructions that need to be followed to test a particular subject and document the results
- **Work papers**—The set of documents used to record all of the work performed during the entire audit engagement and demonstrate compliance with audit standards

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

THE AUDIT PROCESS

The audit process requires the IS auditor to gather evidence, evaluate the strengths and weaknesses of internal controls based on the evidence gathered through audit tests, and prepare an audit report that presents weaknesses and recommendations for remediation in an objective manner to stakeholders.[5]

In general terms, the typical audit process consists of three major phases: planning, fieldwork and reporting, as shown in **figure 1**. Enterprises can choose to break down the main phases into multiple phases; for example, the reporting phase can be broken down into three phases: report writing and issuance, issue follow-up, and audit closing. The organization and naming convention can be customized as long as the procedures and outcomes comply with applicable audit standards like those established by ISACA in *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition*. The IS auditor must be familiar with standard frameworks and the audit process used by the entity under review in order to use the correct terminology and work organization.

Figure 1—Typical Audit Process Phases

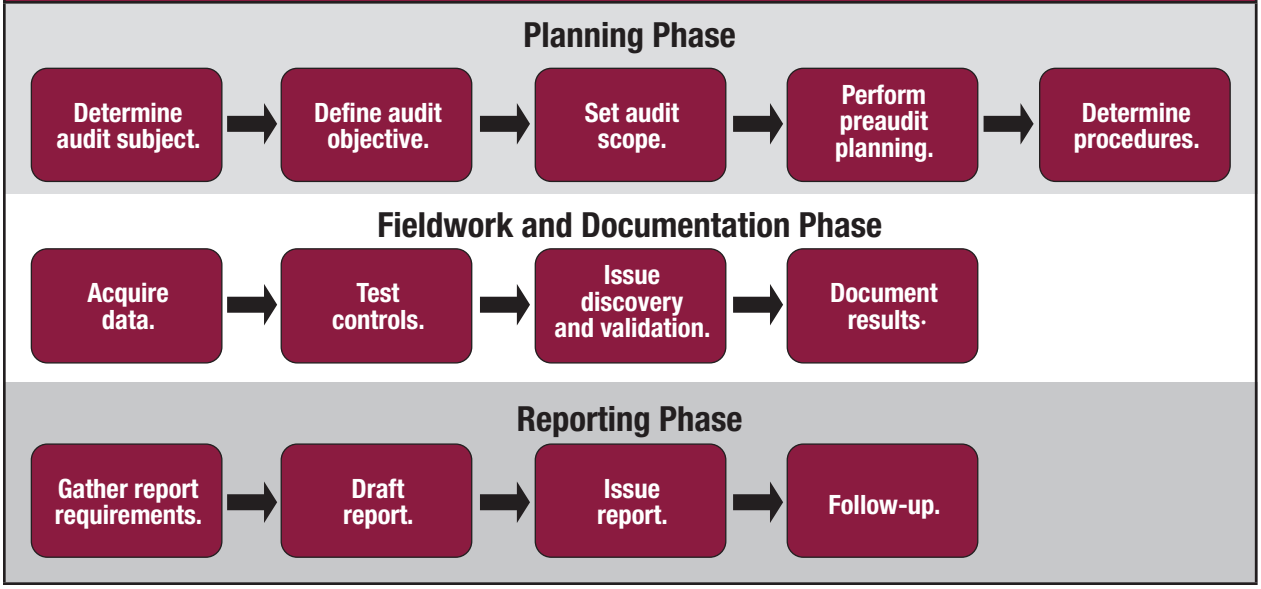
ITAF is a comprehensive and good-practice-setting reference model that:
- Establishes standards that address IS audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments
- Outlines several critical hypotheses that are inherent in any IS audit or assurance assignment, including:[6]
  - The subject matter is identifiable and subject to audit.
  - There is a high probability of successful completion of the project.
  - The approach and methodology are free from bias.
  - The project is of sufficient scope to meet the IS audit or assurance objectives.
  - The project will lead to a report that is objective and will not mislead the reader.

Each phase in the audit process is subsequently divided into key steps to plan, define, perform and report the results of the engagement in line with audit standards, as shown in **figure 2**. The organization and naming convention for the steps described in this guide can be customized to meet enterprise needs as long as the procedures and outcomes comply with applicable audit standards and meet the intended goal for the audit engagement.

[5] ISACA, *Fundamentals of IS Audit and Assurance: Participant Guide*, USA, 2014, p. 29
[6] *Op cit* ISACA, *ITAF*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Figure 2—Typical Audit Process Steps by Phase



The steps shown in **figure 2** can be further broken down into more specific activities. **Figure 3** describes the typical activities that will be performed during each step in the planning phase.

Figure 3—Audit Process Activities by Step

Audit Step	Description
1. Determine audit subject.	Identify the area to be audited (e.g., business function, system, physical location).
2. Define audit objective.	Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
3. Set audit scope.	Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous example (program changes), the scope statement might limit the review to a single application, system or a limited period of time. This step is very important because the IS auditor will need to understand the IT environment and its components to identify the resources that will be required to conduct a comprehensive evaluation. A clear scope will help the IS auditor define a set of testing points that is relevant to the audit and further determine the technical skills and resources necessary to evaluate different technologies and their components.
4. Perform preaudit planning.	• Conduct a risk assessment, which is critical in setting the final scope of a risk-based audit. For other types of audits (e.g., compliance), conducting a risk assessment is a good practice because the results can help the IS audit team to justify the engagement and further refine the scope and preplanning focus. • Interview the auditee to inquire about activities or areas of concern that should be included in the scope of the engagement. • Identify regulatory compliance requirements. • Once the subject, objective and scope are defined, the audit team can identify the resources that will be needed to perform the audit work. Some of the resources that need to be defined follow: – Technical skills and resources needed – Budget and effort needed to complete the engagement – Locations or facilities to be audited – Roles and responsibilities among the audit team – Time frame for the various stages of the audit – Sources of information for test or review, such as functional flowcharts, policies, standards, procedures and prior audit work papers – Points of contact for administrative and logistics arrangements – A communication plan that describes to whom to communicate, when, how often and for what purposes

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Figure 3—Audit Process Activities by Step *(cont.)*	
Audit Step	**Description**
5. Determine audit procedures and steps for data gathering.	At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the **audit program**. Some of the specific activities in this step are: • Identify and obtain departmental policies, standards and guidelines for review. • Identify any regulatory compliance requirements. • Identify a list of individuals to interview. • Identify methods (including tools) to perform the evaluation. • Develop audit tools and methodology to test and verify controls. • Develop test scripts. • Identify criteria for evaluating the test. • Define a methodology to evaluate that the test and its results are accurate (and repeatable if necessary).

An audit plan should comprise all five steps shown in the planning phase. An audit program is the product of steps one, two, three and five. For the remainder of this publication the term **"audit and assurance program"** refers to the outcome of the planning phase that deals with the audit approach and procedures.

The rest of this publication explains and demonstrates the steps necessary to develop audit and assurance programs. For detailed instructions on how to address the reporting phase, refer to the ISACA publication *Information Systems Auditing: Tools and Techniques—IS Audit Reporting* at *www.isaca.org/tools-and-techniques.*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

AUDIT AND ASSURANCE PROGRAMS

The audit and assurance program is an early and critical product of the audit process. It serves as a guide for performing and documenting all the audit steps and the extent and types of evidential matter reviewed to ensure that audit objectives are met. Although an audit program does not necessarily follow a specific set of steps, the IS auditor typically would follow, as a minimum course of action, sequential program steps to gain an understanding of the entity under audit, evaluate the control structure and test the internal controls.[7]

Audit or Assurance

Audit and assurance are two terms that are used interchangeably (similar to audit plan and audit program). According to ISACA:
- **Assurance** refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter.
- **Audit** is a formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met.[8]

Simply put, audit is a form of assurance exclusive to the audit function. Assurance activities can be performed by different compliance functions, for example, risk management, quality, fraud investigation or security assessment. However, audit activities should be performed by audit professionals only. The difference between audit and assurance is that audit is independent from operational functions, which allows audit to provide objective and unbiased opinions about the effectiveness of the internal control environment.[9]

Objectives of Developing Audit and Assurance Programs

The main objectives (value) of developing audit and assurance programs are:
1. Formally document audit procedures and sequential steps.
2. Create procedures that are repeatable and easy to use by internal or external auditors who need to perform similar audits.
3. Document the type of testing that will be used (compliance and/or substantive).
4. Meet general accepted audit standards that relate to the planning phase in the audit process.

Note: Compliance testing is evidence gathering for the purpose of testing an organization's compliance with control procedures. This differs from substantive testing, in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.[10]

ITAF Standard 1201 Engagement Planning[11]

Requires the IS audit and assurance professionals to plan each IS audit and assurance engagement to address:
- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

In addition, the IS audit and assurance professional must develop and document an IS audit or assurance engagement project plan, describing the following:
- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

[7] ISACA, *CISA® Review Manual, 26th Edition*, USA, 2015, p. 45
[8] ISACA, Glossary, *www.isaca.org/pages/glossary.aspx*
[9] Chartered Institute of Internal Auditors, *What is internal audit?*, UK, 2015, *https://www.iia.org.uk/about-us/what-is-internal-audit/*
[10] *Op cit* ISACA, *CISA Review Manual*
[11] *Op cit* ISACA, *ITAF*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Minimum Skills to Develop an Audit and Assurance Program

The most important skill for an IS auditor is understanding the business environment and related risk to determine what to test and why. Developing meaningful audit and assurance programs depends on the ability to customize audit procedures according to the nature of the subject under review and the specific risk that must be addressed in the audit area/organization. The following list describes some of the skills that can enable the IS auditor to develop good audit programs:

- Good understanding of the nature of the enterprise and its industry to identify and categorize the types of risk and threat
- Good understanding of the IT space and its components and sufficient knowledge of the technologies that affect them
- Understanding of the relationship between business risk and IT risk
- A basic knowledge of risk assessment practices
- Understanding of the different testing procedures for evaluating IS controls and identifying the best method of evaluation, for example:
  - The use of generalized audit software to survey the contents of data files (e.g., system logs, user access list)
  - The use of specialized software to assess the contents of operating systems, databases and application parameter files
  - Flowcharting techniques for documenting business processes and automated controls
  - The use of audit logs and reports to evaluate parameters
  - Review of documentation
  - Inquiry and observations
  - Walk-throughs
  - Reperformance of controls

Steps to Develop an Audit and Assurance Program

As defined in the audit process section of this guide, the audit and assurance program is the product of the audit planning phase. **Figure 4** shows the inputs that help produce the audit and assurance program. Please note that step 4 has been shaded in gray to indicate that its input to the audit program is only partial. The document resulting from the input of all five steps is the audit plan, as previously defined in the terminology section of this publication.

Step 4 is an important part of the audit planning phase because it is during this step that resources are estimated based on the engagement objective and scope. Some outputs from step 4 include:

- Resources needed to meet the engagement's objective (e.g., budget, personnel, work hours, travel, etc.)
- Knowledge, skills and experience needed to prepare and execute fieldwork
- Physical locations or business entities that will be part of the scope
- Sources of information about business processes and supporting technologies

While step 4 may generate some inputs for the audit program, e.g., physical locations, business entities and sources of information, the significance of step 4 in this context is decidedly less than other steps.

Figure 4—Audit and Assurance Program Inputs

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

The table in **figure 5** shows some examples of the outputs from the audit planning phase, and some sources of information that can help the IS auditor obtain technical and business details that pertain to the specific audit engagement.

Figure 5—Example Outputs From the Audit Planning Phase

Audit Planning Phase		
Step	**Examples**	**Sources of Information**
1. Define audit subject.	• Enterprise resource planning (ERP) system • Data center • Virtual private network (VPN) • Bring your own device (BYOD) program governance • BYOD security • Change management process • Database • Cloud computing provider quality	• Annual audit plan • Risk assessments • Organizational change plans • Legal or regulatory changes • Mergers and acquisitions
2. Define audit objective.	• Assuring compliance with legal and regulatory requirements • Assuring the confidentiality, integrity, reliability and availability of information and IT resources • Attesting financial reporting accuracy • Assuring system development quality and security	• Annual audit plan • Audit management • Executive management • Audit sponsors • Previous audit reports • Internal policies, standards and procedures • Governance frameworks • Risk assessments • Legislations or regulations applicable to the enterprise
3. Set audit scope.	• Assuring compliance with Sarbanes-Oxley (SOX) • Systems supporting the sales function • Servers in data center X • Network security • Systems in the Payment Card Industry Data Security Standard (PCI DSS) scope	• Organization charts • Previous audit reports • Process maps and system flow diagrams • Network maps • Risk assessments • Legislations or regulations applicable to the audit subject
4. Perform preaudit planning. • Locations and facilities to be audited* • Sources of information to prepare tests	• For example, to review the sales function, the IS auditor must include the locations of the sales organization, the data center hosting the systems supporting the sales function and the accounting organization (to review accounts receivable and application of cash). • A system may be supported by multiple vendors.	• Organization charts • Previous audit reports • Process maps and system flow diagrams • Network maps • Risk assessments • Vendor contracts • Interviews with the auditees • Vulnerability assessment results • Penetration testing results • Service level agreement (SLA) compliance issues • Problem and incident tickets (in-house and with third-party vendors)
5. Determine audit procedures and steps for data gathering.	This step and related activities are described in **figure 6.**	

***Note:** This step is important and must be considered during the preparation of the audit and assurance program because the final scope and audit methodology must include considerations regarding local statutory and regulation requirements that should be part of the audit scope. A scope that includes dispersed locations may impact the skills and resources needed to perform the review.

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

The table in **figure 6** shows the activities listed under step 5 of the audit planning phase. These activities create inputs that are critical to the development of a comprehensive and significant audit and assurance program.

Figure 6—Activities in Step 5 of Audit Planning

Step 5 Activities	Examples	Sources of Information
Identify and obtain departmental policies, standards and guidelines for review.	• Information security policies • Segregation of duties (SoD) policies • Purchasing policies • Authority matrix • Industry standards or guidelines • Compliance requirements	• Legal department • Regulatory organizations • Compliance department • Finance department • Prior audit reports
Identify a list of individuals to interview.	• IT operations manager • User security administrator • Accounts payable clerk • Compliance manager • Software development supervisor • Software quality testing coordinator	• Internal controls questionnaires (ICQs)/standard operating procedures • List provided by management • Organizational charts • Responsible, accountable, consulted, informed (RACI) charts • Prior audit reports
Identify methods (including tools) to perform the evaluation. The IS auditor should translate the overall audit objective into more specific objectives and determine the level of compliance and/or substantive testing required to meet the audit objective. Audit tools can be as simple as questionnaires or as complex as scripts that interrogate systems in order to collect system information.	Methodology examples: • Compliance testing can be used to determine if production systems' library controls are working as intended. The IS auditor can select a sample of programs and compare the versions of the source and local objects. • Compliance testing of internal controls where sampling could be considered includes user access rights, program change control procedures, documentation procedures, program documentation, follow-up of exceptions, review of logs and software license audits. • Substantive testing should be used when the audit objective is to evaluate the validity and integrity of financial transaction processing. • Substantive testing of internal controls where sampling could be considered includes performance of complex calculations using a sample of accounts or a sample of transactions to confirm accuracy and reliability. Audit tools examples: • Questionnaires • Scripts • Relational databases • Spreadsheets • Computer-assisted audit tools (CAATs) • Sampling methodologies for auditing transactions	• Software vendor manuals • Compliance frameworks • Internal procedures • Interviews with support personnel • Training manuals • Process flowcharts • System development documents • Disaster recovery plans • Shadowing of system administrators or other IS personnel who are part of the process under review • Screen prints of administrative console configuration parameters • Exception lists in group policies • White- and black-list exceptions of web sites • Off-the-shelf auditing and administrative reporting applications
Develop audit tools and methodology to test and verify controls.	See the step, "Identify methods (including tools) to perform the evaluation."	

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Figure 6—Activities in Step 5 of Audit Planning *(cont.)*		
Step 5 Activities	**Examples**	**Sources of Information**
Identify criteria for evaluating the test (similar to a test script for the auditor to use in conducting the evaluation). The testing methods will be selected based on audit objectives and the type/amount of evidence that must be collected to substantiate test conclusions. The testing methods will also vary depending on the nature of the internal controls that need to be evaluated (e.g., manual or automated).	• Review of organizational structures • Review of policies, standards and procedures • Review of documentation • Interviews with key personnel • Observation of procedures as they are performed • Reperformance • Walk-throughs • Obtaining snapshots • Review of system information/configuration of applications or systems • Data analysis • Review of access logs for critical functions/tasks • Data extraction at a table level • Sample testing of transactions • Review of the Statements on Standards for Attestation Engagements (SSAE) 16 reports from service organizations. **Note:** Many of these test examples can and should be combined as necessary to obtain sufficient evidence to draw conclusions.	• Criteria for evaluating tests can be found in professional standards and frameworks developed by professional accounting and audit bodies such as: – ISACA (*ITAF* Standard 1008) – COBIT® 5 framework – National Institute of Standards and Technology (NIST) recommendations and frameworks – International Organization for Standardization (ISO) standards – International Federation of Accountants (IFAC) – PCAOB – IIA – AICPA – Recognized government bodies – Recognized professional bodies • Standard operation procedures • Security configuration manuals • Technical configuration manuals • User acceptance criteria/sign-off documents • SoD matrices • Approval level matrices • SLAs • Vendor contracts
Define a methodology to evaluate that the testing and its results are accurate (and repeatable if necessary). Repeatability of tests and results refers to the fact that the IS auditor will obtain objective evidence that is sufficient to enable a qualified independent party to reperform the tests and obtain the same results and conclusions. Effectively evaluating any test results requires the initial test results to be analyzed in the context of the business environment. The business context can help differentiate authorized deviations from true anomalies. The nature of any deviation should be documented and taken into account to reduce errors or bias during testing.	To understand the criteria needed to evaluate evidence, the IS auditor should refer to *ITAF* Standard 1205. • Categorize test results as a process failure or a transaction aberration. • Perform substantive testing to validate an application control failure, if required. • Have discussions with business stakeholders to understand the rationale of a control setting that differs from standard procedures.	• Criteria for evaluating evidence as found in professional standards and frameworks developed by professional accounting and audit bodies • Mitigating actions that have been documented • Operating procedures

In addition to the activities listed under step 5 of the audit planning phase, the following activities are highly suggested to improve the IS auditor's abilities to develop audit and assurance programs.

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Define and record the audit approach/strategy. During this phase the IS auditor should document in an organized way the steps that will be necessary to complete the subsequent phases in the audit process.

Examples:
- The approach can consist of the following steps:
  - Review documentation.
  - Interview key individuals.
  - Establish audit criteria.
  - Conduct visits to the data center.
  - Conduct a review of high-risk areas.
  - Document findings.
  - Prepare the report and provide it to stakeholders for review and comment.
  - Issue the final report.

- A risk-based approach can consist of the following steps:[12]
  - Review documentation.
    - Business and industry information
    - Regulatory statutes
    - Prior year's audit results
    - Inherent risk assessments
    - Recent financial information
  - Understand the internal controls.
    - Control environment
    - Control risk assessment
    - Control procedures
    - Equation of total risk
    - Detection of risk assessment
  - Perform compliance tests.
    - Identification of key internal controls to be tested
    - Performance of tests on reliability, risk prevention and adherence to organizational policies and procedures
  - Perform substantive tests.
    - Analytical procedures
    - Detailed tests of account balances
    - Verification of report logic
  - Conclude the audit.
    - Creation of recommendations
    - Writing of audit report

Identify sources of information to expand the understanding of the audit area/subject. The IS auditor should identify materials that can be referenced as appropriate for each audit to obtain technical and operational information about the subject.

Examples:
- The audit scope includes new VPN technologies the IS auditor must understand in order to identify risk, internal controls and testing procedures.
- The audit scope includes a facility overseas and the IS auditor must understand the statutory and regulation requirements of the location where the facility exists.
- The IS auditor must become familiar with operating systems and databases used to support the application under review.

[12] *Op cit* ISACA, *CISA Review Manual*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

Sources of information:
• Previous audit reports
• Process maps and system flows
• Network maps
• SLAs
• Internal policies, standards and procedures
• Books
• Software development documentation
• Training manuals
• Installation/configuration manuals
• Supplier web sites
• User forums
• Security configuration recommended by vendors
• International standards for specific technologies

Identify and request documentation related to the audit subject. Based on the scope of the review, the IS auditor should prepare a list of documents to be used to complete the planning phase and during fieldwork.

Examples:
• Previous audit reports
• Process maps and system flows
• Network maps
• SLAs
• Process standards and procedures
• List of active users
• Authority level matrix
• Policies
• Software development documentation
• Training manuals
• List of suppliers
• List of employees
• List of terminated employees in a given period of time
• List of newly hired employees in a given period of time

Identify and document risk and internal controls. Risk assessment is necessary to meet audit standards. For instance, *ITAF* 1202 Risk Assessment in Audit Planning requires:

> *The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.*
>
> *IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.*

To start developing the risk assessment, the IS auditor should consider the following:
• Business purpose of the audit subject
• Environment in which the enterprise operates
• Prior audit results
• Statutory and compliance regulations
• Technology-specific risk

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

For each risk identified, the IS auditor should document the nature, potential impact and likelihood of occurrence and define the necessary controls to address the risk. Finally, the IS auditor should perform a preliminary assessment of the risk by inquiring about existing internal controls intended to address the risk.

The result of the assessment of audit objectives, identified risk and existing internal controls will determine the final scope of the audit and the strategy to accomplish the goal of the audit.

Examples:

Ref.	Risk	Impact	Likelihood	Internal Controls in Place
1	The user IDs of terminated employees are not removed promptly, which may result in unauthorized access to enterprise information.			• The human resources (HR) system automatically creates a help desk ticket to disable employee IDs after the employee status has changed to "T" (terminated). • Disabled IDs are completely removed from the system after six months.
2	Access to the database is not restricted to authorized users who have valid business need.			• Requests for database access, which require a description of the business need of the user requesting the access, are reviewed and approved by the business process owners.

Sources of information:
- SLAs
- Audit checklists
- ICQs
- Software development documentation
- Training manuals.
- Software provided installation/configuration manuals
- Process flowcharts
- System interfaces maps
- List of well-known software vulnerabilities

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

APPENDIX A—LIST OF RESOURCES

ISACA Resources

CISA Review Manual, 26th Edition, 2015
COBIT® 4.1
COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT
COBIT® 5 for Assurance
ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition
Information Systems Auditing: Tools and Techniques, IS Audit Reporting

Additional Resources

National Institute of Standards and Technology (NIST), *www.nist.gov*
Center for Internet Security (CIS), *www.cisecurity.org*
National Security Agency (NSA), *www.nsa.gov*
Software vendor web sites (e.g., SAP, Oracle, Microsoft, Cisco, HP)
Cloud Security Alliance (CSA), *https://cloudsecurityalliance.org*
Institute of Electrical and Electronic Engineers (IEEE), *www.ieee.org*
Payment Card Industry Security Standards Council (PCI SSC), *www.pcisecuritystandards.org*
The IT Infrastructure Library (ITIL), *https://www.axelos.com/best-practice-solutions/itil*
TechRepublic, *www.techrepublic.com*
National Vulnerability Database (NVD), *https://nvd.nist.gov*
Common Vulnerability and Exposures (CVE), *https://cve.mitre.org*
International Organization of Supreme Audit Institutions (INTOSAI), *www.intosai.org*
The Institute of Internal Auditors (IIA), *https://theiia.org*
The American Institute of CPAs (AICPA), *www.aicpa.org*
Computer Security Resource Center, *http://csrc.nist.gov*
United States Computer Emergency Readiness Team (US-CERT), *www.us-cert.gov*
Build Security In, *https://buildsecurityin.us-cert.gov/*
Homeland Security—Cybersecurity, *http://www.dhs.gov/topic/cybersecurity*
Open Web Application Security Project (OWASP), *www.owasp.org*
European Network and Information Security Agency (ENISA), *www.enisa.europa.eu*

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.

ISACA®
ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer
ISACA has designed and created *Information Systems Auditing: Tools and Techniques—Creating Audit Programs* (the "Work") primarily as an educational resource for audit professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, audit professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights
©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Provide feedback: *www.isaca.org/tools-and-techniques*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

Information Systems Auditing: Tools and Techniques—Creating Audit Programs

ACKNOWLEDGMENTS

Lead Developer

Eva Sweet, CISA, CISM, ISACA, USA

Expert Reviewers

Gerardo Arancibia Vidal, CISM, CRISC, Ernst & Young, Chile
Sujatha Balakrishnan, CISA, India
David Berkelmans, CISA, Synergy Group, Australia
P. W. Carey, CISA, CISSP, Compliance Partners, LLC, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Joanne De Vito De Palma, MBA, BCMM, The Ardent Group, LLC, USA
Shawna Flanders, CISA, CISM, CRISC, Business-Technology Guidance Associates, LLC, USA
Tomas Thobias Hellum, LinkGRC, Denmark
Zhu Hui, CISA, CISM, CGEIT, BlueImpact Ltd., Canada
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Francis Kaitano, CISA, CISM, CISSP, MCSD, IR, New Zealand
Joanna B. Karczewska, CISA, Poland
Ramaswami Karunanithi, CISA, CRISC, CGEIT, CA, CIA, CFSA, CGAP, CGMA, CMA, CPA, CRMA, CSXF, Department of Family and Community Services, Australia
Debbie Lew, Ernst & Young LLP, USA
Hardik Mehta, Ernst & Young LLP, USA
Karen Norton, CISA, CICA, CPA, CRMA, DIRECTV, USA
Nnamdi Nwosu, CISA, CSTE, CSQA, ITIL, PMP, Fidson Healthcare Plc., Nigeria
Douglas E. Salas Calderon, Credomatic, Costa Rica
Lily M. Shue, CISA, CISM, CRISC, CGEIT, LMS Associates, LLP, USA
Ability Takuva, CISA, PRINCE2, Absa Card, Barclays Africa Group Limited, South Africa
Nancy Thompson, CISA, CISM, CGEIT, Nancy J. Thompson Consulting, USA
Marc Vael, Valuendo, Belgium

ISACA Board of Directors

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chair
Rosemary M. Amato, CISA, CMA, CPA, Deloitte, Amsterdam, The Netherlands, Director
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, MAICD, Vital Interacts, Australia, Director
Zubin Chagpar, CISA, CISM, PMP, Amazon Web Services, UK, Director
Robert A. Clyde, CISM, Clyde Consulting LLC, USA, Director
Theresa Grafenstine, CISA, CGEIT, CRISC, CPA, CIA, CGAP, CGMA, US House of Representatives, USA, Director
Matt Loeb, CGEIT, CAE, ISACA, USA, Director
Leonard Ong, CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck & Co., Singapore, Director
Andre Pitkowski, CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director
Rajaramiyer Venketaramani Raghu, CISA, CRISC, Versatilist Consulting India, Pvt., Ltd., India, Director
Eddie Schwartz, CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director
Gregory T. Grocholski, CISA, SABIC, Saudi Arabia, Past Chair
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair
Robert E Stroud, CGEIT, CRISC, USA, Past Chair

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved.