ISACA®
Trust in, and value from, information systems

Information Systems Auditing:
Tools and Techniques

IS Audit Reporting

ISACA®
With more than 115,000 constituents in 180 countries, ISACA *(www.isaca.org)* helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. The association has more than 200 chapters worldwide.

Disclaimer
ISACA has designed and created *Information Systems Auditing: Tools and Techniques* (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

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

ACKNOWLEDGEMENTS

Lead Developer
John W. Beveridge, CISA, CISM, CGEIT, CRISC, CFE, Bentley University, USA

Expert Reviewers
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA, Myers and Stauffer LC, USA, Lead Reviewer
Christopher Nigel Cooper, CISM, CEng, CITP, FBCS, M.Inst.ISP, HP Enterprises Security Services, UK
Alisdair McKenzie, CISA, CISSP, ITCP, I S Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, JIEC Co. Ltd. (SCSK group), Japan
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgium
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA
Timothy Smith, CISA, CISSP, CPA, LPL Financial, USA

ISACA Board of Directors
Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, BAE Systems Detica, Australia, Vice President
Robert A. Clyde, CISM, Adaptive Computing, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, SABIC, Saudi Arabia, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Credentialing and Career Management Board
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Chairman
Bernard Battistin, CISA, CPA, CMA, Office of the Auditor General of Canada, Canada
Erik Friebolin, CISA, CISM, CRISC, CISSP, PCI-QSA, ITIL, USA
Frank Nielsen, CISA, CGEIT, CCSA,CIA, Nordea, Denmark
Carmen Ozores Fernandes, CISA, CRISC, CIA, EBSERH-Empresa Brasileira de Serviços Hospitalares, Brazil
Eduardo Ritegno, CISA, CRISC, QAR (IIA), Banco de la Nacion Argentina, Argentina
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA
Todd Weinman, CPS, The Weinman Group, USA

Professional Standards and Career Management Committee
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA, Chairman
Christopher Nigel Cooper, CISM, CEng, CITP, FBCS, M.Inst.ISP, HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA, Myers and Stauffer LC, USA
Joshua Onome Imoniana, CGEIT, Ph.D., University of Sao Paulo, Brazil
Alisdair McKenzie, CISA, CISSP, ITCP, I S Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, JIEC Co. Ltd. (SCSK group), Japan
Ian Sanderson, CISA, CRISC, FCA, NATO, Belgium
Todd Weinman, CPS, The Weinman Group, USA
Jane Whitgift, CISM, UK
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, USA (2013-2014)
Timothy Smith, CISA, CISSP, CPA, LPL Financial, USA (2013-2014)

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

PURPOSE OF THE GUIDANCE

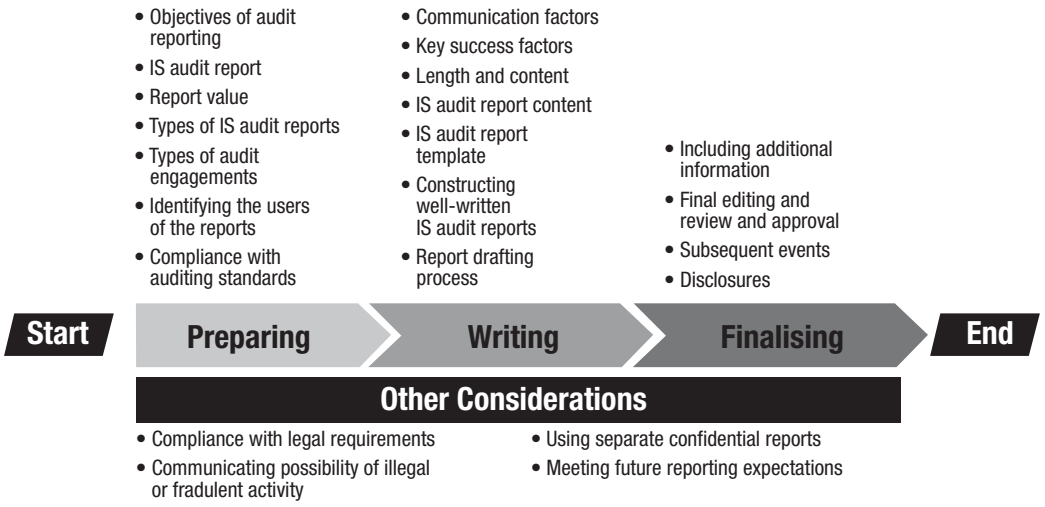
The purpose of this guidance is to assist enterprises in preparing a comprehensible, well-supported audit report that complies with the requirements of the information systems (IS) Audit and Assurance Standards and IS Audit and Assurance Guidelines that are published by ISACA. The guidance is also designed to help ensure that the summary of audit work and audit results are clearly presented and that the IS audit report presents the results of the work performed clearly, concisely and completely.

This guidance is applicable to IS audits that are performed by internal, external or government auditors, although the emphasis that is placed on report content may vary depending on the type of audit engagement and by whom it is performed. Guidance is also provided on report organisation, writing, review and editing, and presentation.

Process of Writing an IS Audit Report

The process of writing an IS audit report includes three high-level phases, as shown in **figure 1**.

Figure 1—Report Writing Phases



Each phase includes key steps to help ensure that the final IS audit report is understandable, meets the needs of its readers and complies with audit standards. To be understandable, the report must be well written and well organised. Decisions need to be made regarding language, readability, and the explanation level that is required to help the expected audience understand technical terms and the complexity of information technology (IT) systems and business processes.

To meet the needs of readers, the auditor needs to identify the audience first, and then determine how various groups of readers will use the audit report. Depending on the report distribution, the audience may have varying degrees of technical knowledge. Making the audit results understandable to each group impacts the report content and presentation. In addition, due diligence must be exercised throughout the process of writing the report to ensure the accuracy, completeness, and validity of report content; compliance with ISACA IS Audit and Assurance Standards and Guidelines and any other mandated requirements; and adherence to reporting protocols that are established by the audit organisation.

Phase One—Preparing to Write

In the first phase, **preparing to write**, the focus is on the content requirements, which are based on the type and logistics of the audit engagement, complexity of the audit subject matter, audit standards and guidelines, readership, and the important messages from the engagement. The first phase also includes determining report structure and, depending on the expected length of the report, whether an executive summary, table of contents or appendices may be needed. If the enterprise audit organisation has already established the report structure, an outline or the template that is included in this guidance can aid the auditor with the writing process. During the first phase, certain details regarding the engagement, e.g., audit entity, audit title, audit engagement number and audit period, can be inserted into the report template.

Phase Two—Writing the Report

During the **report writing phase**, specific details on audit scope, objectives, methodology, conclusions, findings and recommendations are extracted from the audit work papers and inserted into the report template. Much of the report text is also written during this phase. For example, methodology needs to be shortened into a high-level explanation of how the audit was performed; a report introduction and executive summary may need to be written; and the audit results need to be written or redrafted to include the appropriate form of conclusions and findings. The key deliverable of this phase is a formal draft report that can be presented to the auditee for their review, feedback, and provision of a management response or responses to the report's conclusions and recommendations.

Phase Three—Finalising the Report

The **report finalisation phase** prepares the final audit report for issuance to the auditee and any other designated parties. Audit management responses are inserted into the report with possible auditor replies, and final decisions are made regarding report content, reporting subsequent events or disclosures, report distribution, and compliance with audit standards and other requirements.

I. PHASE ONE—PREPARING TO WRITE

Objectives of Audit Reporting

The six objectives of audit reporting are:
1. Formally present the audit results to the auditee (and the audit client if different from the auditee).
2. Serve as formal closure of the audit engagement.
3. Provide statements of assurance and, if needed, identification of areas requiring corrective action and related recommendations.
4. Serve as a valued reference for any party researching the audit entity or audit topic.
5. Serve as the basis for a follow-up audit if audit findings were presented.
6. Promote audit credibility when well developed and well written.

The IS audit-specific **reporting objectives** are developed based on report requirements from auditee management and other users of the report and in compliance with IS audit standards and audit organisation protocols. The audit client or other stakeholders, such as oversight organisations, are identified during audit planning. The auditor develops the audit scope and objectives by considering these requirements and other elements of audit planning, such as the assessments of risk, materiality, and appropriateness of stated controls together with regulatory and IT governance requirements. The audit report formally presents the purpose and the results of the audit in line with these requirements.

Every audit report should provide **unbiased, well-supported responses to the audit's objectives**. For example, if the audit objective is to determine whether adequate controls are in effect to provide reasonable assurance that only authorised physical access can be gained to the data centre, then the report should state the auditor's conclusion or opinion as to the adequacy of the controls to achieve that objective. If controls need to be implemented or strengthened to achieve the objective, then the report should provide a recommendation to meet that need.

IS Audit Report

Reporting is an important phase of the audit process. The value of the audit is communicated to the readers of the report.

The audit report is the primary means of communicating the results of an audit to the client or auditee, oversight bodies, or other stakeholders. For some audit engagements, audit reports are also distributed to external parties, such as the general public or governmental agencies that have regulatory authority over the audit entity.

Although there are several ways that auditors can **maintain a professional level of transparency** and keep management informed regarding the scope, objectives and progress of an audit, the most important way is the formal audit report. Audit reports should assist auditees in understanding control issues, recommendations and the associated risk of not taking corrective action.

Report Value

The value of the IS audit report lies in its ability to communicate the scope, objectives, results and recommendations of the audit. The value also lies in the report's ability to provide information to persuade and assist management in reducing risk, achieving organisational objectives and taking corrective action. To do so, the content of the report must be understandable to all report users and presented in a logical order and a readable style.

The content in the audit report must be sufficiently comprehensive to allow the report to stand on its own. The value of the report rests in the auditor's ability to clearly state how the audit was performed, the findings, and the benefits of taking corrective action, if needed, and the risk of not doing so.

The audit report can fulfil other objectives, such as serving as a statement of assurance of the performance of IS operations, adequacy of internal controls, or the appropriateness of system development policies and procedures. Moreover, the report can be used to assist business process management and IS management in acquiring additional resources to support IT initiatives.

The audit report can have a **significant impact on management decisions** regarding the auditee organisation and those whom it serves. Depending on the audit scope and objectives, conclusions drawn, and the opinion provided, control practices may be enhanced, resources reallocated and performance measures recalibrated. Just as the audit engagement must be performed by competent audit staff in accordance with relevant auditing standards, so too must the development of the audit report. The **credibility of the audit engagement** itself also depends on having a well-written and properly organised audit report.

Types of IS Audit Reports

The IS audit report is driven mainly by the **type of audit engagement**—whether it is a review, an audit (examination) or an agreed-upon procedures engagement—and the reporting requirements from auditing standards. Before writing the audit report, auditors need to be familiar with the reporting requirements from the ISACA IS Audit and Assurance Standards and any other relevant audit standards. While most IS audits result in a single IS audit report, in some situations, more than one report can be applicable. For example, in addition to a report for a general audience, **a separate confidential security report** containing detailed, technical information may need to be issued to ensure that security risk is not made available to unintended parties.

The organisation and **specific content** of the report also depend on the scope and objectives of the audit engagement and the degree to which IT processes and systems are examined or require explanation. The **format and protocols** for audit report presentation can also depend on any **requirements and expectations set forth between the audit organisation and the auditee**. Requirements for audit report contents or format may be requested by the audit client who may or may not be from the same party as the auditee. By definition, the client is the party who retains, or pays for, the independent auditor to perform the audit work. In addition to requesting the type of engagement to be performed, the client may have an impact on audit evidence and the conclusions and how they are to be reported.

Although review, examination and agreed-upon procedure engagements have similar reporting requirements, each type of engagement stipulates different reporting requirements and limitations. The primary distinctions amongst reviews, examinations and agreed-upon procedures engagements are the audit objectives, the nature and extent of audit work, and the level of assurance to be provided.

While all three types of audits include review work, performing audit tests is far more prevalent in audits or examinations that require stronger evidence upon which to base an opinion. Agreed-upon procedures may also include testing, but because of other limitations, an audit opinion is not expressed. Although audit scope may be the same for reviews and examinations, scope is likely to be more narrowly defined for agreed-upon procedure audits.

Types of Audit Engagements

Review

A **review** is designed to provide **limited assurance about an assertion**. As the name implies, a review consists primarily of review work with less emphasis on testing or verification. A review can be more process oriented, focusing on the appropriateness of the tasks and activities that the audit entity performs and the associated controls. The level of evidence that is gathered is less than in an audit, and testing is generally limited or none is performed. As a result, reviews do not include audit opinions. Instead, conclusions may often be stated negatively. For example, ‘Nothing came to our attention to indicate that the assertion is not true’.

Examination

An information system audit can be performed as an examination, which is a systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an entity or event, processes, operations or internal controls, for the purpose of forming an opinion and providing a report on the degree to which the assertions conform to an identified set of standards. An examination is an attestation process that provides the highest level of assurance about an assertion that an auditor can provide. An examination encompasses gathering and evaluating sufficient, competent evidence and performing appropriate tests and other procedures to form the opinion about an assertion for presentation in an audit report.

An examination requires a higher threshold for audit evidence than a review. The audit tests, for example, can focus on a comparison of the auditee's stated and actual practices to established standards or relevant control practices.

The ISACA IS Audit and Assurance Standards require that **sufficient, relevant and reliable evidence** is obtained to support audit conclusions and opinions. The difference that distinguishes an audit from a review is that an examination (audit) includes a level of testing of audit evidence substantive enough to support verification and validity. An audit report can provide three types of opinions: unqualified, qualified and adverse. The audit report can also issue a disclaimer indicating that due to certain circumstances, such as the inability to conduct sufficient audit work or obtain sufficient, relative and valid evidence, the auditor cannot draw conclusions or render an opinion.

Agreed-upon Procedures Engagement

In **agreed-upon procedures engagements**, a third party and the auditor agree on specific procedures that will be performed to obtain the evidence on which the third party is willing to rely as a basis for a conclusion. Depending on the requirements of the third party, the agreed-upon level of evidence may be significantly limited or extensive. The auditor may need to obtain a substantial amount of evidence; in some cases, more than that is required for an audit.

According to the ISACA 'IS Audit and Assurance Guideline 2401 Reporting', the audit report should include a statement that the sufficiency of the procedures is solely the responsibility of the responsible parties and a disclaimer of responsibility for the sufficiency of those procedures. The report should also state that the report relates only to the elements specified and does not extend beyond them.

IS Audit Engagements

IS audits may be performed as a review, examination, or an agreed-upon procedures engagement, but they can be categorised in a number of ways. Although IS audits have focused increasingly on highly technical areas of IT, IS audit engagements are also often one of the following:

- General control examination or facility audit
- Application audit
- System development audit
- Technical or special topic audit

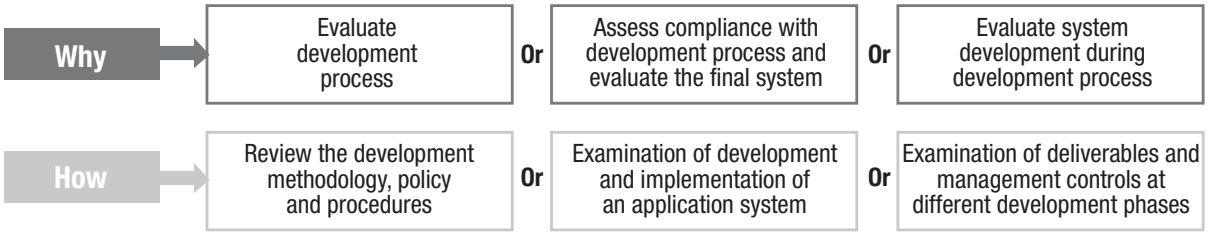
General control audits are usually examinations in which management control practices and general controls are assessed for the adequacy of their design and tested for their effectiveness. As examinations, the performed audit steps and the obtained evidence serve as a basis for audit reports to include conclusions and opinions.

Although general control audits can be limited to a single-topic area such as change control or disaster recovery, the audits typically cover several topics reflecting an array of processes or functions. It is recommended to use the audit report template that is provided in this guidance, especially for extensive (lengthy) reports that contain audit findings pertaining to different control topics. The length of a report is dependent upon the number of audit objectives and findings, requirements to explain how work was performed, complexity of the technology, and information requirements of the readers.

Although application audits typically focus on the reliability, security and availability of the system, application audits may be limited to a particular aspect of the system, such as data integrity, data storage and recovery, or operational value. From an operational perspective, the scope may include an assessment of maintainability, program change control and disaster recovery.

In the realm of system development audits, the three most common types of engagements follow and are also shown in **figure 2**:
- Review of the development methodology, policy and procedures
- Examination of development and implementation of a particular application system
- Examination of deliverables and management controls at different phases, as the system is being developed. The auditor may also serve as a **control advisor** throughout the development and implementation of an application system.

Figure 2—System Development Audit Engagement Types



Although it is possible for all of the types of system development engagements to include opinions, it is more likely that the first and third types will have conclusions, due to the targeted review work on the development process for each of the development phases.

The second type of system development engagement (the development of the system is examined) is most likely to contain an opinion, due to the scope and extent of examination. This type of system development audit combines a compliance audit (determining whether applicable system development control practices were followed) and an operations, or performance, audit (Does the system that was developed meet user needs, and is it reliable and maintainable?).

Although the drafting and issuance of IS audit reports is generally performed at the closure of the audit engagement, an exception to this practice is during the third type of system development audit, when more than one report may be issued. Depending upon the importance of the application system, size of the IT investment, associated risk, and the time period that is needed to develop and implement the system, individual audit reports pertaining to the development phases may be completed.

Technical or special topic audits tend to have more limited scopes and highly technical audit objectives. These engagements usually are more tightly focused than general control examinations and may be performed as reviews or examinations. As such, audit report content depends upon the breadth of audit scope and objectives, complexity and extent of audit work, audit evidence, required technical explanations and defined expectations of audit report users.

IS audits can also be categorised as internal control examinations, compliance audits or operational audits.

Internal Control Examinations

An IS audit can consist almost entirely of an examination of internal controls. In addition, audits that include **tests of control design** may be performed to provide sufficient, relevant and valid evidence that is necessary to support audit opinions. The tests of control design include evaluation of the design of the controls to address control objectives, verification that the controls are in place, and assessment of the operational effectiveness and efficiency of the controls.

For control examinations, the audit report conclusion or opinion needs to be based on **whether there is adequate evidence** that the combination of controls in place and in effect provide reasonable assurance that the relevant control objectives are met.

If the engagement is a review of internal controls and the report is limited to providing a conclusion on the design of controls, then care should be taken to clearly focus on the design and not to imply that the controls are effective. Unless the effectiveness of the controls is reviewed and tested, the conclusion must focus strictly on the appropriateness or quality of the control design to potentially address the related control objectives. Providing an opinion on control effectiveness requires audit evidence obtained from performing control tests.

Compliance Auditing

Each type of IS audit engagement can include **compliance auditing** if the audit determines the degree to which established policies, standards or rules are addressed or followed by the auditee. Auditors can also perform a separate engagement as a **compliance audit** that is driven from the results of their audit planning. Compliance auditing is also used extensively in performing fraud-related audit work.

Similar to other types of audits, the auditor needs to ensure that the audit report adequately identifies, in the methodology, the **criteria** that are used to perform a compliance audit. Material issues of non-compliance and fully attributed audit findings should be identified in the audit report. In the audit conclusion and audit findings, the report should provide a detailed explanation of the impact of non-compliance to persuade the auditee to implement the report recommendations.

Operational Auditing

Certain IS audits are categorised as **performance or operational audits** if the engagement focuses on an examination of all or part of an organisation or an organisational process to assess the degree of efficiency and effectiveness of operations. For an operational audit, the auditee's assertion pertains to the efficiency and effectiveness of the operational performance of a specific activity, process or program.

Considering the importance of achieving and enhancing IT value and managing enterprise risk, the audit report can require an IT governance perspective. The auditor may find persuasive arguments for corrective action within the COBIT 5 products. While overall conclusions or an opinion may be expressed, operational audit reports often report on the problems or deficiencies that are identified during the audit.

Identifying and Understanding the Users of the Report

Users

One of the key elements of communication is to know the audience. When writing an IS audit report, the interests of the readers and their ability to understand the report need to be considered. Following are **six steps** that provide an insight into the degree to which the report needs to include **explanatory information and qualitative and quantitative details**:

1. **Identify the content requirements that are mandated** by professional auditing standards and by the audit organisation. This step provides a required topic list, such as report title, audit scope and audit period. Readers who are familiar with audit reports look for required content.
2. **Identify all categories of readers,** ranging from the most immediate party that has direct responsibility over the area or entity being audited to the most distant reader who may be the general public. This step is used as the basis for readership analysis and helps to determine report distribution.
3. **Determine the interests of each category of reader.** This step ensures that appropriate information is included and useful content is not omitted.
4. **Identify the impact, on each reader category,** of a report that expresses an unqualified, qualified or adverse opinion. This step highlights the need for explanatory information or persuasive text. It identifies when additional instruction should be provided when requesting auditee responses to audit findings.
5. **Assess the ability of the reader categories to understand the material in the report.** This step impacts the need for explanatory content and inclusion of material in an appendix.
6. **Anticipate how each reader category will use the report and the information it contains.** Wide divisions on the ability to act upon the report results can highlight the need to recommend improved communication and collaboration amongst key parties.

Different parties are usually **involved** in an operational process or function that is being examined. Each of the parties can have different interests in the subject matter or the process and different communication requirements. As a general rule, when reporting on the evaluation of a given process, consider the interests of those parties who:
- Perform the functions
- Manage or are accountable for the parties performing the functions
- Maintain the tools and IT resources that are required to support the functions
- Receive, rely upon or could be adversely impacted by the services or products that are provided (or not provided) by the functions
- Measure the performance of the functions
- Assess the risk associated with the functions
- Provide internal/external oversight
- Direct, initiate or review corrective action to address failures in functions
- Allocate and approve resources to support the functions

Additional information may be needed, such as:
- For readers **unfamiliar with audit reports**, ensure that the purpose of the report is clearly identified in the signatory or transmittal page, introduction or scope paragraph.
- For readers **unfamiliar with the audit criteria** that are being cited, it is more helpful to note the value or importance of the criteria, rather than just to list the criteria.
- It may be necessary to **incorporate guidance within the finding or the recommendation** about how the reader can gain a working understanding of the criteria.
- For **web content**, include additional information or a copy of the material, because web content does not remain constant.
- If the report requires **additional persuasive information**, consider inserting specific results of audit tests, quantitative estimates of the impact of taking or not taking action, or IT configuration and operational details. Furthermore, consider how to present a convincing argument for persuading readers who may not already agree with the value of corrective action.

Distribution

The audit organisation's determination of report distribution is the list of parties to whom the issued final audit report will be directed. Unless distribution is restricted, final report copies are provided to the auditee's senior management, audit committee members, relevant business process owners, internal and external stakeholders, and oversight bodies. Governmental IS audit reports have a wider distribution, including avenues for public release, and may be available on an agency web site.

It is recommended that report distribution lists be developed early in the audit engagement process to help ensure that audit report readership is adequately identified and aligned with the list of individuals, organisations and groups, such as the general public.

Compliance With Auditing Standards

Reporting the results of audit engagements requires **compliance with auditing standards**, including ISACA IS Audit and Assurance Standards. In addition to identifying the reporting requirements of professional auditing standards, the specific reporting requirements of the audit organisation and any applicable laws or regulations need to be identified. While reporting requirements that are stipulated by laws or regulations should take precedence, due diligence and due professional care should be exercised in meeting IS audit reporting standards and related guidance.

Auditors who are holders of the Certified Information Systems Auditor® (CISA®) designation or members of ISACA, must comply with ISACA IS Audit and Assurance Standards and IS Audit and Assurance Guidelines when preparing and issuing IS audit reports. The auditor is responsible for ensuring that audit work, including audit reporting, **complies with relevant auditing standards**. Depending on the type of audit, the policies of the audit organisation, and the auditor's professional certifications, a number of auditing standards may be applicable.

ISACA designed the **IS Audit and Assurance Standards and IS Audit and Assurance Guidelines** to establish the minimum level of acceptable performance that is required to meet the professional responsibilities that are set out in the ISACA Code of Professional Ethics. Although 'IS Audit and Assurance Standard 1401 Reporting' and 'IS Audit and Assurance Guideline 2401 Reporting' are the primary standards pertaining to the development of IS audit reports, compliance with all IS Audit and Assurance Standards and Guidelines impacts the quality of audit work and the degree that the audit work and results can be used as a solid foundation for the IS audit report.

The mandatory part of the ISACA **'IS Audit and Assurance Standard 1401 Reporting'** requires IS auditors to **communicate the audit engagement's result by means of an audit report**. According to the standard, the report must include the following:

- *Identification of the enterprise, the intended recipients, and any restrictions on content and circulation*
- *The scope, engagement objectives, period of coverage, and the nature, timing and extent of the work performed*
- *The findings, conclusions and recommendations*
- *Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement*
- *Signature, date and distribution according to the terms of the audit charter or engagement letter*[1]

In addition, the standard requires that the IS auditor 'shall ensure that findings in the audit report are supported by sufficient and appropriate evidence'.[2] While more specific requirements on audit evidence can be found in ISACA 'IS Audit and Assurance Standard 1205 Evidence' and the related guideline, the quality of audit evidence also depends on adherence to auditing standards during the planning and performance of audit steps.

The 'IS Audit and Assurance Standard 1401 Reporting' includes several key aspects that impact the content of the IS audit report. For example, following is a partial list of these aspects:

- *Customise the form and content of the report to support the type of the engagement performed, such as:*
  - *Audit (direct or attest)*
  - *Review (direct or attest)*
  - *Agreed-upon procedures*
- *Describe material or significant weaknesses and their effect on the achievement of the engagement objectives in the report.*
- *Communicate significant deficiencies and material weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority, and disclose in the report that these have been communicated.*
- *Reference any separate reports in the final report.*
- *Communicate to auditee management internal control deficiencies that are less than significant but more than inconsequential. In such cases, those charged with governance or the responsible authority should be notified that such internal control deficiencies have been communicated to auditee management.*
- *Identify standards applied in conducting the engagement, and communicate any non-compliance with these standards, as applicable.*[3]

[1] ISACA, 'IS Audit and Assurance Standard 1401 Reporting', 1 November 2013, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/IS-Audit-and-Assurance-Standard-1401-Reporting.aspx*
[2] *Ibid*.
[3] *Ibid*.

ISACA **'IS Audit and Assurance Guideline 2401 Reporting'** describes the types of audit engagements and lists the required content of the audit engagement reports. An example of required content from the guideline follows:

> *A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected. In addition, the paragraph should state that projections of any evaluation of internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate. An audit engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis.*[4]

The guideline also assists the auditor in **reporting events that occur after the completion of audit field work**, but before the report is issued. If the subsequent events have a material impact on the information that is provided in the audit report, then the auditor should consider providing an explanation in the report of the events and their impact.

The 'IS Auditing and Assurance Guideline 2401 Reporting' also assists with **addressing areas where additional communication should be included** in the report. The auditor should review the elements to be included in IS audit reports, selecting those elements that apply. Element selection is impacted by the type of audit engagement, information required by the report's readership, reporting protocols that are established by the audit organisation or agreed upon with the auditee, and whether auditee responses are needed.

IS audit reports should include a statement that the audit engagement was conducted in accordance with ISACA IS Audit and Assurance Standards and IS Audit and Assurance Guidelines, if all applicable standards and guidelines were followed. If other professional standards were also followed, an appropriate reporting compliance statement for those standards should be included. It is recommended that auditors who are not holders of the CISA designation or members of ISACA consider using ISACA IS Audit and Assurance Standards and Guidelines when developing audit reports.

[4] ISACA, 'IS Audit and Assurance Guideline 2401 Reporting', 1 September 2014, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Guideline-2401-Reporting.aspx*

II. PHASE TWO—WRITING THE REPORT

Communication Factors

Well-structured and clearly written formal IS audit reports promote **audit credibility** and help the reader to understand the key points of the audit in an effective and efficient manner. Formal reporting processes incorporate stringent review and approval, editing reviews, and the exposure of draft reports to the auditees. The importance of a well-written draft report cannot be overstated.

The information in the IS audit report needs to be verifiable and presented in a constructive tone and an unbiased manner. When developing a draft report, it quickly becomes evident that the quality of the audit work papers significantly impacts the auditor's ability to write the report. Well-written reports are usually the product of properly organised, adequately documented and well-written audit work papers.

Starting with audit planning and progressing through the audit process is the continued opportunity to identify the interests and communication requirements of the report's most immediate readership. This assessment enables better determination of the language to be used, the need for defining terminology and the degree of explanation required in the report.

Key Success Factors

In addition to reporting the results of the audit, the IS audit report has objectives to provide assurance, inform auditees and others of management and control issues, recommend corrective action, and represent the quality of the audit and the credibility of the audit organisation. How the audit report is organised and written can significantly impact these objectives.

The IS audit report should assist responsible parties in understanding complex issues, enhance control and performance, manage risk, and promote good practices and solutions. Audit reports are an important vehicle to inform auditee management and other parties on best practices for governance, management and control. The report should help the reader to understand the relationship amongst the audit objectives, the auditee's operational and control objectives, and the related conclusions based on the audit.

Informative

The report should be written in a **clear, concise and persuasive** manner. It should be **informative, balanced**, and presented using language and tone that **promote the ability to understand**. The report should be professionally presented in terms of structure, format, ease of finding information and writing style. The IS audit report should be well organised and well written and present audit results in a balanced, fair and objective manner.

Logical Sequence

To be clear and concise, the report should present the material in a focused and **logical sequence**. Concise implies that words and sentences are direct and sentences are not overly wordy or too lengthy. The auditor can read the report out loud and listen to how it flows, determine whether it is free of difficult phrases, and decide if too many breaths need to be taken to complete the sentence.

Although the audit report may present material in a logical sequence and in a concise manner, it may need to be lengthy to adequately cover the audit and its results. When writing the report, the auditor should consider whether the readers are likely to spend time methodically reading and studying the report. If the report is long and contains complex issues, an executive summary can be inserted at the front of the report to assist the reader in identifying and understanding the most important messages in the report. An executive summary is usually not needed for short and concise reports.

Persuasive

To be persuasive, the report needs to be convincing. It needs to present arguments for action in a manner so that the reader understands the importance of taking action and the risk and opportunity loss of not taking action. The way in which an audit finding is attributed also helps the auditor to be persuasive, because it presents the argument for corrective action logically and informatively. By presenting a problem or deficiency and a recommendation in this manner, it can help persuade the auditee to initiate corrective action.

The auditor should consider ways that information can be presented to assist the reader in understanding the key points of the argument. The use of tables, pie charts, bar charts and other graphics to further convey information should be considered. Although the general rule is to use colour minimally, the use of colours with different fonts and font styles (bold, italics, underline) for drawing attention to key elements or highlighting information should be considered.

Sufficient Information

To determine whether the report is informative, consider whether the report provides **sufficient explanation**. To help make this decision, ask the following questions:
- What is the reader's knowledge of the subject matter?
- To what extent do the readers of the report already know about the issues?

Generally, it is a fair assumption that the more distant the readers are from the specifics, the less likely they are going to be conversant in the subject matter of the audit. However, individuals who are very close to the operations may be unaware of some of the report material; therefore, added background information can enhance the report's value.

Also consider whether additional or supplemental information can be beneficial. Providing references or copies of supplemental information in an appendix can often assist the reader in gaining a better understanding of report material. For example, although sections of an auditee response may be inserted following specific report recommendations, a full copy of the auditee response may be included in the audit report appendix for reference.

Length and Content of an IS Audit Report

The length and content of an IS audit report depend on the following:
- **Predefined requirements that are mandated** by auditing standards
- Additional requirements that are dictated by the needs of various readers
- Complexity of the material
- Reporting protocols that are established by the audit organisation

The factors that impact the content and length of the report include the following:
- Type of audit
- Complexity of entity operations and systems
- Number of audit objectives and audit findings
- Different readership categories
- Details needed to make the content understandable
- Disclosures
- Required supplemental information

Audit reports that are made available to the public are likely to contain a more detailed explanation of business operations and objectives than internal audit reports that are submitted solely to auditee management.

IS Audit Reports

This guidance pertains to IS audit reports that are **prepared at the completion of IS audits**. The reports contain the conclusions of audit work or an opinion that is related to the objectives of the audit. Auditing standards stipulate that reports contain certain information; the order and structure within which that content is presented is driven by relevant practices and the need to make reports readable and understandable.

Report structure, presentation order, appropriate terminology and formatting impact the goals to make reports readable and understandable. For example, the use of headings with recognised terms and different font sizes helps to make report information easily distinguishable and aids the reader with navigating through the report.

Most IS audit reports include the following main sections. Note that certain items are mandatory under ISACA IS Audit and Assurance Standards:

1. Title Page (report identification is mandatory)
2. Signatory and Transmittal Page (signature is mandatory)
3. Table of Contents (optional)
4. Introduction (optional)
5. Executive Summary (optional depending on the length and complexity of the report)
6. Audit Scope (mandatory)
7. Audit Objective(s) (mandatory)
8. Audit Methodology (mandatory)
9. Audit Results (mandatory depending on the results of the audit)
10. Audit Conclusion or Opinion (mandatory)
11. Recommendation (mandatory depending on the results of the audit)
12. Management Response (mandatory depending on the results of the audit)
13. Auditor Reply (optional)
14. Appendix (optional)

The ISACA **'IS Audit and Assurance Guideline 2401 Reporting'** provides details on the elements of an examination. It is recommended that the audit organisation's policies and procedures for audit reporting incorporate the requirements of the 'IS Audit and Assurance Standard 1401 Reporting' and 'IS Audit and Assurance Guideline 2401 Reporting'.

The **key outputs of audit planning** that directly impact report content are the audit scope, objectives and methodology. These audit planning deliverables should be used when developing the audit report. The audit scope and objectives from the audit work papers can be inserted into the draft report with little change. The methodology to be included in the report should be high level; therefore, detailed information does not need to be included.

If an **unqualified or clean opinion** is to be expressed, then the report is not likely to include an audit finding. However, the report can contain recommendations on less material matters and auditee comments. If the audit report **expresses a qualified or adverse opinion**, then it is likely the report will include an audit finding, recommendation, auditee response and auditor reply. An **auditor reply** should be included when the auditee response does not adequately address the recommendation or is in disagreement. The audit report may still require **additional information** to assist readers and address any disclosure requirements.

Regardless of the length of the audit report, readers need to be able to **navigate effectively** and quickly through the report. Presentation and navigational aids should be incorporated in the report to help readers quickly target the information that they need. Material within the report should be adequately cross-referenced to assist readers in accessing supportive or related information.

An audit report can also take the form of a **letter report**. The auditor may use a letter report when responding to a particular request for audit services that did **not require a full-scope, formal audit**. For example, internal audit departments are often asked to review a particular item or to test a particular set of controls. While such audit work may range from review to investigative work, the results are focused on the request for audit assistance. Under such circumstances, the auditor may choose to provide the results of the audit work in a letter report, rather than an audit report. The difference is that the letter report is shorter and is structured as a letter.

The letter report should address the **reporting requirements** that are set forth in the ISACA IS Audit and Assurance Standards. The letter report, which may acknowledge a request for audit services, should address all essential reporting requirements, such as audit scope, objectives, methodology, audit entity, period when the audit work was performed and results of the audit work.

Audit Report Template

This guidance includes an accompanying audit report template, which can be downloaded as a Microsoft Word® file from the ISACA web site. The template includes recommended standard language and identifies areas where audit-specific information should be included. Detailed information on how to complete an audit report using the template follows.

Using the IS Audit Report Template

This section provides directions on how to use the audit report template and examples where relevant.

Title Page

The following information should be included on the title page:
- Heading entitled 'Independent Auditor's Report'
- Name of the audit organisation
- Report title
- Name of the audit entity
- Audit period covered by the audit

Title pages are not used for letter reports or Internal Audit reports, which have limited distribution and contain only a few pages.

Signatory and Transmittal Page

The signatory page is usually presented on the audit organisation's letterhead. The signatory page identifies what the audit organisation is presenting in terms of the audit report. The text identifies the audit, the period when the audit work was completed, and date of report issuance, and indicates that the report contains conclusions and/or an opinion. The signatory page serves as a transmittal page when the audit report is formally transmitted from the audit organisation to the auditee and, if needed, a client.

The transmittal content on the page identifies the purpose of the audit and those to whom the report is directed. The transmittal content also includes a disclaimer of liability for the use of the report for anything other than its stated purpose.

The signatory and transmittal page also provides a statement about compliance with appropriate audit standards and that the evidence obtained provides a reasonable basis for the conclusions and any findings.

This page contains the signature of the chief audit executive of the audit organisation or firm. Because the name and/or logo of the audit organisation should also be on this page, the signatory and transmittal page can be presented on the audit organisation's letterhead.

Example:

Company ABC
123 Audit Street
City
Province/State

We are presenting the results of our IS audit on the development of the materials management and tracking system, covering the system development period of January 21, 2013 to April 9, 2014. The report includes our conclusions and opinion as to whether the system was developed in accordance with company policies and standards and applicable system development practices. In addition, we evaluated system reliability and whether adequate access security controls were in effect.

The audit was conducted in accordance with IS Audit and Assurance Standards and IS Audit and Assurance Guidelines issued by ISACA and applicable guidelines. We believe that the evidence obtained provides a reasonable basis for our conclusions and findings regarding the audit objectives.

Chief Auditor
Auditing Firm

Table of Contents

The auditor should consider inserting a table of contents to assist readers in locating information in lengthy audit reports.

A table of contents is an aid for the reader to quickly identify the scope of content or to find a particular part of the audit report. A table of contents should be used when reports are lengthy or contain a number of items in an appendix. Care should be taken to ensure that the section and subsection title exactly match those contained in the report.

Introduction

Although a separate introduction is not a required element of an audit report, an introduction can enhance the ability to understand reports that will be read by individuals who are unfamiliar with the audit entity or the subject of the audit. The introduction section provides external readers with sufficient information regarding the type of audit entity, its mission and primary business objectives, and the purpose of application systems and supporting technology that was subject to audit.

Typically, an introduction is useful for IS audit reports whose readership likely includes oversight authorities, legislative bodies, government agencies, organisations independent of the audit entity and the general public. An introduction may also be useful for internal audit reports if departments in an organisation may be unfamiliar with the audit entity/technology.

The introduction provides a high-level explanation of the audit entity with respect to its mission, primary business objectives, customer/client base and location and a high-level description of the IT infrastructure applicable to the audit. The introduction may include a high-level statement of the purpose of the audit to support the understanding of external readers of the report.

Executive Summary

An executive summary is an excellent way to present summary information if reports are lengthy and/or complex. The executive summary typically includes a high-level description of the primary message of the report, key audit objectives and a brief summary of audit results. Although an executive summary can be used to persuade management to take corrective action, it should not be used to sensationalise audit results. Rather, it should be informative and to the point.

Example:

We have completed our IS audit, which covered the period of July 1, 2013 through October 15, 2013, for access security, business continuity planning, physical security and environmental protection over the company's data centres.

The results of our IS audit indicated that while certain controls were in place, control deficiencies in access security and business continuity place the company at undue risk. Based on our audit, adequate controls were found to be in effect to provide reasonable assurance that IT-related resources were properly recorded and safeguarded from damage or loss.

Our examination of the primary and alternate processing facilities confirmed that adequate physical security and environmental protection controls were in effect and that IT operations were well managed. However, our audit revealed that additional system access security controls needed to be implemented to strengthen protection over company records and customer information.

Although control practices were in place for offsite storage of backup copies of applications and data files, business continuity planning needed to be strengthened to ensure required availability of automated systems and compliance with regulations. We also noted that documented policies and procedures regarding network security, data classification and deactivating user accounts needed to be updated to reflect the company's current technology.

Our recommendations focused on enhancing administrative and technical controls for access security and disaster recovery testing for mission-critical and essential systems. Although departmental and IT management have agreed with the audit recommendations and are developing plans to address control areas, resource allocations may need to be better aligned to these high-risk functions.

Audit Scope

The audit scope is a statement of the audit subject; essentially, the type of audit and what is being audited. The audit scope identifies the authority to perform the audit, the name of the auditee organisation and audit entity, and the period covered by the audit. The audit entity can be an organisation, a division within the organisation, a business process, an application system or supporting technology, such as a particular platform or network. The audit period specifies the start date and end date of the period of time to which the audit work relates and from which audit evidence is obtained.

To a knowledgeable reader, audit scope should indicate the expected breadth of audit work and topic areas covered by the audit. For example, if the audit covered environmental protection, the exclusion of fire prevention, detection and suppression should be identified under audit scope. The audit scope should identify any limitations or topic areas not included in the audit that the readership will likely think should be included in the audit.

The scope section should indicate the relevant body of auditing standards that governed the audit work. The auditor may use the methodology section to expand upon the auditing standards and guidelines that were followed in concert with the identification of audit criteria. Typically, the length of the audit scope section is less than a page and comprised of one or two paragraphs.

Example:

> In accordance with the audit services agreement, we performed an application audit of the accounting information system at ABC International Manufacturing for the period of February 1, 2013 to December 31, 2013. The scope of our audit consisted of an evaluation of data and processing integrity for the application's sales and collection process.
>
> The audit, which was conducted from February 26, 2014 to March 28, 2014, included an examination of application controls and general controls that are related to system security, change control and business continuity planning. The audit also included a follow-up review of prior audit findings from Internal Audit Report Number xy-xy12, dated March 15, 2013, regarding program change control and disaster recovery testing.
>
> The audit was conducted in accordance with the IS Audit and Assurance Standards and IS Audit and Assurance Guidelines of ISACA and other applicable auditing standards. Those standards require that the audit be planned and performed to obtain sufficient, relevant and valid evidence to provide a reasonable basis for the conclusions, opinion and audit findings.

Audit Objectives

The audit objectives section identifies the items to be evaluated or assessed by the audit. Depending on the scope of audit, several audit objectives may be identified. It is important to note that these are high-level audit objectives and not detailed objectives that are related to specific audit procedures. The auditor needs to consider whether the audit objectives can be presented in hierarchical terms, presenting the uppermost audit objective first with secondary objectives to follow. It is suggested that separate paragraphs be used to group the uppermost and secondary audit objectives together.

When writing an audit objective, be careful to not imply that the auditor is responsible for internal control. That is auditee management's responsibility. While an audit objective may be phrased as a question to be answered by the audit, audit objectives are most commonly phrased as, 'to determine whether' or, for example, 'to assess the adequacy of internal controls'. It is incorrect to phrase the audit objective as, 'to ensure that appropriate controls are in effect', because this is auditee management's responsibility. For example, the role of the auditor is, 'to determine whether appropriate controls are in effect' and then provide a statement of assurance as to whether that is the case. If the audit objectives are properly written during audit planning, then they can be inserted directly into the audit report.

The statements of audit objectives depend on the type and scope of the audit. If the auditee's control objective is to ensure that all changes are authorised and tested, then the audit objective is, 'To determine whether adequate controls were in effect to provide reasonable assurance that all changes are authorised and tested'.

Numbering objectives is helpful for more than three to four objectives. Also, secondary objectives should be identified.

Example:

> Our **primary** audit objective was to determine whether the company's IT-related internal control environment, including policies, procedures, practices and organisational structure, provided reasonable assurance that IT-related control objectives can be met to support business functions.
>
> Our objective regarding system access security was to determine whether adequate controls were in effect to provide reasonable assurance that only authorised personnel had access to automated systems and that password administration was appropriately monitored by management.
>
> In addition, we determined whether adequate disaster recovery and business continuity plans, including onsite and offsite storage of backup media, were in place to provide reasonable assurance that mission-critical and essential operations could be regained within an acceptable period of time should IT functions be rendered inoperable or inaccessible.

Audit Methodology

The audit methodology should provide a high-level explanation of how the audit was performed for each audit objective. The methodology should identify the nature and extent of audit work, audit criteria, sources of audit criteria, whether reliance was placed upon the work of other professionals, the type of analysis performed, and the basis for conclusions drawn. The methodology is not intended to be a detailed description of an audit work program.

The explanation of methodology provides the reader with an understanding of the procedures that were performed to obtain the evidence that was needed to address the audit objectives and the subsequent nature of the assurance that is conveyed by the audit report.

The report should state that a management representation letter was obtained from the auditee acknowledging management's responsibility for establishing and maintaining an effective system of internal control to achieve operational objectives, manage risk, and comply with legal requirements.

The management representation letter should also state that all information that is relevant to the audit was provided in a timely manner to the auditors and that access to policies and procedures, systems of record, electronic systems and files, reports of activities, other audit reports, and personnel was not restricted. This information may also be covered under disclosures.

The methodology should identify whether the work of other auditors or professionals was relied upon and the extent to which such reliance was made.

The audit methodology identifies audit planning and audit engagement procedures. For example, the report can state that to determine audit scope and objectives, audit planning steps included obtaining and recording an understanding of the auditee's mission, relevant business operations, and supporting technology, and legal and regulatory requirements. The methodology is generally limited to including high-level statements of audit procedures, such as, 'We conducted site visits of business and IT operational areas and performed a high-level risk assessment'. The methodology section also indicates the auditing standards followed and any significant audit criteria used.

Example:

1. To determine audit scope and objectives, we performed audit planning steps, which included obtaining and recording an understanding of the company's mission, relevant business operations and supporting technology. We identified the auditee's operational, legal and regulatory requirements and IT infrastructure, by reviewing relevant documentation and conducting interviews with auditee management. We conducted site visits of business and IT operational areas and performed a high-level risk assessment.

2. As part of audit planning, we reviewed policies, procedures, and contracts with third parties; identified critical success factors for IT operations; confirmed control objectives; identified audit criteria; assessed materiality; and determined the appropriateness of stated controls. Through interviews, we gained an understanding of the IT that was used to support business operations. We documented the significant functions and activities that were supported by network services and the automated systems. We developed audit objectives in relation to the identified control and operational objectives and developed our audit strategy in relation to the audit's scope and objectives.

3. We evaluated IT management controls and the degree to which IT strategic planning was aligned with business strategy. We reviewed relevant policies and procedures, assigned responsibilities and point of accountability, reporting lines, and IT-related job descriptions. We determined whether the policies and procedures provided management and users with sufficient standards and guidelines to describe, review, and comply with company directives, legal requirements, and generally accepted control objectives for IT operations and security.

4. To determine whether adequate controls were in effect to prevent and detect unauthorised access to the areas housing IT resources, we evaluated security policies and procedures and tested controls to prevent and detect unauthorised access to secure areas. We reviewed physical security over the administrative offices, data centre and central computer room, file server rooms, and secure storage areas. Our audit included tests of locking devices and alarms, review of lists of authorised personal, ID badges, and surveillance cameras and monitoring. We interviewed department managers, users, IT staff and security personnel.

5. With respect to system access security, we reviewed access privileges of employees who were authorised to access the network and associated application systems. To determine whether control practices regarding system access security adequately prevented unauthorised access to automated systems, we evaluated policies and procedures regarding system access and data security. We reviewed security practices with IT security personnel and selected departmental managers. Because single sign-on capabilities were not in place, we evaluated selected network access controls and access to applications that were available through the network. Moreover, we determined whether the administration of logon ID and passwords was being properly carried out by reviewing onboarding controls, user account review, authentication procedures and mechanisms, and whether user accounts were deactivated in a timely manner should access no longer be required or authorised. In addition, we reviewed logging capabilities and whether adequate security devices and applications were in effect to detect unauthorised access to the network or application systems. We also reviewed the company's draft policies and procedures for providing security over data in transit or at rest.

Audit Conclusion or Opinion

The purpose of this section is to provide an overall conclusion or opinion with respect to the engagement's audit objectives.

For audits that meet the requirements of obtaining sufficient, relevant and reliable evidence and have complied with other auditing standards, the audit reports generally include either an opinion or a disclaimer. A disclaimer states that an opinion could not be provided due to limitations of audit procedures and audit evidence.

Opinions can be one of **three** types:

- **Unqualified Opinion:** An unqualified opinion is presented when the audit evidence substantially reflects what is expected to be in place and in effect, according to the audit criteria. Regarding internal control, the 'IS Audit and Assurance Guideline 2401 Reporting' states that an unqualified opinion is expressed when the auditor concludes, 'in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective, in accordance with the applicable criteria'. Essentially, the unqualified opinion represents a 'clean bill of health' with respect to the audit objectives.

  It is important to convey to the reader that the unqualified opinion relates only to the audit subject. An unqualified opinion is not a statement of assurance that all processes and systems in the organisation are fine.

- **Qualified Opinion:** A qualified opinion is presented when the audit evidence substantially reflects what is expected, except for a deficiency that, on its own, does not render an adverse result. According to the same audit guideline, a qualified opinion may be expressed if the auditor is, 'unable to obtain sufficient and appropriate evidence on which to base an opinion, but concludes that the possible effects on the IS audit objectives of undetected weaknesses, if any, could be material but not pervasive'.

  The audit report should include an explanatory paragraph stating the reasons why a qualified opinion is expressed in the report. It is recommended to present this as a separate paragraph, directly before the qualified opinion. If the qualification is due to a limitation of scope, then the scope paragraph should inform the reader of the qualification. Language such as, 'Except as presented in the following paragraph, we conducted the audit in accordance with . . .', can be inserted in the scope paragraph. This informs the reader that, in all other areas, the audit work was performed without qualifications.

- **Adverse Opinion:** An adverse opinion is presented when the audit evidence substantially reflects a material difference from what is expected to be in place and in effect, according to the audit criteria. From an internal control perspective, an adverse opinion is expressed when adequate controls are not in place or in effect to provide reasonable assurance that control objectives are met, or that there is a reasonable likelihood that the control objectives are not met.

Disclaimer
A disclaimer is a statement that an opinion cannot be rendered due to the lack of sufficient, relevant and valid evidence upon which to base an opinion. According to 'IS Audit and Assurance Guideline 2401 Reporting', a disclaimer is generally expressed when the auditor also concludes, 'the possible effects on the IS audit objectives of undetected weaknesses, if any, could be material and pervasive'.

Examples:

Unqualified opinion:
Based on our audit, we found that IT resources, including the file servers and workstations installed at the administrative office and throughout the operations areas, were adequately safeguarded, environmentally protected and properly accounted for. We determined that appropriate control practices regarding login ID and password administration were in effect to help provide reasonable assurance that only authorised parties could access network resources and the accounting information system.

Qualified opinion:
In our opinion, except for the need to strengthen physical security over offsite storage of backup media, adequate controls were in place and in effect to provide reasonable assurance that automated systems could be recovered within an acceptable period of time should IT capabilities be rendered inoperable or inaccessible.

Although we found that there were documented controls regarding business continuity planning, such as the designation of alternate processing sites, the company needs to strengthen controls, in conjunction with third-party support services, to provide reasonable assurance that normal business operations could be resumed in a timely manner should IT capabilities be unavailable for an extended period. Moreover, we determined that physical security and administrative control over offsite storage needed to be strengthened to safeguard and account for backup media and archival media.

Adverse opinion:
Based on our audit, adequate controls were not in place or in effect to provide reasonable assurance that control objectives would be met for system access security, IT inventory control and configuration management, and disaster recovery and business continuity planning. Adequate controls and assurance mechanisms were not in place to provide reasonable assurance that control objectives would be met regarding the integrity, security, and availability of information systems processing and data management.

We found that controls needed to be strengthened to provide reasonable assurance that user IDs and passwords would be active for only authorised personnel and that appropriate password standards would be followed. Security access privileges should be deactivated in a timely manner for users who no longer needed or were authorised to access to information systems.

Audit Results

The purpose of this section is to provide a more detailed explanation of the engagement audit findings. The overall conclusion or opinion of the audit determines whether the report should contain an audit results section. If the report contains an unqualified opinion, then it is unlikely that audit findings are included. For reports containing qualified or adverse opinion, audit findings are included.

Audit findings are provided in the audit report when action is required to correct a deficiency in a process or its related controls. As a general rule, the audit report includes audit findings for reports with qualified opinions or adverse opinions. Five key elements, or attributes, need to be addressed when presenting an audit finding, as detailed in **figure 3**. The five attributes of an audit finding are: condition, criteria, cause, effect and recommendation.

Figure 3—Five Attributes of an Audit Finding

Attribute	Description	Identifies
Condition	Findings	Identifies the auditor findings. It is a statement of the problem or deficiency. This may be in terms such as control weaknesses, operational problems, or non-compliance with management or legal requirements.
Criteria	Requirements and baseline	Statement of requirements and identification of the baseline that was used for comparison against the auditor findings, based on the audit evidence.
Cause	Reason for the condition	While the explanation of the cause may require the identification of the responsible party, it is suggested that, unless required by audit policy, the report should identify the organisational business unit or person's title and not the individual's name. The same should be applied to the identification of the person representing the relevant point of accountability.
Effect	Impact of the condition	The statement of impact answers the question 'so what?' It explains the adverse impact to the operational or control objective. By articulating impact and risk, element of effect is very important in helping to persuade auditee management to take corrective action.
Recommendation	Suggested corrective action	While the corrective action should eliminate the problem or deficiency noted in the condition, the corrective action should be directed towards addressing the cause.

The auditor should provide fully attributed findings if there are material weaknesses in internal control. This means that audit findings have been fully attributed in the audit work papers. As such, all five attributes need to be included to have an audit finding in the audit report. Note that because several attributed findings may be combined into a high-level audit finding, or audit result, the related attributes need to be developed.

A recommended presentation of the audit finding is a title of the audit topic area, followed by one or more paragraphs explaining the condition, criteria, cause and effect, followed by a clear statement of recommendation.

The formal draft report articulates the audit finding, which includes the recommendation. Because the auditee should be provided the opportunity to respond to the overall audit and to the specific audit findings and their specific associated recommendations, the final audit report can only be prepared after the auditee's management response has been received. At that time, the auditor can insert the auditee response directly after the recommendation and insert an auditor's reply.

The auditor's reply may need to be included under the following circumstances:
- Management response indicates disagreement with the finding or recommendation.
- Management response does not fully address the corrective action as recommended by the auditor.

Example:

Disaster Recovery and Business Continuity Planning
Our audit disclosed that the company would be unable to recover its network and automated systems within an acceptable period of time should IT capabilities be rendered inoperable. Although backup copies of application software and data files are stored in secure onsite and offsite facilities, recovery strategies for different disaster scenarios have not been developed and documented in a disaster recovery plan. Although IT management believes that they could recover the company's systems at the designated alternative processing site, no disaster recovery tests have been performed. **[Condition]**

The procedures for onsite and offsite storage of backup copies of magnetic media were found to be adequately detailed, and appropriate physical security and environmental controls were in effect for the onsite and offsite storage locations. In addition, we confirmed that the alternative processing site housed a similar IT configuration as the primary site. **[Condition]**

Depending on the nature and extent of a loss of IT processing capabilities, the company could experience significant difficulties in regaining mission-critical and essential business processes within an acceptable period of time and without an adverse financial impact. It is also likely that a prolonged absence of business operations would result in the loss of long-term customers who are dependent on continued business support. **[Effect or Impact]**

The company needs to perform a business impact analysis to identify mission-critical systems and identify required recovery points, document all potential disaster scenarios, develop a comprehensive disaster recovery plan, and review and test the recovery strategies. The disaster recovery and business continuity plans should include procedures for employee and customer notification, relocation of IT personnel and essential staff, accessing backup media, establishing security at the alternative processing site, establishing network access, and recovering mission-critical and essential application systems. User area plans should include documented procedures for each business function to follow to restore or continue business activities should automated systems be inoperable or unavailable for an extended time. **[Criteria]**

The objective of business continuity planning is to help ensure that mission-critical and essential business functions can be regained within an acceptable period of time should a disaster cause significant disruption or loss of IT capabilities. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. Disaster recovery and business continuity planning should be viewed as a process to be incorporated within the business enterprise, rather than as a project completed upon the drafting of a written recovery plan. Because the factors that impact recovery requirements and the criticality of systems may change, a process should be in place to identify such changes and modify and verify recovery plans accordingly. Business continuity requirements should be reviewed periodically or upon major changes to user requirements regarding the automated systems. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans. **[Criteria]**

While management acknowledged that disaster recovery was important, responsibilities for business continuity planning had not been assigned and IT policies and procedures were limited to the generation and storage of backup media and designating an alternate processing site. We also found that risk management did not address the loss of IT capabilities. **[Cause**]

Recommendation:
We recommend that to strengthen disaster recovery and business continuity planning, the company should:
- Assign disaster recovery responsibilities and establish a single point of accountability for disaster recovery and business continuity planning.
- Document all potential disaster scenarios that would result in IT capabilities being rendered inoperable or inaccessible.
- Expand existing operational and risk management policies to incorporate a business continuity framework and disaster recovery from an enterprise and IT perspective.
- Establish policies and procedures to ensure that disaster recovery and business continuity plans are re-assessed, updated and tested based on changes to underlying factors and a scheduled timetable.
- Perform business impact analysis and establish required recovery time periods for IT capabilities and application systems.
- Develop a documented disaster recovery plan, including business and IT recovery strategies.
- Test and verify the viability of recovery strategies.
- Ensure that management and staff are adequately trained to effectively execute disaster recovery and business continuity tasks and activities.

Auditee's Response
We have assigned disaster recovery responsibilities to the IT department and rectified, or are currently rectifying, any and all shortcomings that were listed in your IS audit. We are also strengthening existing and implementing controls to address business continuity planning. We will test recovery strategies within the next three months.

Auditor's Reply
We are pleased that corrective action is being initiated to strengthen disaster recovery and business continuity planning. We reiterate the need to establish a single point of accountability and to enhance enterprise risk management to address disaster recovery and business continuity.

Constructing Well-written IS Audit Reports

A good audit report contains precise and concise facts that are easily understood by the readers. In addition to terminology, language, report structure, content requirements and protocol, sentence structure and punctuation are also important considerations. To do this requires more than avoiding technical jargon, slang, complex vocabulary or overly lengthy complex sentences. If a report is misunderstood, it may be discarded, or needed action may not be taken.

Key Rules

Following are key rules of writing that can aid in constructing well-written audit reports.

1. **Avoid technical jargon,** colloquiums or words that the readership is unlikely to fully understand. For technical terms, include a definition or explanation within the text or glossary.

   Ensure that a **logical connection exists in compound phrases** that are joined by 'and', 'or', or 'but'. Avoid mixed constructions where the combinations of words, or word groups, are not grammatically correct or meaningful.

   Example: 'The belief in tighter safeguards promoted enhanced security features in the system'. This is an example of a mismatched subject and transitive verb. The sentence implies that the belief promoted the enhanced security features, but the belief caused management to implement enhanced security features.
2. **Avoid faulty predication** of mismatching a subject with a predicate noun.

   Example: 'The difficulty of deactivating user accounts is the primary worry of the security administrator'. This is an example of a faulty predication, and implies that a difficulty is a worry. Instead, the difficulty is the reason for the worry. The sentence can be changed to, 'The difficulty of deactivating user accounts is the reason for the security administrator's primary worry'.
3. **Use noun markers** like *much* and *less* before nouns that refer to things that cannot be counted. Use *many, few* and *fewer* before nouns that identify a specific number or objects that can be counted.
4. **Ensure that adjective phrases are hyphenated.**

   Examples: 'The manager presented a well-established procedure for reconciling the account'. The hyphens link the words to form a single modifier.
5. **Avoid overusing nouns.** Sentences containing several nouns can be confusing to the reader. Be careful not to use nouns inappropriately as modifiers.
6. **Avoid the double negatives** trap. A double negative may cause the intended meaning to be negated or it may confuse the reader. When the resulting, or potential, adverse impact is significant, it might be tempting to overuse negative meaning words, such as never, not, none, neither, nothing and nor.

   Example: 'Users could not hardly understand the new security policies'. This is an example of the use of double negatives. The sentence can be changed to, 'Users could hardly understand the new security policies' or 'Users could not understand the new security policies'.
7. **Avoid abbreviating comparisons or mismatching superlatives.** Audit reports are likely to contain comparisons when there are audit findings. Ensure that comparatives and superlatives are used correctly when using adjectives and adverbs. Regarding comparatives or superlatives, avoid using '–er' and 'more', or '–est' and 'most', at the same time.

   Example: 'A password comprised of alpha-numeric and special characters is stronger'. This example illustrates abbreviation of a comparison. In the absence of a prior sentence that referred to a password using just alpha characters, or completion of the sentence with a similar reference, the reader is left to guess the full meaning. Unless a sentence is inserted before, the sentence should be changed to, 'A password comprised of alpha-numeric and special characters is stronger than a password comprised of alpha characters'.
8. **Avoid using one or two commas to set off an essential modifier** that is required for the meaning of the sentence.

   The intended meaning of the sentence can be obscured or lost through the improper use of commas. If an editor is unaware of the intended meaning, improperly inserted commas may not be removed, or an editor's newly inserted commas may alter the meaning of the sentence. This risk can be mitigated through an **iterative review and approval process** between the auditor and the editor.

9. As a general rule, **avoid having one or two words between the word 'to' and the verb.** Dividing the word 'to' from the verb, which is referred to as a split infinitive, can lead to confusion or misinterpretation.

   Example: 'The auditor's effort was to quickly and thoroughly verify the numbers'. This is an example of a split infinitive. This sentence can be changed to, 'The auditor's effort was to verify the numbers quickly and thoroughly'.
10. **Avoid misplaced modifiers.** Misinterpretation can result if modifiers are separated from the very words they are intended to modify, or if the intended word is missing.

    Example: 'Changing passwords quickly reduces the threat of unauthorised access'. This is an example of a misplaced modifier. Here the reader would not know whether quickly pertained to changing or reduces. If the intent is to emphasise timely password changes, then the sentence can be changed to, 'Quickly changing passwords reduces the threat of unauthorised access'.
11. Ensure that **appropriate co-ordinating links (e.g., 'and', 'or', 'therefore' or 'however') are used to join independent clauses** when writing compound sentences. This can strengthen a logical sequence and improve the overall flow. Be careful not to overuse the word 'and', because sentences containing too many 'and' words can be confusing to the reader.

Follow these steps to ensure that the report is understandable and well written:
- The content, in terms of stated facts and numbers, should be double-checked and reviewed by another individual. Nothing can hurt the credibility of an audit report like inaccurate numbers, incorrect references and misstatements.
- Read sections of the report in reverse order to focus on stated facts and identify misspellings.
- Read the report out loud to hear (and feel) how it sounds. This technique is useful when assessing the flow of logic and wording.

Report Drafting Process

By adopting a defined template, auditors can begin to populate the template as the audit proceeds, after finalising the audit planning or pre-audit phase. At this point, auditors have defined, and obtained review and approval of, the audit scope, audit period, audit objectives and audit strategy. While some changes may be warranted as the audit proceeds, the sections of the report pertaining to these items can be written.

Guideposts for Writing Effective IS Audit Reports

- Start with a simple, preliminary outline when audit planning is complete (use the template that is provided with this guidance).
- Insert any information that is already established, such as identification of auditee, audit entity, report title, audit number, statement of scope and audit objectives.
- Develop a first draft of the introduction and insert the auditee and audit entity information.
- Develop a more detailed outline as specific content areas that are relevant to the type of audit are inserted and there is a need to provide further information to the readership.
- Summarise and insert the audit strategy in the audit methodology section as field work is completed on topic areas.
- Make the audit report easy to navigate by using numbered headings, page references and a table of contents.
- Identify acronyms; do not assume that every reader knows all of the acronyms.
- Write the material in the work papers in a manner that can be inserted into a report.
- Ensure that the audit report is supported by the evidence that is obtained during the audit and documented in the working papers. This can be performed by referencing supporting evidence from the working papers in the audit report.
- Have the report references validated, preferably by an individual who is not involved in performing the audit.
- Insert in the report explanations of audit work, where needed, conclusions, and the text of audit findings from work papers.
- Read the report out loud—hear how it sounds. Does it flow properly? Do not use language that can be considered pretentious or arrogant. The language should be instructional without speaking down to the reader. Try not to mimic the sources of criteria.
- Place key points at the beginning of paragraphs, not buried within the paragraphs.
- Use sentence structure to emphasise points, vary sentence length and use short sentences to emphasise.

- Try to grab the reader's attention; try to keep the report interesting.
- Stay grounded to the evidence; do not include editorial commentary.
- Keep the report balanced in content and tone; do not get personal.
- Arrange information in a logical manner.
- Use graphics to supplement the text, but not as a complete substitute.
- Keep in mind Aristotle's three appeals that communicators use to increase the effectiveness of the message: Logos—the appeal to reason supported by appropriate and valid evidence; Ethos—the appeal of the communicator's trustworthiness and credibility; and Pathos—the appeal to value and beliefs as expressed by relevant examples and details.
- Read it out loud at a normal reading speed (more than once).
- Have an individual who is not involved in the audit read the report from the perspective of a report recipient.
- Make sure that all information presented is absolutely correct.
- Do not rely entirely on spell checks. Complete a 'hard' read to detect spelling, numerical or other errors.
- Be respectful in language and presentation of formal draft reports and final release versions.

It is recommended that **audit reports identify responsible parties by their title or position**. Depending on the distribution of the report, it is generally not a good practice to identify by name the actual individuals, especially if they hold mid-management, supervisory or staff positions. For audit reports that are issued for external or public distribution, unless otherwise required, the auditor should identify the title of the position that is held by the responsible party.

One of the most valuable steps in the final preparation of an audit report is submitting the formal draft report to the auditee for review and response. This step continues the interactive communication between the auditor and the auditee with discussion, confirmation, and feedback on audit topics, control objectives, controls, and possible corrective actions if deficiencies have been detected. The communication process becomes more focused at the **informal exit**, which is held at the end of audit field work, when potential conclusions and recommendations are discussed.

The **formal exit conference** provides a valuable opportunity to discuss the formal draft report with auditee management. This is the time to solicit feedback regarding the audit and the report recommendations prior to issuing the report. At this conference, the results of the audit and instructions for soliciting management's written response are presented, including the following:

- Restating the audit objectives
- Presenting the conclusions, opinion, audit findings and recommendations
- Highlighting the structure of the report to assist the auditee review
- Indicating areas where the auditee's careful review and feedback is helpful to ensure that information regarding the entity has not changed and is correct
- Pointing out sections of the report where an auditee response is being requested
- Addressing and resolving any areas of auditee disagreement with the report facts and/or recommendations

Formal Draft Report

At the formal exit conference, the auditee is presented with a **formal draft report**. The auditee can see the items that are being discussed at the informal exit. It is very important that the tone and content of the written report reflects the information that is stated at the informal exit. If conclusions or other materials have changed, then the auditor should explain the differences and the reasons for the change.

Cover Letter or Memo

It is recommended that a cover letter or memorandum is attached to the formal draft report. The cover letter should state that the audit report that is being submitted is a formal draft, and that the auditee is provided the opportunity to review the report for any inaccuracies and comment in writing on the audit report. Request the auditee to respond to the audit findings and recommendations, in particular.

The letter should explain that the auditee should include corrective actions that they will take to address the recommendations and the time period by which they will be completed. The cover letter should also include the date by which the responses are to be submitted to the auditor.

III. PHASE THREE—FINALISING THE REPORT

Including Additional Information

During this phase, additional information is included in the audit report. Because the formal draft report did not include management responses to the audit or audit findings, this information is inserted at this time. In addition, if needed, auditor replies are included to acknowledge corrective action that was taken or is planned, or identify any results or recommendations in the audit report that management responses did not address. Other additional information includes a description of subsequent events that may be material to the audit, items to be inserted in an appendix and any additional disclosures.

Final Editing, Review and Approval

Because the audit work and the final draft audit report that was submitted to the auditee have already undergone audit management review and approval, extensive changes to be report are unlikely to be needed. However, new information was added while finalising the report, and depending on the feedback received from the auditee, certain parts of the report may need to be re-written to strengthen the report. After the additional information is included and any changes are made, the audit report should be subject to a final review by senior audit management before the report is issued. If extensive changes were made to the text or difficult concepts were added, the report may require an additional editing review prior to the senior management review and approval.

Subsequent Events

The final audit report should include information pertaining to any events that occurred after the audit field work was completed and before the audit report is issued that have a material impact on the report subject matter and require amendment or disclosure regarding the subject matter. Although the auditor is not responsible for detecting subsequent events, it is advisable to inquire with auditee management about subsequent events that may be material to the audit subject matter.

While the integrity of the audit work, including conclusions and expressions of opinion, are not diminished by subsequent events, disclosure of material events and adjustment to report content, especially regarding recommendations, enhances the usefulness of the final audit report.

Disclosures

If matters regarding material deficiencies in control were brought to the attention of individuals who were responsible for governance during the course of the audit, the report should disclose such communications. The report should also disclose any qualifications or limitations in scope or audit work that was performed during the audit.

Further explanations may be needed regarding reportable items, efforts taken to avoid impairments, events subsequent to the audit, etc.

During the audit, IS auditors may discover certain conditions that can impact control or operational risk, such as discrepancies in recordkeeping, unsupported transactions, conflicting audit evidence or problematic matters. The latter can include difficulties in obtaining evidence, conducting interviews or performing audit tests.

Page intentionally left blank

IV. OTHER CONSIDERATIONS FOR REPORT DISTRIBUTION

Compliance With Legal Requirements

Laws and regulations impact the **responsibilities of the organisations** that are being audited and the **responsibilities of the auditor**. Legal requirements that are incorporated within a contract for audit services, laws and regulations may impact the auditor's responsibility for audit work, especially for reporting.

Information to Include in the Final Report

For certain types of audits, the auditor may be required to include very specific information in the final audit report. For example, in the United States, auditors who are reporting on the single audit are required to **issue an opinion, or disclaimer of opinion**, on the financial statements and supplementary schedule of expenditures for federal grants. Under the same single audit, the auditors are required to provide a **report on internal control over financial reporting** and other matters, which is based on the audit that is performed in accordance with 'Government Auditing Standards'.[5]

IS Audits

Audit report content may be extended to include **internal controls over IT systems** that support financial reporting and business operations, reporting on regulatory compliance, and reporting on potential illegal acts that were detected during the audit. In addition, deadlines by which audit reports must be issued may be detailed in government regulations. Because IS audits are usually focused on complex or new technology, the audit reports may require further explanation and a glossary of terms. An additional concern may involve how legal terms are defined from jurisdiction to jurisdiction. For example, the key elements of fraud are not exactly the same in all countries and jurisdictions.

Identify Legally Mandated Reporting Requirements

Laws and regulations vary across the globe. While the identification of applicable law may extend over municipal, state, provincial and federal law, the auditor should ensure that reporting guidelines that are promulgated by oversight authorities are also included. Even if the auditor is versed in performing legal research, legal services may be needed to ensure that legally-mandated reporting requirements are identified and correctly interpreted. For audits that involve government expenditures, subsidies and grants, granting authorities can have reporting guidelines that need to be addressed. The same body of law that was initially identified regarding the responsibilities of the organisation being audited can be an excellent starting point to identify reporting requirements.

Communicating Possibility of Illegal or Fraudulent Activity

Reporting protocols and requirements regarding possible illegal acts and fraudulent activity should be established by the audit organisation. If, during the course of the audit, sufficient evidence indicates that illegal acts or fraud have occurred, are occurring, or are likely to occur, then these concerns should be reported to **audit management** and **appropriate parties**, which may **include law enforcement**.

When and to Whom to Report Possible Fraud

It is extremely important to ensure that any reporting of possible illegal activity is not construed as the auditor's legal opinion. Even if the auditor were an officer of the court, an explicit determination by the auditor is inappropriate. If, in the course of performing audit steps that are designed to detect fraud, the evidence demonstrated a reasonable likelihood that illegal acts or fraud had or were occurring, then there may be sufficient predication on the part of management or law enforcement to initiate an investigation. At this juncture, reporting protocols are extremely important and additional considerations regarding audit evidence come into effect.

[5] U.S. Government Accountability Office, 'Government Auditing Standards', December 2011, *http://www.gao.gov/assets/590/587281.pdf*

The general requirement placed on the auditor is that evidence of illegal or fraudulent activity should be brought to the attention of entity management. The identification of fraudulent activity during an audit can be based on a number of factors. In addition to performing audit steps that are designed to detect fraud, fraudulent activity may be discovered while reviewing documentation or even through anonymous tips. Because timely notification is crucial to determine predication, initiate an investigation, and deter further exposure, the auditor should not delay informing management of indications of fraudulent activity or wait until a draft report is prepared.

What Is Fraud?

The IS auditor should have a working understanding of how fraud is defined and how to use fraud risk factors in assessing the risk of potential fraudulent activity. Fraud encompasses a range of irregularities and illegal acts. To qualify as fraud, it **must involve intentional deception or misrepresentation known to be such by the perpetrator**. The activity must result in some unauthorised benefit that is obtained by the perpetrator on behalf of themselves or an organisation, or be an unfair or dishonest dealing that took advantage of another party or deceived another party and that action resulted in the party suffering a loss. Not all activities that are likely deemed as fraud are frauds; some may be legally defined as corruption. Because fraudulent activity may be perpetrated by those inside, outside, or both inside and outside of the organisation, the auditor needs to follow approved protocols for alerting senior management or other parties of any concerns that are related to possible fraud or illegal activities.

Reporting Possible Fraud in the Final Report

Unless restricted by law, the final audit report should include occurrences of illegal acts or fraud, or audit findings regarding deficiencies in internal control to prevent or detect fraud. Care must be taken in the presentation of audit evidence if the case before the court is not yet resolved. Generally, the audit report should report the possible fraud that the **evidence** indicates and **to whom** the possible illegal or fraudulent activity has been reported. Internal audit reports may include reporting of any evidence of possible illegal or fraudulent activity, including matters considered inconsequential.

Issuing Separate Confidential Reports

Some circumstances require a separate confidential report, with limited distribution, to be released concurrently with the engagement audit report. Typically, a single audit report is prepared and issued that identifies the audit results for all audit objectives. Occasionally, reports contain information that could be exploited and place the organisation or other stakeholders at increased risk. IS auditors often examine and provide conclusions and opinions on highly sensitive operational areas. For example, an IS audit report is likely to contain audit results and recommendations regarding IS security issues. The concern is heightened when audit reports are to be released to a wide readership potentially allowing the details of the deficiencies to fall into the wrong hands. As a result, great care should be taken to report deficiencies and present recommendations in a manner that does not provide unnecessary detail.

The auditor should determine whether:

1. Adequate reporting can be provided without including a level of detail that can lead to exploitation of the deficiency.
2. The entire report can be designated as confidential and distribution can be limited.
3. A separate report can be issued that contains the highly sensitive or security-related information. The report can be issued as confidential and distribution can be significantly limited.

Depending on the type of operational or control deficiencies, the auditor needs to ensure that only authorised parties have access to the audit report. Under such circumstances, the auditor needs to consider whether a separate report may be warranted, due to the level of detail that is provided and the planned distribution of the report. The confidential report, which is connected to the larger report, should indicate the report number that relates to the public report number or the corresponding finding that relates to the public finding or generic finding.

Although the above issue tends to be far more critical when audit reports are made available to a wide readership, such as to external users and the public, a separate report may be advisable even when distribution is within the business enterprise. Labelling the report as confidential and that further distribution is prohibited also helps to reduce secondary distribution.

As a general rule, the auditor should consider preparing a separate report when security or confidentiality can be jeopardised if the details of the audit findings and recommendations increase the risk of a security breach or loss of confidentiality. For example, IT security can be placed at increased risk if the audit report identifies specific security vulnerabilities that could be exploited by individuals taking advantage of that knowledge to gain unauthorised access for undesirable purposes. ISACA 'IS Audit and Assurance Guideline 2401 Reporting' states that security vulnerabilities should be, 'protected from disclosure and should be distributed to a restricted list of recipients'.

It is recommended that the **cover of audit reports that have been prepared as separate reports should be labelled as confidential** and include a statement about the report's restricted purpose and distribution. Language, such as the following, should be considered: 'This report contains information that is privileged, confidential and only for restricted use. Further distribution of this document is strictly prohibited'.

The auditor should determine whether there are restrictions under current law from public disclosure of security deficiencies. If so, the report cover should contain language such as follows and/or specific language if required by law or regulation: 'This report contains information that is privileged, confidential and exempt from disclosure under applicable law. Any external release of the contents of this document is strictly prohibited'.

If the report is to be issued as a confidential audit report with its distribution strictly limited, then care needs to be taken that the report is handled in a protected manner. For example, the auditor can provide password protected files for electronic files. Depending on the level of sensitivity and associated risk, further distribution control can be exercised.

Meeting Future Reporting Expectations

The trends today reveal that report users have an increased need to be provided with more information about business organisations, rather than less. Continued emphasis has focused on **enhancing disclosures in financial audits** of publicly traded organisations. The demands for further information have been driven by business clients, customers, oversight authorities and legislatures. The trend is for better, faster and more comprehensive reporting. From proponents of governance to regulators, there has been a strong interest in independent assessment and reporting of organisational compliance with laws and regulations.

Enhanced Information

It is likely that auditors will be requested to **provide more direct reporting to regulators** regarding compliance issues. Auditors need to be aware about whether their audit encompasses situations where they could be charged with reporting to regulators when organisation management fails to do so.

The call for enhanced information is coming in the form of integrated reporting. Rather than having a separate financial audit report and separate reports on internal controls and other matters, the move towards integrated reporting has already gained traction in some parts of the globe. Although currently voluntary in the United States, some business organisations have already initiated efforts to provide more comprehensive reporting. The trend is to move towards mandatory integrated reporting.

Objective of Integrated Reporting

The objective of integrated reporting is to provide a **more detailed picture of the organisation's efforts** to:

- Produce and sustain value
- Identify and manage risk
- Employ and develop human capital
- Meet legal requirements
- Address corporate and social responsibility

Essentially, audit reports include more in-depth non-financial reporting. The movement is to shift from solely lag indicators as found in traditional reporting to **lead or forward indicators** with increased focus on management and performance capabilities.

Important Issues

At this point, two important issues are before the IS audit community:

1. The concern that **adequate assurance may not be provided** regarding the reliability of non-financial data pertaining to environmental, social and governance responsibilities. The extent to which data integrity is assured in currently released integrated reports may need to be addressed by auditors. Evaluations of general and application controls for systems generating this data are performed and reported on by IS auditors.
2. Given the pervasive nature and importance of technology to business operations, it is unlikely that integrated reports will exclude information regarding IT management, performance and control. As such, **audit planning and reporting may need to be modified to address different attestation requirements**. IS auditors are uniquely positioned to participate in the discussions that are needed to identify assurance requirements, assess business and IT value delivery, and evaluate internal controls over relevant systems and processes regarding environmental, social responsibility and governance. The reporting of IS audit results may need to shift from separate reports to incorporating the results within an integrated report. If so, the spectrum of information needed, report writing, editing and approval will require collaborative processes.

Use of Technology in Reporting

A final issue involves the use of technology in the reporting process. Demand is likely to increase for using technology to present audit results in a manner that quickly enables recipients to focus on the key points of the audit. Therefore, audit organisations must ensure that the credibility of the audit and the reporting process are not jeopardised. Auditing standards across the globe, including the ISACA IS Audit and Assurance Standards and IS Audit and Assurance Guidelines, provide a foundation for the auditing profession to develop and issue professional audit reports. Considerations of increased use of technology in the reporting process must be benchmarked against applicable auditing standards.

V. APPENDIX A—ISACA IS AUDIT AND ASSURANCE STANDARD 1401 REPORTING

Statements

1401.1 IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:
- Identification of the enterprise, the intended recipients and any restrictions on content and circulation
- The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed
- The findings, conclusions and recommendations
- Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
- Signature, date and distribution according to the terms of the audit charter or engagement letter

1401.2 IS audit and assurance professionals shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.

Key Aspects

IS audit and assurance professionals should:
- Obtain relevant written representations from the auditee that clearly detail critical areas of the engagement, issues that have arisen and their resolution, and assertions made by the auditee.
- Determine that auditee representations have been signed and dated by the auditee to indicate acknowledgement of auditee responsibilities with respect to the engagement.
- Document and retain in the work paper any representations, either written or oral, received during the course of conducting the engagement. For attestation engagements, representations from the auditee should be obtained in writing to reduce possible misunderstanding.
- Customise the form and content of the report to support the type of the engagement performed, such as:
  - Audit (direct or attest)
  - Review (direct or attest)
  - Agreed-upon procedures
- Describe material or significant weaknesses and their effect on the achievement of the engagement objectives in the report.
- Discuss the draft report contents with management in the subject area prior to finalisation and release, and include management's response to findings, conclusions and recommendations in the final report, where applicable.
- Communicate significant deficiencies and material weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. Disclose in the report that these have been communicated.
- Reference any separate reports in the final report.
- Communicate to auditee management internal control deficiencies that are less than significant but more than inconsequential. In such cases, those charged with governance or the responsible authority should be notified that such internal control deficiencies have been communicated to auditee management.
- Identify standards applied in conducting the engagement. Communicate any non-compliance with these standards, as applicable.

Term Definition

Term	Definition
Relevant information	Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information. Refer to COBIT 5 information quality goals.
Reliable information	Information that is accurate, verifiable and from an objective source. Refer to COBIT 5 information quality goals.
Sufficient information	Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable. Refer to COBIT 5 information quality goals.
Suitable information	Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame) information. Refer to COBIT 5 information quality goals.
Timely information	Produced and used in a time frame that makes it possible to prevent or detect control deficiencies before they become material to an enterprise. Refer to COBIT 5 information quality goals.

Linkage to Standards and Guidelines

Type	Title
Guideline	2401 Reporting

Operative Date

This ISACA standard is effective for all IS audit and assurance engagements beginning 1 November 2013.

VI. APPENDIX B—ISACA IS AUDIT AND ASSURANCE GUIDELINE 2401 REPORTING

1. Guideline Purpose and Linkage to Standards

1.0 Introduction
This section clarifies the:
1.1 Purpose of the guideline
1.2 Linkage to standards
1.3 Term usage of 'audit function' and 'professionals'

1.1 Purpose
1.1.1 This guideline provides guidance for IS audit and assurance professionals on the different types of IS audit engagements and related reports.
1.1.2 The guideline details all aspects that should be included in an audit engagement report and provides IS audit and assurance professionals with considerations to make when drafting and finalising an audit engagement report.
1.1.3 IS audit and assurance professionals should consider this guideline when determining how to implement the standard, use professional judgement in its application, be prepared to justify any departure and seek additional guidance if considered necessary.

1.2 Linkage to Standards
1.2.1 Standard 1007 Assertions
1.2.2 Standard 1205 Evidence
1.2.3 Standard 1401 Reporting
1.2.4 Standard 1402 Follow-up Activities

1.3 Term Usage
1.3.1 Hereafter:
- 'IS audit and assurance function' is referred to as 'audit function'
- 'IS audit and assurance professionals' are referred to as 'professionals'

2. Guideline Content

2.0 Introduction
The guideline content section is structured to provide information on the following key audit and assurance engagement topics:
2.1 Types of engagements
2.2 Required contents of the audit engagement report
2.3 Subsequent events
2.4 Additional communication

2.1 Types of Engagements
2.1.1 Professionals may perform any of the following types of audit engagements:
- Examination
- Review
- Agreed-upon procedures

Note: These terms are defined in ITAF, 2nd Edition.

2.1.2 Both examination and review engagements involve:
- Planning the engagement
- Evaluating the design effectiveness of control procedures
- Testing the operating effectiveness of the control procedures (the nature, timing and extent of testing will vary as between both types of engagements)
- Forming a conclusion about, and reporting on, the design and/or operating effectiveness of the control procedures based on the identified criteria:
- The conclusion for a reasonable assurance engagement is expressed as a positive opinion and provides a high level of assurance.
- The conclusion for a limited assurance engagement is expressed as a negative opinion and provides only a moderate level of assurance.

2.1.3 An 'agreed-upon procedures' engagement does not result in the expression of any assurance by professionals. Professionals are engaged to carry out specific procedures to meet the information needs of those parties who have agreed to the procedures to be performed (e.g., executive management, the board or those charged with governance). Professionals issue a report of factual findings to those parties that have agreed to the procedures. The recipients form their own conclusions from this report because the nature, timing and extent of procedures do not enable the professional to express any assurance. The report is restricted to those parties that have agreed to the procedures to be performed because others are not aware of the reasons for the procedures and may misinterpret the result.

2.1.4 An agreed-upon procedures report could also be distributed to a third party (e.g., regulatory body) when predetermined and approved by the parties that have agreed on the procedures before the start of the actual work. Professionals should consider this, using their professional judgement, based on the risk of misinterpretation of the work to be performed.

2.1.5 Professionals, who before the completion of an audit engagement are requested to change the audit engagement from an examination or review engagement to an agreed-upon procedures engagement, need to consider the appropriateness of doing so and cannot agree to a change where there is no reasonable justification for the change. For example, a change is not appropriate to avoid a qualified report.

2.2 Required Contents of the Audit Engagement Report

2.2.1 In developing an audit engagement report, all relevant evidence obtained should be considered, regardless of whether it appears to corroborate or contradict the subject matter information. Where there is an opinion, it should be supported by the results of the control procedures based on the identified criteria. Professionals should conclude whether sufficient and appropriate evidence has been obtained to support the conclusions in the audit engagement report. More detailed guidance can be found in Standard 1205 Evidence.

2.2.2 When concluding on an examination or review engagement, professionals should come to an expression of opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective. This opinion can be:
- Unqualified—Professionals should express an unqualified opinion when they conclude that, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective, in accordance with the applicable criteria.
- Qualified—Professionals should express a qualified opinion when they:
- Having obtained sufficient and appropriate evidence, conclude that control weaknesses, individually or in the aggregate, are material, but not pervasive to the IS audit objectives
- Are unable to obtain sufficient and appropriate evidence on which to base the opinion, but conclude that the possible effects on the IS audit objectives of undetected weaknesses, if any, could be material but not pervasive
- Adverse— Professionals should express an adverse opinion when one or more significant deficiencies aggregate to a material and pervasive weakness
- Disclaimer—Professionals should disclaim an opinion when they are unable to obtain sufficient and appropriate evidence on which to base the opinion, and conclude that the possible effects on the IS audit objectives of undetected weaknesses, if any, could be both material and pervasive.

2.2.3 Professionals' examination or review report about the effectiveness of control procedures should include the following elements:

- An appropriate and distinctive title, clearly distinguishing the report from any other type of report not subject to auditing standards
- Identification of the recipients to whom the report is directed, according to the terms in the audit charter or engagement letter
- Identification of the responsible party, including a statement of the party responsible for the subject matter
- Description of the scope of the audit engagement, the name of the entity or component of the entity to which the subject matter relates, including:
  - Identification or description of the area of activity
  - Criteria used as a basis for professionals' conclusion
  - The point in time or period of time to which the work, evaluation or measure of the subject matter relates
  - A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management
- A statement identifying the source of management's representation about the effectiveness of control procedures
- A statement that professionals have conducted the audit engagement to express an opinion on the effectiveness of control procedures
- Identification of the purpose (i.e., IS audit objectives) for which professionals' report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person
- Description of the criteria or disclosure of the source of the criteria. Furthermore, the professionals should consider disclosing:
  - Any significant interpretations made in applying the criteria
  - Measurement methods used when criteria allow for a choice between a number of measurement methods
  - Changes in the standard measurement methods used
- Statement that the audit engagement has been conducted in accordance with ISACA IS audit and assurance standards or other applicable professional standards. Any non-compliance with these standards should be explicitly mentioned in the report.
- Further explanatory details about the variables that affect the assurance provided and other information as appropriate
- Findings, conclusions and recommendations for corrective action and include management's response. For each management response, professionals should obtain information on the proposed actions to implement or address reported recommendations and the planned implementation or action date.
- Responsible management may decide to accept the risk of not correcting a reported condition because of cost, complexity of the corrective action or other considerations. The board of directors (or those charged with governance) should be informed of recommendations for which management accepts the risk of not correcting the reported situation.
- If professionals and the auditee disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the disagreement. The auditee's written comments may be included as an appendix to the engagement report. Alternatively, the auditee's views may be presented in the body of the report or in a cover letter. Executive management, or those charged with governance, should then make a decision as to which point of view they support.
- A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected. In addition, the paragraph should state that projections of any evaluation of internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate. An audit engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis.
- A summary of the work performed, which will help the intended users of the report to better understand the nature of the assurance conveyed
- An expression of opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective. When professionals' opinion is qualified, a paragraph describing the reasons for qualification should be included.

- Where appropriate, references to any other separate reports that should be considered, such as a separate report that communicates security vulnerabilities that are protected from disclosure and should be distributed to a restricted list of recipients
- Date of issuance of the audit engagement report. In most instances, the date of the report is based upon the issue date. It is recommended to also mention the dates when the audit work was actually performed, if not yet mentioned with the summary of the work performed.
- Names of individuals or entity responsible for the report, appropriate signatures and locations

2.2.4 The agreed-upon procedures report should be in the form of procedures and findings. The report should contain the following elements:

- An appropriate and distinctive title, clearly distinguishing the report from any other type of report not subject to auditing standards
- Identification of the recipients to whom the report is directed, according to the terms in the audit charter
- Identification of the responsible party, including a statement of the party responsible for the subject matter
- A statement that the audit engagement has been conducted in accordance with ISACA IS audit and assurance standards or other applicable professional standards. Any non-compliance with these standards should be explicitly mentioned in the report.
- Identification of the subject matter (or the written assertion related thereto) and the purpose (i.e., IS audit objectives) of the audit engagement
- A statement that the procedures performed were those agreed to by the responsible parties identified in the report
- A statement that the sufficiency of the procedures is solely the responsibility of the responsible parties and a disclaimer of responsibility for the sufficiency of those procedures
- A list of the procedures performed (or reference thereto)
- A description of the findings, including sufficient details of errors and exceptions found
- A statement that professionals only performed the agreed-upon procedures and, as such, no assurance is expressed
- A statement that if the professionals had performed additional procedures, other matters might have come to professionals' attention and would have been reported
- A statement of restrictions on the use of the report because it is intended to be used solely by the specified parties
- A statement that the report only relates to the elements specified and that it does not extend beyond them
- References to any other separate reports that should be considered
- Date of issuance of the audit engagement report. In most instances, the date of the report is based upon the issue date. It is recommended to also mention the dates when the audit work was actually performed, if not yet mentioned with the summary of the work performed.
- Names of individuals or entity responsible for the report, appropriate signatures and locations

2.2.5 There are two types of examination reports:

- Direct reports—On the subject matter rather than on an assertion. The report should make reference only to the subject of the engagement and should not contain any reference to management's assertion on the subject matter.
- Indirect reports—Based on management assertions about the subject matter.

More detailed guidance on the difference between indirect and direct reporting can be found in Standard 1007 Assertions.

2.3 Subsequent Events

2.3.1 Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested but prior to the date of professionals' report, which have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertions. These occurrences are referred to as subsequent events. In performing an audit engagement, professionals should consider information about subsequent events that comes to their attention. However, professionals have no responsibility to detect subsequent events.

2.3.2 Professionals should inquire with management as to whether they are aware of any subsequent events, through to the date of professionals' report, that would have a material effect on the subject matter or assertions.

2.4 Additional Communication

2.4.1 Professionals should discuss the draft report contents with management in the subject area prior to finalisation and release, and include management's response to findings, conclusions and recommendations in the final report, where applicable.

2.4.2 Professionals should communicate significant deficiencies and material weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. They should also explicitly disclose in the report that these have been communicated.

2.4.3 Professionals should communicate to management internal control deficiencies that are less than significant but more than inconsequential. In such cases, those charged with governance or the responsible authority should be notified by the professionals that such internal control deficiencies have been communicated to management.

2.4.4 Professionals should obtain written representations from management acknowledging, at a minimum, the following assertions:

- Management responsibility for establishing and maintaining proper and effective internal controls, including systems of internal accounting and administrative controls over operating activities and information systems under review, and activities to identify all laws, rules and regulations, which govern the subject area under review, and to ensure compliance with them.
- All requested information relevant to the engagement objectives was provided to the engagement team including, but not limited to:
  - Records, related data, electronic files and reports
  - Policies and procedures
  - Pertinent personnel
  - Results of relevant internal and external IS audits, reviews and assessments
- No event(s) has occurred or matters discovered since the end of fieldwork that would have a material effect on the engagement.
- Management has no knowledge of any fraud or suspected fraud, irregularities and illegal acts related to the subject area under review, including management and employees with responsibility for internal control not already disclosed.
- Management has no knowledge of any allegations of fraud or suspected fraud, irregularities and illegal acts affecting the area under review received in communications from employees, clients, contractors or others not already disclosed.
- Acknowledgement of responsibility for the design and implementation of programs and controls to prevent and detect fraud, irregularities and illegal acts.

3. Linkage to Standards and COBIT 5 Processes

3.0 Introduction

This section provides an overview of relevant:
3.1 Linkage to standards
3.2 Linkage to COBIT 5 processes
3.3 Other guidance

3.1 Linkage to Standards

The table provides an overview of:
- The most relevant ISACA IS audit and assurance standards that are directly supported by this guideline
- Those standard statements that are most relevant to this guideline

Note: Only those standard statements relevant to this guideline are listed.

Standard Title	Relevant Standard Statements
1007 Assertions	IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.
1205 Evidence	IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives
1401 Reporting	IS audit and assurance professionals shall provide a report to communicate the results upon completion of engagement including: • Identification of the enterprise, the intended recipients, and any restrictions on content and circulation • The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed • The findings, conclusions and recommendations • Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement • Signature, date and distribution according to the terms of the audit charter or engagement letter IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient, reliable and relevant evidence.
1402 Follow Up	IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations.

3.2 Linkage to COBIT 5 Processes

The table provides an overview of the most relevant:
• COBIT 5 processes
• COBIT 5 process purpose

Specific activities performed as part of executing these processes are contained in *COBIT 5: Enabling Processes*.

COBIT 5 Process	Process Purpose
EDM05 Ensure stakeholder transparency.	Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's strategy.
MEA01 Monitor, evaluate and assess performance and conformance.	Provide transparency of performance and conformance and drive achievement of goals.
MEA02 Monitor, evaluate and assess the system of internal control.	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Monitor, evaluate and assess compliance with external requirements.	Ensure that the enterprise is compliant with all applicable external requirements.

3.3 Other Guidance

When implementing standards and guidelines, professionals are encouraged to seek other guidance when considered necessary. This could be from IS audit and assurance:
• Colleagues from within the enterprise
• Management
• Governance bodies within the enterprise, e.g., audit committee
• Professional organisations
• Other professional guidance (e.g., books, papers, other guidelines)

4. Terminology

Term	Definition
Appropriate evidence	The measure of the quality of the evidence
Inconsequential deficiency	A deficiency is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected deficiencies, that the deficiencies, either individually or when aggregated with other deficiencies, would clearly be trivial to the subject matter. If a reasonable person could not reach such a conclusion regarding a particular deficiency, that deficiency is more than inconsequential.
Sufficient evidence	The measure of the quantity of evidence; supports all material questions to the audit objective and scope. See evidence.

5. Effective Date

5.1 Effective Date

This revised guideline is effective for all IS audit/assurance engagements beginning on or after 1 September 2014.

Page intentionally left blank