A PROFESSIONAL PRACTICES FRAMEWORK FOR IT ASSURANCE
ISACA®
With more than 65,000 members in more than 140 countries, ISACA (www.isaca.org) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences; publishes the Information Systems Control Journal®; and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 50,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by 7,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

Disclaimer
ISACA (the ‘Owner’) and the author have designed and created this publication, titled ITAF™: A Professional Practices Framework for IT Assurance (the ‘Work’), primarily as an educational resource for assurance professionals. The Owner 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, control professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure
© 2008 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are solely permitted for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL  60008 USA
Phone:  +1.847.253.1545
Fax:  +1.847.253.1443
E-mail:  standards@isaca.org
Web site:  www.isaca.org

ITAF™: A Professional Practices Framework for IT Assurance
Printed in the United States of America
Acknowledgements

ISACA wishes to recognise:

Researcher
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada

Expert Reviewers
Colin Booth, CISA, Canada
Mahesh S. Lad, CISA, Vantej Inc., Canada

ISACA Board of Directors
Lynn Lawton, CISA, FBPCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, GCIH, GSEC, Miel e-Security Pvt. Ltd., India,
   Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Peña Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group,
   Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Director
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director

Assurance Committee
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Chair
Pippa G. Andrews, CISA, ACA, CIA, Amcor, Australia
Robert Johnson, CISA, CISM, CISSP, Washington Mutual, USA
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada
Erik Pols, CISA, CISM, Shell International, The Netherlands
Gustavo A. Solis, CISA, CISM, Grupo Cynthus, Mexico
V. Vatsaraman, CISA, CISM, ACA, AICWA, Emirates Air, UAE
Paul A. Zonneveld, CISA, CA, Deloitte & Touche, Canada

Standards Board
Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Services India Private
   Limited, India
Brad David Chin, CISA, CPA, Google Inc., USA
Sergio Fleginsky, CISA, AKZO Nobel, Uruguay
Maria Gonzalez, CISA, CISM, Department of Defense, Spain
John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young, Singapore
Andrew J. MacLeod, CISA, CIA, FCPA, MACS, PCP, Brisbane City Council, Australia
John G. Ott, CISA, CPA, AmerisourceBergen, USA
Jason Thompson, CISA, KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA, Microsoft Corp., USA
Foreword

Why a Common IT Assurance Framework Is So Important

The effectiveness of internal controls represents an important issue on the agendas of senior executives and corporate boards in enterprises across industries and throughout the world.

While internal controls over financial processes may capture the headlines, just as crucial an issue for business leaders—as well as the corporate performance for which they are responsible—is the effectiveness of internal controls over information technology (IT). As IT becomes more pervasive, technology-based solutions are increasingly replacing clerical checking and management approval. As the need to provide regulators and shareholders with information on controls increases, the effective design and operation of automated internal controls are also becoming more and more important.

After all, IT almost always resides at the heart of what an organisation and its stakeholder’s value most: the achievement of the organisation’s mission and objectives in the most effective and efficient—and frequently transparent and auditable—manner possible.

The best way of assuring this, of course, is to undertake a formal audit and assessment of IT controls. The global demand for these services is increasing. To meet this demand and support the needs of IT audit and assurance professionals as well as organisations worldwide, ISACA has tapped its global network of leading IT governance, control, security, and assurance experts to develop a widely embraced framework to help ensure the quality, consistency, and reliability of IT assessments. ITAF also contains a helpful set of good practice-setting guidelines and procedures.
# Table of Contents

## Section 1000—Introducing the IT Assurance Framework ..........................1
1100—ITAF: A Brief Overview .................................................................1
1500—Organisation of the IT Assurance Framework ...............................2
1700—Use of the IT Assurance Framework .............................................3
1800—Important Terms and Definitions ...............................................5
1900—How This Publication is Organised ............................................8

## Section 2000—IT Assurance Standards: Defining a Common Reference Point .................................................................9
2100—IT Assurance Standards: Overview and Use .................................9
      2150—ISACA Code of Professional Ethics ........................................9
2200—General Standards .....................................................................10
2400—Performance Standards .............................................................12
2600—Reporting Standards .................................................................15

## Section 3000—IT Assurance Guidelines: Putting the Standards Into Practice .................................................................18
3100—IT Assurance Guidelines: Overview and Use ................................18
3200—Enterprise Topics .......................................................................18
      3210—Implication of Enterprise-wide Policies, Practices and Standards on the IT Function ........................................19
      3230—Implication of Enterprise-wide Assurance Initiatives on the IT Function .........................................................20
      3250—Implication of Enterprise-wide Assurance Initiatives on IT Assurance Plans and Activities ..................................21
      3270—Additional Enterprise-wide Issues and Their Impact on the IT Function ...............................................................22
3400—IT Management Processes ..........................................................22
      3410—IT Governance (Mission, Goals, Strategy, Corporate Alignment, Reporting) .........................................................23
      3412—Determining the Impact of Enterprise Initiatives on IT Assurance Activities ..........................................................24
      3415—Using the Work of Other Experts in Conducting IT Assurance Activities ...............................................................24
      3420—IT Project Management ..........................................................24
      3425—IT Information Strategy ..........................................................25
      3427—IT Information Management ..................................................25
      3430—IT Plans and Strategy (Budgets, Funding, Metrics) ..................25
      3450—IT Processes (Operations, Human Resources, Development, etc.) .................................................................26
      3470—IT Risk Management ...............................................................27
      3490—IT Support of Regulatory Compliance ....................................28
Section 1000—Introducing the IT Assurance Framework

Section 1100—ITAF: A Brief Overview

The Information Technology Assurance Framework (ITAF™) is a comprehensive and good-practice-setting model that:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, and diligence, conduct and reporting requirements

ITAF is focused on ISACA material as well as content and guidance developed by the IT Governance Institute® (ITGI™) and other organisations, and, as such, provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programmes, and develop effective reports.

While ITAF incorporates existing ISACA Standards and guidance, it has been designed to be a living document. As new guidance is developed and issued, it will be indexed within the framework and made available to ISACA members. To date, current ISACA guidance has been mapped to the framework.

Four common questions:

- **To whom does ITAF apply?** ITAF applies to individuals who act in the capacity of IT audit and assurance professionals and are engaged in providing assurance over some components of IT systems, applications and infrastructure. However, care has been taken to design these standards, guidelines, and IT audit and assurance procedures in a manner that may also be useful, and provide benefits to, a wider audience, including users of IT audit and assurance reports.

- **When should ITAF be used?** The application of the framework is a prerequisite to conducting assurance work. The standards are mandatory. The guidelines, tools and techniques are designed to provide non-mandatory assistance in performing assurance work.

- **Where should ISACA Standards and related guidance be used?** ITAF’s design recognises that IT audit and assurance professionals are faced with different requirements and types of audit and assurance assignments—ranging from leading an IT-focused audit to contributing to a financial or operational audit. ITAF is applicable to any formal audit or assessment engagement.

- **Does ITAF address requirements for consultative and advisory work?** In addition to assessment work, IT audit and assurance professionals frequently undertake consultative and advisory engagements for their employer or on behalf of clients. These assignments usually result in an assessment of a particular area; identification of issues, concerns or weaknesses; and the development of recommendations. For a number of reasons, including nature of the work, scope of the engagement, independence and degree of testing, the work is not considered an audit and, therefore, the audit and assurance professional does not issue a formal audit report. ITAF has not been designed to address specific requirements with respect to this consultative and advisory work.
Section 1500—Organisation of the IT Assurance Framework

ITAF is composed of the elements, as shown in figure 1. These include three categories of standards—general, performance and reporting—as well as guidelines and tools and techniques:

- **General Standards**—The guiding principles under which the IT assurance profession operates. They apply to the conduct of all assignments, and deal with the IT audit and assurance professional’s ethics, independence, objectivity and due care as well as knowledge, competency and skill.

- **Performance Standards**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care.

- **Reporting Standards**—Address the types of reports, means of communication and the information communicated

- **Guidelines**—Provide the IT audit and assurance professional with information and direction about an audit or assurance area. In line with the three categories of standards outlined above, guidelines focus on the various audit approaches, methodologies, tools and techniques, and related material to assist in planning, executing, assessing, testing and reporting on IT processes, controls and related audit or assurance initiatives. Guidelines also help clarify the relationship between enterprise activities and initiatives, and those undertaken by IT.

- **Tools and Techniques**—Provide specific information on various methodologies, tools and templates—and provide direction in their application and use to operationalise the information provided in the guidance. Note that the tools and techniques are directly linked to specific guidelines. They take a variety of forms, such as discussion documents, technical direction, white papers, audit programmes or books—e.g., the ISACA publication on SAP, which supports the guideline on enterprise resource planning (ERP) systems.

![Figure 1—The ITAF Taxonomy: How ITAF is Organised Hierarchically](image-url)
Section 1700—Use of the IT Assurance Framework

The standards are designed to be mandatory in all cases. Any deviations must be addressed prior to completion of the assurance or audit engagement.

The guidelines, on the other hand, are not mandatory—but adhering to them is strongly recommended. Although they do allow the IT audit and assurance professional a degree of freedom in their application, the IT audit and assurance professional must be able to defend and justify significant deviations from the guidelines or the omission of relevant sections of the guidance in the conduct of certain IT assurance engagements. This is particularly true if they are being performed at the more rigorous examination level to support an IT audit. Not all guidance will be applicable in all situations, but it should always be considered.

Tools and techniques represent supplementary material and information that support the guidance. In some cases, the techniques present alternatives or even a range of techniques, many of which may be applicable. The IT audit and assurance professional should adopt only the techniques they deem suitable to the situation. Techniques should be selected only if they are suitable and appropriate and result in the IT audit and assurance professional obtaining appropriate, relevant, objective and unbiased information. Complete information regarding ISACA IS Auditing Standards and Guidelines can be found at www.isaca.org/standards.

Implementing IT Assurance Processes

The IT assurance or audit process involves the conduct of specific procedures to provide an appropriate level of assurance about the subject matter. IT audit and assurance professionals undertake assignments designed to provide assurance at varying levels, ranging from review to attestation or examination.

Each audit or assurance assignment must adhere to prescribed standards in terms of which individuals are qualified to perform the work, how the work is performed, what work is performed, and how the findings will be reported based on various characteristics of the assignment as well as the nature of the results obtained. Unless only one assurance professional is conducting the assignment, the team needs to collectively possess the skill and knowledge to perform the work.

Several critical hypotheses are inherent in any IT assurance or audit assignment. These include the following:

• The subject matter is identifiable and subject to audit.
• The audit or assurance project, if undertaken, has a significant likelihood of successful completion.
• The audit or assurance approach and methodology are free from bias.
• The IT audit or assurance project is of sufficient scope to meet the audit or assurance objectives.
• The IT audit or assurance project will lead to a report that is objective and that will not mislead the reader.
**Standards Issued by Other Standard-setting Bodies**

While the ISACA Standards will provide the IT audit and assurance professional with the guidance and direction required, situations may arise in which the IT audit and assurance professional may have to work as part of a team that has used standards issued by another organisation.

The IT audit and assurance professional may:

- Use ISACA Standards in conjunction with professional standards issued by other authoritative bodies
- Cite the use of other standards apart from ISACA Standards in their reports

When the IT audit and assurance professional is using standards other than the ISACA Standards, care should be taken to ensure conflicts do not arise between the standards.

When the IT audit and assurance professional has cited compliance with ISACA Standards, and inconsistencies exist between ISACA and other standards cited, the IT audit and assurance professional should use ISACA Standards as the prevailing standards for conducting reviews and reporting the results.

**IT Assurance and Audit Scoping**

Critical to the IT assurance or audit process, scoping refers to the process of defining exactly how limited or extensive an area, initiative, investment or set of practices will be examined in the course of the audit review. Scoping has a major impact on whether the audit activities undertaken meet, or fail to meet, the objectives of the users of the assurance report—in terms of factors such as timing, resource utilisation, conduct, reporting and cost. Note that ISACA has developed a scoping document that provides more detailed guidance in precisely how to scope IT and IT assurance projects.1

**Assessing Risk in the Scoping Process**

One of the most important elements of the scoping exercise is the process of assessing risk. The IT audit and assurance professional should consider both the risks of undertaking the work and risks that may exist in dealing with the subject matter.

The first type of risk assessment addresses the risks of undertaking a specific assurance engagement. In particular, the assurance professional should consider whether the risks preclude the professional from reaching a conclusion or expressing an opinion on the subject matter. Risks affecting this consideration include timing, management expectations and the project’s or client’s public profile. The assurance professional must consider the impact of the risk profile on the work to be undertaken, or on whether the work considered should be or can be undertaken at all.

---

The second type of risk assessment involves risks related to the subject matter and applies to the specific area under review. These risks will determine the nature, extent and timing of the assurance work as well as the amount of work and number of tests to be performed.

In all cases, the IT audit and assurance professional should use an appropriate scoping and risk assessment approach in developing the overall IT assurance plan and determining priorities for the effective allocation of IT assurance resources. When planning individual assignments, the IT audit and assurance professional should identify and assess risks relevant to each of the areas within the scope of the assignment.

**Technology and Security Standards**
Also inherent in the scoping of an audit is the need to determine the most appropriate standards and criteria against which to assess the subject matter. This task should include consideration of standards such as Information Technology Infrastructure Library (ITIL), International Organisation of Standardisation (ISO)/IEC 27000, and Information Technology Control Guidelines (ITCGs) developed by the Canadian Institute of Chartered Accountants. In section 2200 of this publication, ITAF provides information on selecting suitable criteria, including the use of standards developed by other organisations.

**Section 1800—Important Terms and Definitions**

**Definition of Audit and Assurance**
Throughout this document, common words are used with specific meaning. Accordingly, a glossary of selected terms is provided at the end of the document to ensure the use of the words and their meaning within the context of this document are understood and consistently applied. In addition, a complete glossary is available on the ISACA web site, [www.isaca.org/glossary](http://www.isaca.org/glossary).

Within the ITAF framework, the words ‘audit’ and ‘assurance’ are used to describe specific activities undertaken by an IT audit and assurance professional.

‘Assurance’ in the context of this publication means that, pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. For example, assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulations.
‘Audit’, in the context of this publication, refers to a specific type of assurance engagement in which an IT audit and assurance professional conducts a formal, independent and systematic inspection or examination of subject matter against a recognised and appropriate standard or against management’s assertions that must meet specific criteria. Audit engagements require a formal approach, adherence to specific standards and guidance, and adoption of specific reporting formats. Audit engagements could include support of the audit of financial statements, opinions of regulatory compliance and other formal expressions of opinion.

Assurance engagements may be performed with various degrees of rigour to reach a conclusion about the subject matter and thereby provide the reader or user with a level of assurance. The degrees of rigour are commonly referred to as the examination level and the review level (which is less rigorous).

Agreed-on or specified procedures engagements are not considered audits in that they likely lack the completeness of scope to be considered an audit. However, the procedures agreed on by the users of the report are audit procedures and they are applied against the subject matter. The resulting report refers to audit procedures but indicates the work performed does not constitute an audit and that no opinion is provided. Distribution of such reports is restricted.

Selected IT Assurance Definitions

We have culled from the glossary at www.isaca.org/glossary some of the most important and pertinent terms. A more detailed glossary than the following is also included at the end of this publication.

Accountable relationship refers to the relationship that exists between the parties in an assurance engagement. An accountability relationship is a prerequisite for an assurance engagement. An accountability relationship exists when one party (the accountable party) is answerable to and/or is responsible to another party (the user) for a subject matter, or voluntarily chooses to report to another party on a subject matter. The accountability relationship may arise as a result of an agreement or legislation, or because a user can be expected to have an interest in how the accountable party has discharged its responsibility for a subject matter.²

Assertion refers to a declaration or set of declarations about the subject matter. Assertions should be based on, or in conformity with, the criteria selected.

Assurance risk refers to the risk that the IT audit and assurance professional may express an inappropriate conclusion based on the work performed. Assurance risk can be further categorised as inherent, control or detection risk.

² Source: Canadian Institute of Chartered Accountants (CICA)
**Assurance team** refers to the person or persons who perform the assurance work. The assurance team may include specialists as required.

**Attestation risk** refers to the risk that the assurance professional will draw an incorrect conclusion based on the assessment of controls, the inherent limitations of those controls, the use of testing rather than examining 100 percent of the transactions or other available information, the quality of the information or evidence available, and the degree to which the assurance professional must use professional judgement in evaluating the subject matter.

**Auditee** refers to the management or executive management directly responsible for the subject matter that is the subject of the audit or review. The subject matter may include business units, technologies, systems and applications, or other matters considered within the scope of the audit or assurance project.

**Competencies** refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.

**Level of assurance** refers to the degree to which the subject matter has been examined or reviewed. There are two levels of assurance:

- **Examination level** refers to an attestation engagement designed to provide a high level of assurance. The assurance professional’s objective is to accumulate sufficient competent evidence to restrict attestation risk to a level that is, in the assurance professional’s professional judgement, appropriately low for the high level of assurance that may be imparted by the resulting report. The accumulation of audit evidence includes an assessment or evaluation of that evidence in terms of its ability to meet the requirements of the engagement and reduce audit risk. In examination-level audits, the assurance professional should select from all available procedures that assess inherent and control risks, and restrict detection risks such that the attestation risk is at an appropriately low level.

- **Review level** refers to an attestation engagement designed to provide a moderate level of assurance. The assurance professional’s objective is to accumulate sufficient evidence to restrict attestation risk to a moderate level. To accomplish this, the types of procedures performed generally are limited to inquiries and analytical procedures, as compared with an examination level where procedures would also include search and verification.

**Professional standards** refer to standards issued by ISACA. The term may extend to related guidelines and techniques that assist the professional in implementing and complying with authoritative pronouncements of ISACA. In certain instances, standards of other professional organisations may be considered, depending on the circumstances and their relevancy and appropriateness.

**Quality review or inspection** refers to procedures employed in a review of completed work or engagements designed to ensure compliance with IT assurance standards, and related quality control policies and procedures of the organisation.
Quality reviews can be performed by different levels of staff members and at different times during the assurance work or at its completion. Quality reviewers must possess sufficient knowledge to assess compliance with professional and organisational policies and standards as well as knowledge of the subject matter to assess appropriateness of the criteria selected and the auditing procedures performed.

**Reasonable assurance** refers to a high, but not absolute, level of assurance.

**Representations** refer to written or oral statements by management and the auditee about the subject matter. They are statements of fact that can be confirmed through audit procedures. Representations may also indicate that the IT audit and assurance professional has been informed of, and given access to, all relevant information, records, files, etc., pertaining to the subject matter.

**Responsible party** refers to the person or persons, either as individuals or representatives of the entity, responsible for the subject matter. If, because of the nature of the subject matter or the proposed engagement, a responsible party is not identified or associated with the subject matter, the party who has a reasonable basis for making a written assertion about the subject matter may provide such assertions and adopt the role of the responsible party.

**Section 1900—How This Publication is Organised**

This publication is divided into four sections.

- **Section 1000** provides an introduction to ITAF.
- **Section 2000** introduces the three categories of standards: general standards, performance standards and reporting standards.
- **Section 3000** introduces the guidelines. In this section, tables provide information in two categories. The first is **IT Processes** or IT audit processes—which includes a narrative description of the guideline item, presents information about the subject area and the assurance issues, and provides direction to IT audit and assurance professionals. Where available, links to relevant guidelines are provided. The second category is **Resources**, which provides references to ISACA Resources (a list of existing ISACA IS Auditing Standards, IS Auditing Guidelines and other ISACA publications relevant to the subject matter). References from other sources may be relevant for specific circumstances.
- **Section 4000** introduces IT audit and assurance tools and techniques as well as other information. (This section is in development.)

In line with ITAF’s design as a living document, section numbers intentionally include gaps where future guidance may be inserted.
As indicated in the introduction, there are three categories of standards in ITAF—general, performance and reporting—which must be followed in all circumstances. In addition, while standards guidance contains narrative information designed to assist the IT audit and assurance professional, compliance with certain information within the standard may be obligatory, and has been identified in bold.

In adopting and using ITAF, IT audit and assurance professionals, particularly ISACA members and certification holders, must consider the Code of Professional Ethics in section 2150.

**Section 2150—ISACA Code of Professional Ethics**

<table>
<thead>
<tr>
<th>Code of Professional Ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the Association and/or its certification holders.</td>
</tr>
</tbody>
</table>

Members and ISACA certification holders shall:
1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with due diligence and professional care, in accordance with professional standards and best practices.
3. Serve the interests of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

ISACA has indicated that failure to comply with the Code of Professional Ethics can result in an investigation into a member’s and/or certification holder’s conduct, and, ultimately, in disciplinary measures.
Section 2200—General Standards

General standards are the guiding principles under which the IT assurance profession operates. They apply to the conduct of all assignments and deal with the IT audit and assurance professional’s ethics, independence, objectivity and due care, as well as knowledge, competency and skill.

General standards include:

- **Independence and Objectivity**—The IT audit and assurance professional should maintain an independent and objective state of mind in all matters related to the conduct of the IT assurance assignment. The IT audit and assurance professional must conduct the IT assurance assignment with an impartial and unbiased frame of mind in addressing assurance issues and reaching conclusions. It is important that the IT audit and assurance professional not only be independent, but also appear to be independent at all times.

- **Reasonable Expectation**—The IT audit and assurance professional should have a reasonable expectation that the IT assurance assignment can be completed in accordance with these IT assurance standards or other appropriate professional, regulatory or industry standards, and result in a professional opinion. The scope of the audit or assurance engagement should be sufficient to permit a conclusion to be drawn on the subject matter and the ability to address any restrictions.

- **Management’s Acknowledgement**—The IT audit and assurance professional should be satisfied that management understands his/her obligations and responsibilities with respect to the provision of appropriate, relevant and timely information that may be required in the performance of the assignment and his/her responsibility to ensure the co-operation of personnel during the audit or assurance activity.

- **Training and Proficiency**—The IT audit and assurance professional and others assisting with the assignment should collectively possess adequate skills and proficiency in conducting IT audit and assurance assignments to enable the professionals to perform the work required.

- **Knowledge of the Subject Matter**—The IT audit and assurance professional and others engaged in performing the IT assurance assignment should collectively possess adequate knowledge of the subject matter.

- **Due Professional Care**—The IT audit and assurance professional should exercise due care in planning, performing and reporting on the results of the IT assurance assignment.

- **Suitable Criteria**—IT audit subject matter should be evaluated against suitable and appropriate criteria. The characteristics of suitable criteria include:
  - **Objectivity**—Criteria should be free from bias that may adversely impact the IT audit and assurance professional’s findings and conclusions, and, accordingly, may mislead the user of the IT assurance report.
  - **Measurability**—Criteria should permit consistent measurement of the subject matter and the development of consistent conclusions when applied by different IT audit and assurance professionals in similar circumstances.
Section 2000—IT Assurance Standards: Defining a Common Reference Point

- **Understandability**—Criteria should be communicated clearly and not be subject to significantly different interpretations by intended users.
- **Completeness**—Criteria should be sufficiently complete so that all criteria that could affect the IT audit and assurance professional’s conclusions about the subject matter are identified and used in the conduct of the IT assurance assignment.
- **Relevance**—Criteria should be relevant to the subject matter and contribute to findings and conclusions that meet the objectives of the IT assurance assignment.

**Available Criteria**—IT assurance criteria should be available to users of the IT audit and assurance professional’s report so that users understand the basis of the assurance activity and the relevance of the findings and conclusions. Sources may include:

- **Publicly available**—Publicly available standards include those developed by professional accounting and auditing bodies such as ISACA, International Federation of Accountants (IFAC) or other recognised government or professional bodies.
- **Available to all users**—Where criteria are not publicly available, they should be communicated to all users through ‘assertions’ that form part of the IT audit and assurance professional’s report. Assertions consist of statements about the subject matter that meet the requirements of ‘suitable criteria’ so that they can be audited.
- **Authoritative**—Criteria should be sought that reflect authoritative pronouncements within the area and appropriate for the subject matter. For example, authoritative pronouncements may come from professional bodies, industry groups, government and regulators.
- **Recognised**—Criteria should be sufficiently well recognised that their use is not questioned by intended users.

**Selection of Criteria**—In addition to suitability and availability, the selection of IT assurance criteria should also consider their source, in terms of their use and the potential audience. For example, when dealing with government regulations, criteria based on assertions developed from the legislation and regulations that apply to the subject matter may be most appropriate. In other cases, industry or trade association criteria may be relevant. The IT audit and assurance professional must consider the selection of criteria carefully and be able to justify the selection. Listed in order of consideration are possible sources:

- **Criteria established by ISACA**—These are publicly available criteria and standards that have been exposed to peer review and a thorough, due-diligence process by recognised international experts in IT governance, control, security and assurance.
- **Criteria established by other bodies of experts**—Similar to ISACA standards and criteria, these are relevant to the subject matter and have been developed and exposed to peer review and a thorough, due-diligence process by experts in various fields.
- **Criteria established by laws and regulations**—While laws and regulations can provide the basis of criteria, care must be taken in their use. Frequently, wording is complex and carries a specific legal meaning. In many cases, it may be necessary to restate the requirements as assertions. Further, IT audit and assurance professionals should exercise care in that expressing an opinion on legislation is usually restricted to members of the legal profession.
– **Criteria established by organisations that do not follow due process**—These include relevant criteria developed by other organisations that did not follow due process and have not been subject to public consultation and debate.

– **Criteria developed specifically for the IT assurance assignment**—While criteria developed specifically for the IT assurance assignment may be appropriate, the IT audit and assurance professional must take particular care to ensure these criteria meet the suitability criteria, particularly completeness, measurability and objectivity. Criteria developed specifically for an IT assurance assignment are in the form of assertions.

Where existing standards and criteria exist that are appropriate to the subject matter of the IT assurance activity, the IT audit and assurance professional must be prepared to defend the decision to depart from a recognised standard. Where criteria are not complete, this must be considered and dealt with in the IT audit and assurance professional’s report. Considerations would range from having the accountable person add criteria to noting the deficiency in the audit or assurance report.

While adhering to local laws and regulations is important and must be considered a mandatory requirement, it is recognised that many audits include areas, such as change management, IT general controls and access controls, not covered by law or regulations. In addition, some industries, such as the payment card industry, have established mandatory requirements that must be met. Further, some legislative requirements are weak and, in the judgement of the IT audit and assurance professional, may not be sufficiently robust to provide adequate protection. Accordingly, the IT audit and assurance professional must carefully consider the selection criteria.

Current ISACA IS Auditing Standards include the following general standards:

- S2 Independence
- S3 Professional Ethics and Standards
- S4 Competence
- S6 Performance of Audit Work

**Section 2400—Performance Standards**

Performance standards establish baseline expectations in the conduct of IT assurance engagements. While these standards apply to assurance professionals performing any assurance assignment, compliance is particularly important when the IT audit and assurance professional is acting in an audit capacity. Accordingly, the performance standards focus on the IT audit and assurance professional’s attention to the design of the assurance work, the conduct of the assurance, the evidence required, and the development of assurance and audit findings and conclusions.
Performance standards include:

• **Planning and Supervision**—IT assurance work should be adequately planned and the IT audit and assurance professional should ensure other persons performing the IT assurance assignment are properly supervised. Planning of the IT assignment should address the:
  – Objective of the IT audit or assurance assignment
  – Criteria to be used in conducting the IT assurance assignment
  – Level of assurance required. This includes whether the engagement is to be conducted at the examination or review level, or as an advisory or consulting assignment; what type of findings and conclusions will be required; and what format reporting will take.
  – Nature of the subject matter and the likely items within the assertion
  – Possible sources of information and evidence, including the tools, techniques and skills required to obtain the evidence. Considerations may include the use of computer-assisted audit techniques (CAATs), audit software and unique analyses.
  – Availability of appropriate and skilled IT audit and assurance resources
  – Availability and access to records and other information
  – Preliminary conclusions on assignment and audit risks, and the means by which these risks will be mitigated
  – Resource and expertise requirements—as well as their source, critical skills required and the timing of their participation in the IT assurance activity
  – Nature, extent and timing of the various IT assurance tasks and, if an audit is being performed, audit tests
  – Conditions that may require extension of modification of assurance work and audit tests
  – Anticipation of time requirements and the establishment of time and cost budgets
  – Nature of the expected report

Planning and supervision work should be documented and form part of the IT assurance work papers. This documentation should clearly indicate the nature, extent and timing of IT assurance work performed; the information and documents obtained; and the conclusions reached regarding the subject matter.

• **Obtaining Sufficient Evidence**—When an audit is being performed, the IT audit and assurance professional should obtain sufficient evidence to provide a reasonable basis for the conclusions drawn and expressed in the IT audit report:
  – IT audit procedures should be applied to obtain and accumulate sufficient and appropriate audit evidence to provide a reasonable basis for conclusions to be drawn and expressed in the IT auditor’s report. Sufficiency addresses the concept of quantity of evidence, and appropriateness addresses the quality of evidence in support of measuring achievement of the audit objective. In determining the sufficiency and appropriateness of IT audit evidence, the IT audit and assurance professional should consider the level of assurance being provided and the assessment of risk.
– Evidence is normally obtained through inspection, observation, enquiry, confirmation, re-performance analysis and discussion. The IT audit and assurance professional may seek corroborating evidence from different sources when forming a conclusion on the results of an IT audit procedure.

– The IT audit and assurance professional should ensure the source of evidence is considered when assessing its appropriateness in supporting the audit procedure.

– The IT audit and assurance professional should document the test performed and the results obtained in sufficient detail to support the conclusions reached.

For other assurance work where an audit is not being performed, the IT audit and assurance professional should look to the requirements as a basis for establishing the sufficiency of information to be obtained and the documentation required. Usually, assurance documentation should be sufficient to allow a knowledgeable individual with appropriate skills to reach the same conclusions based on a review of the relevant documentation.

**Assignment Performance**—The IT assurance assignment must be scheduled with regard to the timing, availability, and other commitments and requirements of management and the auditee. Scheduling should also consider the needs of report users so that their timing requirements are met. In scheduling audit personnel, care must be taken to ensure the correct personnel are available and that issues of continuity, skills and experience are addressed:

– Professional staff must be assigned to tasks that are within their knowledge and skills.

– The work must be conducted with due care and appropriate consideration for management and auditee issues and concerns, including timing and timeliness.

– IT audit performance must address the objectives and mandate of the audit.

**Representations**—The IT audit and assurance professional will receive representations during the course of conducting the IT audit—some written and others oral. As part of the audit process, these representations should be documented and retained in the work-paper file. In addition, for attestation engagements, representations from the auditee should be obtained in writing to reduce possible misunderstandings. Matters that may appear in a representation letter include:

– A statement by the auditee acknowledging responsibility for the subject matter and, when applicable, the assertions

– A statement by the auditee acknowledging responsibility for the criteria, and where applicable, the assertions

– A statement by the auditee acknowledging responsibility for determining that the criteria are appropriate for the purposes

– A list of specific assertions about the subject matter based on the criteria selected

– A statement that all known matters contradicting the assertions have been disclosed to the IT audit and assurance professional

– A statement that all communications from regulators affecting the subject matter or the assertions have been disclosed to the IT audit and assurance professional

– A statement that the IT audit and assurance professional has been provided access to all relevant information and records, files, etc., pertaining to the subject matter
A statement on any significant events that have occurred subsequent to the date of the audit report and prior to release of that report
Other matters that the IT audit and assurance professional may deem relevant or appropriate

Frequently, a summary of all representations made during the assignment is prepared and signed prior to finalisation of the audit or assurance work.

While the same degree of rigour is not essential in non-audit assurance engagements, the assurance professional should obtain representations from management on key issues.

Current ISACA IS Auditing Standards include the following performance standards:

- S1 Audit Charter
- S5 Planning
- S9 Irregularities and Illegal Acts
- S10 IT Governance
- S11 Use of Risk Assessment in Audit Planning
- S12 Audit Materiality
- S13 Using the Work of Other Experts
- S14 Audit Evidence
- S15 IT Controls
- S16 E-commerce

Section 2600—Reporting Standards

The report produced by the IT audit and assurance professional will vary, depending on the type of assignment performed. Considerations include the level of assurance, whether the assurance professional was acting in an audit capacity, whether the assurance professional is providing a direct report on the subject matter or is reporting on assertions regarding the subject matter, and whether that report is based on work performed at the review level or the examination level.

Figure 2 at the end of this section provides information on various types of IT audit assignments and the corresponding reports. Figure 2 also provides information on consulting assignments that the IT audit and assurance professional may be requested to perform. While such reports do not provide assurance, they do provide management with insight into issues and concerns, and frequently provide recommendations to address deficiencies.

Reporting standards address (1) types of reports, (2) the means of communication, and (3) information to be communicated.
At minimum, the IT audit and assurance professional’s report and/or associated attachments should:

- Identify to whom the report is directed
- Identify the nature and objectives of the IT assurance assignment
- Identify the entity or portion thereof covered by the IT assurance report
- Identify the subject matter or assertions on which the IT audit and assurance professional is reporting
- Provide a description of the nature of the scope of the work, including a brief statement on matters that are not within the scope of the assignments as well as those that are, to remove any doubt about the scope
- State the time frame or period covered by the report
- State the period during which the IT assurance was performed
- Provide a reference to the applicable professional standards governing the IT assurance assignment and against which the IT assurance work was conducted
- Identify management assertions, if any
- Describe the responsibilities of management and the IT audit and assurance professional
- Identify the criteria against which the subject matter was evaluated
- State a conclusion on the level of assurance being provided (Depending on the type of assignment, this could range from an audit report to a review report where no assurance is provided.)
- State any reservations that the IT audit and assurance professional may have (These may include scope, timing, and inability to obtain sufficient information or conduct appropriate tests, and are particularly important in audit assignments.)
- State any restrictions on the distribution or use of the report
- State the date of the report
- State where the report was issued
- State who issued the report (name or organisation of the IT auditor)
- Include the IT audit and assurance professional’s signature on the written report

In addition, depending on the nature of the IT audit or assurance assignment, other information should be provided such as specific government directives, corporate policies or other information germane to the reader’s understanding of the IT assurance assignment.

Figure 2 illustrates the various types of reports based on user needs. These needs can vary from an audit conducted at the examination level with no restrictions on use or distribution to reports based on lesser degrees of rigour and, therefore, assurance. The review reports are usually restricted as to use and distribution.

In addition to assurance reports at the examination and review levels, the table contains a reference to consulting services reports. Occasionally, the assurance professional may perform work that is neither an examination nor a review, but rather an assessment and recommendation typical of a consulting service. Consulting
services reports are similar to review reports in that their distribution and use are restricted. However, consulting services reports may contain assessments, analyses, recommendations and other information desired by users of the report.

Reports on topics such as internal control or technology operations usually consist of a letter report accompanied with detailed information organised in such a manner as to permit the reader to understand, in greater depth, the areas included in the scope of the report; the work performed; the findings obtained; and the issues, concerns, risks, etc., identified based on the findings. Consultative or advisory reports may also include recommendations; however, recommendations would not form a part of the audit opinion.

<table>
<thead>
<tr>
<th>The Report User Needs</th>
<th>Consulting Services</th>
<th>Attestation Procedures</th>
<th>Agreed-on Procedures</th>
<th>SAS 70(^3) S-5970(^4)</th>
<th>TrustServices SysTrust and WebTrust(^5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A report that provides:</td>
<td>No assurance</td>
<td>Assurance</td>
<td>No assurance</td>
<td>Assurance</td>
<td>Assurance based on predefined criteria</td>
</tr>
<tr>
<td>A report that will be available for:</td>
<td>Restricted use to a predefined audience</td>
<td>General distribution</td>
<td>Restricted use to those who have agreed on the procedures</td>
<td>Restricted use to current customers and their auditors</td>
<td>General distribution</td>
</tr>
<tr>
<td>A report that will disclose:</td>
<td>Detailed information</td>
<td>Limited information</td>
<td>Specific procedures and factual findings</td>
<td>Detailed information</td>
<td>Specific information that may be in summary or detailed form</td>
</tr>
</tbody>
</table>

Current ISACA IS Auditing Standards include the following reporting standards:
- S7 Reporting
- S8 Follow-up Activities

---

\(^3\) American Institute of Certified Public Accountants (AICPA) standard
\(^4\) CICA standard
\(^5\) Product of the AICPA and CICA
Section 3000—IT Assurance Guidelines: Putting the Standards Into Practice

Section 3100—IT Assurance Guidelines: Overview and Use

Section 3000 addresses guidelines in the following areas:

<table>
<thead>
<tr>
<th>Section</th>
<th>Guideline Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>3200</td>
<td>Enterprise Topics</td>
</tr>
<tr>
<td>3400</td>
<td>IT Management Processes</td>
</tr>
<tr>
<td>3600</td>
<td>IT Audit and Assurance Processes</td>
</tr>
<tr>
<td>3800</td>
<td>IT Audit and Assurance Management</td>
</tr>
</tbody>
</table>

Each section within the guidelines focuses on one of the following:

- IT issues and processes that the IT audit and assurance professional should understand and consider when determining the planning, scoping, execution and reporting of IT audit or assurance activities
- IT audit and assurance processes, procedures, methodologies and approaches that the IT audit and assurance professional should consider when conducting IT assurance activities

The guidelines are supported by references to additional ISACA resources.

Section 3200—Enterprise Topics

Section 3200 addresses enterprise-wide issues that may impact the IT audit and assurance professional in the planning and performance of the IT audit and assurance mission. The guidelines provide the IT audit and assurance professional with an understanding of enterprise-wide issues such as executive actions, external events and decisions that impact the IT department and, hence, the IT audit and assurance planning, designing, executing and reporting processes. This understanding may be provided by executive and senior user management and can be obtained from within the IT department. In addition, relevant information may also be obtained from work performed by non-IT audit and assurance professionals, either as part of an integrated audit assignment or from the other audit findings and reports.

By gaining an understanding of the environment in which the IT function operates—whether a separate IT department or a technology function located within business units—the IT audit and assurance professional should also gain an appreciation for the business and political pressures the IT function must address. The IT audit and assurance professional also gains an appreciation for the perspectives from which the various stakeholders approach the IT services and assess the performance of IT service providers. Thus, the IT audit and assurance professional can put into context the various IT functions and initiatives.
In addition to the operational environment, the IT audit and assurance professional should also consider the control environment and the system of internal control.

Section 3200 addresses guidelines in the following areas:

<table>
<thead>
<tr>
<th>Section</th>
<th>Guideline Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>3210</td>
<td>Implication of Enterprise-wide Policies, Practices and Standards on the IT Function</td>
</tr>
<tr>
<td>3230</td>
<td>Implication of Enterprise-wide Assurance Initiatives on the IT Function</td>
</tr>
<tr>
<td>3250</td>
<td>Implication of Enterprise-wide Assurance Initiatives on IT Assurance Plans and Activities</td>
</tr>
<tr>
<td>3270</td>
<td>Additional Enterprise-wide Issues and Their Impact on the IT Function</td>
</tr>
</tbody>
</table>

The following table represents a drill-down to uncover further information of section 3200. It identifies potential areas for the development of ISACA guidelines, provides information as to the scope and content of the guideline, and lists existing relevant ISACA resources and some illustrative techniques to be considered (whether existing

<table>
<thead>
<tr>
<th>3200—Enterprise Topics</th>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| 3210                   | Implication of Enterprise-wide Policies, Practices and Standards on the IT Function | • G1 Using the Work of Other Experts  
                          |                                           | • G18 IT Governance  
                          |                                           | • Board Briefing on IT Governance, 2nd Edition  
                          |                                           | • IT Governance Domain Practices and Competencies series  
                          |                                           | – Governance of Outsourcing  
                          |                                           | – Information Risks: Whose Business are They?  
                          |                                           | – IT Alignment—Who is in Charge?  
                          |                                           | – Measuring and Demonstrating the Value of IT  
                          |                                           | – Optimising Value Creation From IT Investments  
                          |                                           | • CoeIT:  
                          |                                           | – ME2 Monitor and evaluate internal control. |
### 3210 Implication of Enterprise-wide Policies, Practices and Standards on the IT Function

**Management cont.**
The assurance professional should also be aware of management’s view of IT; perception of IT as a driver, an enabler, a support or a convenience; and willingness to fund IT initiatives. Tight budgets frequently lead to less-than-optimal decisions regarding security, control and risk management.

**Governance**
The IT audit and assurance professional should understand the organisation’s governance model and its implications on information technology.

Issues such as board-level monitoring of technology issues and formal reporting of IT initiatives, participation of IT in strategic initiatives, and the alignment of IT with entity-level goals should be understood by the IT audit and assurance professional.

The IT audit and assurance professional must also appreciate the regulatory drivers and their impact on the board’s perspective in dealing with financial disclosure, transparency and visibility, and other regulatory or marketplace expectations or requirements.

### 3230 Implication of Enterprise-wide Assurance Initiatives on the IT Function

This section identifies and addresses the impact of current or past enterprise-wide audit initiatives on the IT function. As such, it identifies instances where the findings of non-IT auditors may have an impact on the IT function and its management.

**Impact of General Audit Findings and Recommendations**
General audits may be undertaken for a variety of reasons such as:
to express an opinion of financial statements; to express an opinion on the effectiveness of controls; to investigate and report on suspected fraud; or to assess compliance with legislation, regulations or standards.

Because of the pervasiveness of information technology in most organisations, the scope and focus of the many general audits may identify issues, concerns or deficiencies that impact IT and IT management or that result in recommendations that may directly or indirectly impact IT.

Accordingly, the IT audit and assurance professional should become aware of and obtain information on general audit activities that addressed areas in which IT was a significant part, or where the general auditors identified deficiencies or developed recommendations that would affect IT and IT management.

- G1 Using the Work of Other Experts
- G11 Effect of Pervasive IS Controls
- G34 Responsibility, Authority and Accountability
- ConT:
  - P01 Define a strategic IT plan.
  - P04 Define the IT processes, organisation and relationships.
  - P06 Communicate management aims and directions.
  - P07 Manage IT human resources.
  - P08 Manage quality.
  - P09 Assess and manage IT risks.
  - P010 Manage projects.
- A12 Acquire and maintain application software.
3230 Implication of Enterprise-wide Assurance Initiatives on the IT Function

The IT audit and assurance professional should ascertain the current status of such recommendations and the deficiencies they were designed to address. The IT audit and assurance professional should review with IT management their response to any audit recommendations in terms of initiatives undertaken and results achieved.

In addition, the IT audit and assurance professional should consider the impact of the deficiencies on the planned audit work, particularly with respect to the assessment of risk and determination of scope.

- DS2 Manage third-party services.
- DS5 Ensure systems security.
- DS10 Manage problems.
- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure compliance with external requirements.
- ME4 Provide IT governance.

3250 Implication of Enterprise-wide Assurance Initiatives on IT Assurance Plans and Activities

This section identifies and addresses the impact of current or past enterprise-wide audit initiatives on the conduct of the IT audit.

Determining the Role of IT Audit

IT audits may be undertaken as parts of enterprise-wide audit activities or may be performed as stand-alone assignments. Regardless of the role, the IT audit and assurance professional must determine the activities to be undertaken and any reliance on, or integration with, the work undertaken or being undertaken by the non-IT auditors.

Where IT audit is supporting the work of the non-IT auditors, effective co-ordination of all activities is key to effectively assessing risks, identifying controls, designing tests and assessing the results on an enterprise level.

Where the IT audit is being performed as a stand-alone activity, information contained in past reports and working papers is useful in providing context and background information on issues and decisions that may impact the IT audit.

Audit Findings

Where the IT audit and assurance professional is conducting a stand-alone audit, information from prior audit reports may provide additional information or identify issues and problems that impact the risks and controls within the scope of the IT assurance initiative.

- G1 Using the Work of Other Experts
- G15 Planning
- G37 Configuration Management Process
- CoSiT:
  - P06 Communicate management aims and direction.
  - DS3 Manage performance and capacity.
  - DS5 Ensure systems security.
  - DS9 Manage the configuration.
  - DS11 Manage data.
  - ME2 Monitor and evaluate internal control.
Section 3400—IT Management Processes

Section 3400 addresses IT management. Guidelines in this section provide the IT audit and assurance professional with an understanding of various IT management and IT operations topics as a background to the planning and scoping of IT assurance activities. Guidance in this section may also provide the IT audit and assurance professional with direction or information that will be of assistance in conducting an audit and information on IT topics that the IT audit and assurance professional is likely to, or should expect to, encounter during the conduct of IT audit or assurance work.

IT management guidelines also provide the IT audit and assurance professional with insight into the practices and procedures of IT departments. As such, the section focuses on the planning, organisation and strategising of activities of IT departments; acquisition of information and information technology; implementation; support and delivery of IT services; and the monitoring and improvement of IT practices and procedures to enhance security, control and shareholder value. The section provides the IT audit and assurance professional with information on common practices, issues and concerns as well as risks and pitfalls in each area, and approaches and methodologies management can use to enhance value. It also provides the IT audit and assurance professional with guidance on the types of controls that management is likely to or should implement.
Section 3400 addresses guidelines in the following areas:

<table>
<thead>
<tr>
<th>Section</th>
<th>Guideline Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>3410</td>
<td>IT Governance (Mission, Goals, Strategy, Corporate Alignment, Reporting)</td>
</tr>
<tr>
<td>3412</td>
<td>Determining the Impact of Enterprise Initiatives on IT Assurance Activities</td>
</tr>
<tr>
<td>3415</td>
<td>Using the Work of Other Experts in Conducting IT Assurance Activities</td>
</tr>
<tr>
<td>3420</td>
<td>IT Project Management</td>
</tr>
<tr>
<td>3425</td>
<td>IT Information Strategy</td>
</tr>
<tr>
<td>3427</td>
<td>IT Information Management</td>
</tr>
<tr>
<td>3430</td>
<td>IT Plans and Strategy (Budgets, Funding, Metrics)</td>
</tr>
<tr>
<td>3450</td>
<td>IT Processes (Operations, Human Resources, Development, etc.)</td>
</tr>
<tr>
<td>3470</td>
<td>IT Risk Management</td>
</tr>
<tr>
<td>3490</td>
<td>IT Support of Regulatory Compliance</td>
</tr>
</tbody>
</table>

The following table represents a drill-down of section 3400. It identifies potential areas for the development of ISACA guidelines, provides information as to the scope and content of the guideline, and lists existing relevant ISACA resources and some illustrative techniques to be considered (whether existing or not).

<table>
<thead>
<tr>
<th>3400—IT Management Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3410</strong> IT Governance (Mission, Goals, Strategy, Corporate Alignment, Reporting)</td>
<td>• G18 IT Governance • G39 IT Organisation • Aligning CoIT, ITIL and ISO 17799 for Business Benefit—A Management Briefing from ITGI and OGC • Board Briefing on IT Governance, 2nd Edition • CoIT: – P01 Define a strategic IT plan. – ME1 Monitor and evaluate IT performance. • Enterprise Value: Governance of IT Investments—The Val IT Framework</td>
</tr>
</tbody>
</table>

This section provides guidance on IT governance activities. It is recognised that, while some organisations have implemented a formal IT governance programme, others may have adopted only the concepts and engaged in a limited number of IT governance activities.

The section provides an overview of IT governance, the activities comprising an IT governance programme and those that may be considered important.

The section addresses the following topics from a management perspective and indicates what information the IT auditor should expect to find, how it is usually documented, and how to assess its implementation and use within the organisation:

- IT mission and vision
- IT strategic plan aligned with business goals and vision
- Technological strategy and standards
- IT organisational structure—board and department
- Enterprise information architecture
- IT project portfolio management
- IT operations (management perspective) key performance indicators (KPIs)

In addition to providing information on IT governance, the guidance provides specific information on what to audit and advice on the approaches and methodologies available when addressing the various IT governance initiatives.
### ITAF™: A Professional Practices Framework for IT Assurance

**3400—IT Management Processes (cont.)**

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3410 cont.</strong></td>
<td><strong>IT Governance (Mission, Goals, Strategy, Corporate Alignment, Reporting)</strong></td>
</tr>
<tr>
<td>The guidance is supported by a series of technique publications that provide details of how to audit various IT governance initiatives, including sample audit work programmes and illustrative material.</td>
<td></td>
</tr>
</tbody>
</table>

**3412 Determining the Impact of Enterprise Initiatives on IT Assurance Activities**

Enterprise initiatives frequently have an impact on the requirements for information technology and, hence, the activities of the IT department. As such, it is important that the IT audit and assurance professional fully understand the various initiatives and the impact they may have on the audit or review of the IT department.

**3415 Using the Work of Other Experts in Conducting IT Assurance Activities**

Frequently, IT audit and assurance professionals are faced with situations in which additional skills are required to fully understand the potential impact of IT department initiatives and activities on the IT audit or assurance work.

The use of specialists should be carefully planned and resources should be sought with the appropriate skills to enable the IT auditor to understand the initiative, the technology affected, the risks and threats, the potential impacts of problems encountered, and the likely impact on the IT audit or assurance work.

**3420 IT Project Management**

This section provides guidance on the management of IT projects, whether they involve development of client applications, implementation of technology infrastructure or the upgrading of system software.

It addresses issues of scoping, planning, resourcing, key sponsors, critical success factors (CSFs), project completion and project wrap-up. It also addresses performance issues. This section provides guidance on programme and project management issues for a correct prioritisation and co-ordination of all projects.

Projects are unique initiatives that are carried out within specific time and budget boundaries for a specific objective. As such, they present unique challenges to the organisation that have an impact over the risks it faces.

In addition, an organisation usually manages several concurrent projects through time. Organisations should have a strong framework to manage these projects, to ensure the effectiveness of the overall process.

- CoStr: – P010 Manage projects.
Organisations require a strategy under which information they collect, use, disclose and share can be effectively managed. The role has traditionally fallen to the IT department, but the role should include all information with which the organisation deals.

There have been various approaches, all categorised under the term ‘information systems strategic planning’. During the 1980s, when the first enterprise-wide information architectures were being developed, various consulting firms developed strategic planning tools and methodologies.

This section provides guidance on the management of information entrusted to the IT department. It addresses the issues concerning the integrity of the information, provision of access, ownership, custodianship, retention, archiving and destruction.

Information also includes the classification of information so that appropriate levels of security, access, etc., can be developed and managed. Certain information brings with it classification requirements, such as personal information and health information, to mention a few.

The guidance also addresses key issues in information management, including e-mail, security, access and document portfolios.

This section provides guidance on the development, implementation and maintenance of IT strategies and plans, how these are operationalised into annual budgets, funding for infrastructure and portfolio projects, and the various metrics that are used to measure and manage the activities of the IT department.

Information that the IT audit and assurance professional will find useful for planning and conducting an audit of IT strategic and tactical plans as well as an audit of IT of annual plans, budgets and performance reporting is included in this section.

The guidance addresses how the IT initiatives support the enterprise, align with enterprise strategic goals and direction, and align with IT departmental goals.

### 3425 IT Information Strategy

Organisations require a strategy under which information they collect, use, disclose and share can be effectively managed. The role has traditionally fallen to the IT department, but the role should include all information with which the organisation deals.

There have been various approaches, all categorised under the term ‘information systems strategic planning’. During the 1980s, when the first enterprise-wide information architectures were being developed, various consulting firms developed strategic planning tools and methodologies.

### 3427 IT Information Management

This section provides guidance on the management of information entrusted to the IT department. It addresses the issues concerning the integrity of the information, provision of access, ownership, custodianship, retention, archiving and destruction.

Information also includes the classification of information so that appropriate levels of security, access, etc., can be developed and managed. Certain information brings with it classification requirements, such as personal information and health information, to mention a few.

The guidance also addresses key issues in information management, including e-mail, security, access and document portfolios.

### 3430 IT Plans and Strategy (Budgets, Funding, Metrics)

This section provides guidance on the development, implementation and maintenance of IT strategies and plans, how these are operationalised into annual budgets, funding for infrastructure and portfolio projects, and the various metrics that are used to measure and manage the activities of the IT department.

Information that the IT audit and assurance professional will find useful for planning and conducting an audit of IT strategic and tactical plans as well as an audit of IT of annual plans, budgets and performance reporting is included in this section.

The guidance addresses how the IT initiatives support the enterprise, align with enterprise strategic goals and direction, and align with IT departmental goals.

<table>
<thead>
<tr>
<th>COBIT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>– P01 Define a strategic IT plan.</td>
</tr>
<tr>
<td>– P03 Determine technological direction.</td>
</tr>
<tr>
<td>– P05 Manage the IT investment.</td>
</tr>
<tr>
<td>– P09 Assess and manage risks.</td>
</tr>
</tbody>
</table>
### 3450—IT Processes (Operations, Human Resources, Development, etc.)

This section provides guidance on the various operational activities in which the IT organisation is involved. It provides the reader with an introduction to the organisation of an IT department and, based on size, indicates the activities and the separation of duties and responsibilities issues. Classic operational divisions amongst the following are identified and the roles of each explored to provide the assurance professional with background information on the organisational issues the IT audit and assurance professional is likely to encounter:

- Management and administration
- Computer operations
- End-user computing and help desk
- Systems development
- Systems maintenance
- Security

Within management and administration, the HR function, staffing issues, acquisition of resources, and financial and reporting activities are addressed, and issues that may affect an IT audit are identified.

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>G14 Application Systems Review</td>
<td></td>
</tr>
<tr>
<td>G23 System Development Life Cycle (SDLC) Reviews</td>
<td></td>
</tr>
<tr>
<td>G25 Review of Virtual Private Networks</td>
<td></td>
</tr>
<tr>
<td>G29 Post-implementation Review</td>
<td></td>
</tr>
<tr>
<td>G32 Business Continuity Plan (BCP) Review From IT Perspective</td>
<td></td>
</tr>
<tr>
<td>G37 Configuration Management Process</td>
<td></td>
</tr>
<tr>
<td>G39 IT Organisation</td>
<td></td>
</tr>
</tbody>
</table>

**CoIT:**
- PO1 Define a strategic IT plan.
- PO2 Define the information architecture.
- PO3 Determine technological direction.
- PO4 Define the IT processes, organisation and relationships.
- PO5 Manage the IT investment.
- PO7 Manage IT human resources.
- PO8 Manage quality.
- PO9 Assess and manage IT risks.
- PO10 Manage projects.
- AI1 Identify automated solutions.
- AI2 Acquire and maintain application software.
- AI3 Acquire and maintain technology infrastructure.
- AI4 Enable operation and use.
- AI5 Procure IT resources.
- AI6 Manage changes.
- DS1 Define and manage service levels.
- DS2 Manage third-party services.
- DS3 Manage performance and capacity.
- DS4 Ensure continuous services.
### 3400—IT Management Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes (Operations, Human Resources, Development, etc.)</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS5 Ensure systems security.</td>
<td></td>
</tr>
<tr>
<td>DS7 Educate and train users.</td>
<td></td>
</tr>
<tr>
<td>DS9 Manage the configuration.</td>
<td></td>
</tr>
<tr>
<td>DS10 Manage problems.</td>
<td></td>
</tr>
<tr>
<td>DS11 Manage data.</td>
<td></td>
</tr>
<tr>
<td>DS12 Manage the physical environment.</td>
<td></td>
</tr>
<tr>
<td>DS13 Manage operations.</td>
<td></td>
</tr>
<tr>
<td>ME1 Monitor and evaluate IT performance.</td>
<td></td>
</tr>
<tr>
<td>ME4 Provide IT governance.</td>
<td></td>
</tr>
</tbody>
</table>

### 3470 IT Risk Management

This section provides guidance on the risk management activities that should be undertaken by an IT department and how those activities relate to enterprise-wide risk management initiatives.

IT risk management activities include:
- Risk identification:
  - Availability
  - Infrastructure
  - Integrity
  - Investment
  - Project
  - Security
- Identifying and managing multiple and cross-enterprise risks
- Taking into consideration constraint factors that contribute to risk/achievement of business objectives
- Identifying risks of not undertaking a project, course of action or other undertaking (Doing nothing may increase risk.)

- Aligning CoBiT, ITIL and ISO 17799 for Business Benefit—A Management Briefing From ITGI and OGC
- Board Briefing on IT Governance, 2nd Edition
- The CEO’s Guide to IT Value at Risk
- CoBiT:
- IT Governance Domains Practices and Competencies series:
  - Governance of Outsourcing
  - Information Risks—Whose Business are They?
  - IT Alignment—Who is in Charge?
- Val IT series
This section provides guidance on the role and responsibility of IT in addressing regulatory compliance. It explores the various responsibilities of the IT department in assisting the enterprise to meet its compliance responsibilities.

While compliance is a business issue, the guidance identifies the role of IT in such areas as:
- Identifying compliance-related risks and threats
- Performing compliance-based risk assessments
- Working with end users and enterprise legal and compliance departments to identify IT-specific risks, end-user risks and enterprise risks that IT can assist in mitigating
- Designing compliance-friendly systems and applications
- Monitoring changes in legislation, regulations, rulings and court orders that may impact the way risks are addressed by the enterprise and by IT
- Considering the regulatory compliance issues inherent in the introduction of new technology, processes or applications

Organisations are faced with threats from a number of sources—legal, regulatory, security and environmental are but a few. This guidance presents a framework for IT to effectively participate in the risk identification, evaluation and mitigation process, whether the risks are IT-specific or the responsibility of business units.

Compliance need not just be about legislation or regulations. Frequently, organisations must comply with contracts and agreements, many of which offer a role for IT in ensuring contractual terms are complied with and contractual information is provided in an appropriate and timely manner.

Examples of scope/applicable regulations/certification standards:
- US Securities and Exchange Commission (SEC)
- Privacy/data protection
- US Health Insurance Portability and Accountability Act (HIPAA)
- Japan’s Financial Instruments Exchange Law (FIEL), aka J-SOX
- Others, e.g., ISO 20000/27001, ITIL

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| 3490 IT Support of Regulatory Compliance | • G9 Audit Considerations for Irregularities
• G19 Irregularities and Illegal Acts
• G37 Configuration Management Process
• CoSiT:
  – P06 Communicate management aims and direction.
  – A12 Acquire and maintain application software.
  – D33 Manage performance and capacity.
  – D55 Ensure systems security.
  – D9 Manage the configuration.
  – D11 Manage data.
• CoSiT Mapping: Overview of International IT Guidance, 2nd Edition
• IT Control Objectives for Sarbanes-Oxley, 2nd Edition
• IT Control Objectives for Basel II |

---

3400—IT Management Processes (cont.)
Section 3600—IT Audit and Assurance Processes

Section 3600 focuses on audit approaches, methodologies and techniques. It provides the IT audit and assurance professional with information on common practices, issues, concerns and pitfalls when employing various audit and assurance procedures, and guidance on how to plan and conduct the assurance activity to ensure success. It also provides the IT audit and assurance professional with specific guidance on testing controls.

The IT audit and assurance professional should recognise and appreciate the role of IT in the enterprise, and the relationships that exist between IT departments and enterprise operations and management.

When performing audit and assurance work, it is suggested that ISACA members indicate that ‘The work was performed in accordance with ISACA audit and assurance standards’.

Section 3600 addresses guidelines in the following areas:

<table>
<thead>
<tr>
<th>Section</th>
<th>Guideline Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>3605</td>
<td>Relying on the Work of Specialists and Others</td>
</tr>
<tr>
<td>3607</td>
<td>Integrating IT Audit and Assurance Work With Other Audit Activities</td>
</tr>
<tr>
<td>3610</td>
<td>Using COBIT in the IT Assurance Process</td>
</tr>
<tr>
<td>3630</td>
<td>Auditing IT General Controls (ITGCs)</td>
</tr>
<tr>
<td>3650</td>
<td>Auditing Application Controls</td>
</tr>
<tr>
<td>3653</td>
<td>Auditing Traditional Application Controls</td>
</tr>
<tr>
<td>3655</td>
<td>Auditing Enterprise Resource Planning (ERP) Systems</td>
</tr>
<tr>
<td>3657</td>
<td>Auditing Alternative Software Development Strategies</td>
</tr>
<tr>
<td>3660</td>
<td>Auditing Specific Requirements</td>
</tr>
<tr>
<td>3661</td>
<td>Auditing Government-specified Criteria</td>
</tr>
<tr>
<td>3662</td>
<td>Auditing Industry-specified Criteria</td>
</tr>
<tr>
<td>3670</td>
<td>Auditing With Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td>3680</td>
<td>IT Auditing and Regulatory Reporting</td>
</tr>
<tr>
<td>3690</td>
<td>Selecting Items of Assurance Interest</td>
</tr>
</tbody>
</table>

Enterprise resource planning (ERP) systems are business management systems that integrate all facets of the business, including planning, manufacturing, sales and marketing. Popular software applications, such as SAP, PeopleSoft, Oracle, Baan and JDE, are designed to help business managers implement ERP in business activities such as inventory control, order tracking, customer service, finance and HR. ERP systems have clearly defined risk and control features that must be activated upon implementation.

ERP systems controls consist of:
- ERP general controls, which may include logical access controls, program change controls, and performance and capacity planning controls
• ERP business application controls, which support the organisation’s business processes. This includes detailed ERP system-module-specific controls, which should be considered together with related business-operation controls as part of an integrated audit review.

Users of the application control guidance are cautioned to consider the application control issue and guidance in the traditional approach as well as the guidance in the ERP section when dealing with an ERP system.

The following tables represent a drill-down of section 3600. They identify potential areas for the development of ISACA guidelines, provide information as to the scope and content of the guideline, and list existing relevant ISACA resources and some illustrative techniques to be considered (whether existing or not).

<table>
<thead>
<tr>
<th>3600—IT Audit and Assurance Processes</th>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3605</strong> Relying on the Work of Specialists and Others</td>
<td>Assurance professionals are often required to rely on the work of other specialists. As such, they can either undertake specifying the work required, monitoring the results and assuming responsibility as if it were work performed by another member of the team or organisation or, alternatively, assurance professionals can highlight in their report the specific work performed by third parties and limit their responsibility in various ways, such as a review for reasonableness. It is important for both parties to agree on the degree of reliance the assurance professional will be placing on the work of others. In other situations, assurance professionals may rely on others within the same organisation to perform some of the work, or rely on prior reports by others within the organisation, particularly internal audit, risk management, and even previous reports by external consultants and advisors developed in response to a request by the IT department.</td>
<td>• G1 Using the Work of Other Auditors and Experts • CoaT: – ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td><strong>3607</strong> Integrating IT Audit and Assurance Work With Other Audit Activities</td>
<td>Assurance professionals are frequently asked to participate in audit or assurance work being performed by other auditors, such as financial auditors and operational auditors. In such cases, IT audit and assurance professionals may have to integrate the conduct of their work as well as the audit or assurance reporting comments with those of other professionals. Accordingly, IT audit and assurance professionals should ensure the work being undertaken meets appropriate professional standards and requirements. Further, IT audit and assurance professionals should perform the work in accordance with the timing and other requirements such that the IT audit and assurance work is completed and provided to members of the other audit or assurance team in a timely manner, allowing for resolution and inclusion in the overall audit or assurance report.</td>
<td>• S1 Audit Charter • S3 Professional Ethics and Standards • S6 Performance of Audit Work</td>
</tr>
</tbody>
</table>
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>3607 cont.</th>
<th>Integrating IT Audit and Assurance Work With Other Audit Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT audit and assurance professionals should consider the reporting requirements prior to undertaking the work and should clearly distinguish between work required to be performed at a review level vs. work required to be performed at an examination level.</td>
<td></td>
</tr>
</tbody>
</table>

Additional information is provided in section 3850.

### 3610 Using CoBIT in the IT Assurance Process

This guideline provides an introduction to CoBIT. The *IT Assurance Guide: Using CoBIT* discusses what CoBIT is, how the *IT Assurance Guide* relates to CoBIT, how to audit control objectives and how to use the *IT Assurance Guide* to develop tests of selected control practices. It also addresses the topics of risk and risk management, designing effective audit programmes and matching audit tests with related control practices.

This guideline area provides information on adopting CoBIT as a standard against which to audit, dealing with scope limitations and situations when not all of CoBIT is included in the scope of the audit and dealing with control weaknesses, control failures and compensating procedures.

This area also provides guidance in reporting the results of a CoBIT-based audit.

### 3630 Auditing IT General Controls (ITGCs)

#### 3630.1 Introduction to IT General Controls

This section provides information on what IT general controls are and how they relate to other controls, such as application controls, accounting controls, administrative and management controls, and governance initiatives.

The section includes:
- Defining ITGC
- Components of ITGC
- Difference between ITGCs and application controls
- Understanding the implication of ITGC failures

This guidance also discusses the role of IT general controls in providing assurance over various components of an IT organisation. For example, the user requirement for availability would be addressed in ITGCs dealing with backup and recovery, disaster recovery planning and testing, and maintenance and operations controls such as alternate power source (APS)/uninterrupted power source (UPS).
### 3630—Auditing IT General Controls (ITGCs) (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| **3630.2 Information Resource Planning**  
This section provides information on the IT planning processes and their alignment and integration with enterprise initiatives, budgets, plans and timing. The guidance addresses various strategic planning techniques that deal with IT investment considerations, IT portfolio management, and the allocation of resources to best align with business needs and priorities. It provides information on appropriate approaches and methodologies. It also provides information on tactical plans and methodologies for the creation of annual plans from strategic plans and the development of annual budgets based on business requirements and strategic initiatives. (See section 3420 for additional background information.)  
The guidance in this section provides the IT audit and assurance professional with background information on the concepts of IT planning and related processes, and ensures the auditor can develop an audit programme and perform audit tests to obtain and evaluate the required information. | • G11 Effect of Pervasive IS Controls  
• G15 Planning  
• G18 IT Governance  
• G21 Enterprise Resource Planning (ERP) Systems Review  
• G34 Responsibility, Authority and Accountability  
• G37 Configuration Management Process  
• CoaT:  
  – PO1 Define a strategic IT plan.  
  – PO2 Define the information architecture.  
  – PO3 Determine technological direction.  
  – PO4 Define the IT processes, organisation and relationships.  
  – PO5 Manage the IT investment.  
  – PO6 Communicate management aims and direction.  
  – PO7 Manage IT human resources.  
  – PO8 Manage quality.  
  – PO9 Assess and manage IT risks.  
  – PO10 Manage projects.  
  – AI1 Identify automated solutions.  
  – AI2 Acquire and maintain application software.  
  – AI3 Acquire and maintain technology infrastructure.  
  – AI4 Enable operation and use.  
  – AI6 Manage changes.  
  – DS1 Define and manage service levels.  
  – DS2 Manage third-party services.  
  – DS3 Manage performance and capacity. |
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3630 cont.</strong></td>
<td>Auditing IT General Controls (ITGCs)</td>
</tr>
</tbody>
</table>

#### 3630.2 Information Resource Planning (cont.)
- DS4 Ensure continuous service.
- DS5 Ensure systems security.
- DS6 Identify and allocate costs.
- DS7 Educate and train users.
- DS8 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS10 Manage problems.
- DS11 Manage data.
- DS12 Manage the physical environment.
- DS13 Manage operations.
- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure compliance with external requirements.
- ME4 Provide IT governance.

#### 3630.3 IT Service Delivery
The concept of IT as a service to other operating and administrative areas of the organisation is well established. IT departments usually promise certain standards of service, whether informally or formally through service level agreements (SLAs).

Specific guidance on the various components of service delivery and audit and assurance considerations may be found elsewhere in section 3630 as well as in the IT Assurance Guide: Using COBIT.

- **COBIT:**
  - DS1 Define and manage service levels.
  - DS3 Manage performance and capacity.
  - DS4 Ensure continuous service.
  - DS8 Manage service desk and incidents.

#### 3630.4 Information Systems Operations
This section provides information on the IT operations processes. It provides a brief introduction to the process, its primary function, any specific controls that should be in place and why it is important to the establishment of a control environment.

The operations area includes computer operations; end-user computing including help desk, education and other support; hardware; networks and network management; and HR issues, including staffing, training and career management.

- **G37 Configuration Management Process**
  - A12 Acquire and maintain application software.
  - DS3 Manage performance and capacity.
  - DS4 Ensure continuous service.
  - DS7 Educate and train users.
  - DS8 Manage service desk and incidents.
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3630 cont. Auditing IT General Controls (ITGCs)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>3630.4 Information Systems Operations cont.</strong></td>
<td>– DS9 Manage the configuration.</td>
</tr>
<tr>
<td>The guidance in this section reviews each of the position responsibilities usually assigned to the individual responsible for IT operations, provides a position description, and identifies CSFs and key performance indicators (KPIs) for the position or the operations area of the IT department.</td>
<td>– DS10 Manage problems.</td>
</tr>
<tr>
<td></td>
<td>– DS11 Manage data.</td>
</tr>
<tr>
<td></td>
<td>– DS12 Manage the physical environment.</td>
</tr>
<tr>
<td></td>
<td>– DS13 Manage operations.</td>
</tr>
<tr>
<td><strong>3630.5 IT Human Resources</strong></td>
<td>• G30 Competence</td>
</tr>
<tr>
<td>This section describes HR activities that are unique to the management of an IT department. It identifies the various positions within the IT department, the skills required, and the management challenges in attracting and retaining appropriate IT talent. It provides guidance on training and skills enhancement.</td>
<td>• Cost:</td>
</tr>
<tr>
<td></td>
<td>– P07 Manage IT human resources.</td>
</tr>
<tr>
<td></td>
<td>– DS1 Define and manage service levels.</td>
</tr>
<tr>
<td></td>
<td>– DS2 Manage third-party services.</td>
</tr>
<tr>
<td></td>
<td>– DS3 Manage performance and capacity.</td>
</tr>
<tr>
<td></td>
<td>– DS7 Educate and train users.</td>
</tr>
<tr>
<td></td>
<td>– ME1 Monitor and evaluate IT performance.</td>
</tr>
<tr>
<td></td>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td></td>
<td>– ME3 Ensure compliance with external requirements.</td>
</tr>
<tr>
<td></td>
<td>– ME4 Provide IT governance.</td>
</tr>
<tr>
<td><strong>3630.6 Outsourced and Third-party IT Activities</strong></td>
<td>• G4 Outsourcing of IS Activities to Other Organisations</td>
</tr>
<tr>
<td>This section provides information on the various types of outsourcing (outsourcing, insourcing, offshoring, facilities management, etc.), the IT activities that may be outsourced (operations, help desk, technical support, maintenance, systems software support, application software support, etc.), and the issues about each, of which the IT assurance professional must be aware.</td>
<td>• G18 IT Governance</td>
</tr>
<tr>
<td>The guidance in this section also identify the risks associated with the various outsourcing options and provide information on how management can minimise or mitigate the risks.</td>
<td>• G32 Business Continuity Plan (BCP) Review From an IT Perspective</td>
</tr>
<tr>
<td>In addition, this guidance provides helpful hints regarding contracting, reducing outsourced risks, legal remedies and other protection devices.</td>
<td>• G37 Configuration Management Process</td>
</tr>
<tr>
<td></td>
<td>• Cost:</td>
</tr>
<tr>
<td></td>
<td>– P04 Define the IT processes, organisation and relationships.</td>
</tr>
<tr>
<td></td>
<td>– P07 Manage IT human resources.</td>
</tr>
<tr>
<td></td>
<td>– P08 Manage quality.</td>
</tr>
<tr>
<td></td>
<td>– P09 Assess and manage IT risks.</td>
</tr>
<tr>
<td></td>
<td>– AI2 Acquire and maintain application software.</td>
</tr>
<tr>
<td></td>
<td>– AI5 Procure IT resources.</td>
</tr>
</tbody>
</table>
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auditing IT General Controls (ITGCs)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>3630.6 Outsourced and Third-party IT Activities</strong> cont.</td>
<td>– A16 Manage changes.</td>
</tr>
<tr>
<td></td>
<td>– DS1 Define and manage service levels.</td>
</tr>
<tr>
<td></td>
<td>– DS2 Manage third-party services.</td>
</tr>
<tr>
<td></td>
<td>– DS4 Ensure continuous service.</td>
</tr>
<tr>
<td></td>
<td>– DS5 Ensure systems security.</td>
</tr>
<tr>
<td></td>
<td>– DS9 Manage the configuration.</td>
</tr>
<tr>
<td></td>
<td>– DS10 Manage problems.</td>
</tr>
<tr>
<td></td>
<td>– DS11 Manage data.</td>
</tr>
<tr>
<td></td>
<td>– DS12 Manage the physical environment.</td>
</tr>
<tr>
<td></td>
<td>– DS13 Manage operations.</td>
</tr>
<tr>
<td></td>
<td>– ME1 Monitor and evaluate IT performance.</td>
</tr>
</tbody>
</table>

### 3630.7 Information Security Management

Information security management refers to the IT security programme over information entrusted to the IT department, which the department has responsibility to protect, such as end-user computing.

This section addresses the various components of information security, discusses the key issues about each, and provides the IT audit and assurance professional with practices and procedures the IT department should have implemented to enhance security over its operations and other activities in which it is engaged, either directly or in an oversight role. In addition, this section addresses all aspects of IT security.

| | **G11 Effect of Pervasive IS Controls** |
| | **CobIT:** |
| | – P01 Define a strategic IT plan. |
| | – P04 Define the IT processes, organisation and relationships. |
| | – P06 Communicate management aims and direction. |
| | – P08 Manage quality. |
| | – A15 Procure IT resources. |
| | – DS5 Ensure systems security. |
| | – ME1 Monitor and evaluate IT performance. |

### 3630.8 Systems Development Life Cycle

This section provides information about the life cycle that most traditional development projects follow. It also provides information on other forms of system development such as prototyping, acquiring and customising packaged software, acquiring integrated software such as ERP systems, and using nontraditional development models such as outsourcing and offshoring.

| | **G23 System Development Life Cycle (SDLC) Reviews** |
| | **CobIT:** |
| | – P08 Manage quality. |
| | – P010 Manage projects. |
### 3630.8 Systems Development Life Cycle (cont.)

The guidance in this section identifies the issues, concerns and risks of the various approaches and provides the IT assurance professional with information on ways to address and mitigate the risks.

This section also guides the IT auditor through the key audit activities in each of the phases of the SDLC. The section provides useful information on developing an effective audit programme, executing that programme and reporting the results.

This section also provides information on various control models for each phase, such as library models to migrate and promote software into production, and various project management techniques to monitor achievement and minimise scope creep.

### 3630.9 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

This section addresses from an assurance perspective the separate but linked topics of business continuity planning and disaster recovery planning. The section also provides information on the development of BCPs, from the initial business impact assessment to the analysis of scenarios, responses and communications.

The section also addresses IT disaster recovery planning from the threat (risk assessments, impact assessments and plans to respond, stabilise, remediate or revert to an alternate site) through recovery and, eventually, resumption of normal service. In addition, the guidance in this section provides insight into IT assurance issues related to evaluating BCPs/DRPs.
### 3600—IT Audit and Assurance Processes (cont.)

**3630**

**Auditing IT General Controls (ITGCs)**

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| **3630.9 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)** cont. | – DS9 Manage the configuration.  
– DS10 Manage problems.  
– DS11 Manage data.  
– DS12 Manage the physical environment.  
– DS13 Manage operations.  
– ME1 Monitor and evaluate IT performance.  

**3630.10 Database Management and Controls**

Guidance in this section address the security, control, integrity and other requirements necessary to ensure up-to-date, accurate and available information. The difference between active and passive database management systems is addressed. The roles and responsibilities of database managers and data managers as well as their relation to knowledge managers are addressed.

The differences between traditional databases and evolving data marts and knowledge bases are reviewed from an assurance perspective since many corporate decisions are being made on the basis of data mining these types of information bases.

Issues of intellectual property, property rights and the protection of electronic copyrights are reviewed and the role IT can play in ensuring the protection of corporate information assets is addressed.

**3630.11 Network Management and Controls**

This section addresses the management of internal and external networks, and incorporates concepts and requirements from other areas such as outsourcing since many external networks are operated by third parties. The section also addresses the requirements and expectations of users of the IT systems and networks, such as customers and key corporate users.

In addition, this section deals with protection of the networks from a variety of sources, and an assessment of the internal and external risks to the network. The section also addresses protection of traffic over the networks through such means as encryption.

- Oracle Database: Security, Audit and Control Features

- G4 Outsourcing of IS Activities to Other Organisations
- G11 Effect of Pervasive IS Controls
- G16 Effect of Third Parties on an Organisation’s IT Controls
- G22 Business-to-consumer (B2C) E-commerce Reviews
- G27 Mobile Computing
- G33 General Considerations for the Use of the Internet
- G37 Configuration Management Process
- COBIT:  
  – PO1 Define a strategic IT plan.  
  – PO2 Define the information architecture.  
  – PO3 Determine technological direction.
<table>
<thead>
<tr>
<th>3600—IT Audit and Assurance Processes (cont.)</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3630 cont. Auditing IT General Controls (ITGCs)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **3630.11 Network Management and Controls cont.** | – P04 Define the IT processes, organisation and relationships.  
– P06 Communicate management aims and direction.  
– P07 Manage IT human resources.  
– P08 Manage quality.  
– P09 Assess and manage IT risks.  
– P010 Manage projects.  
– AI1 Identify automated solutions.  
– AI2 Acquire and maintain application software.  
– AI3 Acquire and maintain technology infrastructure.  
– AI4 Enable operation and use.  
– AI5 Procure IT resources.  
– AI6 Manage changes.  
– DS1 Define and manage service levels.  
– DS2 Manage third-party services.  
– DS3 Manage performance and capacity.  
– DS5 Ensure systems security.  
– DS8 Manage service desk and incidents.  
– DS9 Manage the configuration.  
– DS10 Manage problems.  
– ME1 Monitor and evaluate IT performance.  
– ME2 Monitor and evaluate internal control.  
– ME4 Provide IT governance. |
<p>| <strong>3630.12 Systems Software Support—Other Than Operating Systems</strong> | This section refers to the support required to maintain the myriad system software—other than the primary operating system that is dealt with separately—required to operate a large-scale computer facility. |</p>
<table>
<thead>
<tr>
<th>3630—IT Audit and Assurance Processes (cont.)</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>**3630 cont.<strong>Auditing IT General Controls (ITGCs)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>3630.12 Systems Software Support—Other Than Operating Systems cont.</strong></td>
<td></td>
</tr>
<tr>
<td>This section also covers the life cycle of systems software and addresses key audit and control issues of selecting additional software; ensuring new systems software does not compromise existing system software; ensuring current applications will operate with new system software; and testing, migration and related activities.</td>
<td></td>
</tr>
<tr>
<td>The guidance in this section offers advice on maintenance of systems software at end-user sites as well as documentation issues. Version management, release control and patch management are addressed, as are scalability and migration paths.</td>
<td></td>
</tr>
<tr>
<td><strong>3630.13 Hardware Support</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Guidance in this section deals with the acquisition, maintenance and deprovisioning of IT hardware. The guidelines include requirements to inventory. | **OS/390-z/OS Security Audit and Control Features**  
**Linux Security, Audit and Control Features** |
| **3630.14 Operating Systems (OSs) Management and Controls** | |
| This section refers to the support required to maintain the OS software. The guidance provides information on OSs, their role in the processing cycle, and the risk associated with implementing and maintaining OSs. | |
| The guidance in this section also addresses ensuring the selection of the correct and appropriate settings and parameters during implementation, and the implementation of appropriate patches and version releases, but only after extensive testing in the host environment and with each of the key applications. | |
| **3630.15 Physical and Environmental Control** | |
| This section addresses the security, integrity and protection of the facilities housing computer processors, network switches, wiring closets and other locations where sensitive technology is located. The guidance in this section also extends to the protection of end-user computing, including the protection of notebooks and data while away from the usual place of business. | |
| **3630.16 Enterprise Portals** | |
| This section addresses the audit and control of e-business and information, and internal and/or external portals. It outlines the risks of external portals operating over the Internet and discusses the difference between open and closed user groups, and various means to protect the organisation’s portals from disruption. | **G22 Business-to-consumer (B2C) E-commerce Reviews**  
**G27 Mobile Computing**  
**G31 Privacy**  
**G37 Configuration Management Process**  
**CoBIT:**  
– P06 Communicate management aims and direction.  
– P07 Manage IT human resources.  
– P08 Manage quality. |
<table>
<thead>
<tr>
<th>3600—IT Audit and Assurance Processes (cont)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Processes</strong></td>
</tr>
<tr>
<td>3630 cont.</td>
</tr>
</tbody>
</table>
| 3630.16 Enterprise Portals cont. | - P09 Assess and manage IT risks.  
- A12 Acquire and maintain application software.  
- A13 Acquire and maintain technology infrastructure.  
- A14 Enable operation and use.  
- A15 Procure IT resources.  
- A16 Manage changes.  
- DS1 Define and manage service levels.  
- DS2 Manage third-party services.  
- DS3 Manage performance and capacity.  
- DS4 Ensure continuous service.  
- DS5 Ensure systems security.  
- DS7 Educate and train users.  
- DS8 Manage service desk and incidents.  
- DS9 Manage the configuration.  
- DS10 Manage problems.  
- DS11 Manage data.  
- DS13 Manage operations.  
- ME2 Monitor and evaluate internal controls.  
- ME3 Ensure compliance with external requirements.  
- ME4 Provide IT governance. |

### 3630.17 Identification and Authentication

Guidance in this section provides the IT audit and assurance professional with information on the various ways to design and manage a process to identify and control access to application resources. Identification and authentication utilise various identity management techniques and are key building blocks in developing a robust security framework.

This section also addresses various authentication methods and provides guidance on auditing each.

- G36 Biometric Controls  
- G37 Configuration Management Process  
- CoIT:  
  - P01 Define a strategic IT plan.  
  - P03 Determine the technological direction.  
  - P05 Manage the IT investment.
<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3630</strong> Auditing IT General Controls (ITGCs) <strong>(cont.)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **3630.17 Identification and Authentication** **(cont.)** | – P06 Communicate management aims and direction.  
– P08 Manage quality.  
– P09 Assess and manage IT risks.  
– P010 Manage projects.  
– AI1 Identify automated solutions.  
– AI2 Acquire and maintain application software.  
– AI3 Acquire and maintain technology infrastructure.  
– AI5 Procure IT resources.  
– AI6 Manage changes.  
– DS1 Define and manage service levels.  
– DS3 Manage performance and capacity.  
– DS4 Ensure continuous service.  
– DS5 Ensure systems security.  
– DS7 Educate and train users.  
– DS9 Manage the configuration.  
– DS10 Manage problems.  
– DS11 Manage data.  
– ME1 Monitor and evaluate IT performance.  
– ME2 Monitor and evaluate internal controls.  
– ME3 Ensure compliance with external requirements.  
• Digital Signatures  
Security and Controls |
The audit of applications combines aspects of general computer controls with controls that are specific to applications. For example, access controls may be exercised at the enterprise level through access control software and at the application level through menus and scripts. Accordingly, application controls may enhance or refine general computer controls. However, many application controls operate only at the application level—for example, controls that enhance the integrity of information, such as edit checks that ensure a valid date or an appropriate numerical sequence or that identify missing documents. There is a third category of application controls—the automation of control processes such as the matching of purchase orders with receipt records and invoices.

Traditionally, controls were designed into applications, but were frequently not well documented or well maintained. Accordingly, many legacy systems, while having controls incorporated into the programs, do not reflect current requirements. In certain cases, additional controls have been designed into legacy systems, often enhancing, while at the same time repeating, existing controls.

New software and particularly ERP systems have incorporated many controls into the software. However, they must be activated and customised to become operational. They offer a range of settings from no controls to extensive controls. From an audit perspective, it is important to select and implement the correct options and procedures to ensure any errors or questionable items are appropriately followed up, assessed and tested.

In this section of the guidance, traditional system and ERP system considerations have been separated. However, when dealing with an ERP system, the IT auditor should review the control and other procedures identified in the traditional system development approach and augment that information with ERP system-specific information.

### 3653 Auditing Traditional Application Controls

#### 3653.1

Traditional applications have usually been developed using a structured process that, in addition to the initial development, deals with subsequent enhancements and maintenance. This is often the SDLC.

Auditing the SDLC can identify the role that security and control experts, risk management personnel, end users, and management have played in the development process and, therefore, the role they played in ensuring the adequacy of the controls designed and implemented into the applications.

Application controls include a wide variety from input/origination controls to controls during processing, controls over information and reporting controls.
<table>
<thead>
<tr>
<th>3653.1 cont.</th>
<th>Auditing Traditional Application Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>– AI4 Enable operation and use.</td>
</tr>
<tr>
<td></td>
<td>– AI5 Procure IT resources.</td>
</tr>
<tr>
<td></td>
<td>– AI6 Manage changes.</td>
</tr>
<tr>
<td></td>
<td>– DS1 Define and manage service levels.</td>
</tr>
<tr>
<td></td>
<td>– DS2 Manage third-party services.</td>
</tr>
<tr>
<td></td>
<td>– DS3 Manage performance and capacity.</td>
</tr>
<tr>
<td></td>
<td>– DS4 Ensure continuous service.</td>
</tr>
<tr>
<td></td>
<td>– DS5 Ensure systems security.</td>
</tr>
<tr>
<td></td>
<td>– DS6 Educate and train users.</td>
</tr>
</tbody>
</table>

3653.2 Input Authorisation
This section addresses the various means by which information is introduced to applications, and the types of controls that can be used to identify and authenticate the user attempting to access the application and input data.

- G27 Mobile Computing
- G33 General Considerations for the Use of the Internet
- G37 Configuration Management Process
- CoSiT:
  - PO6 Communicate management aims and direction.
  - PO7 Manage IT human resources.
  - PO8 Manage quality.
  - PO9 Assess and manage IT risks.
  - AI2 Acquire and maintain application software.
  - AI3 Acquire and maintain technology infrastructure.
  - AI4 Enable operation and use.
  - AI5 Procure IT resources.
  - AI6 Manage changes.
  - DS1 Define and manage service levels.
  - DS2 Manage third-party services.
  - DS5 Ensure systems security.
  - DS8 Manage service desk and incidents.
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>3653 cont.</td>
<td>Auditing Traditional Application Controls</td>
</tr>
</tbody>
</table>
| 3653.2 Input Authorisation cont. | – DS9 Manage the configuration.  
|              | – DS10 Manage problems.  
|              | – ME1 Monitor and evaluate IT performance.  
|              | – ME2 Monitor and evaluate internal control.  
|              | – ME3 Ensure compliance with external requirements.  
|              | – ME4 Provide IT governance. |

### 3653.3 Batch Controls and Balancing

Many financial systems still rely on batch processing and, accordingly, have an opportunity to balance batches of transactions and maintain controls during the process. Applications such as payroll, check payments and pension payments and files received from outside the organisation offer the opportunity to ‘batch’ the information prior to input.

- G23 System Development Life Cycle (SDLC) Reviews
- CoaT:  
  - PO8 Manage quality.  
  - PO10 Manage projects.  
  - AI1 Identify automated solutions.  
  - AI2 Acquire and maintain application software.  
  - AI3 Acquire and maintain technology infrastructure.  
  - AI4 Enable operation and use.  
  - AI5 Procure IT resources.  
  - AI6 Manage changes.  
  - DS1 Define and manage service levels.  
  - DS2 Manage third-party services.  
  - DS3 Manage performance and capacity.  
  - DS4 Ensure continuous service.  
  - DS5 Ensure systems security.  
  - DS7 Educate and train users.  
  - ME3 Ensure compliance with external requirements.
<table>
<thead>
<tr>
<th>3600—IT Audit and Assurance Processes <em>(cont.)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Processes</td>
</tr>
<tr>
<td><strong>3653</strong> <em>(cont.)</em></td>
</tr>
</tbody>
</table>

### 3653.4 Input and Process Editing

Identifying erroneous data at the earliest possible time is an effective means of preventing contamination of existing information and databases when new transactions are introduced. Many financial systems still rely on batch processing; thus, batch control techniques can provide a useful means to establishing control over transactions entering the application and to maintain that control throughout the processing cycle.

### 3653.5 Rejection/Suspense of Transactions

Identifying erroneous or questionable items may be the first line of defence but, to be effective, the identified items must be dealt with. This could involve a number of approaches—from processing the items and tagging them for further follow-up to halting processing until the erroneous items are correct, when processing can resume. The degree of severity of the error or the pervasiveness of the erroneous item will dictate the most appropriate actions.

This section provides the IT audit and assurance professional with information on the rejection or suspension of transactions, when to use specific techniques as well as the advantages and disadvantages of each, and implementing an effective approach.

### 3653.6 Batch Integrity in Online or Database Systems

Online systems present additional security and control issues. The ability to ‘batch’ transactions may not be present until well into the processing cycle. Completeness and integrity have to be addressed and controls designed to afford an appropriate level of control. Database systems and shared environments, where multiple owner/users may access data, present another range of problems in identifying which user/application update to review should errors be found or the database become contaminated. Guidance in this section addresses additional security and control concerns, and provides information and solutions to mitigate or analyse the risks.

### 3653.7 Processing Procedures and Controls

Once data enter the system, they must be controlled. Integrity, completeness, accuracy, etc., are key to ensuring availability and reliability of information. Processing procedures and related controls are essential to achieving a well-controlled environment. Any process that results in an erroneous result is likely to contaminate the database and affect additional users and transactions. Timely identification and correction are essential.

Many systems test the completion of the execution of a transaction and provide a completion or condition code. However, it is up to the application developer to conduct important steps such as testing the completion code after each transaction is executed and providing for a response, recording the transaction elsewhere (suspense file), and canceling the transaction.
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3653 cont. Auditing Traditional Application Controls</strong></td>
<td></td>
</tr>
<tr>
<td><strong>3653.8 Output Controls</strong></td>
<td>This section addresses ensuring processed information, interim processing status and requests for user input reach the correct user in a timely manner through the proper design and implementation of output controls. Output controls focus on two areas: ensuring output information is complete and accurate, and integrity is maintained; and ensuring output reports, documents and screen presentations are sent to, and received by, the appropriate user.</td>
</tr>
</tbody>
</table>
| | **CoIT:**  
| | – ME2 Monitor and evaluate internal control.  
| | – ME3 Ensure compliance with external requirements.  
| | – ME4 Provides IT governance.  |
| **3653.9 Application Access** | While access controls to networks, host computers and other technology resources are usually controlled at the enterprise level by access control software, organisations frequently rely on application-based menus to provide a refinement of the access controls. The application menu ensures users are granted access to only the application features to which, through their menu-based privileges, they have been granted permission. |
| | **CoIT:**  
| | – ME2 Monitor and evaluate internal control.  
| | – ME3 Ensure compliance with external requirements.  
| | – ME4 Provides IT governance.  |
| **3653.10 Log Management** | Computing and network devices as well as database management systems can create logs of various activities. Such logs are usually not maintained for long and are primarily used for restart/recovery activities. The creation of logs can benefit the IT audit and assurance professional in that the logs can be reviewed, using CAATs, to ascertain whether certain rules are being enforced and complied with. |
| | **CoIT:**  
| | – ME2 Monitor and evaluate internal control.  
| | – ME3 Ensure compliance with external requirements.  
| | – ME4 Provides IT governance.  |
| **3653.11 End-user Computing Applications** | End-user computing activities are usually classified into two types:  
| | • End-user personal productivity tools such as word processing and spreadsheet applications  
| | • End-user applications that provide a front end into application programs and data repositories  
| | End-user applications, particularly those based on personal productivity tools, create additional requirements for security and control in that they usually do not have:  
| | • Robust access control  
| | • A change management system  
| | • Quality assurance procedures during their design, development and maintenance  
| | Accordingly, to ensure the integrity of information processed on such systems, management must implement additional controls.  |
| | **CoIT:**  
| | – ME2 Monitor and evaluate internal control.  
| | – ME3 Ensure compliance with external requirements.  
| | – ME4 Provides IT governance.  |
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>3653 cont.</th>
<th>Auditing Traditional Application Controls</th>
</tr>
</thead>
</table>

#### 3653.12 Business Intelligence

Business intelligence software is designed to combine information from a number of sources for presentation to management and others, and forms the basis for sophisticated analysis and decision-making programs.

While business intelligence software offers management some distinct advantages, it also creates security and control issues related to the information being aggregated, the possible violation of privacy laws, the completeness of the information being presented for the proposed purpose and the currency of the information being aggregated.

<table>
<thead>
<tr>
<th>3655</th>
<th>Auditing Enterprise Resource Planning (ERP) Systems</th>
</tr>
</thead>
</table>

#### 3655.1 ERP Systems—IT General Controls (as applicable)

Auditing ERP systems presents the auditor with additional issues, risks and concerns. The IT audit and assurance professional should complete the audit of general controls using the material in section 3630, Auditing IT General Controls.

In addition, the IT audit and assurance professional should be prepared to assess the changed control environment as a result of the introduction of an ERP system, considering the following IT general computer controls:
- Logical access
- Change management
- IT ERP operations

Further, the IT audit and assurance professional should consider such IT general controls as:
- Application configuration
- Security
- Processes (controls specific to the process in the organisation)

Of key concern is the control over access to, and the right to change, configuration, security and audit settings.

#### 3655.2 ERP Systems—Application Controls

Auditing ERP applications presents the auditor with additional issues, risks and concerns. The IT audit and assurance professional should complete the audit of application controls using the material in section 3650, Auditing Application Controls, and section 3653, Auditing Traditional Application Controls.

In addition, the IT audit and assurance professional should be prepared to assess the changed control environment as a result of the introduction of an ERP system, considering the following IT general controls:
- Application configuration
- Security
- Process (controls specific to the process in the organisation)

He or she should be prepared to assess the changed control environment as a result of the implementation of an ERP system.
This section introduces the IT audit and assurance professional to different and non-traditional software development strategies.

In the face of increasing systems complexity, software developers have created alternative strategies to reduce development and maintenance time and costs, and to improve the quality of the software being produced. These new techniques may complement, change or replace traditional SDLC processes. The introduction of portals, web services, service-oriented software, Unified Modeling Language (UML), etc., are key drivers in the need to adopt new internal controls.

This guidance introduces various strategies and addresses their appropriate use, strengths and weaknesses, and special audit considerations. It also provides a comparison with the more traditional strategies.

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| Auditing Alternative Software Development Strategies | • G14 Application Systems Review  
• G23 System Development Life Cycle (SDLC) Reviews  
• G26 Business Process Re-engineering (BPR) Project Reviews  
• CoaT:  
  – P01 Define a strategic IT plan.  
  – P04 Define the IT processes, organisation and relationships.  
  – P05 Manage the IT investment.  
  – P06 Communicate management aims and direction.  
  – P07 Manage IT human resources.  
  – P08 Manage quality.  
  – P09 Assess and manage IT risks.  
  – P010 Manage projects.  
  – A11 Identify automated solutions.  
  – A12 Acquire and maintain application software.  
  – A13 Acquire and maintain technology infrastructure.  
  – A14 Enable operation and use.  
  – A15 Procure IT resources.  
  – A16 Manage changes.  
  – DS1 Define and manage service levels.  
  – DS2 Manage third-party services.  
  – DS3 Manage performance and capacity.  
  – DS4 Ensure continuous service.  
  – DS5 Ensure systems security.  
  – DS7 Educate and train users.  
  – DS10 Manage problems.  
  – DS13 Manage operations. |
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>3657 cont.</td>
<td>Auditing Alternative Software Development Strategies</td>
</tr>
<tr>
<td></td>
<td>– ME1 Monitor and evaluate IT performance.</td>
</tr>
<tr>
<td></td>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td></td>
<td>– ME3 Ensure compliance with external requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3660</th>
<th>Auditing Specific Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This section addresses two specific auditing requirements categorised as follows:</td>
</tr>
<tr>
<td></td>
<td>• Government-specified criteria</td>
</tr>
<tr>
<td></td>
<td>• Industry-specified criteria</td>
</tr>
<tr>
<td></td>
<td>Within each category, ITAF provides information on when the specific criteria are required, which references to the audit procedures should be followed, and which issues in conducting such audits and reporting should be considered.</td>
</tr>
<tr>
<td></td>
<td>• G24 Internet Banking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3661</th>
<th>Auditing Government-specified Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Governments, agencies, regulators and other public-sector oversight bodies frequently specify audit requirements to organisations they regulate. Frequently, such requirements are placed in regulations and require a specific type of audit or dictate the procedures to be followed. Within this section, a number of such requirements are discussed, and work programmes are identified and provided as part of the tools and techniques.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3662</th>
<th>Auditing Industry-specified Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Industry groups frequently require members to adhere to industry standards. As such, members may be required to provide the industry groups with an audit report indicating their compliance with the industry standards. The payment card industry requires audits of some of its merchants. The bank card industry requires audits to maintain membership and, therefore, use such facilities as Interac and Plus.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3670</th>
<th>Auditing With Computer-assisted Audit Techniques (CAATs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3670.1 CAATs</td>
<td>This section introduces CAATs and provides information on three types:</td>
</tr>
<tr>
<td></td>
<td>• Data testing</td>
</tr>
<tr>
<td></td>
<td>• Systems testing</td>
</tr>
<tr>
<td></td>
<td>• Information modeling and analysis</td>
</tr>
<tr>
<td></td>
<td>• G3 Use of Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td></td>
<td>• CosiT:</td>
</tr>
<tr>
<td></td>
<td>– DS5 Ensure system security.</td>
</tr>
<tr>
<td></td>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
</tbody>
</table>
### 3670.1 CAATs cont.
This section also provides information on considering when the use of CAATs may be appropriate; addressing and resolving technical issues; and ensuring integrity of the CAAT process, including security over the CAAT software, the file of selected items and the selection process. It also addresses CAAT planning issues, data retention, data integrity and completeness, privacy and confidentiality concerns, and the removal of files or selected records to the auditor’s computer and potentially offsite. In addition, it addresses the use of CAATs in various environments, including continuous auditing.

### 3670.2 Selecting a Data Analysis Technique
This guidance addresses the advantages and disadvantages of using various data analysis techniques and how to match the various techniques with the IT audit objectives.

### 3670.3 Planning Data Analysis in the Audit Process
This section provides the IT audit and assurance professional with information on how to assess various IT assurance activities and data analysis techniques.

- G3 Use of Computer-assisted Audit Techniques (CAATs)
- CoIT:
  - DS5 Ensure system security.
  - ME2 Monitor and evaluate internal control.

### 3670.4 Data Analysis in Control Testing
This section provides the IT audit and assurance professional with information on how CAATs can be used in support of controls testing. Where controls are automated, where security and control settings are available in electronic format or where historical information such as last access date are recorded, CAATs can be used to quickly and efficiently identify issues, concerns, violations or anomalies for further investigation.

- G3 Use of Computer-assisted Audit Techniques (CAATs)
- CoIT:
  - DS5 Ensure system security.
  - ME2 Monitor and evaluate internal control.

### 3670.5 Establishing a Data Analysis Programme
This section provides the IT audit and assurance professional with information on establishing a data analysis programme within the IT audit organisation. It provides guidance on the various requirements for tools, techniques, staffing, education and training, and for ensuring the tools selected are appropriate for the audit objectives and are compatible with the target client or IT organisation’s technology.

- G3 Use of Computer-assisted Audit Techniques (CAATs)
- CoIT:
  - DS5 Ensure system security.
  - ME2 Monitor and evaluate internal control.

### 3670.6 Integrating CAATs Into the Audit Process
Frequently, IT audit and assurance professionals form part of a larger audit team and may be asked to support that team with CAATs. This section addresses the issues and procedures required to effectively integrate the IT audit CAATs work in support of other audit processes.

- G3 Use of Computer-assisted Audit Techniques (CAATs)
- CoIT:
  - DS5 Ensure system security.
  - ME2 Monitor and evaluate internal control.
## 3670.7 CAATs in Control Testing

The use of CAATs in control testing offers the IT audit and assurance professional a number of opportunities to add efficiency and effectiveness to the audit process. This section provides the IT assurance professional with suggestions, scenarios and case studies that provide information on how to use CAATs in conducting controls testing.

<table>
<thead>
<tr>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• G3 Use of Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td>• G8 Audit Documentation</td>
</tr>
<tr>
<td>• COSI:</td>
</tr>
<tr>
<td>– P01 Define a strategic IT plan.</td>
</tr>
<tr>
<td>– P08 Manage quality.</td>
</tr>
<tr>
<td>– A16 Manage changes.</td>
</tr>
<tr>
<td>– D51 Define and manage service levels.</td>
</tr>
<tr>
<td>– D55 Ensure systems security.</td>
</tr>
<tr>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td>– ME3 Ensure compliance with external requirements.</td>
</tr>
</tbody>
</table>

## 3670.8 Establishing a CAAT Programme

Establishing a CAAT programme requires obtaining the right resources and managing the expectations and fears of the auditee. Traditionally, data owners have been fearful of letting others, including IT audit and assurance professionals, have electronic access to their information. This section explores the issues and concerns, and provides hints and tips for establishing a successful CAAT programme.

<table>
<thead>
<tr>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• G3 Use of Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td>• COSI:</td>
</tr>
<tr>
<td>– D55 Ensure systems security.</td>
</tr>
<tr>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
</tbody>
</table>

## 3670.9 Managing a CAAT Project

The use of CAATs requires considerable planning to ensure files and information are obtained by the IT audit and assurance professional when they are available or are retained by the client until used by the IT audit and assurance professional. This frequently requires retention beyond the normal cycle. Managing client expectations and concerns over assurance professional access to certain files must be dealt with when managing a CAAT project.

<table>
<thead>
<tr>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• G3 Use of Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td>• COSI:</td>
</tr>
<tr>
<td>– D55 Ensure systems security.</td>
</tr>
<tr>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
</tbody>
</table>

## 3670.10 Using CAATs in a Continuous Auditing Environment

CAATs can be used to effectively monitor transactions, identify anomalies or select transactions for further investigation based on predetermined criteria. This section addresses issues the IT assurance professional must consider when using CAATs in a continuous audit environment.

<table>
<thead>
<tr>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• G3 Use of Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td>• G8 Audit Documentation</td>
</tr>
<tr>
<td>• COSI:</td>
</tr>
<tr>
<td>– P01 Define a strategic IT plan.</td>
</tr>
<tr>
<td>– P08 Manage quantity.</td>
</tr>
<tr>
<td>– A16 Manage changes.</td>
</tr>
<tr>
<td>– D51 Define and manage service levels.</td>
</tr>
<tr>
<td>– D55 Ensure systems security.</td>
</tr>
</tbody>
</table>
### 3670.10 Using CAATs in a Continuous Auditing Environment

- ME2 Monitor and evaluate internal control.
- ME3 Ensure compliance with external requirements.

### 3670.11 Using Client Data

CAATs often require that the IT audit and assurance professional have access to and use client data that are in the custody of the IT department but are ‘owned’ by users of the IT service. This section addresses the issues the IT audit and assurance professional must consider when using client data, including custody and control, removal from premises, privacy, security, and effect on existing or other records.

- **G3 Use of Computer-assisted Audit Techniques (CAATs)**
- **G7 Due Professional Care**
- **G8 Audit Documentation**
- **CObIT:**
  - PO1 Define a strategic IT plan.
  - PO6 Communicate management aims and direction.
  - PO7 Manage IT human resources.
  - PO8 Manage quality.
  - PO9 Assess and manage IT risks.
  - AI6 Manage changes.
  - DS1 Define and manage service levels.
  - DS5 Ensure systems security.
  - ME2 Monitor and evaluate internal control.
  - ME3 Ensure compliance with external requirements.
  - ME4 Provide IT governance.

### 3670.12 Documenting CAATs

Regardless of the form or type of CAAT being used, the assurance professional must document the use of the CAAT and the results. Because many CAATs require considerable preparation time, integration and use of client facilities, and control over the CAAT process and the resulting files, documentation of certain key aspects is critical in ensuring effective operation of the CAAT in subsequent periods.

- **G3 Use of Computer-assisted Audit Techniques (CAATs)**
- **G8 Audit Documentation**
- **CObIT:**
  - PO1 Define a strategic IT plan.
  - PO8 Manage quality.
  - AI6 Manage changes.
  - DS1 Define and manage service levels.
  - DS5 Ensure systems security.
### 3600—IT Audit and Assurance Processes (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3670</strong></td>
<td>Auditing With Computer-assisted Audit Techniques (CAATs)</td>
</tr>
<tr>
<td><strong>3670.12</strong> Documenting CAATs</td>
<td>cont.</td>
</tr>
<tr>
<td></td>
<td>– ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td></td>
<td>– ME3 Ensure compliance with external requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3680</strong></th>
<th>IT Auditing and Regulatory Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section is designed to help the IT audit and assurance professional understand the concepts of auditing and reporting on compliance with legislation and regulations.</td>
<td></td>
</tr>
<tr>
<td>In many jurisdictions, it is the purview of the legal profession to express judgements or issue a professional opinion on legislation and regulations. As such, the auditor, particularly if in public accounting, must ensure work being undertaken does not contravene local laws.</td>
<td></td>
</tr>
<tr>
<td>One means to avoid the situation is for management to develop assertions regarding such compliance and, after review for completeness and appropriateness by the IT auditor, use them as the basis for any opinion.</td>
<td></td>
</tr>
<tr>
<td>• <strong>IT Control Objectives for Sarbanes-Oxley, 2nd Edition</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>IT Control Objectives for Basel II</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3690</strong></th>
<th>Selecting Items of Assurance Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section introduces the concept of testing less than 100 percent of the population of items of audit interest. It establishes the requirements for being able to draw conclusions from such samples, the criteria required to consider using samples and the information the auditor can obtain from the use of sampling.</td>
<td></td>
</tr>
<tr>
<td>The section also discusses the pros, cons and considerations for using sampling.</td>
<td></td>
</tr>
<tr>
<td>The section also discusses the various types of samples, including:</td>
<td></td>
</tr>
<tr>
<td>• Risk-based selection</td>
<td></td>
</tr>
<tr>
<td>• Judgemental samples</td>
<td></td>
</tr>
<tr>
<td>• Statistical samples</td>
<td></td>
</tr>
<tr>
<td>• Estimation samples</td>
<td></td>
</tr>
<tr>
<td>• 100-percent testing</td>
<td></td>
</tr>
<tr>
<td>• Continuous auditing</td>
<td></td>
</tr>
<tr>
<td>• Continuous monitoring</td>
<td></td>
</tr>
<tr>
<td>• Other selection techniques</td>
<td></td>
</tr>
<tr>
<td>Also discussed are the types of tests that can be performed, including:</td>
<td></td>
</tr>
<tr>
<td>• Attribute (correct or incorrect, signed or not signed, etc.)</td>
<td></td>
</tr>
<tr>
<td>• Estimation (the project amount)</td>
<td></td>
</tr>
<tr>
<td>Also discussed are the various types of statistical samples commonly used by auditors, including:</td>
<td></td>
</tr>
<tr>
<td>• Monetary unit or cumulative monetary amounts</td>
<td></td>
</tr>
<tr>
<td>• Variables estimation</td>
<td></td>
</tr>
<tr>
<td>The section also introduces the auditor to the various evaluation techniques and their pros and cons.</td>
<td></td>
</tr>
<tr>
<td>• <strong>G2 Audit Evidence Requirement</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>G9 Audit Considerations for Irregularities</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>G10 Audit Sampling</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>G19 Irregularities and Illegal Acts</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>CoSIT:</strong></td>
<td></td>
</tr>
<tr>
<td>– ME2 Monitor and evaluate internal control.</td>
<td></td>
</tr>
</tbody>
</table>
Section 3800—IT Audit and Assurance Management

Section 3800 addresses IT audit and assurance management. Guidance in this section provides the IT audit and assurance professional with an understanding of information required to manage an IT audit assignment. The section commences with information about the creation and management of the IT audit or assurance function and follows with discussion of various IT audit and assurance management topics. These topics include audit and assurance planning and scoping, then refining the initial scoping, putting information into a detailed IT audit plan and scope document that incorporates the IT audit or assurance objectives. Next, this section addresses managing the execution of the IT audit and assurance professional’s work. The section provides guidance in documenting assurance work, and documenting and clearing findings and recommendations. The section also addresses effective assurance reporting considerations.

Section 3800 addresses guidelines in the following areas:

<table>
<thead>
<tr>
<th>Section</th>
<th>Guideline Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>3810</td>
<td>IT Audit or Assurance Function</td>
</tr>
<tr>
<td>3820</td>
<td>Planning and Scoping IT Audit and Assurance Objectives</td>
</tr>
<tr>
<td>3830</td>
<td>Planning and Scoping IT Audit and Assurance Work</td>
</tr>
<tr>
<td>3835</td>
<td>Planning and Scoping Risk Assessments</td>
</tr>
<tr>
<td>3840</td>
<td>Managing the IT Audit and Assurance Process Execution</td>
</tr>
<tr>
<td>3850</td>
<td>Integrating the Audit and Assurance Process</td>
</tr>
<tr>
<td>3860</td>
<td>Gathering Evidence</td>
</tr>
<tr>
<td>3870</td>
<td>Documenting IT Audit and Assurance Work</td>
</tr>
<tr>
<td>3875</td>
<td>Documenting and Confirming IT Audit and Assurance Findings</td>
</tr>
<tr>
<td>3880</td>
<td>Evaluating Results and Developing Recommendations</td>
</tr>
<tr>
<td>3890</td>
<td>Effective IT Audit and Assurance Reporting</td>
</tr>
<tr>
<td>3892</td>
<td>Reporting IT Audit and Assurance Recommendations</td>
</tr>
<tr>
<td>3894</td>
<td>Reporting on IT Advisory and Consultancy Reviews</td>
</tr>
</tbody>
</table>

The following table represents a drill-down of section 3800. It identifies potential areas for the development of ISACA guidelines, provides information as to the scope and content of the guideline, and lists existing relevant ISACA resources and some illustrative techniques to be considered (whether existing or not).

<table>
<thead>
<tr>
<th>3800—IT Audit and Assurance Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Processes</td>
</tr>
<tr>
<td>3810 IT Audit or Assurance Function</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Establishing the IT audit or assurance function is a one-time activity, although monitoring, assessing and implementing improvements are ongoing tasks. Accordingly, guidance in this section differs from the remainder of the IT process guidance, which contemplates adoption and reuse on multiple IT assurance assignments.
### 3800—IT Audit and Assurance Management

#### IT Processes

<table>
<thead>
<tr>
<th>3810</th>
<th>IT Audit or Assurance Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cont.</strong></td>
<td></td>
</tr>
<tr>
<td>Guidance in the IT audit or assurance function addresses the establishment of the function, development of its <em>raison d’etre</em>, its position in the enterprise, its strategic and operational models, and the resources it requires and commands.</td>
<td></td>
</tr>
<tr>
<td>This section will address the following topics:</td>
<td></td>
</tr>
<tr>
<td>• Organising an IT audit capability</td>
<td></td>
</tr>
<tr>
<td>• Establishing the IT audit function</td>
<td></td>
</tr>
<tr>
<td>• Developing an IT audit charter</td>
<td></td>
</tr>
<tr>
<td>• Establishing IT audit strategy</td>
<td></td>
</tr>
<tr>
<td>• Developing an IT auditor staffing and resourcing model</td>
<td></td>
</tr>
<tr>
<td>• Establishing IT audit methodology</td>
<td></td>
</tr>
<tr>
<td>• Considering tools and techniques</td>
<td></td>
</tr>
<tr>
<td>• Formalising lines of reporting</td>
<td></td>
</tr>
<tr>
<td>• Formalising financing and budgeting requirements</td>
<td></td>
</tr>
<tr>
<td>• Establishing key contacts/sponsors</td>
<td></td>
</tr>
<tr>
<td>• Establishing communication channels</td>
<td></td>
</tr>
<tr>
<td>• Creating the IT audit infrastructure</td>
<td></td>
</tr>
<tr>
<td>• Monitoring IT audit performance on an individual engagement</td>
<td></td>
</tr>
<tr>
<td>• Monitoring overall IT audit department performance</td>
<td></td>
</tr>
<tr>
<td>The section also deals with:</td>
<td></td>
</tr>
<tr>
<td>• Responsibility</td>
<td></td>
</tr>
<tr>
<td>• Authority</td>
<td></td>
</tr>
<tr>
<td>• Accountability</td>
<td></td>
</tr>
<tr>
<td>• Communication with auditees, executive management and the board</td>
<td></td>
</tr>
<tr>
<td>• Quality assurance process</td>
<td></td>
</tr>
<tr>
<td>While this section deals with pre-audit considerations, it provides a background and foundation upon which the IT assurance function is based.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3820</strong></th>
<th>Planning and Scoping IT Audit and Assurance Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section deals with working with the board, executive management and the auditee to create an IT audit or assurance plan that meets the objectives of the various stakeholders. Establishing IT audit or assurance objectives incorporates elements of the general audit objectives and those associated with information technology.</td>
<td></td>
</tr>
<tr>
<td>The section also introduces concepts of risks associated with adopting specific technologies, processes, applications and systems.</td>
<td></td>
</tr>
<tr>
<td>This section next addresses the issues associated with identifying the audit universe; determining the issues within business units, processes and organisations; and assessing the technologies used and their implication on the risk environment in which the entity operates and the control structure required.</td>
<td></td>
</tr>
</tbody>
</table>

#### ISACA Resources

- **CobiT**:  
  - ME2 Monitor and evaluate internal control.  
  - ME4 Provide IT governance.

- **IT Assurance Guide**:  
  - *Using CobiT*  
  - CobiT  
  - SS Planning
3800—IT Audit and Assurance Management

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3820</strong> Planning and Scoping IT Audit and Assurance Objectives</td>
<td></td>
</tr>
</tbody>
</table>

**An important part of the process is identifying and addressing the needs of key stakeholders. These could include other groups within internal audit, external auditors, audit committees and corporate compliance groups.**

| **3830** Planning and Scoping IT Audit and Assurance Work |  |

This section addresses scoping IT audit initiatives, projects and assignments. It relies on ISACA’s 14-step scoping model and builds on the information provided therein.

The 14 steps are:
- **Define Audit Initiative**
  - Define audit objectives.
  - Define boundaries of the audit.
  - Define standards against which the subject matter will be assessed.
  - Identify and document risks.
  - Define the change process.
  - Define assignment success.
  - Define audit resources required.
  - Define deliverables.

- **Plan Audit Initiative**
  - Obtain executive support.
  - Finalise required audit resources.
  - Define the audit team to support the IT audit initiative.
  - Document and agree on timelines.
  - Define, finalise and agree on the audit approach and methodology.
  - Define and implement a communications plan.

This section illustrates how to customise ISACA’s scoping and planning methodology for use in conducting IT audits.

| **3835** Planning and Scoping Risk Assessments |  |

Guidance in this section provide the IT audit and assurance professional with information on planning, conducting and evaluating risk assessments.

Three risk assessment topics are addressed: engagement risk, performance risk and reporting risk.

*Engagement risk* refers to the risk of undertaking specific audit or assurance work. This includes risks associated with the type of engagement, type of client, and industry. The guidance provides information on risk identification, mitigation and management.
<table>
<thead>
<tr>
<th><strong>3800—IT Audit and Assurance Management (cont.)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Processes</strong></td>
</tr>
<tr>
<td><strong>3835 cont.</strong></td>
</tr>
</tbody>
</table>

**Performance risk** addresses the risks associated with conducting the engagement. Information may not be available; specialists may be required; location of records, hardware or processing sites may be restricted; etc. Performance risks are risks that, while manageable, may require the IT audit and assurance professional to modify the approach, timing and performance of various tests.

**Reporting risk** addresses issues and concerns over various types of reports. Reporting risks arise when the expectations of clients and users of IT audit and assurance reports differ from what the IT audit and assurance professional can deliver. In addition, reporting risks arise when the nature of the work requires additional procedures or competencies. For example, an examination-level report for use by regulators presents an increased risk compared with a review-level report developed for internal use by the organisation.

Risk assessment techniques can be used to select areas and specific items of audit interest.

| **3840** | **Managing the IT Audit and Assurance Process Execution** |
|-----------------------------------------------|

This section provides information and guidance on the various aspects of managing IT audit or assurance initiatives. IT audits are frequently performed under deadline pressure, so good planning, appropriate resourcing and excellent time management are required to complete the audit and meet expectations.

Management skills are important in ensuring roles, responsibilities, activities and expectations are clearly defined and communicated. Further, monitoring and mentoring are key to maintaining timelines to ensure project budgets and deadlines are met.

This section provides information on the critical activities required to manage an IT audit or assurance initiative, including:

- Planning and budgets
- Timelines and resources
- Roles and responsibilities
- Supervision of work
- Monitoring of progress
- Dealing with errors, compliance deficiencies and other findings
- Use of specialists and other experts
- Communications (team and client)
- Contingency planning
- Client-auditee relations

<table>
<thead>
<tr>
<th><strong>ISACA Resources</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• G1 Using the Work of Other Auditors</td>
</tr>
<tr>
<td>• G6 Materiality Concepts for Auditing Information Systems</td>
</tr>
<tr>
<td>• G7 Due Professional Care</td>
</tr>
<tr>
<td>• G8 Audit Documentation</td>
</tr>
<tr>
<td>• G13 Use of Risk Assessment in Audit Planning</td>
</tr>
<tr>
<td>• G15 Planning</td>
</tr>
<tr>
<td>• G30 Competence</td>
</tr>
<tr>
<td>• COBIT:</td>
</tr>
</tbody>
</table>
  - P01 Define a strategic IT plan.  |
  - P05 Manage the IT investment.  |
  - P07 Manage IT human resources.  |
  - P08 Manage quality.  |
  - A11 Identify automated solutions.  |
  - A16 Manage changes.  |
  - DS1 Define and manage service levels.  |
  - DS2 Manage third-party services.  |
  - DS3 Manage performance and capacity.  |
  - DS7 Educate and train users.  |
### 3800—IT Audit and Assurance Management (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
</table>
| **3840 cont.** Managing the IT Audit and Assurance Process Execution | – DS10 Manage problems.  
– DS13 Manage operations.  
– ME1 Monitor and evaluate IT performance.  
– ME2 Monitor and evaluate internal control.  
– ME3 Ensure compliance with external requirements.  
– ME4 Provide IT governance. |

### 3850 Integrating the Audit and Assurance Process

This section addresses the need for and considerations in dealing with other assurance professionals in the execution of an IT audit or assurance initiative. It provides guidance on integrating IT audit or assurance planning with the initiatives of business auditors and risk managers. It also addresses the integration of audit or assurance planning activities.

- **IT Assurance Guide: Using CoSiT.**

### 3860 Gathering Evidence

Guidance in this section addresses identifying items of audit or assurance interest, gathering audit or assurance evidence, and addressing the assertions regarding the subject matter about which the evidence is being gathered.

- **G2 Audit Evidence Requirement**
- **G28 Computer Forensics**
- **CoSiT:**  
  – ME2 Monitor and evaluate internal control.

### 3870 Documenting IT Audit and Assurance Work

This section addresses the documentation requirements necessary to ensure the audit or assurance work undertaken, the decisions made, the testing performed, the audit observations and findings generated the analyses performed, the conclusions reached and recommendations made are all adequately supported.

The section provides guidance in each area of the audit or assurance cycle; identifies the issues, risks and pitfalls; and gives the IT assurance professional a road map to follow.

- **G2 Audit Evidence Requirement**
- **G8 Audit Documentation**
- **G20 Reporting**
- **G35 Follow-up activities**
- **CoSiT:**  
  – PO1 Define a strategy IT plan.  
  – PO8 Manage quality.  
  – AI6 Manage changes.  
  – DS1 Define and manage service levels.  
  – ME2 Monitor and evaluate internal control.  
  – ME3 Ensure compliance with external requirements.
Section 3000—IT Assurance Guidelines: Putting the Standards Into Practice

<table>
<thead>
<tr>
<th>3870 cont.</th>
<th>Documenting IT Audit and Assurance Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>The section provides direction on a number of related issues, including:</td>
<td></td>
</tr>
<tr>
<td>• Types of evidence, electronic work papers and third-party evidence</td>
<td></td>
</tr>
<tr>
<td>• Legal requirements and work paper security</td>
<td></td>
</tr>
<tr>
<td>• Documentation requirements, records management and retention</td>
<td></td>
</tr>
<tr>
<td>• Consequences of findings for the audit, timing and content of exposure to management and management response</td>
<td>ISACA Resources</td>
</tr>
<tr>
<td>− ME4 Provide IT governance.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3875</th>
<th>Documenting and Confirming IT Audit and Assurance Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section focuses on creating effective audit working papers that adequately support the audit or assurance work performed, the conclusions reached, and the resulting recommendations.</td>
<td></td>
</tr>
<tr>
<td>Audit or assurance findings must be supported by appropriate evidence. The evidence may be manual, electronic or consist of some other media. The evidence may be direct, such as an erroneous document, or indirect, such as a third-party confirmation of an event. Care should be taken since audit evidence may become involved in litigation. Depending on the audit, documentation will be a legal and/or professional requirement as will adequate security over the working papers.</td>
<td>ISACA Resources</td>
</tr>
<tr>
<td>• G2 Audit Evidence Requirement</td>
<td></td>
</tr>
<tr>
<td>• G8 Audit Documentation</td>
<td></td>
</tr>
<tr>
<td>• G20 Reporting</td>
<td></td>
</tr>
<tr>
<td>• G35 Follow-up activities</td>
<td></td>
</tr>
<tr>
<td>• CoSI:</td>
<td></td>
</tr>
<tr>
<td>− P01 Define a strategic IT plan.</td>
<td></td>
</tr>
<tr>
<td>− P08 Manage quality.</td>
<td></td>
</tr>
<tr>
<td>− A6 Manage changes.</td>
<td></td>
</tr>
<tr>
<td>− DS1 Define and manage service levels.</td>
<td></td>
</tr>
<tr>
<td>− ME2 Monitor and evaluate internal control.</td>
<td></td>
</tr>
<tr>
<td>− ME3 Ensure compliance with external requirements.</td>
<td></td>
</tr>
<tr>
<td>− ME4 Provide IT governance.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3880</th>
<th>Evaluating Results and Developing Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process of evaluating the results of audit or assurance testing, after confirmation, to arrive at conclusions and recommendations can be complex. What appears to be a problem may, in fact, be the effect of a problem, not the cause. This section assists the IT assurance professional with guidance in recognising cause and effect, and determining root cause.</td>
<td></td>
</tr>
<tr>
<td>The section leads the IT audit and assurance professional through the process, from confirming facts with key individuals in the areas being audited, to determining root causes. The guidance then illustrates how individual findings can be used to provide examples that support higher-level analysis.</td>
<td></td>
</tr>
<tr>
<td>This section illustrates how to use higher-level analysis to:</td>
<td></td>
</tr>
<tr>
<td>• Develop various scenarios leading to potential recommendations</td>
<td></td>
</tr>
<tr>
<td>• Develop techniques to select an appropriate recommendation that is practical and achievable</td>
<td></td>
</tr>
<tr>
<td>• Identify steps necessary to ensure buy-in of key stakeholders</td>
<td>ISACA Resources</td>
</tr>
<tr>
<td>• G1 Using the Work of Other Auditors and Experts</td>
<td></td>
</tr>
<tr>
<td>• G6 Materiality Concepts for Auditing Information Systems</td>
<td></td>
</tr>
<tr>
<td>• G9 Audit Considerations for Irregularities</td>
<td></td>
</tr>
<tr>
<td>• G10 Audit Sampling</td>
<td></td>
</tr>
<tr>
<td>• CoSI:</td>
<td></td>
</tr>
<tr>
<td>− P05 Manage the IT investments.</td>
<td></td>
</tr>
<tr>
<td>− A11 Identify application solutions.</td>
<td></td>
</tr>
<tr>
<td>− DS10 Manage problems.</td>
<td></td>
</tr>
<tr>
<td>− DS13 Manage operations.</td>
<td></td>
</tr>
<tr>
<td>− ME2 Monitor and evaluate internal control.</td>
<td></td>
</tr>
<tr>
<td>− ME4 Provide IT governance.</td>
<td></td>
</tr>
</tbody>
</table>
### 3800—IT Audit and Assurance Management (cont.)

#### 3890 Effective IT Audit and Assurance Reporting

Effective audit and assurance reporting provides guidance in developing effective audit and assurance reports. Guidance includes report structure, contents and presentation, and addresses written, oral and presentation-style reports and the issues and concerns with each.

This section provides information on leveling and balancing findings, determining and reporting the root cause (not simply the effects), and ensuring audit observations support the findings and can be presented as such. The section also addresses the requirements of the ITAF reporting standard.

When performing audit and assurance work, it is suggested that ISACA members indicate that ‘The work was performed in accordance with ISACA audit and assurance standards’.

- S7 Reporting
- G9 Audit Considerations for Irregularities
- G20 Reporting
- G34 Responsibility,
  - Authority and
  - Accountability
- G35 Follow-up Activities
- CoSiT:
  - P06 Communicate management aims and direction.
  - P07 Manage IT human resources.
  - P08 Manage quality.
  - DS1 Define and manage service levels.
  - DS2 Manage third-party services.
  - DS10 Manage problems.
  - ME1 Monitor and evaluate IT performance.
  - ME2 Monitor and evaluate internal control.
  - ME3 Ensure compliance with external requirements.
  - ME4 Provide IT governance.

#### 3892 Reporting IT Audit and Assurance Recommendations

Section 3880 discusses analysing findings and developing effective recommendations. It also deals with reporting those recommendations.

Recommendations resulting from the conduct of audit and assurance engagements should be reported in a separate report and not as part of the audit or assurance report. The recommendations, which, as part of the reporting process require review and agreement by management and the auditee or other stakeholders, should be presented in a clear, concise and actionable manner.

Reports to senior management and executives should address issues and concepts, with detailed audit findings used as illustrations of the issue, problem or result. Reports to middle and line management should contain sufficient information to allow them to fully understand the issue and deal with the problem. Where appropriate, recommendations should include provision for timely monitoring and follow-up.

- S7 Reporting
- G9 Audit Considerations for Irregularities
- G20 Reporting
- CoSiT
### 3800—IT Audit and Assurance Management (cont.)

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>ISACA Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3892 cont.</strong> Reporting IT Audit and Assurance Recommendations</td>
<td></td>
</tr>
<tr>
<td>When performing audit and assurance work, it is suggested that ISACA members indicate that ‘The work was performed in accordance with ISACA audit and assurance standards’.</td>
<td></td>
</tr>
<tr>
<td><strong>3894</strong> Reporting on IT Advisory and Consultancy Reviews</td>
<td>ISACA IS Auditing Standards</td>
</tr>
<tr>
<td>ITAF focuses on standards and guidelines associated with conducting IT audit and assurance projects. It is recognised that IT audit and assurance professionals may be asked to perform other work that would not be classified as audit or assurance. For example, IT audit professionals are frequently asked to undertake work of an advisory or consultative nature. When IT audit professionals undertake such engagements, they should ensure the scope of the work to be undertaken and the type of report to be delivered are clearly communicated and understood. Such work, while beneficial to management, is usually not conducted with the rigour or scope of an audit or assurance project. Further, it usually does not involve testing of compliance.</td>
<td></td>
</tr>
<tr>
<td>IT audit and assurance professionals should take guidance from the information on reporting in section 2600. Such reports should indicate the scope of the work performed; any procedures used, such as interviews, observation and review of documents; and any restrictions placed on the use of the report.</td>
<td></td>
</tr>
<tr>
<td>Advisory and consultative work should comply with the appropriate general and performance standards contained in sections 2200 and 2400. In addition, ISACA members are expected to comply with the association’s Code of Professional Ethics as noted in section 2150.</td>
<td></td>
</tr>
</tbody>
</table>
Section 4000 — IT Assurance Tools and
Techniques (Reserved for
Future Development)

Section 4000 is reserved for those tools and techniques that provide additional examples an assurance professional could follow when performing IT assurance work. The tools and techniques section will include ISACA publications, books, white papers, relevant articles, audit programmes, internal control questionnaires (ICQs), auditing procedures, interview guides, templates, examples, instructions on how to use audit and assurance software and other techniques, and references to other relevant and reliable sources. Some resources in section 3000 may be recast to the tools and techniques category.
Appendix—Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:
1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member’s and/or certification holder’s conduct, and, ultimately, in disciplinary measures.
Glossary

Accountable party—In these standards:
• ‘Accountable party’ is referred to as management
• ‘User’ could include a variety of stakeholders, depending on the circumstances, such as shareholders, creditors, customers, the board of directors, the audit committee, legislators or regulators
• ‘Practitioner’ is the person who has overall responsibility for the performance of the assurance engagement and for the issuance of the report on the subject matter

Accountable relationship—Refers to the relationship that exists between the parties in an assurance engagement. An accountability relationship is a prerequisite for an assurance engagement. An accountability relationship exists when one party (the accountable party) is answerable to and/or is responsible to another party (the user) for a subject matter or voluntarily chooses to report to another party on a subject matter. The accountability relationship may arise either as a result of an agreement or legislation, or because a user can be expected to have an interest in how the accountable party has discharged its responsibility for a subject matter. (Source: Canadian Institute of Chartered Accountants)

Assertion—Refers to a declaration or set of declarations about the subject matter. Assertions should be based on, or be in conformity with, the criteria selected.

Assurance—In the context of this publication, the term means where, pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. For example, assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulations.

Assurance engagement—An engagement in which, pursuant to an accountability relationship between two or more parties, a practitioner is engaged to issue a written communication expressing a conclusion concerning a subject matter for which the accountable party is responsible. The following chart illustrates the relationship amongst the three parties in an assurance engagement.
**Assurance level**—Practitioners should, in theory, be able to vary infinitely the level of assurance provided in assurance engagements. However, to help users understand the level of assurance being provided by the practitioner, the standards in ITAF section 2000 limit assurance to two distinct levels—a high level and a moderate level. Both attestation engagements and direct reporting engagements can be completed with either a high or a moderate level of assurance. The level of assurance appropriate for a particular engagement depends on the needs of users and the nature of the subject matter.

**Assurance risk**—Refers to the risk that the IT audit and assurance professional may express an inappropriate conclusion based on the work performed. Assurance risk can be further categorised as inherent, control or detection risk.

**Assurance team**—Refers to the person or persons who perform the assurance work. The assurance team may include specialists as required.

**Attestation risk**—Refers to the risk that the assurance professional will draw an incorrect conclusion based on the assessment of controls, the inherent limitations of those controls, the use of testing rather than examining 100 percent of the transactions or other available information, the quality of the information or evidence available, and the degree to which the assurance professional must use professional judgement in evaluating the subject matter.

**Audit**—Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. In the context of this publication, the term refers to a specific type of assurance engagement in which an IT audit and assurance professional conducts a formal, independent and systematic inspection or examination of subject matter against a recognised and appropriate standard or against management’s assertions that must meet specific criteria. Audit engagements require a formal approach, adherence to specific standards and guidance, and adoption of specific reporting formats. Audits could include support of audit financial statements, opinions of regulatory compliance and other formal expressions of opinion.

**Auditee**—Refers to the management or executive management directly responsible for the subject matter that is the subject of the audit or review. The subject matter may include business units, technologies, systems and applications, or other matters considered within the scope of the audit or assurance project.

**Audit engagement**—In an audit engagement, the practitioner provides a high, although not absolute, level of assurance by designing procedures so that, in the practitioner’s professional judgement, the risk of an inappropriate conclusion is reduced to a low level through procedures such as inspection, observation, enquiry, confirmation, recalculation, reperformance and analytical procedures. Use of the term ‘high level of assurance’ refers to the highest reasonable level of assurance a practitioner can provide concerning a subject matter. Absolute assurance is not attainable as a result of factors such as the use of judgement, the use of testing, the inherent limitations of control and the fact that much of the evidence available to the practitioner is persuasive rather than conclusive in nature. Assurance is also influenced by the degree of precision associated with the subject matter itself.
**Competencies**—The strengths of an organisation, what it does well. Competencies can refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.

**Conclusion**—The practitioner’s communication varying, depending on whether the assurance engagement is an attestation engagement or a direct reporting engagement:

- In an attestation engagement, the practitioner’s conclusion is a written assertion prepared by the accountable party. The assertion evaluates, using suitable criteria, the subject matter for which the accountable party is responsible.
- In a direct reporting engagement, the practitioner’s conclusion evaluates directly, using suitable criteria, the subject matter for which the accountable party is responsible.

**Criteria**—The standards and benchmarks used to measure and present the subject matter and against which the IS auditor evaluates the subject matter. In an attestation engagement, benchmarks against which management’s written assertion on the subject matter can be evaluated. The practitioner forms a conclusion concerning subject matter by referring to suitable criteria.

**Engagement**—See ‘assurance engagement’ and ‘review engagement’. Not all engagements performed by practitioners are assurance engagements. An engagement in which the practitioner does not provide a conclusion concerning a subject matter is not an assurance engagement. For example, a practitioner may be engaged to report the results of applying certain procedures specified by management or the users of the practitioner’s report. An engagement to apply specified procedures is not an assurance engagement because the practitioner would not necessarily perform all of the procedures that, in his or her judgement, would be necessary to express a conclusion concerning the subject matter as a whole. Other engagements typically undertaken by practitioners include management consulting engagements in which the practitioner is engaged to provide advice or recommendations to a client, and taxation engagements in which a practitioner is engaged to provide tax advice to a client. Such engagements are not assurance engagements because, for example, they do not involve an accountability relationship between management and a user.

**Engagement risk**—Risk that the practitioner may express an inappropriate conclusion. The three components of engagement risk are inherent risk, control risk and detection risk. In an assurance engagement, the practitioner reduces engagement risk to a level that is appropriate for the assurance provided in his or her report.

**Examination level**—Refers to an attestation engagement designed to provide a high level of assurance. The assurance professional’s objective is to accumulate sufficient competent evidence to restrict attestation risk to a level that is, in the assurance professional’s professional judgement, appropriately low for the high level of assurance that may be imparted by the resulting report. The accumulation of audit evidence includes an assessment or evaluation of that evidence in terms of its ability to meet the requirements of the engagement and reduce audit risk. In examination-level audits, the assurance professional should select from all available procedures that assess inherent and control risks, and restrict detection risks such that the attestation risk is at an appropriately low level.
Glossary

Level of assurance—Refers to the degree to which the subject matter has been examined or reviewed. See ‘examination level’ and ‘review level’.

Professional standards—Refers to standards issued by ISACA. The term may extend to related guidelines and techniques that assist the professional in implementing and complying with authoritative pronouncements of ISACA. In certain instances, standards of other professional organisations may be considered, depending on the circumstances and their relevancy and appropriateness.

Quality review or inspection—Refers to procedures employed in a review of completed work or engagements designed to ensure compliance with IT assurance standards, and related quality control policies and procedures of the organisation. Quality reviews can be performed by different levels of staff members and at different times during the assurance work or at its completion. Quality reviewers must possess sufficient knowledge to assess compliance with professional and organisational policies and standards as well as knowledge of the subject matter to assess appropriateness of the criteria selected and the auditing procedures performed.

Reasonable assurance—A level of comfort short of a guarantee but considered adequate given the costs of the control and the likely benefits achieved.

Representation—Refers to a written or oral statement by management and the auditee about the subject matter. It is statement of fact that can be confirmed through audit procedures. A representation may also indicate that the IT audit and assurance professional has been informed of, and given access to, all relevant information, records, files, etc., pertaining to the subject matter.

Responsible party—Refers to the person or persons, either as individuals or representatives of the entity, responsible for the subject matter. Where, because of the nature of the subject matter or the proposed engagement, a responsible party is not identified or associated with the subject matter, the party who has a reasonable basis for making a written assertion about the subject matter may provide such assertions and adopt the role of the responsible party. In a RACI chart, responsible refers to the person who must ensure that activities are completed successfully.

Review engagement—In a review engagement, the practitioner provides a moderate level of assurance by designing procedures so that, in the practitioner’s professional judgement, the risk of an inappropriate conclusion is reduced to a moderate level through procedures that are normally limited to enquiry, analytical procedures and discussion. Such risk is reduced to a moderate level when the evidence obtained enables the practitioner to conclude the subject matter is plausible in the circumstances.

Review level—Refers to an attestation engagement designed to provide a moderate level of assurance. The assurance professional’s objective is to accumulate sufficient evidence to restrict attestation risk to a moderate level. To accomplish this, the types of procedures performed generally are limited to enquiries and analytical procedures, as compared with an examination level where procedures also include search and verification.
References

Canadian Institute of Chartered Accountants (CICA), *Information Technology Control Guidelines (ITCG), 3rd Edition*, Canada

Financial Instruments Exchange Law (FIEL) (commonly referred to as J-SOX), Japan, 2006

Health Insurance Portability and Accountability Act (HIPAA), USA, 1996

International Organisation of Standardisation (ISO)/International Electrotechnical Commission (IEC) standards:

ISACA, *Digital Signatures Security and Controls*, USA, 1999


ISACA, *Linux Security, Audit and Control Features*, USA, 2005

ISACA, *Oracle® Database Security, Audit and Control Features*, USA, 2004


ISACA, *OS390-z/OS Security, Audit and Control Features*, USA, 2004


IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

IT Governance Institute, *The CEO’s Guide to IT Value at Risk*, USA, 2005

IT Governance Institute, *COBIT 4.1*, USA, 2007


IT Governance Institute, *Enterprise Value: Governance of IT Investments—The Val IT Framework*, USA, 2006

IT Governance Institute, *IT Assurance Guide: Using COBIT*, USA, 2007

IT Governance Institute, *IT Control Objectives for Basel II*, USA, 2007

IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, USA, 2007

IT Governance Institute, IT Governance Domain Practices and Competencies Series, USA, 2005:

- Governance of Outsourcing
- Information Risks—Whose Business are They?
- IT Alignment—Who is in Charge?
- Measuring and Demonstrating the Value of IT
- Optimising Value Creation From IT Investments


Office of Government Commerce, *Information Technology Infrastructure Library (ITIL)*, UK

Securities and Exchange Commission, USA
Other Publications

Many publications issued by ITGI and ISACA contain detailed assessment questionnaires and work programmes. For further information, please visit www.isaca.org/bookstore or e-mail bookstore@isaca.org.

Assurance Publications

• IS Auditing Standards, Guidelines, Procedures, www.isaca.org/standards
• Stepping Through the IS Audit, 2nd Edition, 2004

ERP Series:

Specific Environments
• Electronic and Digital Signatures: A Global Status Report, 2002
• Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment, 2004
• Linux: Security, Audit and Control Features, 2005
• Managing Risk in the Wireless LAN Environment: Security, Audit and Control Issues, 2005
• Oracle® Database Security, Audit and Control Features, 2004
• OS/390—z/OS: Security, Control and Audit Features, 2003
• Risks of Customer Relationship Management: A Security, Control and Audit Approach, 2003
• Security Provisioning: Managing Access in Extended Enterprises, 2002

IT Governance Publications

• Board Briefing on IT Governance, 2nd Edition, 2003
• IT Governance Global Status Report, 2008

COBIT and Related Publications
• COBIT® 4.1, 2007
• COBIT® Quickstart™, 2nd Edition, 2007
• IT Assurance Guide: Using COBIT®, 2007
• IT Control Objectives for Basel II, 2007

COBIT Mapping Series:
• Aligning COBIT®, ITIL and ISO 17799 for Business Benefit
• COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0
• COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0
• COBIT® Mapping: Mapping of ITIL With COBIT® 4.0
• COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1
• COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0
• COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0
• COBIT® Mapping: Mapping of SEI’s CMM for Software With COBIT® 4.0
• COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0
• COBIT® Mapping: Overview of International IT Guidance, 2nd Edition

IT Governance Domain Practices and Competencies:
• Information Risks: Whose Business Are They?, 2005
• Optimising Value Creation From IT Investments, 2005
• Measuring and Demonstrating the Value of IT, 2005
• Governance of Outsourcing, 2005
• IT Alignment: Who Is in Charge?, 2005

Val IT:
• Enterprise Value: Governance of IT Investments: The Val IT Framework 2.0, 2005
• Enterprise Value: Governance of IT Investments: The Business Case, 2005
• Enterprise Value: Governance of IT Investments: The ING Case Study, 2005

Security Publications

• Cybercrime: Incident Response and Digital Forensics, 2005
• Information Security Governance—Top Actions for Security Managers, 2005
• Information Security Harmonisation—Classification of Global Guidance, 2005
• Managing Information Integrity: Security, Control and Audit Issues, 2004
• Security Awareness: Best Practices to Serve Your Enterprise, 2005
• Security Critical Issues, 2005
Comment Submission Form

We are interested in your reaction to ITAF and any additions/revisions you might suggest. Please provide detailed information about your suggestion as well as your rationale for the revision. Submit your comments to the attention of the director of research, standards and academic relations via fax at +1.847.253.1443, e-mail to research@isaca.org or mail to ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA.

Name: _______________________________________________________________

Organisation: __________________________________________________________

Country: ___________________________ E-mail address: _______________________

Section: _______________________________________________________________

Suggested revision: _____________________________________________________.
____________________________________________________________________.
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

Reason for the revision: _________________________________________________.
____________________________________________________________________.
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

Thank you!