



ITAFTM

A PROFESSIONAL PRACTICES
FRAMEWORK FOR IT ASSURANCE

SUMMARY DOCUMENT



ITAF™

A PROFESSIONAL PRACTICES
FRAMEWORK FOR IT ASSURANCE

SUMMARY DOCUMENT

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—Summary Document* (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

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, FBCS 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.

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.

Organisation of ITAF

ITAF is composed of elements including 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.

Use of ITAF

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.

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.

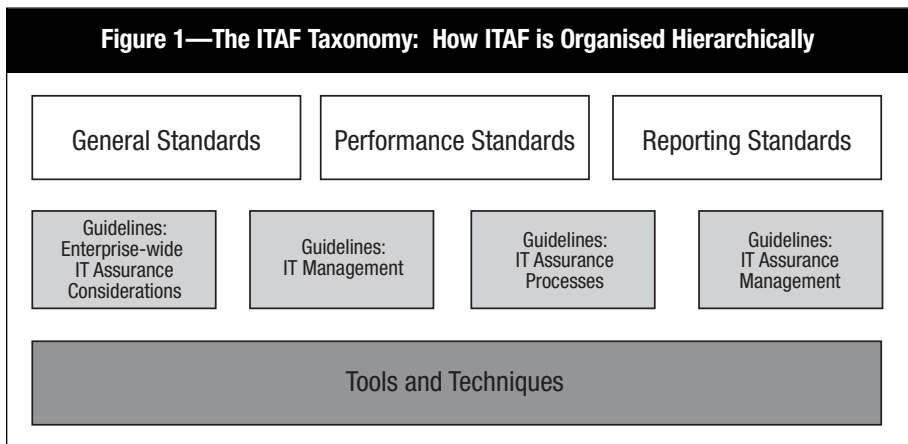
Technology and Security Standards

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.

How ITAF is Organised

ITAF is divided into three sections, as shown in **figure 1**.

- **Standards** categorised as general, performance and reporting standards.
- **Guidelines** information in two categories:
 - **IT Processes**—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.
 - **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.
- **Tools and techniques** as well as other information.



IT Assurance Standards: Defining a Common Reference Point

There are three categories of standards in ITAF—general, performance and reporting—which must be followed in all circumstances.

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
- Reasonable expectation
- Management's acknowledgement
- Training and proficiency
- Knowledge of the subject matter
- Due professional care
- Suitable criteria
- Available criteria
- Selection of criteria

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
- Obtaining sufficient evidence
- Assignment performance
- Representations

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. Reporting standards address:

- Types of reports
- The means of communication
- Information to be communicated

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.



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*