IT Audit Framework (ITAF™)

A Professional Practices Framework for IT Audit

4th Edition

ISACA®

About ISACA

For more than 50 years, ISACA® (*www.isaca.org*) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

Disclaimer

ISACA has designed and created its *IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition* (the "Work") primarily as an educational resource for assurance practitioners. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance practitioners should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

Provide Feedback: https://support.isaca.org
Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

ISBN 978-1-60420-834-4
IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition
Printed in the United States of America

Acknowledgments

ISACA wishes to recognize:

Expert Reviewers

Manoj Agarwal, CISA, CIA, CRMA, CA, DISA, Metro Brands Limited, India
G.M. Faruk Ahmed, CISA, Rupali Bank Limited, Bangladesh
Winnie Ang, CISA, CISM, Singapore
Anagha Apte, CISA, CRISC, CISM, Birlasoft Ltd., USA
Kenia Arias, CISA, A-FE Consulting LLC, USA
Bode Bary Aro, CISA, CRISC, Enugu Electricity Distribution Company, Nigeria
Mais Barouqa, CISA, CRISC, CGEIT, ISO27K, ITIL, COBIT FL, GRCP, Deloitte, Jordan
Marquita Bass, CISA, PMP, Rausch Advisory, USA
Cindy Baxter, CISA, ITIL, State Street Corporation, USA
Zsolt Bederna, CISA, CRISC, CISM, CGEIT, CISSP, CEH, ITIL-F, Cyex OÜ, Hungary
Vijay Bhalerao, CISA, COBIT-F, ISO 27001 LA, MCSA, ITIL-F, Unisoft Computrade Pvt. Ltd., India
Parmeet Bhatiya, CISA, PricewaterhouseCoopers, United Arab Emirates
Bakan Borupile, CISA, MCSE, MCSA, Btech, Mascom Wireless, Botswana
Ricardo Jimenez Caicedo, CISA, Ernst & Young, Colombia
Jules Chachine, CISA, CISM, PMP, Jconseil, Lebanon
Elastos Chimwanda, CISA, CIA, ZWMB Bank Limited, Zimbabwe
Joyce Chua, CISA, CISM, CDPSE, CIPP(E), (C)CISO, CIPM, CIPP(A), CFE, CIA, PMP, CITPM, ITIL, MCP, IRCA ISMS Associate Auditor, Sony Electronics, Singapore
Ari Ecrument, CISA, CRISC, CDPSE, FIP, CIPP/E, CIPM, CRMA, CEH, ISO 27001/22301/20000
Bhaskar Ghosh, CISA, Wintrust Financial Corporation, USA
Miguel A. Gonzalez, CISA, ITESM, Mexico
J. Winston Hayden, CISA, CRISC, CISM, CGEIT, South Africa
Andrew Hinder, CISA, CMIIA, QIAL, CRMA, CIA, BAE Systems, United Kingdom
Marko Jagodic, CISA, CRISC, VRIS, LLC, Slovenia
Ashane J.W. Jayasekara, CISA, BDO, Sri Lanka
Daniel Jones, CISA, CRISC, CISM, Devon Energy, USA
Abbie Anne Julien, CISA, CDPSE, Life Extension Foundation Buyers Club Inc., USA
Mladen Kandic, CISA, CIA, Eurobank, Serbia
Joanna Karczewska, CISA, Poland
Glenn Kirke, CISA, Integrated Audit and Compliance, USA
Matthias Kraft, CISA, CRISC, CISM, CGEIT, CAC, DPO, Fidelity International, Luxembourg
Abhishek Kumar, CISA, ISO 27001 LA, ISO 22301 LA, Deloitte, India
Hiu Sing Lam, CISA, FRM, PMP, Hong Kong
James Lam, CISA, CRISC, CISM, TOGAF, Aon Cybersecurity Advisory, USA
Larry L. Lliran, CISA, CISM, Precelsus Consulting, Puerto Rico
Angel Giovanni Vasquez Lopez, CISA, Banco GYT Continental, Guatemala
Michael Malcolm, CISA, CIA, CRMA, CFSA, CGAP, CFE, Opentext Corporation, Canada
A T Manjunath, CISA, CCSK, CSA STAR AUDITOR, Applied Materials, India
Rafael Pérez Marín, CISA, Venezuela
Larry Marks, CISA, CRISC, CISM, CGEIT, CDPSE, CISSP, ITIL, PMP, USA
Vivek Mathivanan, CISA, CRISC, CGEIT, Worley, Australia
Benedicta Mlingi, CISA, NMB Bank Plc., Tanzania
Juan Carlos Morales, CISA, CRISC, CISM, CGEIT, COBIT 2019, Guatemala
Donald Morgan, CISA, Farm Credit Canada, Canada
Syed Aun Muhammad, CISA, Canada

Acknowledgments *(cont.)*

Christine Lilian Mukhongo, CISA, CRISC, CISM, Kenya Universities & Colleges Central Placement Service, Kenya
Sitambaram Ainslei Naidu, CISA, CIA, Edcon, South Africa
Tushar Nerurkar, CISA, CISSP, PMP, PricewaterhouseCoopers USA
Daisha Ngo, CISA, CPA, CRMA, Spectrum Health, USA
Geoffrey Nkuutu, CISA, Fellow Chartered Certified Accountant (FCCA), Wazalendo Savings & Credit Cooperative Society Limited, Uganda
Alexander Obraztsov, CISA, CISSP, PMP, Societe Generale (New York), USA
Darren O'Brien, CISA, CRISC, Vitality, United Kingdom
Iroko Oluwatosin, CISA, CRISC, CISM, ITIL, CEH, ISO 27001, Alberta Blue Cross, Canada
Anas Olateju Oyewole, CISA, CRISC, CISM, CDPSE, CISO, CISSP, CCSP, PMP, Indigo Books and Music, Canada
Chirag Ali Peerzada, CISA, CEH, ISO 27001 LA, ISO 22301 LI, Mahindra Special Service Group, India
John Pouey, CISA, CRISC, CISM, CIA, Entergy, USA
Shahid Qureshi, CISA, CPA, CGA (Canada), FCCA (UK), CIA (USA), FCMA, FCIS, FCSM, Leverage Global Inc., Canada
Sreechith Radhakrishnan, CISA, CRISC, CISM, CGEIT, CDPSE, COBIT Assessor, ISO 27001 LA, ISO 20000 LA, ISO 37001 LA, ISO 22301 LA, Global Success Systems FZ LLC, United Arab Emirates
Allan Rono, CISA, CISM, ITIL, Liberty Group, Kenya
Sampa David Sampa, CISA, World Vision International, Zambia
Megah Santio, CISA, CISM, COBIT Assessor, CIA, Australia
Garimella Chandrasekhar Sarma, CISA, CRISC, CDPSE, CFE, CtrlS Datacenters, India
S. Phani Krishna Sunkaranam, CISA, CRISC, CISM, CISSP, ITIL, Trianz, India
Luong Trung Thanh, CISA, CISM, CGEIT, Vietnam
Catalin Tiganila, CISA, CRISC, CISM, CISSP, CBCP, CIPM, Deloitte, Luxembourg
Marisela Parra Valencia, CISA, ITIL, Costa Rica
Kaysi Veatch, CISA, CSX-F, CIA, Maxar, USA
Ionnis Vittas, CISA, CISM, Quest Holdings SA, Greece
Ross Wescott, CISA, CUERME, CCP, CIA (ret), Wescott & Associates, USA
Surendra Yakkali, CISA, CSM, ITIL, SAFe 5, CMMI Associate, OptumServe Technology Services, Inc., USA

Board of Directors

Table of Contents

Introduction

ISACA's Information Technology Audit Framework (ITAF) is a comprehensive IT audit framework that:

- Establishes standards that address IT audit and assurance practitioners' roles and responsibilities, ethics, expected professional behavior, and required knowledge and skills;
- Defines terms and concepts specific to IT audit and assurance;
- Provides guidance and techniques for planning, performing and reporting of IT audit and assurance engagements.

Based on ISACA material, ITAF provides a single source for IT audit and assurance practitioners to obtain guidance on the performance of audits and the development of effective audit reports. The 3rd Edition of ITAF incorporated IT audit and assurance standards and guidance effective 1 November 2013. Prior to issuing the 4th Edition of ITAF, ISACA released an exposure draft for comment, and more than 65 reviewers provided their feedback. The 4th Edition of ITAF is effective October 2020.

Translations of these standards are available at *https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4*.

Frequently Asked Questions

- **To whom does ITAF apply?** ITAF applies to individuals who act in the capacity of IT audit and assurance practitioners and are engaged in providing assurance over IT processes, components of IT applications, systems and infrastructure. However, care has been taken to design these standards, guidelines and auditing techniques in a manner that also may be beneficial 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 IT audit and assurance work. The standards are mandatory. The guidelines, tools and techniques are designed to provide nonmandatory assistance in performing assurance work.
- **In which circumstances should ITAF IT audit and assurance standards and related guidance be used?** ITAF's design recognizes that IT audit and assurance practitioners are faced with different requirements and types of assignments—ranging from leading an IT-focused audit to contributing to a financial, compliance or operational audit. ITAF is applicable to any IT audit or assessment engagement.
- **Does ITAF address requirements for consultative and advisory work?** In addition to performing audits, IT audit and assurance practitioners may undertake nonaudit engagements for their employers or on behalf of clients. These consultative and advisory engagements usually involve review of a particular area. For a number of reasons, including the nature of the work (particularly the degree of testing and the scope of the engagement), the IT audit and assurance practitioner usually does not issue a formal audit report. Instead, the consultative and advisory work typically concludes with an opinion (possibly expressed via memorandum) on current performance and suggestions for improvement.
- **When will the 4th Edition of ITAF be available?** The revised IT audit framework is available October 2020.

Organization

ITAF standards are divided into three categories:

- **General standards (1000 series)**—Detail the IT assurance profession's guiding principles. These principles apply to all engagements, including but not limited to the IT audit and assurance practitioner's ethics, independence, objectivity and due care, as well as knowledge, competency and skill.

- **Performance standards (1200 series)**—Deal with the conduct of the engagement, such as planning and supervision, scoping, risk assessment, resource mobilization, engagement management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, the means of communication, and the information communicated.

ITAF guidelines provide the IT audit and assurance practitioner with information and direction about an IT audit or assurance engagement. In line with the three categories of standards outlined above, guidelines focus on various audit approaches, methodologies and related material to assist in planning, executing, assessing, testing and reporting on IT processes, controls, and related IT audit or assurance initiatives. Guidelines also help clarify the relationships between activities and initiatives undertaken by the enterprise and those undertaken by IT. Applicable guidelines follow related standards.

ISACA's website provides specific information on various methodologies, tools and templates, and includes direction in their application and use to operationalize the information in the guidance. An example is ISACA's creation of the Performance Guidelines 2208: Information Technology Audit Sampling, which is a companion to the ITAF framework. These guidelines support IT audit and assurance practitioners' use of sampling where a conclusion about a total population is reached when audit procedures are applied to less than 100 percent of that population. Additional tools and techniques, which also include white papers, audit programs and books, are available at *www. isaca.org/resources/insights-and-expertise/audit-programs-and-tools*.

Using ITAF

The IT audit or assurance process involves the performance of specific procedures to provide reasonable assurance about the subject matter. IT audit and assurance practitioners undertake assignments designed to provide assurance at varying levels, ranging from review to attestation or examination.

Each IT audit or assurance assignment must adhere to prescribed standards in terms of whether 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 and the nature of the results obtained.

If the engagement is to be performed by one individual, that individual must possess the skill and knowledge required to complete the engagement. If more than one individual is to perform the engagement, the collective team needs to possess the skill and knowledge to perform the work.

Several critical suppositions are inherent in any IT audit or assurance assignment, including the following:

- The subject matter is identifiable and subject to audit.
- There is a high probability of successful completion of the project.
- The approach and methodology are free from bias.
- The project is of sufficient scope to meet the IT audit or assurance objectives.
- The project will lead to a report that is objective and that will not mislead the reader.

The standards are mandatory in all cases. The term "shall" indicates "must." Any deviations from the standards shall be addressed prior to completion of the IT audit or assurance engagement.

The guidelines may not be applicable in all situations, but they should always be considered. The guidelines do allow IT audit and assurance practitioners a degree of flexibility. So when reviewing guidelines to determine applicability, practitioners should use professional judgment, be prepared to justify any significant deviation from the guidelines or omission of relevant sections of the guidance, and seek additional guidance if necessary.

Resources for additional guidance may include:

- Colleagues within and/or outside the enterprise (e.g., through professional associations or professional network groups)
- Management
- Governance bodies of the enterprise (e.g., audit committee)
- Professional guidance materials (e.g., books, papers, other guidelines)

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 practitioner should select only suitable techniques that produce relevant, objective and unbiased information.

In line with ITAF's continued evolution, section numbers intentionally include gaps for insertion of future guidance.

Standards Issued by Other Standard-Setting Bodies

While the ITAF standards provide IT audit and assurance practitioners with comprehensive guidance and direction, some situations may require practitioners to use standards issued by another organization.

When the IT audit and assurance practitioner has cited compliance with ITAF standards and conflicts arise between ITAF and the applicable standards of another organization, the IT audit and assurance practitioner should use ITAF standards as the prevailing standards for conducting reviews and reporting the results.

Should the IT audit and assurance practitioner be required to adhere to standards other than ITAF for regulatory purposes or operational expectations, the IT audit and assurance practitioner may:

- Use professional standards required by other authoritative bodies in conjunction with ITAF standards,
- Cite the use of other required standards in their reports.

Terms and Definitions

Throughout this document, common words are used with specific meanings that apply to the most common types of engagements performed by IT audit and assurance practitioners. In those instances, a definition is provided in Appendix C to ITAF. This ensures that the words and their meanings within the context of this document are understood and consistently applied.

Where practical, ITAF's terms and definitions generally are consistent with commonly used terminology in the practice of professional auditing and in information technology and security; however, practitioners should consult the most current, original source standards relevant to the specific type of engagement(s) to be performed to ensure the most current and appropriate terms and definitions are used.

For other terms and definitions not included in ITAF, a complete glossary is available on the ISACA website, *www.isaca.org/glossary.*

ISACA 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 and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities 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 the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

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

IT Audit and Assurance Standards Statements

The standards in ITAF contain key aspects designed to assist the IT audit and assurance practitioner. ITAF standards are periodically reviewed for continual improvement and amended as necessary to keep pace with the evolution of the IT audit and assurance profession.

Standards Statements

General Standards

1001 Audit Charter

1001.1 The IT audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1001.2 The IT audit and assurance function shall have the audit charter agreed upon and formally approved by those charged with governance and oversight of the audit function, e.g., the board of directors and/or the audit committee.

1001.3 The IT audit and assurance function shall communicate the audit charter to executive/senior management. Also, relevant elements of the audit charter shall be shared with groups being audited at entrance meetings and/or through engagement letters.

1001.4 Through review of the audit charter on a periodic basis, the audit and assurance function's responsibilities, as reflected in the audit charter, shall remain aligned with the enterprise's mission and strategies. Immediate review of the audit charter is warranted should the enterprise's mission or strategies change, or if the audit function's responsibilities change.

1002 Organizational Independence

1002.1 The IT audit and assurance function shall be free from conflicts of interest and undue influence in all matters related to audit and assurance engagements. Any impairment of independence (in fact or appearance) is identified and disclosed to the appropriate parties.

1002.2 The IT audit and assurance function shall have a functional reporting relationship (e.g., reporting to the board of directors) that supports the function's ability to remain free from undue influence.

1002.3 The IT audit and assurance function shall have an administrative reporting relationship that supports the function's unhindered performance of its responsibilities (e.g., scope of engagement, fieldwork or reporting).

1003 Auditor Objectivity

1003.1 IT audit and assurance practitioners shall be objective in all matters related to audit and assurance engagements.

1004 Reasonable Expectation

1004.1 IT audit and assurance practitioners shall have reasonable expectation that the engagement can be completed in accordance with applicable IT audit and assurance standards and, where required, other industry standards or applicable laws and regulations that will result in a professional opinion or conclusion.

1004.2 IT audit and assurance practitioners shall have reasonable expectation that the scope of the engagement enables a conclusion on the subject matter and that any scope limitations are addressed.

1004.3 IT audit and assurance practitioners shall have reasonable expectation that management understands its obligations and responsibilities with respect to providing appropriate, relevant and timely information required to perform the engagement.

1005 Due Professional Care

1005.1 In accordance with ISACA's Code of Professional Ethics, auditors will exercise due diligence and professional care. They will maintain high standards of conduct and character, and they will refrain from engaging in acts that may discredit themselves or the profession. Privacy and confidentiality of information obtained during the course of the auditor's duties should be maintained. Further, this information should not be used for personal benefit, nor should the information be disclosed unless required by legal authority.

1006 Proficiency

1006.1 IT audit and assurance practitioners, collectively with others assisting with the audit and assurance engagement, shall possess the professional competence to perform the work required.

1006.2 IT audit and assurance practitioners shall possess adequate knowledge of the subject matter to perform their roles in IT audit and assurance engagements.

1006.3 IT audit and assurance practitioners shall maintain professional competence through appropriate continuing professional education and training.

1007 Assertions

1007.1 IT audit and assurance practitioners shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

1008 Criteria

1008.1 IT audit and assurance practitioners shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative, and understood by, or available to, all readers and users of the report.

1008.2 IT audit and assurance practitioners shall consider the acceptability of the criteria and focus on criteria that are recognized, authoritative and publicly available.

Performance Standards

1201 Risk Assessment in Planning

1201.1 The IT audit and assurance function shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and to determine priorities for the effective allocation of IT audit resources.

1201.2 IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements.

1201.3 IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.

1202 Audit Scheduling

1202.1 The IT audit and assurance function shall establish an overall strategic plan resulting in short-term and long-term audit schedules. Short-term planning consists of audits to be performed within the year, while long-term planning is comprised of audits based on risk-related matters within the enterprise's information and technology (I&T) environment that may be performed in the future.

1202.2 Both short-term and long-term audit schedules should be agreed upon with those charged with governance and oversight (e.g., audit committee) and communicated within the enterprise.

1202.3 The IT audit and assurance function shall modify its short-term and/or long-term audit schedules to be responsive to organizational needs (i.e., unexpected events or unplanned initiatives). Any audit displaced to accommodate an audit of an unexpected event or unplanned initiative should be reassigned to a future period.

1203 Engagement Planning

1203.1 IT audit and assurance practitioners shall plan each IT audit and assurance engagement to address the nature, timing and extent of audit procedures to be performed. The plan should include:

- Areas to be audited
- Objectives
- Scope
- Resources (e.g., staff, tools and budget) and schedule dates
- Timeline and deliverables
- Compliance with applicable laws/regulations and professional auditing standards
- Use of a risk-based approach for engagements that are not related to legal or regulatory compliance
- Engagement-specific issues
- Documentation and reporting requirements
- Use of relevant technology and data analysis techniques
- Consideration of the cost of the engagement relative to the potential benefits
- Communication and escalation protocols for situations that may arise during the performance of an IT audit engagement (e.g., scope limitations or unavailability of key personnel)

During fieldwork, it may become necessary to modify audit procedures created during planning as the engagement progresses.

1203.2 IT audit and assurance practitioners shall develop and document an IT audit and assurance engagement audit program that describes the step-by-step procedures and instructions to be used to complete the audit.

1204 Performance and Supervision

1204.1 IT audit and assurance practitioners shall conduct the work in accordance with the approved IT audit plan to cover identified risk, and within the agreed-on schedule.

1204.2 IT audit and assurance practitioners shall provide supervision to IT audit staff for whom they have supervisory responsibility to accomplish audit objectives and meet applicable professional audit standards.

1204.3 IT audit and assurance practitioners shall accept only tasks that are within their knowledge and skills, or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.

1204.4 IT audit and assurance practitioners shall obtain and preserve sufficient and appropriate evidence to achieve the audit objectives.

1204.5 IT audit and assurance practitioners shall document the audit process and describe the audit work and the audit evidence that support findings and conclusions.

1204.6 IT audit and assurance practitioners' findings and conclusions are to be supported by root cause analysis and interpretation of this evidence.

1204.7 IT audit and assurance practitioners shall provide an appropriate audit opinion or conclusion and include any scope limitation where required evidence is obtained through additional test procedures.

1205 Evidence

1205.1 IT audit and assurance practitioners shall obtain sufficient and appropriate evidence to draw reasonable conclusions.

1205.2 Applying professional skepticism, IT audit and assurance practitioners shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

1205.3 Along with other working papers, IT audit and assurance practitioners shall preserve evidence for a time period that aligns with formally defined and approved retention periods.

1206 Using the Work of Other Experts

1206.1 IT audit and assurance practitioners shall consider using the work of other experts for the engagement, where appropriate.

1206.2 IT audit and assurance practitioners shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.

1206.3 IT audit and assurance practitioners shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.

1206.4 IT audit and assurance practitioners shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives. The practitioners should also clearly document the conclusion.

1206.5 IT audit and assurance practitioners shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

1206.6 IT audit and assurance practitioners shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.

1206.7 IT audit and assurance practitioners shall provide an audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

1207 Irregularities and Illegal Acts

1207.1 IT audit and assurance practitioners shall consider the risk of irregularities and illegal acts during the engagement.

1207.2 IT audit and assurance practitioners shall document and communicate irregularities or illegal acts to the appropriate party in a timely manner. Note that some communications (e.g., with regulators) may be restricted. As a result, the practitioner's communications may require discussion with those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee).

Reporting Standards

1401 Reporting

1401.1 IT audit and assurance practitioners shall provide a report to communicate the results of each engagement.

1401.2 IT audit and assurance practitioners shall ensure findings in the audit report are supported by sufficient and appropriate evidence.

1402 Follow-up Activities

1402.1 IT audit and assurance practitioners shall monitor and periodically report to those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee) management's progress on findings and recommendations. The reporting should include a conclusion on whether management has planned and taken appropriate, timely action to address reported audit findings and recommendations.

1402.2 Progress on the overall status of the implementation of audit findings should be regularly reported to the audit committee, if one is in place.

1402.3 Where it is determined that the risk related to a finding has been accepted and is greater than the enterprise's risk appetite, this risk acceptance should be discussed with senior management. The acceptance of the risk (particularly failure to resolve the risk) should be brought to the attention of the audit committee (if one is in place) and/or the board of directors.

Page intentionally left blank

GENERAL STANDARDS

General Standard 1001: Audit Charter

Statements	**1001.1** The IT audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.
	1001.2 The IT audit and assurance function shall have the audit charter agreed upon and formally approved by those charged with governance and oversight of the audit function, e.g., the board of directors and/or the audit committee.
	1001.3 The IT audit and assurance function shall communicate the audit charter to executive/senior management. Also, relevant elements of the audit charter shall be shared with groups being audited at entrance meetings and/or through engagement letters.
	1001.4 Through review of the audit charter on a periodic basis, the audit and assurance function's responsibilities, as reflected in the audit charter, shall remain aligned with the enterprise's mission and strategies. Immediate review of the audit charter is warranted should the enterprise's mission or strategies change, or if the audit function's responsibilities change.

General Guidelines 2001: Audit Charter

2001.1 Practitioners should have a clear mandate to perform the audit function. This mandate is normally documented in an audit charter that should be formally approved by those charged with governance, e.g., board of directors and/or audit committee. Where an audit charter exists for the audit function as a whole, the IT audit and assurance mandate should be incorporated.

2001.2 Contents of Audit Charter

2001.2.1	An audit charter shall document the IT audit and assurance function's: ● Independence, code of ethics and standards ● Purpose, responsibility, authority and accountability ● Protocols that the IT audit and assurance practitioner will follow in the performance of engagements, including but not limited to communication and escalation ● Roles and responsibilities of the auditee during the IT audit or assurance engagement ● The IT audit and assurance function's role in reporting irregularities and illegal acts
2001.2.2	The audit charter should clearly address the purpose, responsibility, authority and accountability of the audit function (see 2001.2.1). These four aspects are set out in the following sections.
2001.2.3	**Purpose** of the audit function is to evaluate and test the design and execution of controls implemented by management. The audit charter should contain the following sections that support the audit function in achieving its purpose: ● **Aims/goals of the audit function** provide a functional and organizational framework in which the audit function operates. ● **Objectives of the audit function and the audit function's mission statement** (should the audit function have one) bring a structured approach to evaluate and improve the design and operational effectiveness of the risk management processes, internal control system and operations/governance of information systems. ● **Scope of the audit function** applies either to the entire enterprise or to a specific organization within the enterprise. ● **Work performed by the audit function** may include information systems audits, compliance audits, financial audits, operational audits, integrated audits, administrative audits, specialized audits (third-party service audits, fraud audits or forensic audits), computer forensic audits and functional audits. It also may include nonaudit services, such as consulting services on projects.

2001.2.4	**Responsibility** of the audit function is to add value to the enterprise, ensuring that organizational perspectives such as strategy, mission and regulatory/compliance expectations are integrated in its work, and to abide by professional expectations (e.g., ethics, professional development). The audit charter should contain the following sections to facilitate the audit function: • **Independence** details the implementation of the independence requirement for the audit function and practitioners, as described in Standards 1002 Organizational Independence and 1003 Auditor Objectivity. The IT audit and assurance function should ensure its independence by: ▪ Assessing its independence on a periodic basis, at least annually ▪ Creating and maintaining a formal protocol related to identification and reporting of potential impairments to independence The results of the independence assessment and the impairments protocol should be reported to those charged with governance and oversight of the audit function, e.g., the board of directors and/or the audit committee. • **Relationship with external audit firms** details the internal IT audit and assurance function's reliance strategy with the external auditor: ▪ Meeting with the external auditors to coordinate the work effort to minimize duplication of effort ▪ Providing access to practitioners' working papers, documentation and evidence ▪ Considering the work planned by the external auditors when drafting the audit plan for the coming period • **Auditee's expectations** detail the services and deliverables the auditees can expect from the audit function and practitioners: ▪ Description of identified problems, consequences and possible resolutions relating to the area of responsibility of the auditee ▪ Possibility of including management response and corrective actions taken on findings in the audit report. This includes references to related service level agreements (SLAs) for items such as delivery of reports, response to auditee complaints, quality of service, review of performance, reporting process and agreement of findings. • **Auditee requirements** detail the responsibilities of the auditee, e.g., all auditees are required to make themselves available and assist the audit function and practitioners in fulfilling assigned responsibilities. Auditee requirements also provide clarity concerning management's responsibilities and the audit function's responsibilities. • **Abide by professional standards** established by the auditor's organization and any standard-setting body to which the auditor has membership. • **Compliance** with standards that detail the requirements with which the audit function and practitioners will adhere, e.g., the audit function and practitioners will adhere and act according to all the ISACA ITAF Audit and Assurance Standards and Guidelines.

2001.2.5	**Authority** of the audit function should contain the following sections: ● **Right of access** to relevant information, systems (i.e., logs, activities and controls built into systems), personnel and locations by practitioners performing an audit engagement. The audit function, represented by IT audit practitioners: ■ Has authorized access to any and all records, documentation, systems and locations necessary for performance of an audit engagement, and can seek assistance from executive management in obtaining such access ■ Has the authority to seek any information from an employee, consultant or contractor when performing an audit engagement ● **Limitations of authority** of the audit function and practitioners, if any ● **Processes to be audited** that the audit function is authorized to audit—e.g., the audit function is free to determine the processes it will audit, based on the risk-based audit plan
2001.2.6	**Accountability** of the audit and assurance function includes, but is not limited to: ● **Distributing written communications** (e.g., reports for audits and memoranda for nonaudit engagements) to the appropriate stakeholders and to those charged with governance and oversight of the audit and assurance function (e.g., the board of directors and/or the audit committee) ● **Monitoring and reporting of management's progress** on agreed-on implementations (i.e., corrective actions) taken in response to audit recommendations ● **Reporting of the audit and assurance function's performance metrics** (e.g., performance relative to the audit plan and budget) to those charged with governance and oversight of the audit and assurance function (e.g., the board of directors and/or the audit committee) ● **Reporting to those charged with governance and oversight** of the audit and assurance function (e.g., the board of directors and/or the audit committee) on the function's independence and any potential impairments to independence and the four aspects of the purpose, responsibility, authority and accountability of the audit function ● **Quality assurance process** (e.g., interviews, customer satisfaction surveys, assignment performance surveys) that establishes an understanding of auditees' needs and expectations relevant to the audit function. These needs should be evaluated against the audit charter with a view to improving the service or changing the service delivery or audit charter, as necessary. ● **Staffing rules for audit engagements**, which may include but are not limited to: ■ Reliance on the audit charter permitting practitioners to be involved in performing nonaudit services (e.g., consulting services) and the broad nature, timing and extent of such services, to ensure that independence and objectivity are not impaired. This could eliminate or minimize the need to obtain specific mandates for each nonaudit service on a case-by-case basis. ■ Establishing a minimum time period that must elapse before practitioners can participate on audit engagements in areas in which they performed nonaudit services that impair independence. ■ Agreed-on actions regarding the audit function's and practitioners' behavior, e.g., penalties when either party fails to carry out its responsibilities. ■ Communication with auditees details the frequency and communication channels through which the audit function will communicate with the auditees.

Linkage to COBIT® 2019 for Standard 1001 and Guideline 2001

COBIT 2019 Management Objectives	Purpose
MEA02 Managed System of Internal Control	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1002: Organizational Independence

Statement	**1002.1** The IT audit and assurance function shall be free from conflicts of interest and undue influence in all matters related to audit and assurance engagements. Any impairment of independence (in fact or appearance) is identified and disclosed to the appropriate parties.
	1002.2 The IT audit and assurance function shall have a functional reporting relationship (e.g., reporting to the board of directors) that supports the function's ability to remain free from undue influence.
	1002.3 The IT audit and assurance function shall have an administrative reporting relationship that supports the function's unhindered performance of its responsibilities (e.g., scope of engagement, fieldwork or reporting).

General Guidelines 2002: Organizational Independence

2002.1 Introduction The guideline content section is structured to provide information on the IT audit and assurance function's independence:

2002.2 Position in the enterprise

2002.3 Reporting level

2002.4 Assessing independence

2002.2 Position in the Enterprise

2002.2.1	To enable organizational independence, the audit function needs to have a position in the enterprise that allows it to perform its responsibilities without interference. This can be achieved by: ● Establishing the audit function in the audit committee charter as an independent function or department outside of the operational departments. The audit function should not be assigned any operational responsibilities or activities. ● Ensuring that the audit function reports to a level within the enterprise that allows it to achieve organizational independence. Reporting to the head of an operational department could compromise organizational independence.
2002.2.2	The audit function should avoid performing nonaudit roles in IT initiatives that require assumption of management responsibilities, because such roles could impair future independence. The independence and accountability of the audit function should be addressed in the audit charter. The audit function's independence may be impaired if an auditor is scheduled to plan or to participate on an engagement in an area in which the auditor had direct management responsibility. Note that the IT audit and assurance function, in collaboration with the enterprise's external audit firm, can determine responsibilities that constitute direct or indirect management. These two groups can also identify the acceptable time frame between the auditor's performance of direct management responsibilities and participation on an engagement in the area.

2002.3 Reporting Level

2002.3.1	The audit function should report to a level within the enterprise that allows it to act with complete organizational independence. The independence should be defined in the audit charter and confirmed by the audit function to the board of directors and those charged with governance on a regular basis, at least annually.
2002.3.2	To ensure organizational independence of the audit function, the following should be reported to those charged with governance (e.g., the board of directors) for their input and/or approval: ● The audit resource plan and budget ● The risk-based audit plan ● Performance follow-up performed by the audit function on the IT audit activity ● Follow-up of significant scope or resource limitations
2002.3.3	To ensure organizational independence of the audit function, explicit support is needed from both the board and executive management. Executive management's support could include written communication to all levels of the organization.

2002.4 Assessing Independence

2002.4.1	Independence should be assessed regularly by the audit function and confirmed with those charged with governance and oversight of the audit function, e.g., the board of directors and/or the audit committee. This assessment needs to occur on at least an annual basis. The assessment should consider factors such as: ● Changes in personal relationships ● Financial interests ● Prior job assignments and responsibilities as well as proposed changes to current job assignment roles and responsibilities
2002.4.2	The audit function needs to disclose possible issues related to organizational independence and discuss them with the board of directors or those charged with governance. A resolution needs to be found and confirmed in the audit charter.

Linkages to COBIT® 2019 for Standard 1002 and Guideline 2002

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
APO01 Managed I&T Management Framework	Implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1003: Auditor Objectivity

Statement	**1003.1** IT audit and assurance practitioners shall be objective in all matters related to audit and assurance engagements.

General Guidelines 2003: Auditor Objectivity

These guidelines provide a framework that enables the IT audit and assurance practitioner to:

- Establish whether objectivity may be, or may appear to be, impaired
- Consider potential alternative approaches to the audit process when objectivity is, or may appear to be, impaired
- Reduce or eliminate the impact of impaired objectivity of IT audit and assurance practitioners performing nonaudit roles, functions and services
- Determine disclosure requirements when required objectivity may be, or may appear to be, impaired.
- Conduct the IT audit or assurance engagement with an impartial and unbiased frame of mind in addressing assurance issues and reaching conclusions
- Be mindful of potential impairments to objectivity during all phases of engagements
- Disclose the details of impairments to objectivity to the appropriate parties

2003.1 Introduction The guidelines are structured to provide information on the following key IT audit and assurance engagement topics:

2003.2 Conceptual framework

2003.3 Threats and safeguards

2003.4 Managing threats

2003.5 Nonaudit services or roles

2003.6 Nonaudit services or roles that do not impair independence

2003.7 Nonaudit services or roles that do impair independence

2003.8 Audit charter and nonaudit services/advisory roles

2003.9 Reporting

2003.2 Conceptual Framework

2003.2.1	Different circumstances or combinations of circumstances may be relevant in assessing threats to objectivity or independence. It is impossible to define every situation that creates a threat to objectivity or independence and to specify the appropriate action. Therefore, this guideline establishes a conceptual framework that requires the professional to identify, evaluate and address potential threats to objectivity or independence. The conceptual framework approach assists in complying with the independence standards, and it accommodates many variations in circumstances that create threats to independence.
2003.2.2	The conceptual framework approach should be applied by practitioners to: ● Identify threats to objectivity or independence ● Evaluate the significance of the threats identified ● Apply safeguards, when necessary, to eliminate the threats or reduce them to acceptable levels
2003.2.3	When practitioners determine that appropriate safeguards are not available or cannot be applied to eliminate objectivity threats or reduce threats to an acceptable level, practitioners should either eliminate the circumstance or relationship creating the threats, or decline or terminate the audit or assurance engagement. If practitioners cannot decline or terminate the engagement, appropriate disclosure of the impairment to objectivity or independence must be made to those charged with governance, and included in any report resulting from the engagement.
2003.2.4	Practitioners should consider applying ITAF guidance to identify potential threats to objectivity, evaluate the significance of the threats and implement appropriate safeguards when performing nonaudit services or roles.
2003.2.5	An auditor should not perform nonaudit services or roles in areas where it is likely that a current or future audit or assurance engagement is planned and would likely be performed by the same auditor. If the entity has no other recourse (i.e., engaging an alternative internal or external resource), the auditor's involvement in the nonaudit service should be approved by the chief audit executive (or VP/director of audit) and by those formally charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee).

2003.3 Threats and Safeguards

2003.3.1	Threats to objectivity may be created by a broad range of relationships and circumstances. When a relationship or circumstance creates a threat, such a threat could impair, or could be perceived to impair, professional objectivity. A circumstance or relationship may create more than one threat to objectivity. Threats fall into one or more of the following categories: • **Self-interest**—The threat that a financial or other interest will influence professional judgment or behavior inappropriately • **Self-review**—The threat that practitioners will not appropriately evaluate the results of previous judgments made or services performed, either by themselves or by other individuals within the audit function, which practitioners will rely upon when forming judgments in the current engagement • **Advocacy**—The threat that practitioners will promote an auditee's position to the point that professional objectivity is compromised • **Familiarity**—The threat that due to a long or close relationship with the auditee, practitioners will be too sympathetic to the interests of the auditee, or will be too accepting of the auditee's work, views or arguments • **Intimidation**—The threat that practitioners will be deterred from acting with integrity and objectivity because of actual or perceived pressures, including attempts to exercise undue influence over practitioners • **Bias**—The threat that political, ideological, social, psychological or other convictions will influence practitioners to take positions that are not objective • **Management participation**—The threat of impairments to objectivity resulting from practitioners taking on the role of management, or otherwise performing management functions on behalf of the entity undergoing an audit or assurance engagement
2003.3.2	Safeguards can be designed and implemented to reduce or minimize threats to objectivity. Examples of safeguards that can be considered by practitioners in response to identified threats are: • Internal procedures within the enterprise and audit function that ensure objective choices in assigning engagements, (e.g., the practitioner does not audit an area over which the practitioner previously had direct management responsibilities) • Assigning management and staff from outside the audit function, such as borrowing staff from another function, division or external organization to supplement practitioners • Periodic rotation in IT audit assignments, reducing the practitioner's familiarity with people in the assigned areas • Adequate hiring practices, such as background screening and vetting, to improve the likelihood that practitioners are free from bias or conflicts of interest (i.e., competing professional or personal interests) • Removing an individual from an engagement should that individual's interests or relationships pose a threat to objectivity • Appropriate documentation and reporting requirements, ensuring that assessment of professional independence is documented in the work papers and consistently reported in deliverables • Assigning an independent resource—from within the audit function or other sources referenced previously—to carry out a peer review or to act as an independent observer during planning, fieldwork and reporting • Having an external review of the reports, communications or information produced by practitioners by a recognized third party, e.g., accepted authority in the field or independent specialist

2003.4 Managing Threats

2003.4.1	The audit function and practitioners should determine whether identified threats to objectivity have been eliminated or reduced to an acceptable level. Threats to objectivity must be managed, as a loss of objectivity could impact a professional's ability to perform an audit or assurance engagement without being affected by influences that compromise professional judgment, or it could expose practitioners or the audit function to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity or professional skepticism of a member of the IT audit and assurance team had been compromised.

2003.5 Nonaudit Services or Roles

2003.5.1	In many enterprises, the expectation of management, IT staff and the internal audit function is that practitioners may be involved in nonaudit services or roles such as: ● Advising on IT strategies relating to areas such as technology, applications and resources ● Evaluating, selecting and implementing technologies ● Evaluating, selecting, customizing and implementing third-party IT applications and solutions ● Designing, developing and implementing custom-built IT applications and solutions ● Establishing good practices, policies and procedures relating to various IT functions ● Designing, developing, testing and implementing IT security and IT controls ● Advising on IT projects
2003.5.2	Providing nonaudit services or roles, in general, involves full-time or part-time participation in IT initiatives and IT project teams to provide advisory or consultative capabilities. IT audit and assurance practitioners may fulfill a nonaudit function through activities such as: ● Full-time temporary assignment or loan of IT audit and assurance staff to an IT project team ● Part-time assignment of an IT audit and assurance staff member as a member of an IT project, such as the project steering group, project working group, evaluation team, negotiation and contracting team, implementation team, quality assurance team or trouble-shooting team ● Acting as an advisor or reviewer of IT projects or IT controls on an *ad hoc* basis
2003.5.3	Providing nonaudit services or roles may create threats to professional objectivity or independence or create the appearance of such threats if the area in which the nonaudit services or roles were performed currently is the subject of an audit or assurance engagement or becomes the subject of an engagement in the future. In this situation, the perception may be that both the independence and the objectivity of practitioners were impaired by performance of the nonaudit services or roles.
2003.5.4	Practitioners providing nonaudit services or roles should use the conceptual framework to evaluate whether the nonaudit services or roles generate an impairment of objectivity or independence for current or future audit or assurance engagements. This applies to engagements in which the nonaudit services or roles are performed in an area that is significant or material to the subject matter or stakeholders of those engagements. If necessary, practitioners should seek guidance from IT audit and assurance colleagues and management, and/or those charged with governance, to determine whether safeguards can be implemented to adequately mitigate any actual or perceived threats to objectivity.

2003.5.5	Prior to commencing nonaudit services or roles, practitioners should establish and document their understanding with IT audit management and/or those charged with governance, as appropriate, regarding: ● The objectives of the nonaudit services or roles ● The nature of the nonaudit services or roles to be performed ● The audited entity's acceptance of its responsibilities related to the nonaudit services or roles ● Professional responsibilities related to the nonaudit services or roles ● Any limitations of the nonaudit services or roles ● Any limitations to the scope of future audit services practitioners can provide
2003.5.6	In the case of an IT audit or assurance engagement in which there is potential for impaired objectivity or independence in attitude or appearance due to nonaudit services or roles performed, IT audit and assurance management should implement safeguards such as: ● Monitoring the conduct of the audit closely ● Evaluating any significant indications of impairment of objectivity or independence arising out of nonaudit services or roles performed, and initiating necessary safeguards ● Informing those charged with governance of the potential impairment of objectivity or independence and the safeguards implemented

2003.6 Nonaudit Services or Roles That Do Not Impair Independence

2003.6.1	Activities that are routine and administrative or involve matters that are insignificant generally are deemed not to be management responsibilities and therefore would not impair objectivity.
2003.6.2	Nonaudit services or roles that would not impair independence or objectivity if adequate safeguards are implemented include providing routine advice on IT risk and controls.
2006.6.3	To avoid the risk of assuming a management responsibility when providing nonaudit services or roles in an area that is (or could become) the subject of an audit or assurance engagement, practitioners should provide the nonaudit services or roles only if satisfied that management performs or will perform the following functions in connection with the nonaudit services or roles: ● Assume all management responsibilities ● Oversee the services by designating an individual, preferably within senior management, who possesses suitable skill, knowledge or experience ● Evaluate the adequacy and results of the services performed ● Accept responsibility for the results of the services Practitioners should document their consideration of management's ability to effectively oversee the nonaudit services or roles performed.

2003.7 Nonaudit Services or Roles That Do Impair Independence

2003.7.1	If practitioners were to assume management responsibilities or perform management activities, the threats to independence could become so significant that no safeguards could reduce them to an acceptable level. Whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgment. Examples of activities that would generally be considered a management responsibility include: ● Setting policies and strategic direction ● Directing and taking responsibility for the actions of the entity's employees ● Authorizing transactions ● Deciding which recommendations of the audit function, internal audit function, organization, firm or other third parties to implement ● Taking responsibility for designing, implementing or maintaining internal control ● Accepting responsibility for the management of an IT project or initiative
2003.7.2	In addition to assuming management responsibilities, the following nonaudit services or roles may impair independence and objectivity: ● Material involvement of practitioners in the supervision or performance of designing, developing, testing, installing, configuring or operating information systems that are material or significant to the subject matter of the audit or assurance engagement ● Designing controls for information systems that are material or significant to the subject matter of the audit or assurance engagement ● Serving in a governance role in which practitioners are independently or jointly responsible for either making management decisions or approving policies and standards ● Providing advice that forms the primary basis of management decisions or performing management functions
2003.7.3	The following nonaudit services are considered to impair objectivity, because the threats created would be so significant that no safeguards could reduce them to an acceptable level: ● Assuming management responsibilities or performing management activities ● Material involvement of practitioners in the supervision or performance of designing, developing, testing, installing, configuring or operating information systems that are material or significant to the subject matter of the audit or assurance engagement ● Designing controls for information systems that are material or significant to the subject matter of current or planned future audit engagements ● Serving in a governance role in which the practitioners are responsible for either independently or jointly making management decisions or approving policies and standards ● Providing advice that forms the primary basis of management decisions

2003.8 Audit Charter and Nonaudit Services/Advisory Roles

2003.8.1	The IT audit charter should establish whether practitioners are permitted to perform nonaudit services or roles, and the broad nature, timing and extent of such services or roles, to ensure that neither objectivity nor independence is impaired with respect to the technologies practitioners may audit. This could eliminate or minimize the need to obtain specific mandates for each nonaudit service or role on a case-by-case basis.
2003.8.2	Practitioners should provide reasonable assurance that the terms of reference (TOR) of specific nonaudit services or roles conform with the audit charter. Any deviations should be expressly spelled out in the TOR and approved by IT audit and assurance management and/or those charged with governance.
2003.8.3	If the audit charter does not specify the nonaudit services or roles, or if there is no audit charter, practitioners should report the nature of their involvement in nonaudit services or roles to IT audit and assurance management and those charged with governance. The timing and extent of practitioners' involvement in nonaudit services or roles should be subject to individual TOR signed by management of the function in which the services or roles will be performed, and approved by those charged with governance.

2003.9 Reporting

2003.9.1	If the objectivity or independence of practitioners performing an IT audit or assurance engagement is, could be or could appear to be impaired, and if those charged with governance have made the decision to continue the engagement, the IT audit and assurance engagement report should include sufficient information to allow the users of the report to understand the nature of the potential impairment. Information that practitioners should consider disclosing in an IT audit and assurance engagement report includes: ● Names and seniority of practitioners involved in the IT audit and assurance engagement who may have, or may appear to have, an impairment to objectivity or independence ● Analysis and description of any potential impairment to objectivity or independence ● Safeguards implemented to eliminate or mitigate different threats to independence and objectivity during the course of the engagement work and the reporting process ● Documentation of disclosure of the potential impairment of objectivity or independence to those charged with governance, and their approval to perform or continue the assurance engagement and/or the nonaudit services or roles

Linkages to COBIT® 2019 for Standard 1003 and Guidelines 2003

COBIT 2019 Management Objectives	Purpose
MEA02 Managed System of Internal Control	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1004: Reasonable Expectation

Statement	**1004.1** IT audit and assurance practitioners shall have reasonable expectation that the engagement can be completed in accordance with applicable IT audit and assurance standards and, where required, other industry standards or applicable laws and regulations that will result in a professional opinion or conclusion.
	1004.2 IT audit and assurance practitioners shall have reasonable expectation that the scope of the engagement enables a conclusion on the subject matter and that any scope limitations are addressed.
	1004.3 IT audit and assurance practitioners shall have reasonable expectation that management understands its obligations and responsibilities with respect to providing appropriate, relevant and timely information required to perform the engagement.

General Guidelines 2004: Reasonable Expectation

2004.1 Introduction The purpose of this guideline is to assist IT audit and assurance practitioners in implementing the principle of reasonable expectation in the execution of audit engagements. This guideline further assists IT audit and assurance practitioners in addressing scope limitations, and provides guidance on accepting a change in engagement terms.

2004.2 Standards and regulations

2004.3 Scope

2004.4 Scope limitations

2004.5 Information

2004.6 Acceptance of a change in engagement terms

2004.7 Other considerations

2004.2 Standards and Regulations

2004.2.1	Practitioners should gather and assess all applicable standards listed in the audit charter and regulations before the audit engagement, and revisit them throughout the engagement, to determine whether they have reasonable expectation that they can complete the audit engagement in accordance with these standards and regulations, and to ensure that the audit engagement will result in a professional opinion or conclusion.
2004.2.2	Should practitioners determine that the audit engagement cannot be completed in accordance with one or more of the applicable standards and regulations, and that expression of a professional opinion or conclusion would therefore be impossible, they should: ● Inform IT audit and assurance management and those charged with governance of the identified compliance issues with the standards and regulations ● Either propose a change in engagement terms or decline the proposed engagement

2004.3 Scope

2004.3.1	Before undertaking the audit engagement, the practitioners should determine that the scope of the audit is clearly documented and permits a professional opinion or conclusion to be drawn on the subject matter.
2004.3.2	The scope of the audit engagement should be clearly documented, with no room for interpretation as to which areas (e.g., processes, activities, systems) are in the scope of the engagement. A scope that is described too vaguely will not allow practitioners to form a professional opinion or conclusion, because they will lack certainty that all areas in the scope have been assessed.
2004.3.3	Should practitioners determine that the scope of the audit engagement does not enable them to express a professional opinion or conclusion, they should: ● Inform IT audit and assurance management and those charged with governance of the audit function about the scope issues identified ● Propose a change in engagement terms or decline the proposed engagement

2004.4 Scope Limitations

2004.4.1	Specific scope limitations may occur before or during the audit engagement. These scope limitations can be influenced by different factors, such as: ● Appropriate, relevant and timely information required to complete the audit engagement is unavailable. ● Key auditees are unavailable. ● The time frame allotted is insufficient to complete the entire scope of the audit engagement. ● Management tries to limit the scope of the audit engagement to selected areas. ● The scope of the audit engagement is either too small or too large to come to a conclusion on the subject matter. ● The level of decentralization makes it difficult to reach a conclusion on the totality of the subject matter. ● The number of appropriately skilled practitioners available to perform the audit engagement with its current scope is insufficient. ● The reporting structure of the audit function (e.g., if the audit function does not report to the appropriate level within the enterprise, it may be directed not to assess certain elements in the scope). ● Third-party contracts may also introduce scope limitations. ● Delivery of client documentation is delayed ● Remediation of existing nonconformances (identified in a prior audit or self-identified by the auditees) is still in process.

2004.4.2	Practitioners should consider whether scope limitations still allow for a reasonable expectation that the audit engagement will result in a professional opinion or conclusion. Should they determine that this condition will not be fulfilled, they should not accept the engagement.
2004.4.3	Should practitioners conclude that they still have a reasonable expectation that, despite the scope limitations, the engagement will result in a professional opinion or conclusion, practitioners should accept or continue the audit engagement. The scope limitations should be explicitly described in the IT audit and assurance engagement report.
2004.4.4	Consider whether the scope is sufficient to permit an auditor's opinion to be expressed on the subject matter. Scope limitations may occur when information required to complete the engagement is unavailable, when the time frame included in the IT audit or assurance engagement is insufficient, or when management attempts to limit the scope to selected areas. In such cases, other types of engagements may be considered, such reviews of controls; compliance with required standards and practices; or compliance with agreements, licenses, legislation and regulation.

2004.5 Information

2004.5.1	The audit charter will determine the right of access to information, systems, personnel and locations relevant to the performance of the audit engagement.
2004.5.2	Before undertaking the audit engagement, practitioners should identify and address any restrictions placed on their right of access to appropriate, relevant and timely information for the audit engagement. Practitioners should have a reasonable expectation that their right of access for the audit engagement is in accordance with the stipulations in the audit charter, or that potential deviations from the stipulations do not preclude the practitioners from reaching a professional opinion or conclusion on the subject matter.

2004.5.3	Should practitioners conclude that their right of access to information does not enable them to express a professional opinion or conclusion, they should: ● Inform IT audit and assurance management and those charged with governance of the audit function of the identified issues concerning their right to access appropriate, relevant and timely information. ● Propose a change in engagement terms or not accept the proposed audit engagement.
2004.5.4	Performing an audit or assurance engagement could involve assessing activities performed by executive management. That possibility should be assessed prior to execution of the audit engagement. Practitioners should assess whether their need to access such individuals or related information will be challenged. Mitigating actions that might be required before the execution of the audit engagement include but are not limited to: ● Audit charter provisions assigning appropriate authority to the audit function and professionals ● Explicit written support from those charged with governance, e.g., board of directors and audit committee ● Attendance by a member of the board or executive management when access to executive or senior management is required

2004.6 Acceptance of a Change in Engagement Terms

2004.6.1	Practitioners should not accept a change in terms of the audit engagement if, based on their professional judgment, there is no justification for doing so.
2004.6.2	If, during the course of the audit engagement, practitioners are requested to accept a change in terms that lowers the level of assurance, they should determine whether there is justification for doing so, based on their professional judgment.
2004.6.3	If the terms of an audit engagement are changed, they should be recorded and formally approved by both practitioners and IT audit and assurance management. The IT audit and assurance engagement report should mention this change in terms explicitly.
2004.6.4	If practitioners do not accept a change in terms of the audit engagement and management does not permit them to continue the original audit engagement, in consultation with audit and assurance management, practitioners should: ● Withdraw from the audit engagement. ● Determine, according to their professional judgment, whether to report the circumstances to those charged with governance, e.g., the board of directors or even regulators.

2004.7 Other Considerations

2004.7.1	IT audit and assurance practitioners should: ● Undertake the IT audit or assurance engagement only if the work can be successfully completed in accordance with professional standards. ● Undertake the IT audit or assurance engagement only if the subject matter of the engagement can be assessed against relevant criteria. ● Review the scope of the IT audit or assurance engagement to determine that it is clearly documented so it can be clearly communicated to the auditees. ● Identify and address any restrictions being placed upon the engagement to be performed, including but not limited to access to appropriate, relevant and timely information. ● Make provisions for instances when written representations cannot be obtained from responsible auditee management. For example, oral representations could be obtained and documented in the work papers.

Linkages to COBIT® 2019 for Standard 1004 and Guidelines 2004

COBIT 2019 Management Objectives	Purpose
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1005: Due Professional Care

Statement	**1005.1** In accordance with ISACA's Code of Professional Ethics, auditors will exercise due diligence and professional care. They will maintain high standards of conduct and character, and they will refrain from engaging in acts that may discredit themselves or the profession. Privacy and confidentiality of information obtained during the course of the auditor's duties should be maintained. Further, this information should not be used for personal benefit, nor should the information be disclosed unless required by legal authority.

General Guidelines 2005: Due Professional Care

2005.1 The purpose of this guideline is to clarify the term "due professional care" as it applies to planning, performing and reporting on an audit engagement with integrity and care in compliance with the ISACA Code of Professional Ethics. Note that due professional care implies reasonable care and competence, not infallibility or extraordinary performance.

2005.2 Professional skepticism and competency

2005.3 Application

2005.4 Life cycle of the engagement

2005.5 Communication

2005.6 Obtaining and managing information

2005.7 Other considerations

2005.2 Professional Skepticism and Competency

2005.2.1	Due professional care applies to the exercise of professional judgment in the conduct of work performed. Due professional care implies that practitioners should approach matters requiring professional judgment with professional skepticism, diligence, integrity and care. They should maintain this attitude throughout the whole engagement.
2005.2.2	Practitioners should maintain competence, objectivity and independence, both in mind and appearance, in all matters related to the conduct of the audit engagement. They should be honest, impartial and unbiased in addressing issues and reaching conclusions.
2005.2.3	Exercising due professional care requires that practitioners consider the possible existence of inefficiencies, misuses, errors, scope limitations, incompetence, conflicts of interest or fraud. It should also make practitioners attentive to specific conditions or activities where these issues can occur.
2005.2.4	Practitioners should keep informed of and comply with developments in professional standards to demonstrate understanding and professional competence sufficient to achieve the IT audit and assurance objectives.
2005.2.5	Practitioners should conduct the audit engagement with diligence while adhering to professional standards and statutory and regulatory requirements.

2005.3 Application

2005.3.1	Due professional care should extend to every aspect of the audit, including but not limited to evaluating audit risk, accepting audit assignments, establishing audit scope, formulating audit objectives, planning the audit, conducting the audit, allocating resources to the audit, selecting audit tests, evaluating test results, documenting the audit, arriving at audit conclusions, reporting and delivering audit results, and conducting follow-up activities. In doing this, practitioners should determine or evaluate the following: ● Type, level, skill and competence of resources required to meet IT audit and assurance standards ● Significance of identified risk and the potential effect of such risk on the subject of the audit ● Sufficiency, validity and relevance of audit evidence gathered ● Competence, integrity and conclusions of others upon whose work practitioners place reliance
2005.3.2	Due professional care also requires practitioners to conduct all engagements with the concept of reasonable assurance in mind.
2005.3.3	Practitioners should serve the interests of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and should not engage in acts discreditable to the profession.

2005.4 Life Cycle of the Engagement

2005.4.1	Practitioners should plan the audit engagement completely and in a timely manner by exercising due professional care to ensure the availability of the appropriate resources and a timely completion of the audit engagement. Practitioners assigned to the project should collectively possess the needed skills, knowledge and relevant competencies to perform the audit engagement.
2005.4.2	Practitioners should conduct the audit engagement by applying due professional care, i.e., by following the appropriate professional standards to ensure a quality and complete audit conclusion or opinion.
2005.4.3	Practitioners should exercise due professional care in determining that management's corrective actions effectively address findings from the audit.

2005.5 Communication

2005.5.1	The defined roles and responsibilities should be communicated to the team members before the start of the project to ensure the team's adherence to the appropriate professional standards during the audit engagement.
2005.5.2	During the audit engagement, practitioners should appropriately communicate with auditees and relevant stakeholders to ensure their cooperation.
2005.5.3	Practitioners should address their findings to auditees of the audit engagement.
2005.5.4	Practitioners should document and communicate to appropriate parties any concerns regarding the application of professional standards in order to resolve those concerns.
2005.5.5	Practitioners should exercise due professional care while informing appropriate parties of the results of work performed.

2005.6 Obtaining and Managing Information

2005.6.1	Practitioners should have a reasonable expectation that management understands its obligations and responsibilities to provide appropriate, relevant and timely information required for the performance of the audit engagement.
2005.6.2	Practitioners should take reasonable measures to maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by a legal authority. Such information must not be used for personal benefit or released to inappropriate parties.

2005.6.3	Information should be obtained, used, retained and properly disposed of in accordance with organizational policies and relevant laws, rules and regulations.

2005.7 Other Considerations

2005.7.1	IT audit and assurance practitioners should: ● Perform engagements with integrity and care. ● Demonstrate sufficient understanding and competency to achieve engagement objectives. ● Maintain professional skepticism throughout the engagement. ● Maintain professional competency by keeping informed of and complying with developments in professional standards. ● Communicate team roles and responsibilities to team members, and ensure the team's adherence to the appropriate standards in conducting engagements. ● Address all concerns regarding the application of standards during the conduct of the engagement. ● Maintain effective communication with relevant stakeholders throughout the engagement. ● Take reasonable measures to protect information obtained or derived during the engagement from inadvertent release or disclosure to unauthorized parties. ● Conduct all engagements with the concept of reasonable assurance. The level of testing will vary with the type of engagement. ● Consider the use of relevant technology and data analysis techniques and auditors' competency using the technology and techniques. ● Consider the cost of the engagement relative to the potential benefits.

Linkages to COBIT® 2019 for Standard 1005 and Guidelines 2005

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
APO07 Managed Human Resources	Optimize human resources capabilities to meet enterprise objectives.
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1006: Proficiency

Statements	**1006.1** IT audit and assurance practitioners, collectively with others assisting with the audit and assurance engagement, shall possess the professional competence to perform the work required.
	1006.2 IT audit and assurance practitioners shall possess adequate knowledge of the subject matter to perform their roles in IT audit and assurance engagements.
	1006.3 IT audit and assurance practitioners shall maintain professional competence through appropriate continuing professional education and training.

General Guidelines 2006: Proficiency

2006.1 Introduction This guideline assists IT audit and assurance practitioners to acquire the necessary skills and knowledge and maintain professional competencies while carrying out audit engagements. The guideline content section is structured to provide information on the following key IT audit and assurance engagement topics:

2006.2 Professional competence

2006.3 Evaluation

2006.4 Reaching the desired level of competence

2006.5 Other considerations

2006.2 Professional Competence

2006.2.1	Professional competence denotes possession of skills, knowledge and expertise, through an adequate level of education and experience, to appropriately perform an audit engagement.
2006.2.2	IT audit and assurance management should communicate the desired and/or expected level of professional competence, based on appropriate benchmarks, for the different roles in audit engagements, and ensure such benchmarks are periodically reviewed and updated. IT audit and assurance management should document the professional competence required for various job levels, e.g., by documenting job/position descriptions or by formulating a skills matrix that indicates the professional competence required for the various job levels.
2006.2.3	IT audit and assurance management should provide reasonable assurance of the availability of competent resources required to carry out the audit engagements defined in the IT audit plan. The availability of such competent resources should be confirmed and ensured prior to commencement of the audit engagement.
2006.2.4	IT audit and assurance management should ensure that team members are competent to perform the audit engagement. Identification of core professional competencies of team members will assist in efficient utilization of available resources.
2006.2.5	Practitioners should provide reasonable assurance that they possess the required level of professional competence. They should acquire the professional and technical skills and knowledge required to carry out any assignment they agree to perform.
2006.2.6	Practitioners' required skills and knowledge vary with their positions and roles in the audit engagement. Requirements for management skills and knowledge should be commensurate with levels of responsibility.

2006.2.7	Skills and knowledge include proficiency in the identification and assessment of risk and controls, as well as in the application and use of audit tools and techniques. Practitioners should possess analytical and technical knowledge together with interviewing, interpersonal and presentation skills.
2006.2.8	Practitioners should possess the knowledge to identify and determine the impact of possible conditions or deviations material to the audit engagement, and to communicate them appropriately.
2006.2.9	Practitioners should possess the ability to recognize possible fraud indicators.
2006.2.10	In addition to information technology knowledge, practitioners should have a general knowledge of business fundamentals, e.g., economics, finance, accounting, risk, tax and law, to prevent them from overlooking potential issues or shortcomings.
2006.2.11	It is appropriate for practitioners to share their experiences, adopted good practices, lessons learned and knowledge gained with team members to improve their professional competencies. The professional competencies of team members are improved through team building sessions, workshops, conferences, seminars, lectures and other modes of interaction.
2006.2.12	To ensure availability of appropriate skills, alternative means of acquiring them should be assessed, e.g., subcontracting specific resources, outsourcing a portion of the IT audit and assurance tasks, and/or delaying the audit engagement until the required skills are available.
2006.2.13	External expertise can be obtained by outsourcing part or all of the engagement. Collaboration between outsourced resources and internal practitioners ensures that knowledge and skills are developed and maintained internally.
2006.2.14	If any part of the audit engagement is outsourced or expert assistance is obtained, reasonable assurance must be provided that the outsourced agency or the external expert possesses the requisite professional competence.
2006.2.15	If expert assistance is obtained on a continual basis, professional competence of such external experts should be periodically measured, monitored and reviewed against professional standards or benchmarks.

2006.3 Evaluation

2006.3.1	Practitioners should monitor their skills and knowledge continually to maintain the appropriate level of professional competence. IT audit and assurance management should periodically evaluate professional competence.
2006.3.2	Evaluation of the performance of practitioners should be carried out in a manner that is fair, transparent, easily understood, unambiguous, without bias and considered a generally acceptable practice given the employment environment.
2006.3.3	Evaluation criteria and procedures should be clearly defined but may vary depending upon circumstances such as geographic location, political climate, nature of assignment, culture and other similar circumstances.
2006.3.4	In the case of a team of practitioners, evaluation should be carried out internally among teams or individuals on a cross-functional basis.
2006.3.5	In the case of a single (sole) independent practitioner, peer evaluations should be carried out to the extent possible. If a peer review is not possible, self-evaluation should be conducted and documented.
2006.3.6	Evaluation of the performance of practitioners should be conducted by an appropriate level of management.
2006.3.7	Gaps noted during evaluation should be addressed appropriately.

2006.4 Reaching the Desired Level of Competence

2006.4.1	Gaps noted based upon variance in the actual level of professional competence and the expected level of professional competence should be recorded and analyzed. If a significant deficiency exists in any resource, that resource should not be used in conducting an audit engagement.
2006.4.2	It is important to ascertain the cause for the gap and to take appropriate corrective measures, e.g., training and continuing professional education (CPE), as soon as possible.
2006.4.3	Training activities required for an audit engagement should be completed within a reasonable time and before commencement of the audit activity.
2006.4.4	Effectiveness of training should be measured upon completion of training.
2006.4.5	Documentation of the required skills, e.g., a skills matrix, as formulated by IT audit and assurance management, will aid in identifying gaps and training needs. A matrix can be cross-referenced to available resources and their skills and knowledge.
2006.4.6	Records of training provided, together with feedback on training and effectiveness of training, should be maintained, analyzed and referenced for future use.
2006.4.7	CPE is a methodology adopted by ISACA to maintain professional competence and update skills and knowledge.
2006.4.8	CPE programs should aid in the enhancement of skills and knowledge related to professional and technical requirements of IT audit, risk, security, privacy and governance. Professional bodies ordinarily specify programs eligible for CPE recognition. Practitioners should adhere to the norms prescribed by their respective professional bodies.
2006.4.9	Professional bodies ordinarily prescribe the methodology of attaining CPE credits and the minimum credits that their constituents should periodically obtain. Practitioners must adhere to the norms prescribed by their respective professional bodies. If practitioners are associated with more than one professional body for the purpose of attaining minimum credits, they may use their professional judgment to attain CPE credits in a common manner from the eligible programs, provided the same is consistent with the rules/guidelines framed by the respective professional bodies.
2006.4.10	ISACA has a comprehensive policy on CPE, applicable to its members and holders of the CISA designation. Practitioners with the CISA designation must comply with ISACA's CPE policy. Details of the policy are available at *www.isaca.org/credentialing/cisa/maintain-cisa-certification*.
2006.4.11	As prescribed by respective professional bodies, including ISACA, practitioners are required to maintain appropriate records of CPE programs, retain them for specific periods and, if required, make them available for audit.

2006.5 Other Considerations

2006.5.1	IT audit and assurance practitioners should: ● Demonstrate possession of sufficient professional competencies (skills, knowledge and experience relevant to the planned engagement) prior to the commencement of the work. ● Assess alternative means of acquiring the skills needed to perform an engagement, including subcontracting, outsourcing a portion of the tasks, delaying the assignment until such skills are available or otherwise ensuring the appropriate skills are available. ● Ensure that team members involved in the IT audit and assurance engagement hold either a CISA or other relevant professional designation and have sufficient formal education, training and work experience. ● Provide reasonable assurance when leading an IT audit or assurance engagement that all team members have the appropriate level of professional competency to carry out the work they are expected to perform. ● Have sufficient knowledge of key areas to enable conduct of the IT audit or assurance engagement effectively and efficiently, together with other team members and any specialists involved. ● Meet continuing professional education or development requirements of CISA or other relevant professional designations. ● Update professional knowledge continually through educational courses, seminars, conferences, webcasts and on-the-job training to provide a level of professional service commensurate with the requirements of the IT audit or assurance role. ● If the required competencies are unlikely to become available in the required time frame, consider accommodating the engagement through the use of external resources.

Linkages to COBIT® 2019 for Standard 1006 and Guidelines 2006

COBIT 2019 Governance and Management Objectives	Purpose
EDM04 Ensured Resource Optimization	Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.
APO07 Managed Human Resources	Optimize human resources capabilities to meet enterprise objectives.

General Standard 1007: Assertions

Statement	**1007.1** IT audit and assurance practitioners shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

General Guidelines 2007: Assertions

2007.1 Introduction The purpose of this guideline is to detail the different assertions, guide IT audit and assurance practitioners in assuring that the criteria against which the subject matter is to be assessed support the assertions, and provide guidance on formulating a conclusion and drafting a report on the assertions. The guideline section is structured to provide information on the following key audit and assurance topics:

2007.2 Assertions

2007.3 Subject matter criteria

2007.4 Assertions developed by third parties

2007.5 Conclusion and report

2007.6 Other considerations

2007.2 Assertions

2007.2.1	Assertions are any declarations or sets of declarations about whether the subject matter is based on or in conformity with the criteria selected. Practitioners should consider these assertions throughout the execution of an audit engagement, obtain assurance on their achievement and address them in the audit report.
2007.2.2	Common assertions that may be considered include: ● **Confidentiality**—Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information. ● **Completeness**—All activities, information and other data that should have been recorded are recorded, e.g., all IT system changes promoted to production are recorded in the change management tracking application. ● **Accuracy**—Amounts, dates and other data related to recorded activities have been recorded appropriately, e.g., data related to the promotion of IT system changes into production are accurately displayed in the change records of the change management tracking application. ● **Integrity**—Information, evidence and other data received come from trustworthy and reliable sources and are protected throughout their life cycles, e.g., comparing the hash after a backup is completed with the hash immediately before a backup is restored to check for indications of tampering. ● **Availability**—Information, evidence and other data required for the audit engagement exist and are accessible, e.g., the requested change records exist and are readily accessible in the change management tracking application. ● **Compliance**—Information, evidence and other data are recorded according to the enterprise, regulatory or other applicable stipulations, e.g., required fields, according to the applicable stipulations, are present on the change records of the change management tracking application. ● **Efficiency**—Level of performance used allows the lowest number of inputs to create the greatest number of outputs. ● **Effectiveness**—The desired output or objective is produced.
2007.2.3	Management is responsible for defining and approving subject matter and related assertions. Practitioners should ensure that any assertions developed by management are what a knowledgeable reader or user would expect compared to other standards of authoritative pronouncements.

2007.2.4	A precondition for practitioners to accept the audit engagement should be confirmation from management that it fully understands its responsibility to provide all required information regarding the subject matter and the assertions to practitioners. If practitioners believe that management will not be able to fulfill this responsibility, they should: • Inform IT audit and assurance management and those charged with governance of the audit function of the identified issue. • Not accept the proposed audit engagement or determine an appropriate course of action based on the level of risk associated with the engagement.
2007.2.5	Practitioners should review the selected assertions for the audit engagement and ensure that they are: • **Sufficient**—Enough to meet the purpose of the audit engagement, which is to express an opinion or conclusion on the subject matter in scope • **Valid**—Able to be tested, given the subject matter in scope • **Relevant**—Directly connected to the subject matter in scope and useful to meeting the purpose of the audit engagement

2007.3 Subject Matter Criteria

2007.3.1	Practitioners should assess the subject matter of the audit engagement against predetermined criteria to express an opinion or conclusion on the subject matter. Practitioners should evaluate the criteria to ensure that they support the relevant assertions.
2007.3.2	One criterion can link to multiple assertions. Also, one assertion can be supported by multiple criteria. All may contribute to assurance in attaining the assertion.
2007.3.3	If practitioners conclude that the criteria do not fully support all the relevant assertions, they should recommend changes or additions to the existing criteria. IT audit and assurance management must review and approve or reject the new or modified criteria.
2007.3.4	After assessing that the criteria fully support the relevant assertions, practitioners should assess whether the criteria can be subject to objective and measurable analysis.

2007.4 Assertions Developed by Third Parties

2007.4.1	Enterprises outsourcing operations to third parties will receive reports about the control environment of the outsourced operations. If IT audit and assurance relies on reports related to outsourced operations to support an audit engagement, then practitioners should review each report to determine whether: • The report is issued by a relevant independent professional body. • The audit opinion is qualified or unqualified. • The scope of the control objectives adequately covers the controls required by the enterprise. • The period being audited is in line with enterprise expectations. • Specific control deficiencies (that did not lead to an overall qualification of the report) are relevant to the enterprise. • The assertions being used are in line with the required assertions. IT audit and assurance management should document the analysis made and conclusions reached. Practitioners should ensure that the assertions are verified and formally approved by management, as part of an audit engagement that has the outsourced operations in scope.
2007.4.2	Enterprises may also receive reports from third parties such as consultants or external auditors.

2007.5 Conclusion and Report

2007.5.1	After assessing the subject matter of the audit engagement against the criteria, practitioners should form a conclusion on each assertion, based on the aggregate of the findings against related criteria, along with professional judgment.
2007.5.2	After forming a conclusion, practitioners should issue an indirect or direct report on the subject matter: ● **Indirect report**—On the assertions about the subject matter, e.g., on the assertion "completeness," for a component of the subject matter: "Based on our operating effectiveness testing, in our opinion the IT system changes promoted to production, in all material respects according to the selected criteria, have been completely recorded in the change management tracking application." ● **Direct report**—On the subject matter itself, e.g., on the entire subject matter: "Based on our testing, in our opinion the IT system changes are following, in all material respects according to the selected criteria, the required change management procedure."

2007.6 Other Considerations

2007.6.1	IT audit and assurance practitioners should: ● Evaluate the criteria against which the subject matter is to be assessed to assure they support the assertions. ● Determine whether the assertions are auditable and supported by corroborating information. ● Determine whether the assertions are based on criteria that are appropriately determined and subject to objective and measurable analysis. ● Ensure that any assertions developed by management, in comparison to other standards of authoritative pronouncements, are sufficient to meet reasonable expectations that the assertions are correct. ● Ensure that any assertions developed by third parties who operate controls on behalf of the enterprise are verified and accepted by management. ● Report either directly against the subject matter (direct report) or against an assertion about the subject matter (indirect report). ● Form a conclusion about each assertion based on the aggregate of the findings against criteria, along with professional judgment.

Linkages to COBIT® 2019 for Standard 1007 and Guidelines 2007

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02 Ensured Benefits Delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 Ensured Risk Optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
EDM04 Ensured Resource Optimization	Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

General Standard 1008: Criteria

Statements	**1008.1** IT audit and assurance practitioners shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative and understood by, or available to, all readers and users of the report.
	1008.2 IT audit and assurance practitioners shall consider the acceptability of the criteria and focus on criteria that are recognized, authoritative and publicly available.

General Guidelines 2008: Criteria

2008.1 Introduction The purpose of this guideline is to assist IT audit and assurance practitioners in selecting criteria, against which the subject matter will be assessed, that are suitable, acceptable, and come from a relevant source. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2008.2 Selection and use of criteria

2008.3 Suitability

2008.4 Acceptability

2008.5 Source

2008.6 Change in criteria during the audit engagement

2008.2 Selection and Use of Criteria

2008.2.1	Practitioners shall select criteria against which the subject matter will be assessed. When selecting the criteria, practitioners shall carefully consider the suitability, acceptability and source of the criteria.
2008.2.2	Practitioners should consider the selection of criteria carefully. Adhering to local laws and regulations is important and should be considered a mandatory requirement. However, it is recognized that many audit engagements 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. The relevance of local and international data protection rules and privacy and security regulations should be considered. If legislative requirements are not prescriptive, practitioners should ensure that criteria selected meet the audit objectives to ensure compliance with the legislation.
2008.2.3	The use of suitable and acceptable criteria is required to ensure a consistent evaluation of the subject matter. Otherwise, any conclusion or opinion formed will be open to misunderstanding and misinterpretation by the reader.
2008.2.4	Practitioners should refrain from evaluating the subject matter on the basis of personal expectations, experiences or judgments.
2008.2.5	If criteria are not readily available, or if they are incomplete or subject to interpretation, practitioners should include a description of the criteria and any other information necessary to ensure that the report is fair, objective and understandable.
2008.2.6	Professional judgment should be used in ensuring that use of the criteria will enable the development of a fair and objective opinion or conclusion that will not mislead the reader or user. It is recognized that management might put forth criteria that do not meet all the requirements.

2008.3 Suitability

2008.3.1	Practitioners should assess the suitability and appropriateness of the criteria used for assessing subject matter. The sample criterion "Local law stipulates that all personal information of clients should always remain private when conducting data transactions" is used to clarify the following criteria attributes: • **Objectivity**—Free from bias that may adversely impact practitioners' findings and conclusions and thus may mislead the user of the audit report, e.g., the criterion is objective because it was ratified by local law. • **Completeness**—Sufficiently complete so that all criteria that could affect practitioners' conclusions about the subject matter are identified and used in the conduct of the audit engagement. Thus, completeness of all criteria used should be achieved, given the objectives of the audit engagement. • **Relevance**—Relevant to the subject matter and contributes to findings and conclusions that meet the objectives of the audit engagement. Criteria can be context-sensitive; even for the same subject matter, there can be different criteria, depending on the objectives and circumstances of the audit engagement, e.g., the criterion is considered relevant because data transactions are in the scope of the audit engagement. • **Reliability**—Criteria should allow reasonably consistent measurement or evaluation of the underlying subject matter and the development of consistent conclusions when applied by different practitioners in similar circumstances. • **Measurability**—Permits consistent measurement of the subject matter and the development of consistent conclusions when applied by different practitioners in similar circumstances, e.g., the criterion is measurable because every data transaction with unprotected personal information can be uniquely identified and thus consistently measured. • **Understandability**—Communicated clearly and not subject to significantly different interpretations by intended users, e.g., the criterion is understandable because this section of the law has already been the subject of multiple court rulings, helping to establish a clear understanding about the practical execution and interpretation of the law.

2008.4 Acceptability

2008.4.1	The acceptability of criteria is affected by the availability of the criteria to the users of the audit report, so that they understand the basis of the assurance activity and the relevance of the findings and conclusions. Acceptable criteria include those that are: • **Recognized**—Sufficiently well recognized so that their use is not questioned by intended users. • **Authoritative**—Reflect authoritative pronouncements within the area and are appropriate for the subject matter, e.g., authoritative pronouncements may come from professional bodies, industry groups, government and regulators. • **Publicly available**—Includes standards developed by professional accounting and audit bodies such as ISACA, International Federation of Accountants (IFAC), and other recognized government, legal or professional bodies. • **Available to all users**—Where not publicly available, criteria should be communicated to all users through assertions that form part of the audit report. Assertions consist of statements about the subject matter that meet the requirements of "suitable criteria" so they can be audited.

2008.4.2	Practitioners should ensure that the criteria used in an audit engagement are either: • **Externally accepted**—Recognized, authoritative and publicly available; or • **Externally confirmed**—Criteria developed by management for a specific audit engagement are not considered recognized, authoritative and publicly available. Before use, such criteria require external validation by a recognized independent third party to ensure that management does not implicitly compel a desired outcome of the audit engagement.

2008.5 Source

2008.5.1	In addition to considering the suitability and availability of IT assurance criteria, practitioners should consider the criteria's source, in terms of use and potential audience. For example, if the subject matter involves 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. Possible criteria sources, listed in order of consideration, include: • **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 recognized international experts in IT audit, risk, privacy, governance and security. • **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. Wording is often complex and carries a specific legal meaning. In many cases, it may be necessary to restate requirements as assertions. Further, expressing an opinion on legislation is usually restricted to members of the legal profession. • **Criteria established by entities that did not follow due process**—These include relevant criteria developed by entities that did not follow due process and thus have not been subject to public consultation and debate. • **Criteria developed specifically for the audit engagement**—While criteria developed specifically for the audit engagement may be appropriate, practitioners should take particular care to ensure that the criteria are suitable—especially objective, complete and measurable. Criteria developed specifically for an audit engagement are in the form of assertions. They usually pertain to the needs of a specific user. For example, various frameworks can be used as established criteria for evaluating the effectiveness of the internal control system. However, a certain user may develop a set of criteria that meets a specific need, e.g., a hierarchy of authorized approvals. Practitioners should clearly mention in the audit report that certain criteria are specific to the audit engagement. They should consider whether the developed criteria could mislead the intended user, and provide more information on the criteria if required. If management developed the criteria, external confirmation should be sought and mentioned in the report.

2008.6 Change in Criteria During the Audit Engagement

2008.6.1	As the audit progresses, additional information and insights on the subject matter may result in a change of selected criteria: ● Certain criteria may no longer be needed to achieve the audit objective, rendering further audit work related to the criteria unnecessary. ● If extra criteria are needed to achieve the audit objective, practitioners will select the criteria and conduct related audit work.

Linkages to COBIT® 2019 for Standard 1008 and Guidelines 2008

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

PERFORMANCE STANDARDS

Performance Standard 1201: Risk Assessment in Planning

Statements	**1201.1** The IT audit and assurance function shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and determine priorities for the effective allocation of IT audit resources.
	1201.2 IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements.
	1201.3 IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.

Performance Guidelines 2201: Risk Assessment in Planning

2201.1 Introduction The purpose of this guideline is to assist in identification of risk and threats in the IT environment. The guideline provides guidance in applying a risk assessment approach to develop an:

- IT audit plan that covers all annual audit engagements
- Audit engagement project plan that focuses on one specific audit engagement

The guideline provides details of the different types of risk the IT audit and assurance practitioners encounter. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2201.2 Risk assessment of the IT audit plan

2201.3 Risk assessment methodology

2201.4 Risk assessment of individual engagements

2201.5 Audit risk

2201.6 Inherent risk

2201.7 Control risk

2201.8 Detection risk

2201.9 Other considerations

2201.2 Risk Assessment of the IT Audit Plan

2201.2.1	A risk assessment should be conducted during the audit planning process and proactively modified based on changing business conditions and emerging risk. Practitioners should consider the organizational strategic plans and objectives and the enterprise risk management framework and initiatives. This will facilitate the development process of the IT audit schedule.

2201.2.2	To correctly and completely assess the risk that is related to the complete scope of the IT audit area, practitioners should consider the following elements when developing the IT audit schedule: ● Full coverage of all areas within the scope of the IT audit universe, which encompasses the range of all possible audit activities and considers the criticality of systems, applications and processes ● Reliability and suitability of the risk assessment provided by management ● Management's processes for supervising, examining and reporting possible risk or issues ● Cover risk in related activities relevant to the activities under review
2201.2.3	The applied risk assessment approach should help with the prioritization and scheduling process of the IT audit and assurance work. It should support the selection of areas and items of audit interest. It should guide the decision process for designing and conducting particular IT audit engagements.
2201.2.4	Practitioners should ensure that the applied risk assessment approach is approved by those charged with governance, and distributed to the various engagement stakeholders.
2201.2.5	Practitioners should use risk assessments to quantify and justify the amount of IT audit resources needed to complete the IT audit plan and to meet the requirements for specific engagements.
2201.2.6	Based on risk assessment, practitioners should develop an IT audit schedule that acts as a framework for the IT audit and assurance activities. It should: ● Consider non-IT audit and assurance requirements and activities ● Be updated at least annually ● Be approved by those charged with governance ● Address responsibilities set by the audit charter
2201.2.7	When developing the overall IT audit plan, a suitable risk assessment approach should be followed. The goal of risk assessment is to identify the parts of an activity that should receive more audit focus and to reduce the risk of reaching an incorrect conclusion.

2201.3 Risk Assessment Methodology

2201.3.1	Practitioners should consider the appropriate risk assessment methodology to ensure complete and accurate coverage of the audit engagements in the IT audit schedule.
2201.3.2	Practitioners should at least include within the methodology an analysis of the risk to the enterprise related to system availability, data integrity and business information confidentiality.
2201.3.3	Many risk assessment methodologies are available to support the risk assessment process. These range from simple classifications of high, medium and low, based on practitioners' judgment, to more quantitative and scientific calculations that provide a numeric risk rating. There are other methodologies that are a combination of the two. Practitioners should consider the level of complexity and detail appropriate for the enterprise or subject(s) being audited. Specific guidance on performing risk assessments can be found in the ISACA publications, *Risk IT Framework* and *Risk IT Practitioner Guide*.
2201.3.4	All risk assessment methodologies rely on subjective judgments at some point in the process (e.g., for assigning weights to the various parameters). Practitioners should identify the subjective decisions required to use a particular methodology and consider whether judgments can be made and validated to an appropriate level of accuracy and reasonableness.

2201.3.5	To determine the most appropriate risk assessment methodology, practitioners should consider: ● Type of information required to be collected. Some systems use financial effects as the only measure, which is not always appropriate for IT audit engagements. ● Cost of software or other licenses required to use the methodology ● Extent to which the information required is already available ● Amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting the information (including the required time investment in the collection exercise) ● Opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits ● Willingness of those charged with governance of the IT audit area to accept the methodology as the means of determining the type and level of audit work carried out
2201.3.6	No single risk assessment methodology can be expected to be appropriate for all situations. Practitioners should periodically reevaluate the appropriateness of the chosen risk assessment methodology because risk, threats, vulnerabilities, risk appetite and risk tolerance may change.
2201.3.7	Practitioners should use the selected risk assessment techniques in developing the overall IT audit schedule and in planning specific audit engagements. Risk assessment, in combination with other audit techniques, should be considered in planning decisions, such as: ● Areas or business functions to be audited ● Amount of time and resources to be allocated to an audit ● Nature, extent and timing of audit procedures
2201.3.8	The risk assessment methodologies adopted should produce consistent, valid, comparable and repeatable results and should be agreed upon by management. Risk assessments produced by the methodology should be consistent (over a period), valid, comparable (with earlier/later assessments using the same assessment methodology) and repeatable (given a similar set of facts, using the same assessment methodology will produce a similar outcome).

2201.4 Risk Assessment of Individual Engagements

2201.4.1	When planning an individual engagement, practitioners should identify and assess risk relevant to the area under review. The risk assessment results should be reflected in the audit engagement objectives. During the risk assessment, practitioners should consider: ● Results of prior audit engagements, reviews and findings, including any remedial activities ● The enterprise risk assessment process ● The likelihood of occurrence of a particular risk ● The impact of a particular risk (in monetary or other value measures) if it occurs
2201.4.2	Practitioners should ensure full understanding of the activities in scope before assessing risk. They should request comments and suggestions from stakeholders and other appropriate parties. Full understanding is required to correctly determine possible risk in the audit engagement and examine the related impact.

2201.4.3	When planning a specific IT audit and assurance procedure, practitioners should recognize that the lower the materiality threshold is, the more precise the audit expectations will be, and the greater the audit risk.
2201.4.4	When planning a specific IT audit and assurance procedure, practitioners should consider possible illegal acts that might require a modification of the nature, timing or extent of the existing procedures and corresponding documentation necessary to support potential litigation.
2201.4.5	To gain additional assurance in instances of high audit risk or lower materiality threshold, practitioners should compensate either by extending the scope or nature of the IT audit tests or by increasing or extending the substantive testing.

2201.5 Audit Risk

2201.5.1	Audit risk refers to the risk of reaching an incorrect conclusion based upon audit findings. The three components of audit risk are: • Inherent risk • Control risk • Detection risk
2201.5.2	Practitioners should consider each of the risk components to determine the overall level of risk. Audit risk is comprised of subject matter risk, which includes inherent risk and control risk, and detection risk.

2201.6 Inherent Risk

2201.6.1	Inherent risk is the susceptibility of an audit area to an error that could be material (individually or in combination with other errors), assuming that there were no related internal controls. For example, the inherent risk associated with operating systems without appropriate controls is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC without controls, when a proper analysis demonstrates it is not used for business-critical purposes, ordinarily is low.
2201.6.2	Since the IT auditor considers the scope of areas to be tested that affect major business systems, inherent risk is expected to be high.

2201.7 Control Risk

2201.7.1	Control risk is the risk that an error that could occur in an audit area and that could be material, individually or in combination with other errors, will not be prevented or detected and corrected in a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because a large volume of logged information can result in inadvertent failure to identify an anomaly resulting from human error. The control risk associated with computerized data validation procedures ordinarily is low because the processes are applied consistently.

2201.7.2	Practitioners should assess the control risk as high unless relevant internal controls are: ● Identified ● Validated via testing (i.e., comparison of performance to design) and proved to be operating effectively
2201.7.3	Practitioners should consider both pervasive and detailed IT controls: ● Pervasive IT controls are considered a subset of general controls; they are those general controls that focus on the management and monitoring of the IT environment. They affect all IT-related activities. The effect of pervasive IT controls on practitioners' work is not limited to the reliability of application controls in the business process systems. Pervasive IT controls also affect the reliability of detailed IT controls over, for example, application program development, system implementation, security administration and backup procedures. Weak pervasive IT controls, and thus weak management and monitoring of the IT environment, should alert practitioners to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective. ● Detailed IT controls are comprised of application controls plus the general controls not included in pervasive IT controls. Following the COBIT 2019 framework, detailed IT controls relate to the governance and management of information and technology.
2201.7.4	Practitioners should consider the risk that limitations and shortcomings in detailed IT controls may result from inadequacies in the pervasive IT controls.

2201.8 Detection Risk

2201.8.1	Detection risk is the risk that practitioners' substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying security breaches in an application system is often high, because logs for the whole period of the audit may not be available at the time of the audit. The detection risk associated with identifying the lack of disaster recovery plans tends to be low, since their existence is easily verified.
2201.8.2	In determining the level of substantive testing required, practitioners should consider: ● Assessment of inherent risk ● Conclusions on control risk following compliance testing
2201.8.3	The higher the assessment of inherent and control risk, the more audit evidence practitioners normally should obtain from the performance of substantive audit procedures.

2201.9 Other Considerations

2201.9.1	When planning ongoing activities, the IT audit and assurance function should:
	• Conduct and document a risk assessment to facilitate the development of the IT audit plan, at least annually.
	• Include in the risk assessment the organizational strategic plans and objectives and the enterprise risk management framework and initiatives.
	• Use risk assessments in the selection of areas and items of audit interest and in the decisions to design and conduct particular IT audit and assurance engagements. Some areas or items of interest may warrant continuous monitoring by management and continuous auditing by practitioners.
	• If management's risk assessment is relied upon, ensure that the assessment was approved by the appropriate parties. The risk assessment should document any instances of management acceptance of risk.
	• If the risk assessment was performed by the audit function, compare it with any risk assessments performed by others throughout the organization (e.g., an independent risk management function). Resolve any discrepancies (e.g., the audit function rates a risk high while risk management rates the risk low).
	• Prioritize and schedule IT audit and assurance work based on assessments of risk.
	• Based on the risk assessment, develop a plan that:
	  ▪ Serves as a framework for IT audit and assurance activities
	  ▪ Considers non-IT audit and assurance requirements and activities
	  ▪ Is updated at least annually and approved by those charged with governance
	  ▪ Addresses responsibilities set by the audit charter
	When planning an individual engagement, IT audit and assurance practitioners should:
	• Identify and assess risk relevant to the area under review.
	• Conduct a preliminary assessment of the risk relevant to the area under review for each engagement. Objectives for each specific engagement should reflect the results of the preliminary risk assessment.
	• Consider prior audits, reviews and findings—including any remedial activities—related to risk areas in a specific engagement. Also consider the board's overarching risk assessment process.
	• Attempt to reduce audit risk to an acceptable level and meet audit objectives by conducting an appropriate assessment of the IT subject matter and related controls, while planning and performing the IT audit.
	• To reduce audit risk for higher materiality, compensate either by extending the test of controls (reduce control risk) and/or by extending the substantive testing procedures (reduce detection risk) to gain additional assurance.

Linkages to COBIT® 2019 for Standard 1201 and Guidelines 2201

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.

EDM03 Ensured Risk Optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
APO12 Managed Risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Performance Standard 1202: Audit Scheduling

Statements	**1202.1** The IT audit and assurance function shall establish an overall strategic plan resulting in short-term and long-term audit schedules. Short-term planning consists of audits to be performed within the year, while long-term planning is comprised of audits based on risk-related matters within the enterprise's information and technology (I&T) environment that may be performed in the future.
	1202.2 Both short-term and long-term audit schedules should be agreed upon with those charged with governance and oversight (e.g., audit committee) and communicated within the enterprise.
	1202.3 The IT audit and assurance function shall modify its short-term and/or long-term audit schedules to be responsive to organizational needs (i.e., unexpected events or unplanned initiatives). Any audit displaced to accommodate an audit of an unexpected event or unplanned initiative should be reassigned to a future period.

Performance Guidelines 2202: Audit Scheduling

2202.1 Introduction This guideline provides guidance in audit scheduling for IT audit and assurance practitioners.

The guideline content section is structured to provide information on the key audit and assurance engagement topics:

2202.2 Developing and maintaining an audit schedule

2202.3 Audit schedule and engagement planning

2202.2 Developing and Maintaining an Audit Schedule

2202.2.1	IT audit and assurance practitioners shall develop and maintain an audit schedule that is based on an inventory of audit areas, often referred to as the audit universe. Audit scheduling helps to ensure that appropriate attention is devoted to the audit function's responsibilities as identified in the audit charter, and also that adequate assurance is provided regarding the enterprise's strategic objectives and organizational goals in important audit areas.
2202.2.2	Long-term audit schedules should be reevaluated on a periodic basis (at least annually) to be responsive to organizational needs. This reevaluation allows the audit function to include any additional assurance and audit engagements that may be required in response to unexpected critical events or situations. Any replaced planned audits should be reassigned to a future period.

2202.3 Audit Schedule and Engagement Planning

2202.3.1	The audit schedule can be communicated to the enterprise with tentative audit start dates, preliminary scope and key stakeholders.

Linkages to COBIT® 2019 for Standard 1202 and Guidelines 2202

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02 Ensured Benefits Delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
BAI11 Managed Projects	Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.

Performance Standard 1203: Engagement Planning

Statements	**1203.1** IT audit and assurance practitioners shall plan each IT audit and assurance engagement to address the nature, timing and extent of audit procedures to be performed. The plan should include: ● Areas to be audited ● Objectives ● Scope ● Resources (e.g., staff, tools and budget) and schedule dates ● Timeline and deliverables ● Compliance with applicable laws/regulations and professional auditing standards ● Use of a risk-based approach for engagements that are not related to legal or regulatory compliance ● Engagement-specific issues ● Documentation and reporting requirements ● Use of relevant technology and data analysis techniques ● Consideration of the cost of the engagement relative to the potential benefits ● Communication and escalation protocols for situations that may arise during the performance of an IT audit engagement (e.g., scope limitations or unavailability of key personnel) During fieldwork, it may become necessary to modify audit procedures created during planning as the engagement progresses.
	1203.2 IT audit and assurance practitioners shall develop and document an IT audit and assurance engagement program that describes the step-by-step procedures and instructions to be used to complete the audit.

Performance Guidelines 2203: Engagement Planning

2203.1 Introduction This guideline provides guidance in engagement planning for IT audit and assurance practitioners. The guideline content section is structured to provide information on the key audit and assurance engagement topics:

2203.2 Objectives

2203.3 Scope and business knowledge

2203.4 Risk-based approach

2203.5 Documenting the audit engagement project plan and audit program

2203.6 Changes during the course of the audit

2203.2 Objectives

2203.2.1	Practitioners should define the audit engagement objectives and document them in the audit engagement project plan. In addition to confirming an understanding of the enterprise's goals, operations and challenges, documentation of the audit engagement objectives ensures that testing lends assurance that controls are in place and operating effectively.
2203.2.2	Practitioners should develop an audit engagement project plan that takes into consideration the objectives of the audit engagement. These objectives might influence the audit engagement, e.g., resources, timeline and deliverables.

2203.3 Scope and Business Knowledge

2203.3.1	Before beginning an audit engagement, practitioners should plan their work in a manner appropriate for meeting the audit objectives. As part of the planning process, practitioners should obtain an understanding of the enterprise and its processes. This will assist them in determining the significance of the areas being reviewed as they relate to the objectives of the enterprise. Practitioners should establish the scope of the audit work based on the audit objectives.
2203.3.2	As part of a preliminary assessment, practitioners should gain an understanding of the types of personnel, events, transactions and practices that can have a significant effect on the specific enterprise, function, process or data that is the subject of the audit engagement. The auditor's knowledge of the enterprise should include the business and financial risk facing the enterprise, conditions in the enterprise marketplace, and the extent to which the enterprise relies on outsourcing to meet its objectives. Practitioners should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work, and considering actions of management for which they should be alert.

2203.4 Risk-Based Approach

2203.4.1	A risk assessment should be performed to gain an understanding of the enterprise and its environment (i.e., strategic objectives and internal and external obligations). This understanding will enable the practitioner to identify areas and activities for review.
2203.4.2	A risk assessment and prioritization of identified risk for the area under review and the enterprise IT environment should be carried out to the extent necessary.

2203.4.3	During the planning process, practitioners should establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system, practitioners should evaluate materiality of the various components of the system in planning the audit engagement for the work to be performed. Both qualitative and quantitative aspects should be considered in determining materiality.
2203.4.4	Before beginning an audit engagement and during the course of the audit, practitioners should consider compliance with applicable laws and professional auditing standards.
2203.4.5	When practitioners evaluate internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of a larger audit exercise (such as an audit of historical financial information), they should make a preliminary evaluation of the controls and develop the audit engagement project plan on the basis of that evaluation.

2203.5 Documenting the Audit Engagement Project Plan and Audit Program

2203.5.1	Practitioners' work papers should include the audit engagement project plan.
2203.5.2	A clear project definition is a critical factor to ensure project effectiveness and efficiency. An audit engagement project plan ("project plan") should include in the terms of reference items such as: ● Areas to be audited ● Type of work planned ● High-level objectives and scope of the work ● Fact-finding interviews to be conducted ● Relevant information to be obtained ● Procedures to verify or validate the information obtained and its use as audit evidence ● General topics, such as: ■ Budget ■ Resource availability and allocation ■ Schedule dates ■ Type of report ■ Intended audience ■ Deliverables ● Specific topics, such as: ■ Identification of tools needed for gathering evidence, performing tests and preparing/summarizing information for reporting ■ Assessment criteria (enterprise policies, procedures or protocol) to be used to evaluate current practices ■ Risk assessment documentation ■ Reporting requirements and distribution ■ External reports available (information that can be relied upon, if any) ■ Reports to be requested, if necessary, such as Statement on Standards for Attestation Engagements 18 (SSAE18)
2203.5.3	The project plan should include the requirements related to the timeline of the audit engagement. These elements include but are not limited to the period covered and the different completion dates to perform the audit engagement within the agreed-on schedule. The project plan should include budgetary expenditures and audit team resource allocations for each project phase.

2203.5.4	Practitioners should ensure that audit team resources assigned to the audit engagement have the right skills, knowledge and experience to successfully complete the audit engagement. Practitioners should assign the roles and responsibilities that best match the competencies of the IT audit team members.
2203.5.5	The project plan should list all deliverables that are linked to the audit engagement.
2203.5.6	The project plan and any changes to the project plan should be approved by IT audit and assurance management.
2203.5.7	After approval by IT audit and assurance management, parts of the project plan (e.g., scope, timeline, document requirements, interview schedule) should be communicated to the auditees so they can ensure access to and availability of the needed documents and resources.

2203.6 Changes During the Course of the Audit

2203.6.1	The audit engagement project plan should be updated and changed as necessary (with appropriate approvals by IT audit and assurance management) during the course of the audit engagement. If a concern that warrants the auditor's attention should arise once the audit is under way, practitioners should determine how to address the concern. Options include but are not limited to expanding the scope of the audit or scheduling a separate assessment. The IT audit practitioner shall immediately inform the auditee of any changes to the scope of the audit or the schedule based on the newly identified concern.
2203.6.2	Planning an audit engagement is a continual and iterative process. As a result of unexpected events, changes in conditions or audit evidence obtained, practitioners may need to modify the planned nature, timing and extent of further audit procedures. For example, when a new regulation is released, an assessment may need to be done immediately to determine any possible impact to the enterprise in terms of compliance.
2203.6.3	The audit plan should consider the possibility of unexpected events that imply risk for the enterprise. Accordingly, the audit engagement project plan should support prioritization of such events within the audit and assurance processes, based on risk.

2203.7 Other Considerations

2203.7.1	IT audit and assurance practitioners should: ● Obtain an understanding of the activity being audited. The extent of the knowledge required should be determined by the nature of the enterprise, its environment, its business objectives, its areas of risk and the objectives of the engagement. ● Consider subject matter guidance or direction, as afforded through legislation, regulations, rules, directives and guidelines issued by government or industry. ● Perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the engagement. Audit strategies, materiality levels and resource requirements can then be developed. ● Develop an engagement project plan using appropriate project management methodologies to ensure that activities remain on track and within budget. ● Develop a protocol to follow if the engagement will include reliance on professionals external to the audit function (co-sourcing or outsourcing) or reliance on prior testing performed by other entities (external auditors or regulators). The protocol should define: ■ Circumstances in which reliance on the work of others is an appropriate strategy ■ Initial assessment and ongoing monitoring of the qualifications of those external to the audit function who will perform work for the audit function ■ Circumstances that might warrant exclusions from engagements due to reliance on work of others: - Example 1: If the payment gateway process of an e-commerce system being audited is already under Payment Card Industry Data Security Standard (PCI-DSS) compliance, the audit function can exclude auditing the payment gateway process because it is already audited under another framework. - Example 2: If an environmental health and safety (EHS) framework certified by another body is in place at a big manufacturing firm, environmental security controls can be excluded from the audit engagement. ● Include in the audit plan assignment-specific issues, such as: ■ Availability of resources with appropriate knowledge, skills and experience ■ Identification of tools needed for gathering evidence, performing tests and preparing/summarizing information for reporting ■ Assessment criteria to be used ■ Reporting requirements and distribution ● Document the IT audit and assurance engagement's project plan and audit program to clearly indicate: ■ Objectives, scope and timing ■ Resources ■ Roles and responsibilities ■ Areas of risk identified and their impact on the engagement plan ■ Tools and techniques to be employed ■ Fact-finding interviews to be conducted ■ Relevant information to be obtained ■ Procedures to verify or validate the information obtained and its use as evidence ■ Assumptions regarding the approach, methodology, procedures, and anticipated results and conclusions ● Schedule the engagement with regard to the timing, availability, and other commitments and requirements of management and the auditee, to the extent possible.

2203.7.1 *(cont.)*	• Adjust the audit program during the course of the IT audit and assurance engagement to address issues that arise during the engagement, such as new risk, incorrect assumptions or findings from procedures already performed.
	• Ensure that the work being performed remains aligned with business objectives during post-planning phases of the audit.
	• For internal engagements:
	  ■ Prepare a separate engagement letter for each internal IT audit and assurance engagement.
	  ■ Communicate relevant elements of the audit charter to the auditee, using an engagement letter or equivalent to further clarify or confirm involvement in specific engagements.
	  ■ Communicate the plan so that the auditee is fully informed and can provide appropriate access to individuals, documents and other resources when required.
	• For external engagements:
	  ■ Prepare a separate engagement letter for each external IT audit and assurance engagement.
	  ■ Prepare a project plan and audit program for each external IT audit and assurance engagement, which should document the objectives and scope of the engagement, at a minimum.
	• Quantify and justify the amount of IT audit resources needed to meet the engagement requirements of each IT audit and assurance engagement.

Linkages to COBIT® 2019 for Standard 1203 and Guidelines 2203

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02 Ensured Benefits Delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 Ensured Risk Optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

Performance Standard 1204: Performance and Supervision

Statements	**1204.1** IT audit and assurance practitioners shall conduct the work in accordance with the approved IT audit plan to cover identified risk and within the agreed-on schedule.
	1204.2 IT audit and assurance practitioners shall provide supervision to IT audit staff for whom they have supervisory responsibility to accomplish audit objectives and meet applicable professional audit standards.
	1204.3 IT audit and assurance practitioners shall accept only tasks that are within their knowledge and skills, or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.
	1204.4 IT audit and assurance practitioners shall obtain and preserve sufficient and appropriate evidence to achieve the audit objectives.
	1204.5 IT audit and assurance practitioners shall document the audit process and describe the audit work and the audit evidence that support findings and conclusions.
	1204.6 IT audit and assurance practitioners' findings and conclusions are to be supported by root cause analysis and interpretation of this evidence.
	1204.7 IT audit and assurance practitioners shall provide an appropriate audit opinion or conclusion and include any scope limitation where required evidence is obtained through additional test procedures.

Performance Guidelines 2204: Performance and Supervision

2204.1 Introduction This guideline provides guidance to IT audit and assurance practitioners in performing the audit engagement and supervising IT audit team members. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2204.2 Performing the work

2204.3 Roles and responsibilities, knowledge and skills

2204.4 Supervision

2204.5 Evidence

2204.6 Documenting

2204.7 Findings

2204.8 Other considerations

2204.2 Performing the Work

2204.2.1	Practitioners shall plan and perform each audit engagement in accordance with the approved IT audit plan. Setting up an audit engagement project plan, as detailed in Standard 1203 Engagement Planning, allows practitioners to understand all elements in scope, cover all identified risk and ensure that the skills and knowledge required to execute the audit engagement within the agreed-on schedule are available.
2204.2.2	The main tasks in performing an audit engagement include: ● **Planning and risk assessment** ● **Identifying controls**—Based on the scope, audit objectives and main areas of risk identified in the IT audit plan, practitioners should identify the controls in scope of the audit engagement. ● **Assessing controls and gathering evidence**—Practitioners should assess the controls in scope by gathering and analyzing information and evidence on the design effectiveness and operating effectiveness of the controls. ● **Documenting work performed and identifying findings**—Practitioners should document the work performed, record the information and evidence gathered, and document any identified findings. ● **Confirming findings and following up on corrective actions**—Practitioners should confirm their findings with the auditee. Should the auditee perform corrective actions on the findings before the end of the audit engagement, practitioners should include the actions taken in the documentation (and conclusion) but also mention the original findings. ● **Drawing conclusions and reporting**—Practitioners should draw conclusions and report the impact of the findings on achieving the audit objectives. Focusing only on the control findings, without assessing the impact on the audit objectives, is insufficient.

2204.3 Roles and Responsibilities, Knowledge and Skills

2204.3.1	Practitioners in charge of the audit engagement should define and manage the roles and responsibilities of the IT audit team members throughout the engagement, addressing the following at a minimum: ● Designing the methodology and approach ● Creating audit work programs ● Defining execution and review roles ● Dealing with issues, concerns and problems as they arise ● Documenting and clearing the findings ● Writing the report
2204.3.2	Based on the engagement needs, practitioners in charge should consider the required competencies for the specific audit engagement. They should set up an engagement team that has the combined skills, knowledge and experience to complete the audit engagement successfully. Practitioners should make sure to assign those roles and responsibilities to the IT audit team members who have the skill sets that best match the requirements of the engagement.

2204.3.3	Practitioners should accept only the roles, responsibilities and associated tasks that are consistent with their knowledge and skills. Time and cost issues might prohibit practitioners from acquiring all the necessary knowledge and skills before the start of an audit engagement; therefore, practitioners are allowed to accept roles, responsibilities and associated tasks if they have reasonable expectation that appropriate measures will be taken during the audit engagement to ensure successful completion. The following measures would allow for such a reasonable expectation: ● **Learning on the job**—In certain circumstances, it will be possible for practitioners to acquire the necessary skills and knowledge during the audit engagement. ● **Supervision**—Practitioners in charge could arrange for adequate supervision of the IT audit team members, allowing them to successfully achieve the task under supervision. ● **External resources**—Practitioners in charge could hire external experts for those areas of the audit engagement for which the team lacks adequate internal knowledge and skills. Practitioners in charge should consider promoting the development of internal IT audit team members by having them work closely with the external experts to ensure a transfer of knowledge and skills to the team.

2204.4 Supervision

2204.4.1	Every task executed during an audit engagement by the IT audit team members should be under oversight of practitioners who have supervisory responsibilities to ensure that audit objectives and applicable professional audit standards are met. The extent of supervision required will depend highly on the skills, knowledge and experience of practitioners executing the task under review, and on the complexity of the audit engagement.
2204.4.2	Supervision is a process that is present in every step of the audit engagement. Supervision includes: ● Ensuring the IT audit team members have the combined skills, knowledge and experience to complete the audit engagement successfully ● Ensuring an appropriate audit engagement project plan and audit program are set up and approved ● Reviewing the audit engagement work papers ● Ensuring that audit engagement communication with auditees and other relevant stakeholders is accurate, clear, concise, objective, constructive and timely ● Ensuring that the approved audit engagement work program is completed at the end of the audit engagement, unless changes were justified and approved in advance, and that the audit engagement objectives are met ● Providing opportunities for IT audit team members to develop their skills and knowledge
2204.4.3	Reviewing audit engagement work papers is required to ensure that all necessary audit procedures are performed; evidence gathered is sufficient and appropriate; and conclusions adequately support the findings of the audit, engagement objectives, and conclusion or opinion. Considering the objectives, the review should be performed by IT audit team members who have supervisory responsibilities over the practitioners who perform the audit work.
2204.4.4	During the review process, reviewers should record questions as they arise. When practitioners respond to questions, care should be taken to retain evidence showing that questions were raised and answered.

2204.4.5	Evidence of review should be documented and retained. Options to document evidence of performing a review include but are not limited to: ● Signing and dating each audit engagement work paper after review ● Completing an audit engagement work paper review checklist ● Preparing a signed document that provides a reference to the audit engagement work papers under review and details the nature, timing, extent and result of the review Both digital and hard copy executions of all these options are valid.
2204.4.6	Supervision allows for development and performance evaluation of practitioners. Reviewers have a privileged view of the work performed by other IT audit team members, which allows for a detailed and adequate evaluation of their performance. Reviewers should point out areas of development that can improve performance and advise on ways to advance skills and knowledge.

2204.5 Evidence

2204.5.1	Practitioners should obtain evidence that is sufficient and appropriate to form an opinion or support the conclusions and achieve the audit objectives. Determinations of whether evidence is sufficient and appropriate should be based on the importance of the audit objectives and the effort involved in obtaining the evidence.
2204.5.2	Practitioners should obtain additional evidence if, in their judgment, the evidence obtained does not meet the criteria of being sufficient and appropriate to form an opinion or support the conclusions and achieve the audit objectives.
2204.5.3	Practitioners should select the most appropriate procedures to gather evidence, depending on the subject matter being audited.
2204.5.4	Practitioners should consider reliability of audit evidence (i.e., independence of the provider of the evidence, qualifications of the provider of the information, objectivity of the evidence, and timing of the evidence).
2204.5.5	Practitioners should perform appropriate analysis and interpretation to support the audit findings and form conclusions. Evidence and information received should be compared with expectations identified or developed by practitioners. Practitioners should be aware of: ● Unexpected differences ● Absence of anticipated differences ● Potential errors ● Fraud or illegal acts ● Noncompliance with laws or regulations ● Unusual or nonrecurring activities
2204.5.6	If deviations from expectations are identified, practitioners should ask management about the reasons for the differences. If management's explanations are adequate, based on practitioners' professional judgment, practitioners should modify their expectations and reanalyze the evidence and information.
2204.5.7	Significant deviations the auditee does not adequately explain should result in audit findings and be communicated to executive management or those charged with governance and oversight of the audit function. Depending on the circumstances, practitioners may recommend appropriate actions to take.

2204.6 Documenting

2204.6.1	Practitioners should prepare, in a timely manner, sufficient, appropriate and relevant documentation that provides a basis for conclusions and that contains evidence of the review performed. Sufficient, appropriate and relevant documentation should enable a prudent and informed person with no previous connection to the audit engagement to re-perform the tasks performed during the audit engagement and reach the same conclusion. Documentation should include: ● Audit engagement objectives and scope of work ● Audit engagement project plan ● Audit work program ● Audit steps performed ● Evidence gathered ● Conclusions and recommendations
2204.6.2	Documentation aids in planning, performing and reviewing audit engagements because it: ● Identifies the IT audit team members who performed each audit task and specifies their roles in preparing and reviewing the documentation ● Records the evidence requested ● Supports the accuracy, completeness and validity of the work performed ● Provides support for the conclusions reached ● Facilitates the review process ● Documents whether the engagement objectives were reached ● Provides the basis for a quality improvement program
2204.6.3	Practitioners should establish a preliminary program for review before the work begins. The audit program should be documented in a manner that permits practitioners to record completion of the audit work and identify work that remains to be done. As the work progresses, practitioners should evaluate the adequacy of the audit program based on information gathered during the audit engagement. When practitioners determine that the planned procedures are not sufficient, they should modify the audit program accordingly.
2204.6.4	Performance and supervision activities should be documented in audit engagement work papers. The design and content of the audit engagement work papers vary, depending on the circumstances of the particular audit engagement. However, IT audit and assurance management should create a limited number of standard template work papers for different types of audit engagements. Standard work papers improve the efficiency of the audit engagement and facilitate supervision. IT audit and assurance management should also determine the media carriers to be used and the storage and retention procedures for the work papers.
2204.6.5	Practitioners should ensure that documentation of the work performed is completed on a timely basis. All information and evidence required to form a conclusion or opinion should be obtained prior to the issue date of the audit report. Audit engagement work papers should include the date they were prepared and reviewed.
2204.6.6	IT audit and assurance management controls the audit engagement work papers and provides access to authorized personnel. Access requests to audit engagement work papers by external auditors should be approved by executive management and those charged with governance. Access requests by external parties, other than external auditors, should be approved by executive management and those charged with governance and oversight of the audit function, with the advice of legal counsel.

2204.7 Findings

2204.7.1	Practitioners should analyze the evidence and information gathered. Significant deviations from expectations should result in findings. Practitioners should confirm the findings with the auditee and assess the impact of the findings on other aspects of the control environment.
2204.7.2	Practitioners may propose corrective actions to be taken but should never execute them. Should the auditee perform corrective actions that remediate the original finding before the end of the audit engagement, practitioners should include the corrective actions taken in the documentation.
2404.7.3	Practitioners should conclude on the findings identified and assess their impact on the audit objectives. Conclusions should be formed on the original findings. If corrective actions have been performed, an addendum to the conclusion can be formulated explaining the corrective action and the impact of the corrective action on the original conclusion.
2404.7.4	All the conclusions formulated and whether the audit objectives have been achieved should be documented in the audit engagement report. Detailed guidance on reporting can be found in Reporting Standard 1401 and Guidelines 2401.

2204.8 Other Considerations

2204.8.1	IT audit and assurance practitioners should: ● Assign team members to match their skills and experience with the engagement needs. ● Add external resources to the IT audit team, if appropriate, and ensure that their work is properly supervised. ● Manage the roles and responsibilities of the specific IT audit team members throughout the engagement, addressing the following at a minimum: ■ Assigning execution and review roles ■ Delegating responsibility for designing the methodology and approach ■ Creating the audit or assurance programs ■ Conducting the work ■ Dealing with issues, concerns and problems as they arise ■ Analyzing of root causes ■ Coordinating with the team to review, document and clear findings ■ Writing the report ● Have engagement tasks executed by a team member reviewed by another appropriate team member. ● Use the best audit evidence attainable, consistent with the importance of the audit objective and the time and effort involved in obtaining the evidence. ● Obtain additional evidence if, in the professional's judgment, the evidence obtained does not meet the criteria of being sufficient and appropriate to form an opinion or support the findings and conclusions. ● Organize and document the work performed during the engagement following predefined documented and approved procedures.

	• Include in documentation:
	  ▪ Audit objectives and scope of work, the audit program, audit steps performed, evidence gathered, findings, conclusions and recommendations
	  ▪ Detail sufficient to enable a prudent, informed person to re-perform the tasks performed during the engagement and reach the same conclusion
	  ▪ Identification of who performed each task and each team member's role in preparing and reviewing the documentation
	  ▪ The date the documentation was prepared and reviewed
	• Obtain relevant written representations from the auditee that clearly detail critical areas of the engagement, issues that have arisen and their resolution, and assertions made by the auditee.
	• Determine that auditee representations have been signed and dated by the auditee to indicate acknowledgment of responsibilities with respect to the engagement.
	• Document and retain in work papers any representations received during the course of conducting the engagement, either written or oral.

Linkages to COBIT® 2019 for Standard 1204 and Guidelines 2204

COBIT 2019 Management Objectives	Purpose
APO07 Managed Human Resources	Optimize human resources capabilities to meet enterprise objectives.
APO08 Managed Relationships	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Performance Standard 1205: Evidence

Statements	**1205.1** IT audit and assurance practitioners shall obtain sufficient and appropriate evidence to draw reasonable conclusions.
	1205.2 Applying professional skepticism, IT audit and assurance practitioners shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.
	1205.3 Along with other working papers, IT audit and assurance practitioners shall preserve evidence for the time period that aligns with formally defined and approved retention periods.

Performance Guidelines 2205: Evidence

2205.1 Introduction The purpose of this guideline is to provide guidance to IT audit and assurance practitioners in obtaining sufficient and appropriate evidence, evaluating the received evidence and preparing appropriate audit documentation. The guideline content section is structured to provide information on the following key audit and assurance topics:

2205.2 Types of evidence

2205.3 Obtaining evidence

2205.4 Evaluating evidence

2205.5 Preparing audit documentation

2205.6 Other considerations

2205.2 Types of Evidence

2205.2.1	When planning and performing an engagement, practitioners should consider the types of evidence to be gathered, its use to meet engagement objectives and its varying levels of reliability. The various types of evidence that practitioners should consider using include: ● Observed processes and existence of physical items ● Documentary evidence ● Representations ● Analysis
2205.2.2	Observed processes and existence of physical items can include observations of activities, property and IT functions, such as: ● A network security monitoring system in operation ● An inventory of media in an offsite storage location
2205.2.3	Evidence documented on paper or other media can include: ● Written policies and procedures ● Results of data extractions ● Records of transactions ● Program listings ● Other documents and records produced in the ordinary course of business ● External confirmation from third parties
2205.2.4	Written and oral representations of those being audited can include: ● Written statements by management, such as representations about the existence and effectiveness of internal controls or plans for a new system implementation ● Oral representations of such things as how a process works or plans for management follow-up on actions related to the security awareness program
2205.2.5	The results of analyzing information through comparisons, simulations, calculations and reasoning can also be used as evidence. Examples include: ● Benchmarking IT performance against other enterprises or past periods ● Comparison of error rates between applications, transactions and users ● Re-performance of processes or controls

2205.3 Obtaining Evidence

● **2205.3.1**	Practitioners should obtain sufficient and appropriate evidence to allow them to draw reasonable audit conclusions. This evidence includes: ● Procedures performed ● Results of procedures performed ● Source documents (in either electronic or paper format), records and corroborating information used to support the audit engagement ● Documentation that the work was performed and complies with applicable laws, regulations and policies
● **2205.3.2**	If evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, practitioners should consider obtaining confirmation of the representations, either in writing or electronically (such as through email). Practitioners should also consider alternative evidence to corroborate such representations to ensure their reliability.
2205.3.3	When gathering evidence, the professional should consider the following: ● The time, level of effort and cost of obtaining the evidence compared to the sufficiency of the evidence in reducing audit risk ● Significance of the matter being evaluated and of the audit procedure requiring the evidence in achieving the audit objectives and reducing audit risk ● Electronic evidence may not be retrievable in whole or in part after the passage of time

2205.3.4	Procedures used to gather evidence vary, depending on the characteristics of the information system being audited, timing of the audit, audit scope and objectives, and professional judgment. Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both. Practitioners should select the most appropriate procedure in relation to the IT audit objective. The following procedures should be considered: • **Inquiry and confirmation**—The process of seeking information from experienced people who are familiar with the subject matter. The experienced people need not be members of the enterprise being audited. This procedure can range from formal written inquiries to informal oral inquiries. • **Observation**—Observing a procedure or process being performed by those individuals who are typically responsible for its performance or observing physical items such as facilities, computer hardware, or information system settings or configurations. This type of evidence is limited to the point in time when the observation took place. Practitioners should take into account that observing the performance of a process or procedure may affect the way the procedure or process is performed. • **Inspection**—Examination of internal or external documents and records. The items to be inspected can be supplied in paper or electronic form. Inspection can also include physical asset examination. • **Analytical procedures**—Evaluating data by examining possible relationships within the data or between the data and other relevant information. This also includes examining fluctuations, trends and inconsistent relationships. • **Recalculation/computation**—The process of checking the arithmetical and mathematical accuracy of documents or records either manually or through the use of CAATs. • **Re-performance**—Independent performance of procedures and/or controls that were originally executed by the information system or by the enterprise itself. • **Other generally accepted methods**—Other generally accepted procedures that practitioners can follow in gathering sufficient and appropriate evidence, such as engaging in social engineering, acting as a mystery guest or conducting ethical intrusion testing.
2205.3.5	When gathering evidence, practitioners should consider the independence and qualifications of the entity providing the evidence. For example, corroborative audit evidence from an independent third party can be more reliable than audit evidence obtained from the enterprise being audited. Physical audit evidence is generally more reliable than the representations of an individual.
2205.3.6	If there is a possibility that the gathered evidence will become part of a legal proceeding, practitioners should consult with the appropriate legal counsel to determine whether there are any special requirements that will impact the way evidence needs to be gathered, presented and disclosed.
2205.3.7	In situations where practitioners are not able to obtain sufficient audit evidence—e.g., if individuals or management should refuse to provide the satisfactory and appropriate evidence necessary to achieve the IT audit objectives—practitioners should disclose the situation to audit management and, if necessary, to those charged with audit governance, in accordance with the audit organization's established procedures. Restrictions or limitations on the scope of the audit and achievement of the audit objectives should also be disclosed in the communication of the audit results.

2205.3.8	Practitioners should retain evidence after completion of the audit work to ensure that the evidence is: ● Available for a time period and in a format that complies with the audit organization's policies and relevant professional standards, laws and regulations ● Protected from unauthorized disclosure or modification throughout its preparation and retention ● Properly disposed of at the end of the retention period

2205.4 Evaluating Evidence

2205.4.1	Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives. If, in the practitioner's judgment, the evidence does not meet these criteria, the practitioner should obtain additional evidence or perform additional procedures to reduce the limitations or uncertainties related to the evidence. For example, a program listing may not be adequate evidence until other evidence has been gathered to verify that it represents the actual program used in the production process.
2205.4.2	When evaluating the reliability of evidence obtained during an audit, practitioners should consider the characteristics and properties of the evidence, such as its source, nature (written, oral, visual or electronic), authenticity (presence of digital or manual signatures, date/time stamps) and relationships between evidence that provides corroboration from multiple sources. In general, the reliability of evidence is ranked from low to high based on the procedures used to obtain the evidence, as follows: ● Inquiry and confirmation ● Observation ● Inspection ● Analytical procedures ● Recalculation or computation ● Re-performance For each of the previous procedures, evidence reliability is generally greater when it is: ● In written form, rather than obtained from oral representations ● Obtained directly by the practitioners rather than indirectly by the entity being audited ● Obtained from independent sources ● Certified by an independent party ● Maintained by an independent party
2205.4.3	Practitioners should consider the time period during which information exists or is available in determining the nature, timing and extent of substantive testing and, if applicable, compliance testing. For example, evidence processed by electronic data interchange (EDI), document image processing (DIP) and spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or if the files are not backed up. Documentation availability could also be impacted by the enterprise document retention policies.
2205.4.4	If there is an independent third-party audit, practitioners should consider whether testing of controls relevant to the subject of the audit was performed, and whether any reliance can be placed on the results of that testing.
2205.4.5	Practitioners should obtain evidence that is sufficient and appropriate to enable a qualified independent party to re-perform the tests and obtain the same results and conclusions.

2205.5 Preparing Audit Documentation

2205.5.1	During the performance of the audit, practitioners should document the evidence obtained and ensure that documentation is retained and available during a predefined time period, in a format that complies with enterprise policies and relevant professional standards, laws and regulations.
2205.5.2	Evidence obtained during the performance of the audit should be appropriately identified, cross-referenced and cataloged to facilitate determination of the overall sufficiency and appropriateness of evidence. These steps are necessary to provide a reasonable basis for the findings and conclusions within the context of the audit objectives, and to allow for easy retrieval by other IT audit team members or an independent party.
2205.5.3	Practitioners should ensure that documentation of evidence is protected from unauthorized access, disclosure or modification throughout its preparation and retention. Periods of retention may be influenced by external requirements. For example, for enterprises subject to U.S. Securities and Exchange Commission (SEC) requirements, financial auditors must retain certain records for a period of seven years from conclusion of the audit or review.[1]
2205.5.4	Practitioners should dispose of evidence documentation at the end of the established retention period.

2205.6 Other Considerations

2205.6.1	In performing an engagement, IT audit and assurance practitioners should: ● Appropriately identify, cross-reference and catalog evidence. ● Consider the most cost-effective and timely means of gathering the necessary evidence to satisfy the objectives and risk of the engagement. However, difficulty or cost is not a valid basis for omitting a necessary procedure. ● Obtain evidence commensurate with the materiality of the item and the risk involved. ● Place due emphasis on the accuracy and completeness of the information when information obtained from the enterprise is used by the IT audit and assurance practitioner to perform audit procedures.

Linkages to COBIT® 2019 for Standard 1205 and Guidelines 2205

COBIT 2019 Management Objective	Purpose
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

[1] US Securities and Exchange Commission, "Final Rule: Retention of Records Relevant to Audits and Reviews," www.sec.gov/rules/final/33-8180.htm#:~:text=Under%20the%20new%20rule%2C96,of%20the%20audit%20or%20review

Performance Standard 1206: Using the Work of Other Experts

Statements	**1206.1** IT audit and assurance practitioners shall consider using the work of other experts for the engagement, where appropriate.
	1206.2 IT audit and assurance practitioners shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.
	1206.3 IT audit and assurance practitioners shall assess, review and evaluate the work of other experts as part of the engagement and document the conclusion on the extent of use and reliance on their work.
	1206.4 IT audit and assurance practitioners shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives. The practitioners should also clearly document the conclusion.
	1206.5 IT audit and assurance practitioners shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.
	1206.6 IT audit and assurance practitioners shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.
	1206.7 IT audit and assurance practitioners shall provide an audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

Performance Guidelines 2206: Using the Work of Other Experts

2206.1 Introduction This guideline provides guidance to IT audit and assurance practitioners considering the use of work of other experts. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2206.2 Considering the use of work of other experts

2206.3 Assessing the adequacy of other experts

2206.4 Planning and reviewing the work of other experts

2206.5 Evaluating the work of other experts

2206.6 Additional test procedures

2206.7 Audit opinion or conclusion

2206.8 Other considerations

2206.2 Considering the Use of Work of Other Experts

2206.2.1	Practitioners who do not have the required competencies to perform the audit engagement, either in whole or in part, should consider seeking assistance from other experts with the required skills.
2206.2.2	Using the work of other experts should be considered if there are constraints that could impair the audit work to be performed, such as lack of technical knowledge required by the nature of the tasks to be performed, scarce audit resources, time constraints and potential independence issues. The use of other experts also should be considered if it would enhance the quality of the engagement.
2206.2.3	Practitioners are not expected to have a knowledge level equivalent to that of the other experts. Practitioners should, however, have sufficient knowledge of the work performed to be able to guide and review the work of the other experts. When relying on the work of others, practitioners should present objective evidence that verifies the competency and skill level of the experts.
2206.2.4	Practitioners should base their choice of specific experts and the use of other experts' work on objective criteria.
2206.2.5	Practitioners should communicate and document performance requirements to other experts in a contract or agreement prior to the experts beginning work on the engagement.
2206.2.6	If other experts' access to records or systems is prohibited by enterprise internal policies, practitioners should determine the appropriate extent of use and reliance on the other experts' work.
2206.2.7	If the necessary experts cannot be obtained, practitioners should document the impact on achieving the audit objectives and include specific tasks in the audit plan to manage the resulting audit risk. If the resulting audit risk cannot be managed, practitioners may need to decline the audit engagement.
2206.2.8	IT audit and assurance practitioners may place reliance on System and Organization Control (SOC) reporting as part of their reviews.

2206.3 Assessing the Adequacy of Other Experts

2206.3.1	If an audit engagement involves using the work of other experts, practitioners should consider the adequacy of the other experts while planning the IT audit work by assessing the other experts' professional qualifications, competencies, relevant experience, resources and use of quality control processes.
2206.3.2	Practitioners should consider the independence and objectivity of other experts before relying on their work. The processes for selection and appointment, the organizational status, the reporting line, and the effect of the other experts' recommendations on management practices are typical indicators of the other experts' independence and objectivity.

2206.4 Planning and Reviewing the Work of Other Experts

2206.4.1	Practitioners should verify that the audit charter or engagement letter specifies their right of access to the other experts' work. Practitioners should have access to all work papers, supporting documentation and reports created by the other experts, if such access does not create legal or privacy issues.

2206.4.2	Practitioners should consider the activities of other experts and their effects on the IT audit objectives while planning the IT audit work, including: ● Obtaining an understanding of the other experts' scope of work, approach, timing and use of quality control processes ● Determining the level of review required
2206.4.3	The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other experts' work. During the planning process, practitioners should identify the level of review that is required to provide sufficient and appropriate audit evidence to achieve the overall IT audit objectives effectively. Practitioners should review the other experts' final report, methodology or audit programs, and work papers.
2206.4.4	In reviewing work papers, practitioners should assess whether the other experts' work was appropriately planned, supervised, documented and reviewed, in order to consider the appropriateness and sufficiency of the audit evidence provided and to determine the extent of use and reliance on the experts' work. This assessment may include a retest of the work of other experts. Compliance with relevant professional standards should also be assessed. Overall, practitioners should assess whether the work of other experts is adequate and complete to enable them to conclude on the current IT audit objectives and document a conclusion.
2206.4.5	Practitioners should perform sufficient reviews of other experts' final reports to confirm that: ● The scope specified in the audit charter, terms of reference or letter of engagement has been met. ● Any significant assumptions used by the other experts have been identified. ● The findings and conclusions reported are adequately supported by evidence.

2206.5 Evaluating the Work of Other Experts

2206.5.1	Interdependencies between customers and suppliers regarding the processing and outsourcing of noncore activities contribute to a complex audit environment. Parts of the environment being audited can be controlled and audited by other independent functions or enterprises. The outsourcing enterprise will receive reports from those third parties about the control environment of the outsourced operations. In some cases, these operations may lessen the need for IT audit coverage even though practitioners do not have access to supporting documentation and work papers. Practitioners should be cautious in providing an opinion in such cases.

2206.5.2	Practitioners should assess the usefulness and appropriateness of the work performed by other experts and consider any significant findings reported by the other experts. Practitioners are responsible for determining the extent to which the work of other experts may be relied upon, incorporated directly or referred to separately in the report. Practitioners should also assess the effect of other experts' findings and conclusions on the overall IT audit objective. Practitioners also should verify that any additional work required to meet the overall IT audit objective was completed. All assertions made by other experts should be verified and formally approved by management. Detailed guidance on this topic can be found in Standard 1007 Assertions.

2206.6 Additional Test Procedures

2206.6.1	Based on their assessment of the work of other experts, practitioners should apply additional test procedures to gain sufficient and appropriate audit evidence if the work of other experts does not provide such evidence.
2206.6.2	Practitioners should consider whether supplemental testing of the other experts' work is required.

2206.7 Audit Opinion or Conclusion

2206.7.1	It is the practitioner's responsibility to formulate an audit opinion or conclusion. Practitioners need to determine whether the work performed by other experts was sufficient to support the audit opinion or conclusion.
2206.7.2	If additional test procedures performed do not provide sufficient and appropriate audit evidence, practitioners should provide an appropriate audit opinion or conclusion, and include scope limitations if required.
2206.7.3	Practitioners' views and comments on the adoptability and relevance of the other experts' report should form a part of the audit engagement report if the experts' report is utilized in forming practitioners' opinion.
2206.7.4	If appropriate, practitioners should consider the extent to which management has implemented any recommendations of other experts. This should include assessing whether management has committed to remediating issues identified by other experts within appropriate time frames and the current status of remediation.

2206.8 Other Considerations

2206.8.1	IT audit and assurance practitioners should: ● Document the impact on achieving the engagement objectives if required experts cannot be obtained, and insert specific tasks in the engagement plan to manage risk and evidence requirements. ● Determine and conclude on the extent of use and reliance on other experts' work, if they are not granted access to records due to legal issues. ● Document the use of other experts' work in the report.

Linkages to COBIT® 2019 for Standard 1206 and Guidelines 2206

COBIT 2019 Management Objective	Purpose
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Performance Standard 1207: Irregularities and Illegal Acts

Statements	**1207.1** IT audit and assurance practitioners shall consider the risk of irregularities and illegal acts during the engagement.
	1207.2 IT audit and assurance practitioners shall document and communicate irregularities or illegal acts to the appropriate party in a timely manner. Note that some communications (e.g., with regulators) may be restricted. As a result, the practitioner's communications may require discussion with those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee).

Performance Guidelines 2207: Irregularities and Illegal Acts

2207.1 Introduction This guideline details the responsibilities of both management and IT audit and assurance practitioners with regard to irregularities and illegal acts. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2207.2 Irregularities and illegal acts

2207.3 Responsibilities of management

2207.4 Responsibilities of practitioners

2207.5 Irregularities and illegal acts during engagement planning

2207.6 Designing and reviewing engagement procedures

2207.7 Responding to irregularities and illegal acts

2207.8 Internal reporting

2207.9 External reporting

2207.10 Other considerations

2207.2 Irregularities and Illegal Acts

2207.2.1	Irregularities and illegal acts can directly impact an enterprise in many negative ways, affecting finances and reputation, and indirectly affecting productivity and the retention of employees. It is important that enterprises have awareness, prevention and detection mechanisms in place to identify irregularities and illegal acts quickly. Irregularities and illegal acts are more likely to occur if there are nonexistent, poorly designed or malfunctioning controls.
2207.2.2	Irregularities and illegal acts can be committed by an employee at any level within the enterprise. They include activities such as, but not limited to: ● Fraud, which is any act involving the use of deception to obtain illegal advantage ● Deliberate misrepresentation of facts with the aim of gaining advantage or hiding irregularities or illegal acts ● Acts that involve noncompliance with laws and regulations, including failure to ensure that IT systems or processes meet applicable laws and regulations ● Unauthorized disclosure of data subject to privacy laws ● Data retention practices that violate applicable privacy laws and regulations ● Acts that involve noncompliance with enterprise agreements and contracts entered with third parties, such as banks, suppliers, vendors, service providers and stakeholders ● Manipulation, falsification, forgery or alteration of records or documents, whether in electronic or paper form ● Suppression or omission of the effects of transactions from records or documents, whether in electronic or paper form ● Inappropriate or deliberate leakage of confidential information ● Recording transactions (whether in electronic or paper form) that lack substance and are known to be false—e.g., false disbursements, payroll fraud, tax evasion ● Misappropriation and misuse of assets ● Skimming or defalcation, which is the misappropriation of cash before it is recorded in the financial records of an enterprise ● Acts that violate intellectual property (IP) rights, such as copyrights, trademarks and patents, whether intentional or unintentional ● Granting unauthorized access to information and systems ● Errors in financial or other records that arise due to unauthorized access to data and systems
2207.2.3	The determination of whether a particular act is illegal generally is based on the advice of an informed legal professional or may have to await final determination by a court of law. Practitioners should be concerned primarily with the effect or potential effect of the irregular action, irrespective of whether the act is suspected or proved to be illegal.
2207.2.4	Not all irregularities should be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the respective jurisdiction. Fraudulent irregularities include but are not limited to: ● Deliberate circumvention of controls with the intent to conceal the perpetuation of fraud ● Unauthorized use of assets or services ● Abetting or helping to conceal these types of activities Nonfraudulent irregularities may include: ● Gross negligence ● Unintentional illegal acts

2207.2.5	There may be instances in which a practitioner experiences retaliation or intimidation after reporting potential illegal acts or fraud. Taking into consideration the parties involved, the chief audit executive (or VP/director of audit), executive management, and those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee) should collaborate with legal counsel to address the matter. Their efforts should include actions that will resolve issues related to the threats or intimidation and may include coordination with local law enforcement agencies.

2207.3 Responsibilities of Management

2207.3.1	It is primarily the responsibility of management and the board to provide controls to deter, prevent and detect irregularities and illegal acts.
2207.3.2	Management typically uses the following means to obtain reasonable assurance that irregularities and illegal acts are deterred, prevented or detected in a timely manner: ● Designing, implementing and maintaining internal control systems—including transaction review and approval, and management review procedures—to prevent and detect irregularities or illegal acts. ● Policies and procedures governing employee conduct ● Compliance validation and monitoring procedures ● Designing, implementing and maintaining suitable systems for reporting, recording and managing incidents relating to irregularities or illegal acts ● Policies and procedures governing compliance and regulatory requirements
2207.3.3	Management should disclose to practitioners its knowledge of any irregularities or illegal acts, the areas affected, and any action taken, whether such acts are alleged, suspected or proved.
2207.3.4	If an act of an irregular or illegal nature is alleged, suspected or detected, management should aid the process of investigation and inquiry.

2207.4 Responsibilities of Practitioners

2207.4.1	Practitioners should consider defining in the audit charter the responsibilities of management and the responsibilities of IT audit and assurance management with respect to preventing, detecting and reporting irregularities so that these are clearly understood for all audit work. Where these responsibilities are documented in enterprise policy or a similar document, the audit charter should include a statement to that effect.
2207.4.2	Practitioners should understand that control mechanisms cannot completely eliminate the possibility of irregularities or illegal acts occurring. Practitioners are responsible for assessing the risk of irregularities or illegal acts, evaluating the impact of identified irregularities, and designing and performing tests that are appropriate for the nature of the audit assignment.
2207.4.3	Practitioners are not responsible for the prevention or detection of irregularities or illegal acts. An audit engagement cannot guarantee that irregularities will be detected. Even if an audit is planned and performed appropriately, irregularities can go undetected, for instance, if there is collusion between employees or collusion between employees and outsiders, or if management is involved in the irregularities. The aim is to determine that the control is in place, adequate, effective and complied with.
2207.4.4	Practitioners who have specific information about the existence of an irregularity or illegal act have an obligation to report it.
2207.4.5	Practitioners should inform management and those charged with governance if they have identified situations in which there is a higher level of risk for a potential irregularity or illegal act, even if none is detected.
2207.4.6	Practitioners should be reasonably familiar with the area under review to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.

2207.5 Irregularities and Illegal Acts During Engagement Planning

2207.5.1	Practitioners should assess the risk of occurrence of irregularities or illegal acts connected with the area under audit following the use of the appropriate methodology. In preparing this assessment, practitioners should consider factors including: ● Organizational characteristics, such as corporate ethics, organizational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures, and enterprise direction ● History of the enterprise, past occurrences of irregularities, and the activities subsequently taken to mitigate or minimize the findings related to irregularities ● Recent changes in management, operations or IT systems, and the current strategic direction of the enterprise ● Impacts resulting from new strategic partnerships ● Types of assets held or services offered, and their susceptibility to irregularities ● Evaluation of the strength of relevant controls and vulnerabilities that could allow established controls to be circumvented or bypassed ● Applicable regulatory or legal requirements ● Internal policies such as a whistle-blower policy, an insider trading policy, and employee and management codes of ethics ● Stakeholder relations and financial markets ● Human resources capabilities ● Confidentiality and integrity of market-critical information ● Findings from previous audits ● The industry and the competitive environment in which the enterprise operates ● Findings of reviews conducted outside the scope of the audit, such as findings from consultants, quality assurance teams or specific management investigations ● Findings from the day-to-day conduct of business ● Existence of process documentation and/or a quality management system ● Technical sophistication and complexity of the information systems supporting the area under audit ● Existence of in-house developed/maintained application systems for core business systems compared with packaged software ● Effects of employee dissatisfaction ● Potential layoffs, outsourcing, divestiture or restructuring ● Existence of assets that are easily susceptible to misappropriation ● Poor organizational financial and/or operational performance ● Management's attitude with regard to ethics ● Irregularities and illegal acts that are common to a particular industry or have occurred in similar enterprises

2207.5.2	As part of the planning process and performance of the risk assessment, practitioners should inquire of management, and obtain written representations if appropriate, about the following: ● Management's understanding regarding the level of risk of irregularities and illegal acts in the enterprise ● Whether management has knowledge of irregularities and illegal acts that have or could have occurred within the enterprise, or may have been directed toward it ● Management's responsibility for designing and implementing internal controls to prevent irregularities and illegal acts ● How the risk of irregularities or illegal acts is monitored or managed ● What processes are in place to communicate alleged, suspected or existent irregularities or illegal acts to appropriate stakeholders ● Applicable national and regional laws in the jurisdiction in which the organization operates, and the extent of the legal department's coordination has with the risk committee and/or audit committee

2207.6 Designing and Reviewing Engagement Procedures

2207.6.1	Practitioners have no explicit responsibility to detect or prevent illegal acts or irregularities, but they should design procedures for the audit engagement that take into account irregularities and illegal acts that have been identified.
2207.6.2	Practitioners should use the results of the risk assessment to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence of reasonable assurance that the following are identified: ● Irregularities that could have a significant effect on the area under audit or on the enterprise as a whole ● Control weaknesses that would result in failure to prevent or detect material irregularities ● All significant deficiencies in the design or operation of internal controls that could potentially affect the issuer's ability to record, process, summarize and report business data
2207.6.3	Practitioners should review the results of engagement procedures for indications that irregularities or illegal acts may have occurred. Using computer-assisted audit techniques (CAATs) could aid significantly in the effective and efficient detection of irregularities or illegal acts.

2207.6.4	When evaluating results of engagement procedures, risk factors identified should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risk has been addressed.

2207.7 Responding to Irregularities and Illegal Acts

2207.7.1	During an audit engagement, indications of the existence of irregularities or illegal acts may come to the attention of practitioners. They should consider the potential effect of the irregularities or illegal acts on the subject matter of the engagement, the audit objectives, the audit engagement report and the enterprise.
2207.7.2	Practitioners should demonstrate an attitude of professional skepticism. Indicators (sometimes called "fraud" or "red flags") of persons committing irregularities or illegal acts include: ● Overrides of controls by management ● Irregular or poorly explained management behavior ● Consistent overperformance, compared to set targets ● Problems with, or delays in, receiving requested information or evidence ● Transactions not following the normal approval cycles ● Increase in activity of a certain customer ● Increase in complaints from customers ● Deviating access controls for some applications or users Practitioners should pay close attention if they notice any of these indicators.
2207.7.3	If practitioners become aware of information concerning a possible irregularity or illegal act, they should consider taking the following steps after receiving direction from the appropriate legal authority: ● Obtain an understanding of the nature of the act ● Understand the circumstances in which the act occurred ● Gather evidence of the act (e.g., letters, system records, computer files, security logs, and customer or vendor information) ● Identify all persons involved in committing the act ● Obtain sufficient supportive information to evaluate the effect of the act ● Perform limited additional procedures to determine the effect of the act and whether additional acts exist ● Document and preserve all evidence and work performed
2207.7.4	After taking appropriate steps related to a possible irregularity or illegal act, practitioners should consult with audit management to determine next actions, such as reporting the "event" to enterprise management, passing further action to internal fraud investigators, and/or reporting to law enforcement or regulators
2207.7.5	When an irregularity involves a member of management, practitioners should reconsider the reliability of representations made by management. Practitioners should work with an appropriate level of management, typically the level of management above the one associated with the irregularity or illegal act.

2207.8 Internal Reporting

2207.8.1	Practitioners should communicate the detection of irregularities and illegal acts to the appropriate people in the enterprise in writing or orally and in a timely manner. The notification should be directed to management at a higher level than the level at which the irregularities and illegal acts are suspected to have occurred. In addition, irregularities and illegal acts should be reported to those charged with enterprise governance, such as the board of directors, trustees, audit committee or equivalent body. Matters that are clearly insignificant in terms of both financial effect and indications of control weaknesses may not require reporting to a higher level. If practitioners suspect that all levels of management are involved, then the findings should be confidentially reported directly to those charged with enterprise governance, such as the board of directors, trustees, audit committee or equivalent body, according to the local applicable laws and regulations. Local laws and regulations may prohibit reporting to parties other than the prescribed legal authority.
2207.8.2	Practitioners should use professional judgment when reporting an irregularity or illegal act. They should discuss the findings and the nature, timing and extent of any further procedures to be performed with an appropriate level of management at least one level above the level of the individuals who appear to be involved. In these circumstances, it is particularly important that practitioners maintain their independence.
2207.8.3	Practitioners should carefully consider which individuals to include in the internal distribution of reports of irregularities or illegal acts. Identification of the occurrence and effects of irregularities or illegal acts is a sensitive issue, and report distribution carries risks, including: ● Further abuse of the control weaknesses as a result of publishing details of them ● Loss of customers, suppliers and investors when disclosure (authorized or unauthorized) occurs outside the enterprise ● Loss of key staff and management, including those not involved in the irregularity or illegal act, due to decreased confidence in management and the future of the enterprise
2207.8.4	Practitioners should consider reporting the irregularity or illegal act separately from any other audit issues as a way to control the distribution of the report.
2207.8.5	Practitioners should avoid alerting any person who may be implicated or involved in the irregularity or illegal act, to reduce the potential for those individuals to destroy or suppress evidence.
2207.8.6	The audit charter should define practitioners' responsibilities with regard to reporting irregularities or illegal acts.

2207.9 External Reporting

2207.9.1	External reporting of fraud, irregularities or illegal acts may be a legal or regulatory obligation. The obligation may apply to enterprise management, to the individuals involved in detecting the irregularities or to both. Legal reporting requirements for the auditor are subject to local jurisdiction and supersede internal policy and/or contractual agreements. Additional situations that may require external reporting include: ● Compliance with legal or regulatory requirements ● Court order ● Involvement of funding agency or government agency, in accordance with requirements for the audits of entities that receive governmental financial assistance ● External auditor requests
2207.9.2	If external reporting is required, the form and content of the information reported should be approved by the appropriate level of IT audit and assurance management and reviewed with auditee executive management prior to external release, unless prohibited by applicable regulations or specific circumstances of the audit engagement. Examples of specific circumstances that may prevent obtaining auditee executive management's agreement include: ● Auditee executive management's active involvement in the irregularity or illegal act ● Auditee executive management's passive acquiescence to the irregularity or illegal act
2207.9.3	If auditee executive management does not agree to the external release of the report, and if external reporting is a statutory or a regulatory obligation, then practitioners should consider consulting the audit committee and legal counsel about the advisability and risk of reporting the findings outside the enterprise. Even in situations in which practitioners are protected by attorney-client privilege, they should seek external legal advice and counsel prior to making external disclosure to confirm that they are in fact protected by attorney-client privilege.
2207.9.4	With the approval of IT audit and assurance management, practitioners should report irregularities or illegal acts to appropriate regulators on a timely basis. If the enterprise fails to disclose a known irregularity or illegal act or requires practitioners to suppress these findings, practitioners should seek legal advice and counsel.
2207.9.5	If practitioners detect an irregularity or illegal act, they should inform the external auditors in a timely manner.
2207.9.6	If practitioners are aware that management is required to report fraudulent activities to an outside organization, practitioners should formally advise management of its responsibility.

2207.10 Other Considerations

2207.10.1	IT audit and assurance practitioners should: ● Reduce audit risk to an acceptable level in planning and performing the engagement by: ■ Being aware that material errors, control deficiencies, or misstatements due to irregularities and illegal acts could exist, irrespective of evaluation of the risk of irregularities and illegal acts ■ Gaining an understanding of the enterprise and its environment, including internal controls that are relevant to the engagement subject matter, scope and objectives and are intended to prevent or detect irregularities and illegal acts ■ Obtaining sufficient and appropriate evidence to determine whether management or others within the enterprise have knowledge of any actual, suspected or alleged irregularities and illegal acts ● Consider unusual or unexpected relationships that may indicate a risk of material errors, control deficiencies or misstatements due to irregularities and illegal acts. ● Design and perform procedures to test the appropriateness of internal controls and the risk that management could override controls intended to prevent or detect irregularities and illegal acts. ● Assess whether identified errors, control deficiencies or misstatements may indicate an irregularity or illegal act. If there is such an indication, consider the implications relative to other aspects of the engagement and, in particular, the representations of management. ● Obtain written representations from management at least annually or more often, depending on the engagement, in order to acknowledge management's responsibility for the design and implementation of internal controls to prevent and detect irregularities and illegal acts. ● Disclose the pertinent results of any risk assessment that indicates errors, control deficiencies or misstatements that may exist as a result of an irregularity or illegal act. ● Disclose management's knowledge of irregularities and illegal acts affecting the enterprise in relation to management and employees who have significant roles in internal control. ● Disclose management's knowledge of any alleged or suspected irregularities and illegal acts affecting the enterprise as communicated by employees, former employees, regulators and others. ● Communicate in a timely manner to: ■ The appropriate level of management, any information identified or obtained that a material irregularity or illegal act may exist. ■ Those charged with governance, any material irregularity and illegal acts involving management or employees who have significant roles in internal control. ■ Those charged with governance, any material weakness in the design and implementation of internal controls intended to prevent and detect any irregularities and illegal acts that are identified during the engagement, even if they are outside of scope. ■ Consider the legal and professional reporting requirements applicable in the circumstances. ■ Consider withdrawing from the engagement if material errors, control deficiencies, misstatements or illegal acts affect the continued effectiveness of the engagement. ■ Document all communications, planning, results, evaluations and conclusions relating to material irregularities and illegal acts that have been reported to management, those charged with governance, regulators and others.

Linkages to COBIT® 2019 for Standard 1207 and Guidelines 2207

COBIT 2019 Governance and Management Objectives	Purpose
EDM03 Ensured Risk Optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
APO12 Managed Risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

REPORTING STANDARDS

Reporting Standard 1401: Reporting

Statements	**1401.1** IT audit and assurance practitioners shall provide a report to communicate the results of each engagement.
	1401.2 IT audit and assurance practitioners shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.

Reporting Guidelines 2401: Reporting

2401.1 Introduction This guideline details all aspects that should be included in an audit engagement report and provides IT audit and assurance practitioners with considerations to make when drafting and finalizing an audit engagement report. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2401.2 Required contents of the audit engagement report

2401.3 Subsequent events

2401.4 Additional communication

2401.5 Other considerations

2401.2 Required Contents of the Audit Engagement Report

2401.2.1	The audit report should include a statement that the audit engagement has been conducted in accordance with ISACA's IT audit and assurance standards or other applicable professional standards: any noncompliance with these standards should be explicitly mentioned in the report. The scope of the audit engagement should also be included in the audit report. The scope includes identification or description of the audit subject or activity, the period under review and the period when the audit was performed, the nature and extent of the work performed, and any qualifications or limitations in scope.
2401.2.2	The audit report should include a summary of the work performed, which will help the intended users of the report to better understand the nature of the assurance provided.
2401.2.3	The audit report should include a section with the opinion of the auditor. In developing an audit report, practitioners should consider all relevant evidence, regardless of whether it appears to corroborate or contradict the subject matter information. Opinions should be supported by results of the control procedures based on identified criteria. Practitioners should conclude whether sufficient and appropriate evidence has been obtained to support the conclusions in the audit engagement report. The report should express an opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective.

2401.2.4	The audit report should include a statement identifying the source of management's representation about the effectiveness of control procedures. Also, it should note that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management.
2401.2.5	The audit report should include identification of the audit objectives.
2401.2.6	The audit report should include a description of the criteria or disclosure of the source of the criteria. Furthermore, practitioners should consider disclosing: ● Any significant interpretations made in applying the criteria ● Measurement methods used when criteria allow a choice among a number of measurement methods ● Changes in the standard measurement methods used
2401.2.7	The audit report should include intended recipients and any restrictions on circulation.
2401.2.8	The audit report should include signatures and locations of the individuals or entities responsible for the report.
2401.2.9	The audit report should include the date of issuance of the audit engagement report. In most instances, the date of the report is the issue date. It is recommended that the report mention the dates when the audit work was performed, if not noted in the summary of the work performed.
2401.2.10	The audit report should mention that distribution (i.e., intended recipients and any restrictions on circulation) is in accordance with the terms of the audit charter or engagement letter. In some regions, IT audit and assurance practitioners may be required to disclose their credentials (e.g., certificate number and/or membership number from ISACA or other professional organizations).
2401.2.11	The audit report should include observations, findings, conclusions and recommendations with remediation costs, if determinable. Findings, conclusions and recommendations for corrective action should include management's response. For each management response, practitioners should obtain information on the proposed actions to implement or address reported recommendations and the planned implementation or action date. If practitioners and the auditee disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the differences. The auditee's written comments may be included as an appendix to the audit report, in the body of the report or in a cover letter. Executive management or those charged with governance of the IT audit and assurance function should decide which point of view it supports.

2401.3 Subsequent Events

2401.3.1	Events that have a significant impact on the audit subject or activity sometimes occur subsequent to testing but prior to the audit report issuance date. Such occurrences, referred to as subsequent events, may require disclosure because they may change an assertion or a conclusion. In performing an audit engagement, practitioners should consider information about subsequent events that comes to their attention. However, practitioners have no responsibility to detect subsequent events.
2401.3.2	Practitioners should obtain written representation from management that no subsequent events have occurred.

2401.4 Additional Communication

2401.4.1	Practitioners should discuss the draft report contents with management in the subject area prior to finalization and release, and include management's response to findings, conclusions and recommendations in the final report.
2401.4.2	Practitioners should communicate significant deficiencies and weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. They should also explicitly disclose in the report that the deficiencies and weaknesses have been communicated.
2401.4.3	Practitioners should communicate to management any internal control deficiencies that are less than significant but more than inconsequential. In such cases, practitioners should notify those charged with governance or the responsible authority that such internal control deficiencies have been communicated to management.
2401.4.4	Practitioners should obtain written representations from management acknowledging, at a minimum, the following assertions: ● Management is responsible for establishing and maintaining proper and effective internal controls, including systems of internal accounting and administrative controls over operating activities and information systems under review, and activities to identify all laws, rules and regulations that govern the subject area under review, and for ensuring compliance with them. ● All requested information relevant to the engagement objectives was provided to the engagement team, including but not limited to: ■ Records, related data, electronic files and reports ■ Policies and procedures ■ Pertinent personnel ■ Results of relevant internal and external IT audits, reviews and assessments ■ Management is responsible to report any subsequent events. ■ Management has no knowledge of any fraud or suspected fraud, irregularities, and illegal acts related to the subject area under review, including management and employees with responsibility for internal control not already disclosed. ■ Management has no knowledge of any allegations of fraud or suspected fraud, irregularities, and illegal acts affecting the area under review received in communications from employees, clients, contractors or others not already disclosed. ■ Management acknowledges responsibility for the design and implementation of programs and controls to prevent and detect fraud, irregularities and illegal acts.

2401.5 Other Considerations

2401.5.1	IT audit and assurance practitioners should: ● Obtain relevant written representations from the auditee that clearly detail critical areas of the engagement, issues that have arisen and their resolution, and assertions made by the auditee. ● Determine that auditee representations have been signed and dated by the auditee to indicate acknowledgment of auditee responsibilities with respect to the engagement. ● Obtain and document oral representations in the work papers if written representations cannot be obtained from responsible auditee management. ● Document and retain in the work papers any representations, either written or oral, received during the course of conducting the engagement. For attestation engagements, representations from the auditee should be obtained in writing to reduce possible misunderstanding. ● Describe material or significant weaknesses and their effect on the achievement of the engagement objectives in the report. ● Discuss the draft report contents with management in the subject area prior to finalization and release, and include management's response to findings, conclusions and recommendations in the final report, where applicable. ● Discuss significant deficiencies and weaknesses with management prior to communication with those charged with governance and, where applicable, to the responsible authority. Disclose in the report that significant deficiencies and weaknesses have been communicated. ● Reference any separate reports in the final report. ● Communicate to auditee management internal control deficiencies that are less than significant but more than inconsequential. In such cases, those charged with governance of the audit function or the responsible authority should be notified that such internal control deficiencies have been communicated to auditee management. ● Identify standards applied in conducting the engagement. Communicate any noncompliance with standards, as applicable.

Linkages to COBIT® 2019 for Standard 1401 and Guidelines 2401

COBIT 2019 Governance and Management Objectives	Purpose
EDM05 Ensured Stakeholder Engagement	Ensure that stakeholders are supportive of the I&T strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.
MEA01 Managed Performance and Conformance Monitoring	Provide transparency of performance and conformance and drive achievement of goals.
MEA02 Managed System of Internal Control	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.

MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Reporting Standard 1402: Follow-up Activities

Statements	**1402.1** IT audit and assurance practitioners shall monitor and periodically report to those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee) management's progress on findings and recommendations. The reporting should include a conclusion on whether management has planned and taken appropriate, timely action to address reported audit findings and recommendations.
	1402.2 Progress on the overall status of the implementation of audit findings should be regularly reported to the audit committee, if one is in place.
	1402.3 Where it is determined that the risk related to a finding has been accepted and is greater than the enterprise's risk appetite, this risk acceptance should be discussed with senior management. The acceptance of the risk (particularly failure to resolve the risk) should be brought to the attention of the audit committee (if one is in place) and/or the board of directors.

Reporting Guidelines 2402: Follow-up Activities

2402.1 Introduction The purpose of this guideline is to provide guidance on monitoring whether management has taken appropriate and timely action on reported recommendations and audit findings. The guideline content section is structured to provide information on the following key audit and assurance engagement topics:

2402.2 Follow-up process

2402.3 Management's proposed actions

2402.4 Assuming the risk of not taking corrective action

2402.5 Follow-up procedures

2402.6 Timing and scheduling of follow-up activities

2402.7 Nature and extent of follow-up activities

2402.8 Deferring follow-up activities

2402.9 Form of follow-up responses

2402.10 Follow-up by practitioners on external audit recommendations

2402.11 Reporting of follow-up activities

2402.2 Follow-up Process

2402.2.1	Follow-up activity is a process through which practitioners determine the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others.
2402.2.2	A follow-up process should be established to help provide reasonable assurance that each review conducted by practitioners provides optimal benefit to the enterprise by requiring that agreed-on outcomes arising from reviews are implemented in accordance with management undertakings, or that executive management recognizes and acknowledges the risk of delaying or not implementing proposed outcomes and/or recommendations.

2402.3 Management's Proposed Actions

2402.3.1	As part of their discussions with the auditee, practitioners should obtain agreement on the results of the audit engagement and on a plan of action to improve operations, as needed.
2402.3.2	Practitioners should discuss with management the proposed actions to implement or address reported recommendations and audit comments. Proposed actions should be provided to practitioners and should be recorded as a management response in the final report with a committed implementation and/or action date.
2402.3.3	If practitioners and the auditee come to an agreement on the proposed actions, practitioners should initiate the procedures for follow-up activities.

2402.4 Assuming the Risk of Not Taking Corrective Action

2402.4.1	Management may decide to accept the risk of not correcting a reported condition because of cost, complexity of the corrective action or other considerations. The board of directors, or those charged with governance, should be informed of recommendations for which management accepts the risk of not correcting the reported situation. Acceptance of risk should be documented and formally approved by executive management and communicated to those charged with governance.
2402.4.2	If practitioners believe that the auditee has accepted a level of residual risk that is inappropriate for the enterprise, they should discuss the matter with IT audit and assurance management and executive management. If practitioners remain in disagreement with the decision regarding residual risk, they, along with executive management, should report the matter to the board, or those charged with governance, for resolution.

2402.5 Follow-up Procedures

2402.5.1	Procedures for follow-up activities should be established, including: ● The recording of a time frame within which management should respond to agreed-on recommendations ● An evaluation of management's response ● A verification of the response, if appropriate ● Follow-up work, if appropriate ● A communication procedure that escalates outstanding and unsatisfactory responses and/or actions to the appropriate levels of management and to those charged with governance ● A process for obtaining management's assumption of associated risk, in the event that corrective action is delayed or not proposed to be implemented
2402.5.2	An automated tracking system or database can assist in carrying out follow-up activities.
2402.5.3	Factors that should be considered in determining appropriate follow-up procedures include: ● The importance and impact of the findings and recommendations on the IT environment or IT application at issue ● Any changes in the IT environment that may affect the importance and impact of the findings and recommendations ● The complexity of correcting the reported situation ● The time, cost and effort needed to correct the reported situation ● The effect if correcting the reported situation should fail
2402.5.4	Responsibility for follow-up actions, reporting and escalation should be defined in the audit charter.

2402.6 Timing and Scheduling of Follow-up Activities

2402.6.1	Decisions on the timing of follow-up activities should take into account the significance of the reported findings and the effect on enterprise strategy and objectives if corrective actions are not taken. The timing of follow-up activities in relation to the original reporting is a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risk and costs to the enterprise.
2402.6.2	Because they are an integral part of the IT audit process, follow-up activities should be scheduled, along with the other steps necessary to perform each review. Specific follow-up activities and the timing of such activities may be influenced by the degree of difficulty, the risk and exposure involved, the results of the review, the time needed for implementing corrective actions, and other factors, and may be established in consultation with management.
2402.6.3	Practitioners should follow up on agreed-on outcomes relating to high-risk issues soon after the due date for action, and may monitor them progressively.
2402.6.4	The implementation of all management responses to different audit engagements may be followed up on a regular basis (e.g., each quarter) together, even though the implementation dates committed to by management may be different. Another approach is to follow up on individual management responses according to the due date agreed on with management.

2402.7 Nature and Extent of Follow-up Activities

2402.7.1	The auditee typically is given a time frame within which to provide details of actions taken to implement recommendations.
2402.7.2	Management's response detailing the actions taken should be evaluated, if possible, by the practitioners who performed the original review. Wherever possible, audit evidence of actions taken should be obtained.
2402.7.3	If management provides information on actions taken to implement recommendations and practitioners have doubts about the information provided or the effectiveness of the actions taken, appropriate testing or other audit procedures should be undertaken to confirm the true position or status prior to concluding further follow-up activities.
2402.7.4	As part of the follow-up activities, practitioners should evaluate whether unimplemented recommendations are still relevant or have a greater significance. Practitioners may decide that the implementation of a particular recommendation is no longer appropriate. This could occur if application systems have changed, if compensating controls have been implemented, or if business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk. Similarly, a change in the IT environment may increase the significance of the effect of a previous observation and the need for its resolution.
2402.7.5	A follow-up engagement may have to be scheduled to verify the implementation of critical and/or important actions.
2402.7.6	Practitioners' opinions on unsatisfactory management responses or actions should be communicated to the appropriate level of management.

2402.8 Deferring Follow-up Activities

2402.8.1	Practitioners are responsible for scheduling follow-up activities as part of developing engagement work schedules. The scheduling of follow-ups should be based on the risk and exposure involved and on the degree of difficulty and time needed to implement corrective actions.
2402.8.2	There may be instances in which practitioners judge that management's oral or written response shows that action already taken is sufficient when weighed against the relative importance of the engagement observation or recommendation. On such occasions, actual follow-up verification activities may be performed as part of the next engagement that deals with the relevant system or issue.

2402.9 Form of Follow-up Responses

2402.9.1	The most effective way to receive follow-up responses from management is in writing because a written response helps to reinforce and confirm management's responsibility for follow-up action and progress achieved. Also, written responses ensure an accurate record of actions, responsibilities and current status. Oral responses may be received and recorded by practitioners and, if possible, approved by management. Proof of action or implementation of recommendations may be provided with the response.
2402.9.2	Practitioners should request and/or receive periodic updates from management responsible for implementing agreed-on actions to evaluate the progress management has made, particularly in relation to high-risk issues and corrective actions with long lead times.

2402.10 Follow-up by Practitioners on External Audit Recommendations

2402.10.1	Depending on the scope and terms of the audit engagement and in accordance with the relevant IT auditing standards, external practitioners may rely on internal practitioners to follow-up on their agreed-on recommendations. Responsibilities regarding follow-up can be determined in the audit charter or engagement letters.

2402.11 Reporting of Follow-up Activities

2402.11.1	A report on the status of agreed-on corrective actions arising from audit engagement reports, including agreed-on recommendations not implemented, should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).
2402.11.2	If, during a subsequent audit engagement, practitioners find that corrective action that management reported as "implemented" in fact has not been implemented, the practitioners should communicate the status to the appropriate level of management and those charged with governance. If appropriate, the practitioners should obtain a current corrective action plan and planned implementation date.
2402.11.3	When all the agreed-on corrective actions have been implemented, a report detailing all the implemented and/or completed actions can be forwarded to executive management and those charged with governance.

Linkages to COBIT® 2019 for Standard 1402 and Guidelines 2402

COBIT 2019 Governance and Management Objectives	Purpose
EDM01 Ensured Governance Framework Setting and Maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02 Ensured Benefits Delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 Ensured Risk Optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
MEA03 Managed Compliance With External Requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04 Managed Assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

Page intentionally left blank

APPENDIX A: Related Standards and Guideline per Standard

Standard	Related Standards	Related Guidelines
1001 Audit Charter	No standard related to Standard 1001	• Guideline 2001 Audit Charter
1002 Organizational Independence	No standard related to Standard 1002	• Guideline 2002 Organizational Independence
1003 Auditor Objectivity	No standard related to Standard 1003	• Guideline 2003 Audit Objectivity
1004 Reasonable Expectation	No standard related to Standard 1004	• Guideline 2004 Reasonable Expectation
1005 Due Professional Care	No standard related to Standard 1005	• Guideline 2005 Due Professional Care
1006 Proficiency	No standard related to Standard 1006	• Guideline 2006 Proficiency
1007 Assertions	No standard related to Standard 1007	• Guideline 2007 Assertions
1008 Criteria	No standard related to Standard 1008	• Guideline 2008 Criteria
1201 Risk Assessment in Planning	No standard related to Standard 1201	• Guideline 2201 Risk Assessment in Planning
1202 Audit Scheduling	No standard related to Standard 1202	• Guideline 2202 Audit Scheduling
1203 Engagement Planning	No standard related to Standard 1203	• Guideline 2203 Engagement Planning
1204 Performance and Supervision	• Standard 1005 Due Professional Care • Standard 1205 Evidence • Standard 1401 Reporting	• Guideline 2204 Performance and Supervision • Guideline 2201 Risk Assessment in Planning
1205 Evidence	No standard related to Standard 1205	• Guideline 2205 Evidence
1206 Using the Work of Other Experts	No standard related to Standard 1206	• Guideline 2206 Using the Work of Other Experts

Standard	Related Standards	Related Guidelines
1207 Irregularities and Illegal Acts	• Standard 1008 Criteria • Standard 1201 Risk Assessment in Planning • Standard 1205 Evidence	• Guideline 2206 Using the Work of Other Experts • Guideline 2207 Irregularities and Illegal Acts
1401 Reporting	No standard related to Standard 1401	• Guideline 2401 Reporting
1402 Follow-up Activities	No standard related to Standard 1402	• Guideline 2402 Follow-up Activities

Appendix B: Related Standards per Guideline

Guideline	Related Standards
2001 Audit Charter	• 1001 Audit Charter • 1002 Organizational Independence • 1003 Auditor Objectivity
2002 Organizational Independence	• 1001 Audit Charter • 1002 Organizational Independence • 1003 Auditor Objectivity • 1004 Reasonable Expectation • 1006 Proficiency
2003 Audit or Objectivity	• 1001 Audit Charter • 1002 Organizational Independence • 1003 Auditor Objectivity • 1005 Due Professional Care
2004 Reasonable Expectation	• 1001 Audit Charter • 1004 Reasonable Expectation
2005 Due Professional Care	• 1002 Organizational Independence • 1003 Auditor Objectivity • 1005 Due Professional Care • 1006 Proficiency • 1205 Evidence
2006 Proficiency	• 1005 Due Professional Care • 1006 Proficiency • 1203 Engagement Planning • 1204 Performance and Supervision
2007 Assertions	• 1007 Assertions • 1008 Criteria • 1206 Using the Work of Other Experts • 1401 Reporting
2008 Criteria	• 1007 Assertions • 1008 Criteria
2201 Risk Assessment in Planning	• 1201 Risk Assessment in Planning • 1203 Engagement Planning • 1204 Performance and Supervision • 1207 Irregularities and Illegal Acts
2202 Audit Scheduling	• 1201 Risk Assessment in Planning • 1203 Engagement Planning • 1204 Performance and Supervision • 1207 Irregularities and Illegal Acts
2203 Engagement Planning	• 1201 Risk Assessment in Planning • 1203 Engagement Planning • 1204 Performance and Supervision
2204 Performance and Supervision	• 1005 Due Professional Care • 1006 Proficiency • 1203 Engagement Planning • 1204 Performance and Supervision • 1205 Evidence • 1401 Reporting

Page intentionally left blank

Appendix C: Terms and Definitions

A

Appropriate evidence—The measure of the quality of the evidence

Assertion—Any formal declaration or set of declarations about the subject matter made by management.

Scope Notes: Assertions should usually be in writing and commonly contain a list of specific attributes about the subject matter or about a process involving the subject matter.

Assurance engagement—An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise.

Scope Notes: Examples may include financial, performance, compliance and system security engagements

Attestation—An engagement in which an IT auditor is engaged to either examine management's assertion regarding a particular subject matter or the subject matter directly.

Audit charter—A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity.

Scope Notes: The charter should:
- Establish the internal audit function's position within the enterprise
- Authorize access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements
- Define the scope of audit function's activities

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

Audit plan—1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.

Scope Notes: Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work.

2. A high-level description of the audit work to be performed in a certain period of time.

Audit program—A step-by-step set of audit procedures and instructions that should be performed to complete an audit.

Audit risk—The risk of reaching an incorrect conclusion based upon audit findings.

Scope Notes: The three components of audit risk are:
- Control risk
- Detection risk
- Inherent risk

Auditor's opinion—A formal statement expressed by the IS audit or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether or not the findings support that the audit criteria have been met.

Scope Notes: The types of opinions are:
- **Unqualified opinion**—Notes no exceptions or none of the exceptions noted aggregate to a significant deficiency
- **Qualified opinion**—Notes exceptions aggregated to a significant deficiency (but not a material weakness)
- **Adverse opinion**—Notes one or more significant deficiencies aggregating to a material weakness

C

Control risk—The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls (See Inherent risk).

Criteria—The standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.

Scope Notes: Criteria should be:
- **Objective**—free from bias
- **Measurable**—provide for consistent measurement
- **Complete**—include all relevant factors to reach a conclusion
- **Relevant**—relate to 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.

D

Design effectiveness—If the company's controls are operated as prescribed by persons possessing the necessary authority and competence to perform the

control effectively, and if they satisfy the company's control objectives and can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements, they are considered to be designed effectively. See Public Company Accounting Oversight Board (PCAOB), Auditing Standard No. 2201, "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements," 15 November 2007, Section 42, *https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx*.

Detection risk—The risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors.

Scope Notes: See audit risk

F

Follow-up activity—Activity that determines whether management has taken appropriate corrective actions to resolve deficiencies.

I

Impairment—A condition that causes a weakness or diminished ability to execute audit objectives.

Scope Notes: Impairment to organizational independence and individual objectivity may include personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment, or facilities; and resource limitations (such as funding or staffing).

Independence—1. Self-governance. 2. The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels. Independence includes Independence of mind and Independence in appearance.

Inherent risk—The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

Integrity—The guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

Irregularity—Violation of an established management policy or regulatory requirement. It may consist of deliberate misstatements or omission of information concerning the area under audit or the enterprise as a whole, gross negligence or unintentional illegal acts.

M

Material weakness—A deficiency or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement will not be prevented or detected on a timely basis. Weakness in control is considered 'material' if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. A weakness classified as material implies that:

- Controls are not in place and/or controls are not in use and/or controls are inadequate
- Escalation is warranted

There is an inverse relationship between materiality and the level of audit risk acceptable to the IS audit or assurance professional, i.e., the higher the materiality level, the lower the acceptability of the audit risk, and vice versa.

Materiality—An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.

O

Objective in appearance—The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm, audit function or a member of the audit team's integrity, objectivity or professional skepticism has been compromised.

Objective of mind—The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

Objectivity—The ability to exercise judgment, express opinions and present recommendations with impartiality

Operating effectiveness—If a control is operating as designed and the person performing the control possesses the necessary authority and competence to perform the control effectively, the control is considered to be operating effectively. See Public Company Accounting Oversight Board (PCAOB), Auditing Standard No. 2201, "AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements," 15 November 2007, *https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx*.

Other expert—Internal or external to an enterprise, other expert could refer to:
- An IT auditor from an external firm
- A management consultant
- An expert in the area of the engagement who has been appointed by top management or by the team

P

Professional competence—Proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards.

Professional judgement—The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement

Professional skepticism—An attitude that includes a questioning mind and a critical assessment of audit evidence.

Scope Notes: Source: American Institute of Certified Public Accountants (AICPA) AU 230.07

R

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

Relevant information—Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information.

Scope Notes: Refer to COBIT 2019 information quality goals

Reliable information—Information that is accurate, verifiable and from an objective source.

Scope Notes: Refer to COBIT 2019 information quality goals

Representation—A signed or oral statement issued by management to professionals, where management declares that a current or future fact (e.g., process, system, procedure, policy) is or will be in a certain state, to the best of management's knowledge.

Residual risk—The remaining risk after management has implemented a risk response.

Risk assessment—A process used to identify and evaluate risk and its potential effects.

Scope Notes: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.

S

Significant deficiency—A deficiency or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight.

Scope Notes: A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesirable event(s) not being prevented or detected.

Subject matter—The specific information subject to an IS auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity).

Substantive testing—Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.

Sufficient evidence—The measure of the quantity of audit evidence; supports all material questions to the audit objective and scope. Scope Notes: See evidence

Sufficient information—Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable.

Scope Notes: Refer to COBIT 2019 information quality goals

Suitable information—Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame) information.

Scope Notes: Refer to COBIT 2019 information quality goals

T

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.

Scope Notes: A potential cause of an unwanted incident (ISO/IEC 13335)

Page intentionally left blank