audit and IT audits

SECURITY GOVERNANCE 2024-25

definition

traditionally, audit is a review of the financial statement of an organization

- financial statement: U.S. publicly-traded must provide regular financial statements to investors and public.
- (by law) required by the Securities and Exchange Commission (SEC)
- statements give investors a financial snapshot of a company's immediate past performance
- results are important to investors because they have an interest ($$) in how a company is performing
  - **certified** statements have been audited for accuracy by an independent accountant
  - **compiled** statements may provide investors with useful information, but they have not been audited

on audit

a financial audit is an objective examination and evaluation of the financial statements of an organization to make sure that the financial records are a fair and accurate representation of the transactions they claim to represent

it can be conducted internally by employees of the organization or externally by an outside certified public accountant (CPA) firm

- CPA is a designation provided to licensed accounting professionals
- CPA licenses are provided by the Board of Accountancy for each USA state

goals of audits

1. provide reasonable assurance that financial statements are free from material misstatement
2. assess the effectiveness of an organization's internal controls
   - internal controls are processes and procedures designed to prevent and detect errors, fraud, and non-compliance with laws and regulations
3. identify areas where an organization can improve its operations, efficiency, and effectiveness
4. ensure compliance with laws and regulations
5. establish procedures for monitoring
6. investigate suspected fraud or other wrongdoing
7. prepare an organization for sale or merger
8. meet the requirements of a government or other regulatory body

types of audit

there are many different types of audits, each with its own specific purpose and focus

MANY TYPES

the type of audit that is appropriate for a particular organization will depend on its size, industry, and risk profile

types of audit

- financial audits are conducted to assess the fairness and accuracy of financial statements
- operational audits are conducted to assess the efficiency and effectiveness of operations
- compliance audits are conducted to assess compliance with specific laws and regulations
- information system audits are conducted to assess the security and effectiveness of information systems
- internal audits assess the overall risk profile, identify and mitigate risks, and improve operational efficiency and effectiveness
- external audits are required for publicly traded companies and other organizations that are subject to government or regulatory oversight

other types of audits include

- forensic audits are conducted to investigate suspected fraud or other financial wrongdoing
- tax audits are conducted by the Internal Revenue Service to verify the accuracy of a taxpayer's tax return
- single audits are conducted to assess the compliance of organizations that receive federal grants
- employee benefit plan audits are conducted to assess the financial condition and compliance of employee benefit plans, such as pension plans and health insurance plans

auditors

type	conducted by
financial	independent CPAs
operational	internal auditors or external consultants
compliance	internal auditors, external auditors, or government agencies
information system	specialized auditors with expertise in information security
internal audits	organization's own internal audit department
external audits	independent third party, such as a CPA firm

IS and IT audits

IT audits are a part of IS audit

- modern information systems heavily use information technology

modern IS audits are mainly based on IT audits

- in fact, this depends on the use of paper material

IT audits are still audits, but today they are very specific and require expertise in IT, regulations, standards, best practices, etc.

standards for audits

- principles/procedures that auditors must follow when conducting an audit
- designed to ensure that audits are performed in a consistent and professional manner, and that their results are reliable and accurate
- two main types of auditing standards:
  - general standards : apply to all audits, regardless of the type of organization being audited. General auditing standards include requirements for the auditor's independence, professional competence, due care, and reporting obligations.
  - specific standards : apply to specific types of audits, such as audits of financial statements or audits of internal controls. Specific auditing standards provide more detailed guidance on how to perform audit procedures and evaluate audit results
- issued by a variety of organizations, including the following
  - International Auditing and Assurance Standards Board (IAASB): independent organization that sets international auditing standards, widely accepted around the world
  - Public Company Accounting Oversight Board (PCAOB): USA government-established organization that oversees the audits of public companies in the United States. Mandatory for all audits of public companies in the US
  - American Institute of Certified Public Accountants (AICPA): professional organization for certified public accountants (CPAs). It issues auditing standards for audits of non-public companies in the US
- auditors must comply with the applicable auditing standards
  - failures can result in disciplinary action against the auditor, and it can also undermine the credibility of the audit report

benefits of auditing standards

- Consistency
  - help to ensure that audits are performed in a consistent manner, regardless of the auditor or the organization being audited
  - improve the reliability and accuracy of audit results
- Credibility
  - standards are developed by independent organizations that have expertise in auditing
  - ensure that auditing standards are credible and that auditors are following best practices
- Public protection
  - help to protect the public by ensuring that the financial statements of publicly traded companies are accurate and reliable. This helps to prevent fraud and other financial irregularities

In addition to the auditing standards issued by the IAASB, PCAOB, and AICPA, there are also several other organizations that issue auditing standards or guidance. They include:

- Governmental auditing standards bodies. They issue standards for audits of government entities
- Professional accounting bodies. They issue standards for audits of non-public companies
- Industry-specific auditing standards bodies. They issue auditing standards for audits of entities in those industries

Auditors should be aware of the auditing standards that are applicable to their audit engagements and should comply with those standards

IT audit standard organizations

- Information Systems Audit and Control Association (ISACA)
  - professional organization for IT auditors and control professionals
  - issues the COBIT 5 framework and the ISACA IT Audit Framework (and others)
- Institute of Internal Auditors (IIA)
  - professional organization for internal auditors
  - issues a few standards and guidance on IT auditing, including the IIA Standards for the Professional Practice of Internal Auditing
- Information Technology Infrastructure Library (ITIL)
  - ITIL is a framework for managing IT services. ITIL includes a number of guidance on IT auditing, such as the ITIL Continual Service Improvement process

IT Audit Framework (ITAF™)

4th edition, 2020

5 chap[illegible]

introductory

2. IT Audit and Assurance Standards Statements
3. General Standards
4. Performance Standards
5. Reporting Standards

A - Related standards and guidelines for standards

B - Related standards per guideline

C - Terms and definitions

General Standards

- General Standard 1001: Audit Charter
- General Guidelines 2001: Audit Charter
- General Standard 1002: Organizational Independence
- General Guidelines 2002: Organizational Independence
- General Standard 1003: Auditor Objectivity
- General Guidelines 2003: Auditor Objectivity
- General Standard 1004: Reasonable Expectation
- General Guidelines 2004: Reasonable Expectation
- General Standard 1005: Due Professional Care
- General Guidelines 2005: Due Professional Care
- General Standard 1006: Proficiency
- General Guidelines 2006: Proficiency
- General Standard 1007: Assertions
- General Guidelines 2007: Assertions
- General Standard 1008: Criteria
- General Guidelines 2008: Criteria

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

2001.2.1	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.

About the IT audit charter

Purpose

- Define the framework for IT audits within the organization
- Emphasize the importance of IT audits in supporting organizational objectives.

Objectives of IT Audit

- Ensure data integrity and confidentiality
- Evaluate IT controls and governance
- Support risk mitigation and compliance efforts

Scope

- **Cybersecurity**
- **Data management**
- **Software audits and IT governance**

Possible exclusions:

- **Resource Constraints**. Certain areas may require too many resources (time, budget, expertise) to audit thoroughly.
- **Relevance**: Some systems or activities might not be critical to the audit's objectives.
- **External Jurisdiction**: If other departments or external auditors are responsible for certain areas, those might be excluded to avoid overlap.
- **Regulatory Boundaries**: Some data or systems may be excluded if accessing them would violate privacy regulations or contractual agreements.

Authority of IT Audit

- Reporting Structure: Reports to the board or audit committee
- Access Rights: Full access to data, personnel, and IT infrastructure necessary for auditing.

See later

Roles and Responsibilities

- IT Audit Team: Perform assessments and generate reports
- Management and Stakeholders: Support the audit process by providing access to resources and data.

See later

Audit Process and Methodology

- **Overview of Audit Process**: Planning, Execution, Reporting stages

- **Methodologies**: Use of risk-based approaches and sampling methods.

Standards and Frameworks

- **Frameworks Referenced**: COBIT, ISO/IEC 27001, …

- **Compliance Requirements**: Address relevant industry standards and regulatory requirements.

Communication and Reporting

- **Reporting Frequency**: Quarterly, annually, or as needed

- **Deliverables**: Findings, risk assessments, and action recommendations.

Ethics and Confidentiality

- **Confidentiality**: Ensure sensitive data is protected during audits

- **Ethics**: Maintain high ethical standards in all audit activities.

Continuous Improvement

- **Feedback**: Gather feedback to enhance audit processes
- **Adaptation**: Keep the charter updated to reflect technological changes.

Responsibility

In an audit, *responsibility* refers to the duties or obligations that individuals or teams are expected to perform. Auditors are responsible for planning, executing, and reporting the audit with due care and professionalism. This includes identifying the scope of the audit, gathering evidence, evaluating internal controls, and drawing conclusions based on their findings

For management, responsibility also involves ensuring that records are accessible, providing truthful information, and enabling a supportive environment for the auditors to complete their work

Authority

Authority is the right or power given to auditors to access relevant information, documents, and personnel required to carry out the audit. It allows auditors to conduct interviews, inspect records, verify procedures, and access areas or resources essential to evaluate compliance and accuracy. Authority is essential for auditors to function independently and objectively, and it is usually outlined in an audit charter or agreement with the entity being audited.

Accountability

Accountability involves holding auditors and other relevant parties answerable for their actions and decisions within the audit process. Auditors must be accountable for the accuracy, fairness, and integrity of their findings and reports.

Meanwhile, management is accountable for addressing any identified issues, taking corrective actions, and implementing audit recommendations, as necessary.

Accountability ensures that all stakeholders understand their obligations and follow up on audit results, leading to improvements and compliance.

In short

- **Responsibility** defines who does what within the audit process.
- **Authority** grants the power to access resources needed to complete the audit.
- **Accountability** ensures that individuals answer for their actions and outcomes.

Each of these elements is crucial for an effective audit, fostering transparency, adherence to standards, and improvements in processes or controls.

other contents

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 • Objectives of the audit function and the audit function's mission statement • Scope of the audit function • Work performed by the audit function
2001.2.4	• Independence • Relationship with external audit firms • Auditee's expectations • Auditee requirements • Abide by professional standards • Compliance

other contents

2001.2.5	• Right of access • Limitations of authority • Processes to be audited
2001.2.6	• Distributing written communications • Monitoring and reporting of management's progress • Reporting of the audit and assurance function's performance metrics • Reporting to those charged with governance and oversight • Quality assurance process • Staffing rules for audit engagements

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.

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

General Guidelines 2003: Auditor Objectivity

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

Tables on each of the items follow, from .2 to .9

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.

Guidelines follows

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.

Guidelines follows

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.

Guidelines follows

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.

Guidelines follows

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.

Guidelines follows

Performance Standards

- Performance Standard 1201: Risk Assessment in Planning
- Performance Guidelines 2201: Risk Assessment in Planning
- Performance Standard 1202: Audit Scheduling
- Performance Guidelines 2202: Audit Scheduling
- Performance Standard 1203: Engagement Planning
- Performance Guidelines 2203: Engagement Planning
- Performance Standard 1204: Performance and Supervision
- Performance Guidelines 2204: Performance and Supervision
- Performance Guidelines 2204: Performance and Supervision
- Performance Standard 1205: Evidence
- Performance Guidelines 2205: Evidence
- Performance Standard 1206: Using the Work of Other Experts
- Performance Guidelines 2206: Using the Work of Other Experts
- Performance Standard 1207: Irregularities and Illegal Acts
- Performance Guidelines 2207: Irregularities and Illegal Acts

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.

Guidelines follows

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.

Guidelines follows

Standard 1203: Engagement Planning

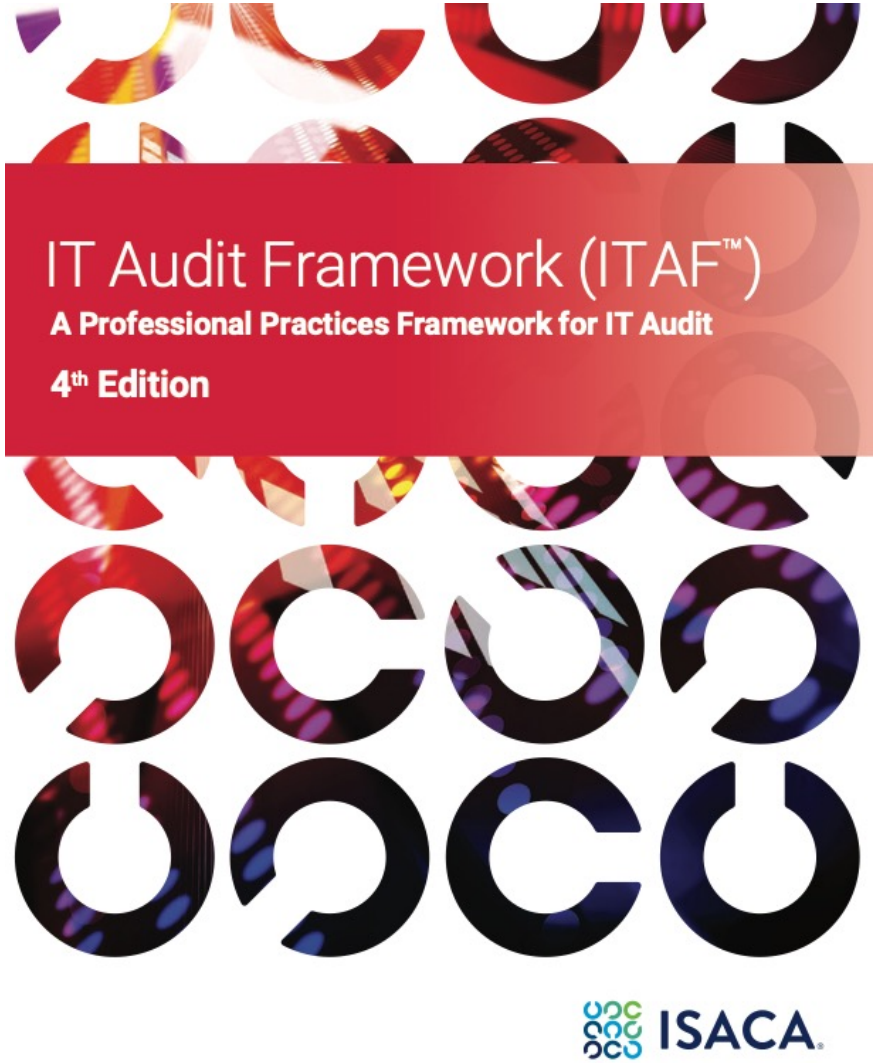
Statements	
	1203.1 IT audit and assurance practitioners shall plan each IT audit and assurance engagement to address the nature, timing and extent of audit procedures to be performed. The plan should include: • Areas to be audited • Objectives • Scope • Resources (e.g., staff, tools and budget) and 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.

Guidelines follows

Reporting Standards

- Reporting Standard 1401: Reporting
- Reporting Guidelines 2401: Reporting
- Reporting Standard 1402: Follow-up Activities
- Reporting Guidelines 2402: Follow-up Activities

…many slides have been skipped…



- document (with details, 106 pages) available for download from ISACA website: https://www.isaca.org/about-us/newsroom/press-releases/2020/isaca-updates-it-audit-framework-itaf
- for free