**System Auditing (PART 1)**

* Professional auditing in any IT area.

1. Develop a risk based IT audit system.
2. Specific audits to check if the current system is protected.
3. Conduct audits in accordance with standards.
4. Give recommendations and follow-ups for stakeholders.

**Management of the Audit Function.**

* Maintain independence and competence (for the auditing team)
* Senior management needs audit information to mitigate risk, or the controls they placed are doing what they are supposed to do.
* Business objectives should be kept in mind.

**Organization of the IS audit function.**

* Internal Audit – audit should be established by the contractor and be approved by senior management. Should work independently. (These are employed by the company itself)
* External Audit – outside firm. The scope and objectives should be mentioned in a formal contract way. Some information is not supposed to be leaked (where the company do not want some information to be accessed and should be specifically mentioned in the contract) based on the agreement of the firm.

Independence is a very important factor. The goal is to report everything to the senior management.

**IS audit Resource Management.**

With technology change, it is important that the audit team is up to date with skills.

* New audit techniques and updates technology
* The audit team should be technically competent.
* Management should consider the auditor’s skills and knowledge when planning the audit.

**Audit Planning - 1**

Short term goals – goals taken in account in around 1 year (next year)

Long term goals – changes to the organization and IT strategies throughout the future. Could be planning to bring in something completely new like new strategies or new technologies.

Both long and short terms should be checked annually, to check if it matches the business objectives.

**Audit Planning – 2**

Other planning considerations:

1. Periodic risk assessments
2. Changes in technology
3. Changing privacy issues
4. Regulatory requirements (law changes)
5. System implementations
6. Future technologies
7. IS resource limitations

**Audit Planning – 3**

Information gathering is important. Taken into consideration:

1. Understanding of the overall environment
2. Business practices and workings related to the audit.
3. Types of information systems and technologies supporting the business
4. Listing of all regulatory requirements in which the business operates

**Audit Planning – 4**

Auditing standards require the auditor to address the audit objectives and to comply with professional standards.

The auditor should have a plan that considers the objectives of the organization that is relevant to the audited technology infrastructure. (Should keep in mind the understanding of the organizations IT architecture)

**Audit Planning – 5**

Guidelines that IS auditor should follow:

1. Reviewing background information such as annual reports
2. Reviewing prior audit reports
3. Understanding the business and IT long term plans (IT is to support the business objectives)
4. Talking with managers to learn about business issues.
5. Researching the specific regulations that apply
6. Check upon the IT functions and check whether any functions are outsourced.
7. Walking through the organization’s facilities.

**Effects of Laws and Regulations**

Almost every organization will need to check upon government rules and contract rules that need to be followed.

This could include how data is processed, stored, and transmitted.

Special consideration should be given to issues for highly regulated industries. (Knowledgeable about the laws and regulations of a country or a contract)

* Privacy issues: need to consider all privacy laws and regulations.
* Possible regulations to be considered: establishment and organization of the regulatory requirements, responsibilities assigned to the organization, financial, operational, and IT audit functions.

**Two major areas of concern:**

1. Legal requirements for auditors: need to follow laws and regulations based on contracts or laws.
2. Legal requirements for the audit t: reporting, data management

**Steps for checking up organization level of compliance:**

1. Identification of requirements dealing with electronic data, computer system practices, how information is stored.
2. Documentation of applicable laws and regulations
3. Determining if organization has planned to support law requirements.
4. Determining if organization has addressed the adherence to any applicable laws.
5. Determining if there are established procedures to follow these requirements.

**ISACA IT Audit**

* Code of professional ethics
* Professional care in accordance with professional standards.
* Need to be up to date with the rules and laws. (Makes someone liable)
* Serving the interests of stakeholders and be honest with the reports
* Should not post information about good or bad audits to anyone other than those of interest (Code of Ethics)
* Maintain competency (Make sure that you can do with confidence)
* Inform the company with all the results. Don’t sugar coat and hide things related to audits.
* Support professional education for the stakeholders and help them to understand what is being reviewed.
* We have global applicable standards that can be found in the ISACA body of knowledge.
* One of ISACA’s goals is to advance standards to meet these needs.

The objective of ISACA IT audit assurance standards is to inform:

* IS auditors of the minimum acceptable performance
* Management of expectations concerning the work of audit practitioners
* ISACA certified members should be aware of the requirements that failing to comply with standards can result in an investigation of their conduct.

The framework ISACA IT audit and assurance standards has following levels:

1. Standards: mandatory requirements for IT audits and assurance reporting
2. Guidelines: does require professional judgement on how it should be applied
3. Procedures: examples of process that an auditor might follow.

**Auditing Standards – 1**

The contract is defining for the auditor. Outline all the basic rules for the audit and those who are being audited. Organizational independence of what is being audited. Internal employees can be pressurized by the manager or owner of something that could be embarrassing. Regardless of whether anyone likes it or not. The goal is to make them better. The auditor should adhere to the standards mentioned above.

**Auditing Standards – 2**

Professional competence is another standard for the auditor. The skills must be used professionally and not put on things the auditor is not aware of. Another standard is planning. Make sure to cover all the objectives and laws. Document should document everything about the audit, nature, time and types

**Auditing Standard – 3**

Another standard is performance of audit work.

1. Supervision – Audit staff should be supervised if they are accomplishing the objectives.
2. Evidence – the audit team should give reliable and relevant evidence to document their findings.
3. Documentation – Audit process should be recorded and the evidence to support the findings and conclusions.

**Auditing Standard – 4**

One of the standards should be the way the report has to be given in a professional or formal way. Should give evidence, documentation, and recommendations.

**Auditing Standard – 5**

Follow-up activities would be reporting of recommendations to the organization for the purpose of bringing them into compliance.

Irregularities and illegal acts also be a part of a reporting and finish body of work – we might have located areas of fraud, things that people are doing illegally (even if it can cause legal procedures). There can be attempts to hide those acts. If illegal acts are found, the auditor should obtain sufficient evidence to support their findings.

**Auditing Standard – 6**

IT governance – the auditor can assess if the IS function is in alignment with the company’s objectives and mission. The audit should be done based on a risk-based approach. The risks can affect the IS functions directly.

**Auditing Standard – 7**

Appropriate assessment techniques should be used. Should know the proper allocations for the resources. Should also find the absence of any controls that can affect the company. (Example: a minor deficiency, but if there are 10 15 minor deficiencies then it could have an overall effect to the company). Should be included in the report.

**Auditing Standards – 8**

Using the work of other experts. The outside work should be assessed and determined if it meets special qualifications and competencies. The audit process should determine if the outside work is adequate and complete; the results of that review should be documented.

**Auditing Standard – 9**

Audit evidence should be adequate to support the audit conclusion.

The auditor can assist management by providing advice regarding the design, implementation, operation, and improvement of IT controls.

E-commers should be evaluated along with the applicable controls. Risk assessment should be used in reviewing in the e-commerce environment.

**Audit Guidelines – 1**

Many guidelines will be mentioned to go through the audit process following a guideline as a guidance.

**Audit Guidelines – 2**

Using the work of other auditors. Addresses how we should go about with the work of other auditors. Could be highly technical or the audit team has the resources or knowledge of specific areas that need to be audited.

**Audit Guidelines – 3**

Audit evidence requirement, how the auditor should obtain sufficient and appropriate evidence and draw reasonable conclusions based on the audit results.

Use of Computer-assisted Audit Techniques (CAAT), the auditor may need to utilize tools to record, transact, and process data that comes from an audit. The sheer amount of information we look at can be easily done through these tools. The tools could include specific audit software, customized scripts etc.

**Audit Guidelines – 4**

Outsourcing of IS activities to other organizations. The organization may partially or fully outsource some of its IS activities to a third party. The auditor is responsible for confirming compliance of the third-party resource with existing contract agreements and regulations. The auditors should take caution in knowing that their rights to audit are often unclear.

Audit Charter Effective – This guideline is designed to help the auditor prepare a charter, or contract defining their responsibilities, authority, and accountability.

**Audit Guidelines – 5**

Materiality concepts for auditing information systems: IS auditors are often faced with the problem of determining its reality. Unlike their financial auditor counterparts, they can measure materiality in monetary terms, the IS auditor may need guidance on how materiality should be assessed.

**Audit Guidelines – 6**

Due professional care effective: applies to the performance of doing the audit. Applying the IT audit and assurance standards as well as complying with the ISACA code

Audit documentation: the auditor should prepare and retain in support of the audit findings. This report can determine how to achieve the implementation of standards, and the auditor should use professional judgement in its application as well as being able to justify any departure from existing standards.

**Audit Guidelines – 7**

Audit considerations for irregularities: finding of any illegal things during the audit.

Audit sampling: effective sample to be audited, especially with large amount of information.

Effect of pervasive IS controls: ways to evaluate controls and monitoring of these controls.

**Audit Guidelines – 8**

Organizational relationship and independents: we need to look at the structure of the organization. Management and their authorities, therefore, need to be independent.

Use of risk assessment and audit planning: There is a risk in doing auditing. If the plan did not work as planned, or not enough evidence were collected to give bad results.

Application systems review: applications that are running and controls we use to protect them. Guidelines about the way we look at how we can do audit of an application and the controls that are related applications

**Audit Guidelines – 9**

Planning revised: to revise plans based on the current audit planning findings

Effect of third parties on organizations IT controls: talk about the involvement of auditor doing evaluation for the third parties based on the standards

Effect of non-audit role on IS auditor’s independence: Generally talking about upper management, they have an effect on the auditor that can take away the independence of the auditor.

IT governance: auditor’s planning audits of those running the show

Enterprise resource planning: process that we go through that we have effective resources to go about with the auditing section

**Audit Guidelines – 10**

Business to consumer e-commerce review: use of e-commerce coming from clients

Internet banking effective: process of auditing those organizations that have internet banking

Review of virtual private networks: effectiveness of secure communications

Mobile computing: mostly dealing with laptops during that time

Post implementation review: after reports has been turned in, and recommendations done. The process done to see if any of the recommendations are implemented

**Audit Guidelines – 11**

General consideration on the use of the internet: what are the expectations of the organization? The guidelines we need to see if it is acceptable or not

Responsibility, authority and accountability: help plan to come up with agreements and who to report to after auditing process

Follow-up activities: a way of being able to review and being accountable after certain points of auditing

Biometric controls: fingerprints etc. when we review them there is a lot of information related to false positives, negatives etc.

Access control effective: access control check

**Audit Guidelines – 12**

IT organizations: every IT organization is different. It is difficult when going through audits on how the organization should be running efficiently. Achieve results to determine the IT organizations structure on how it is running efficiently or effectively

Review of security management practices: how the organization are currently using to secure

Return on security investment: auditing some of the controls that to check if the investment on controls were effective or not

Continuous assurance: giving assurance whether the controls are as effective and accomplishing the same

**Audit Assurance and Tools and Techniques**

The ISACA developed standards that give examples of guidelines to follow. The tools are mentioned to meet these standards. Audits on different things such as firewall, database etc.

The standards that ISACA set out are meant to be followed by the auditor. The tools and techniques give guidance for you for steps to perform a specific type of audit.

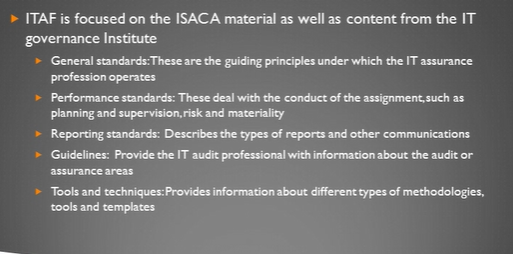
**Information Technology Assurance Framework:**

Provides guidance on design, conduct and reporting of IT audit

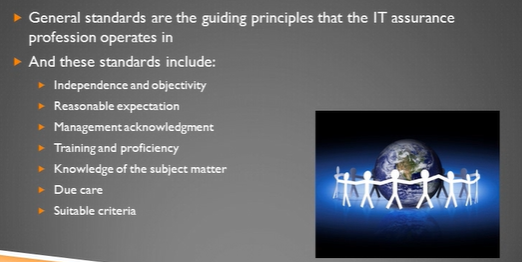
It defines terms and concepts specific to IT assurance

It establishes standards for the IT audit and assurance professional role and responsibilities

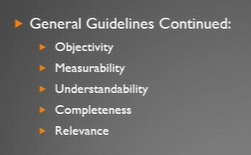
It is focused on the ISACA material as well as IT governance institute



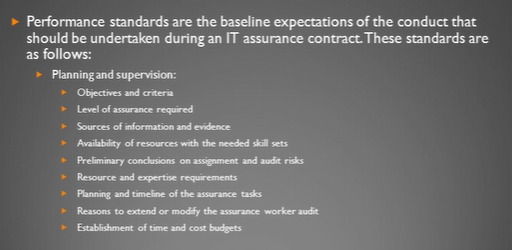
**ITAF General Standards (Section 2200)**

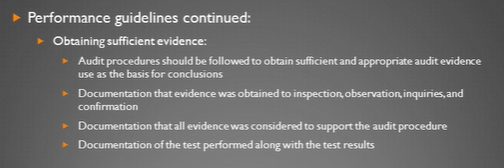


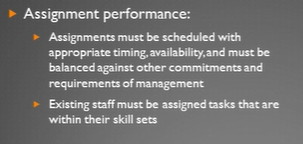
1. Auditors are independent and objective
2. Reasonable expectations from auditors on what they work
3. Management understand the audit is going on
4. Auditor maintaining their training and proficiency
5. Knowledge of the subject



**ITAF Performance Standards (Section 2400)**





 A picture containing text, font, screenshot, design

Description automatically generated

**Reporting Standards (Section 2600)**

A screen shot of a computer

Description automatically generated with low confidence

A picture containing text, screenshot, font, design

Description automatically generated

A picture containing text, screenshot, font, design

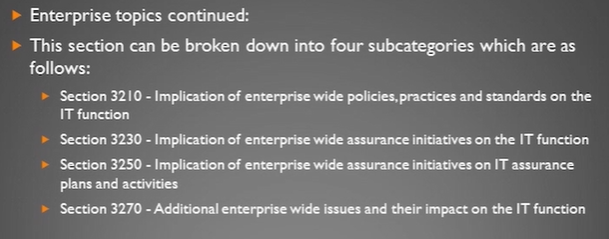
Description automatically generated

**IT Assurance Guidelines (Section 3000)**

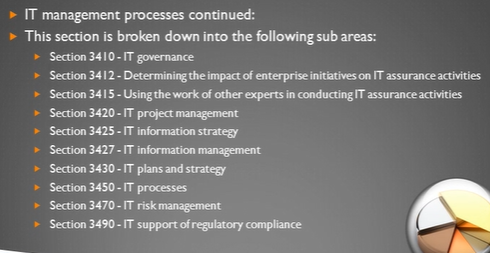
A grey background with white text

Description automatically generated with low confidence

**Enterprise topics:**



**IT management Process**



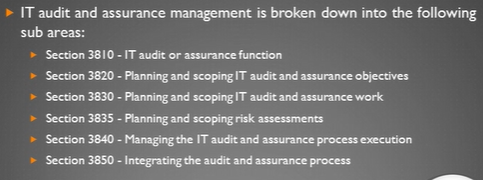
**IT audit and assurance processes**A picture containing text, screenshot, font, design

Description automatically generated

A picture containing text, screenshot, font, design

Description automatically generated

**IT audit and assurance management:**



A grey screen with white text

Description automatically generated with low confidence

**Risk Analysis:** analyzing risks, detecting and also finding solutions for it.

The purpose and nature of the business is important, to understand the risks that it could face.