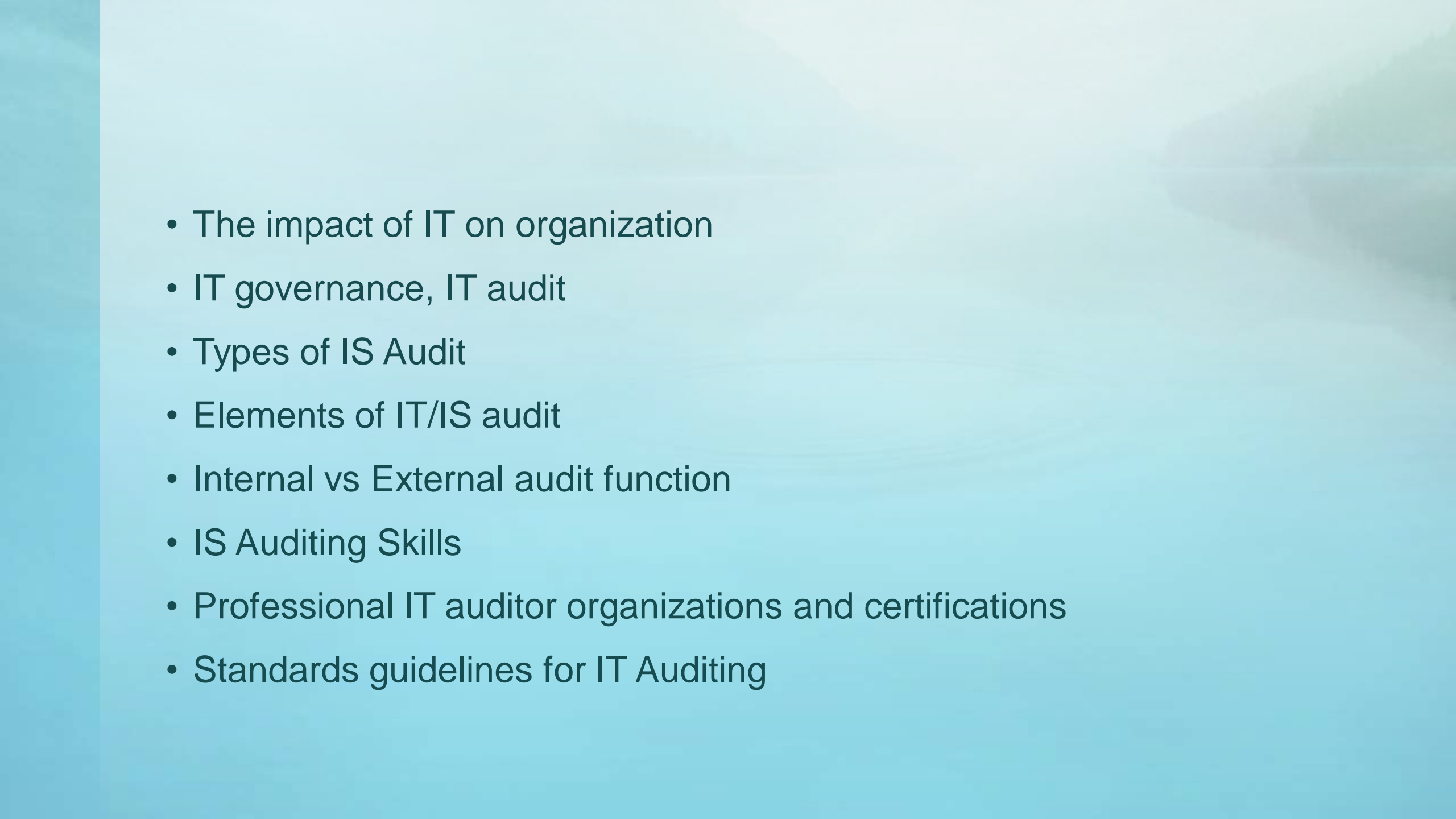




Introduction to IT/IS Auditing

CISB424

- 
- The background of the slide features a soft-focus photograph of a calm body of water, likely a lake, with misty mountains in the distance. The sky is a pale, hazy blue, and the overall atmosphere is serene and ethereal. The water reflects the light from the sky and the distant land.
- The impact of IT on organization
 - IT governance, IT audit
 - Types of IS Audit
 - Elements of IT/IS audit
 - Internal vs External audit function
 - IS Auditing Skills
 - Professional IT auditor organizations and certifications
 - Standards guidelines for IT Auditing

The impact of IT c

- E
 - I
 - a
 - V
- a)

b)

c) Inc

- Unforeseen System Outage
- Attacks Targeting Websites
- Password Cracking
- Internal Attacks
- Phishing



Q4 2013

Q3 2013

Dollar-Value IT Spending

ot
ces

The impact of IT on organization

- IT audit has traditionally been based upon the paradigms that control equals to management control, and management control starts with governance
- So, what are **management** and **governance**?

a) Management

The optimization of corporate resources through planning, organizing, leading and controlling of members of organization or the activities of a business in order to achieve defined objectives.

b) Governance

Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization.

The impact of IT on organization

Management process



The impact of IT on organization

Management process



...:VISION & MISSION :...

OUR VISION

"A leading computer science and information technology faculty that shapes innovations for a sustainable future"

OUR MISSION

"COIT is committed to generate, preserve, and disseminate knowledge by advancing computer science and information technology through quality education and innovative research, at the highest level of international excellence. This embodiment of excellence is personified by its graduates and scholars whom will best serve the society, the nation and humankind towards a sustainable future. "



Objective –

To know what are the requirements to achieve the organizational goals



Establish performance objectives



How?

Study the mission statement of the company
Study the strategic plans of the company
Interview staff

Implement and monitor the controls

The impact of IT on organization

Management process

Why is it important to identify the CORE business processes?

Perez-Soltero et al. (2006) have identified five (5) characteristics of core business processes, which are:

1. Core business process has direct impact with the organization's mission and vision
2. Core business process generates revenues or is the most critical to the overall success of the organization
3. Core business process has impact and added value to the organization
4. Core business process satisfies customer requirements
5. Core business process has valuable human, technological and information resources

Objective –

To identify the products and services provided to meet the goals

How?

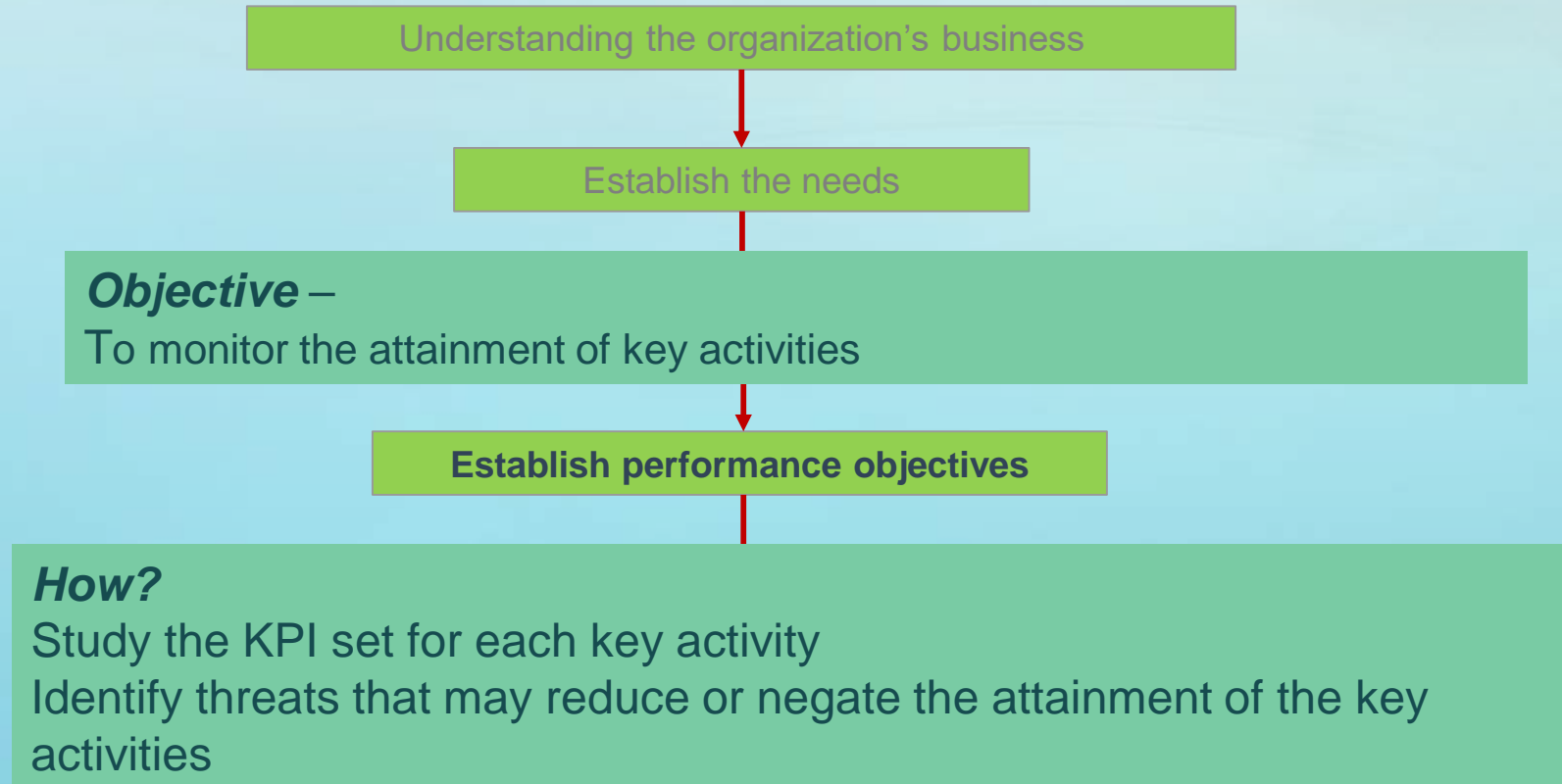
Identify the core business processes

Determine whether management understand customers' needs, competition

Key performance areas

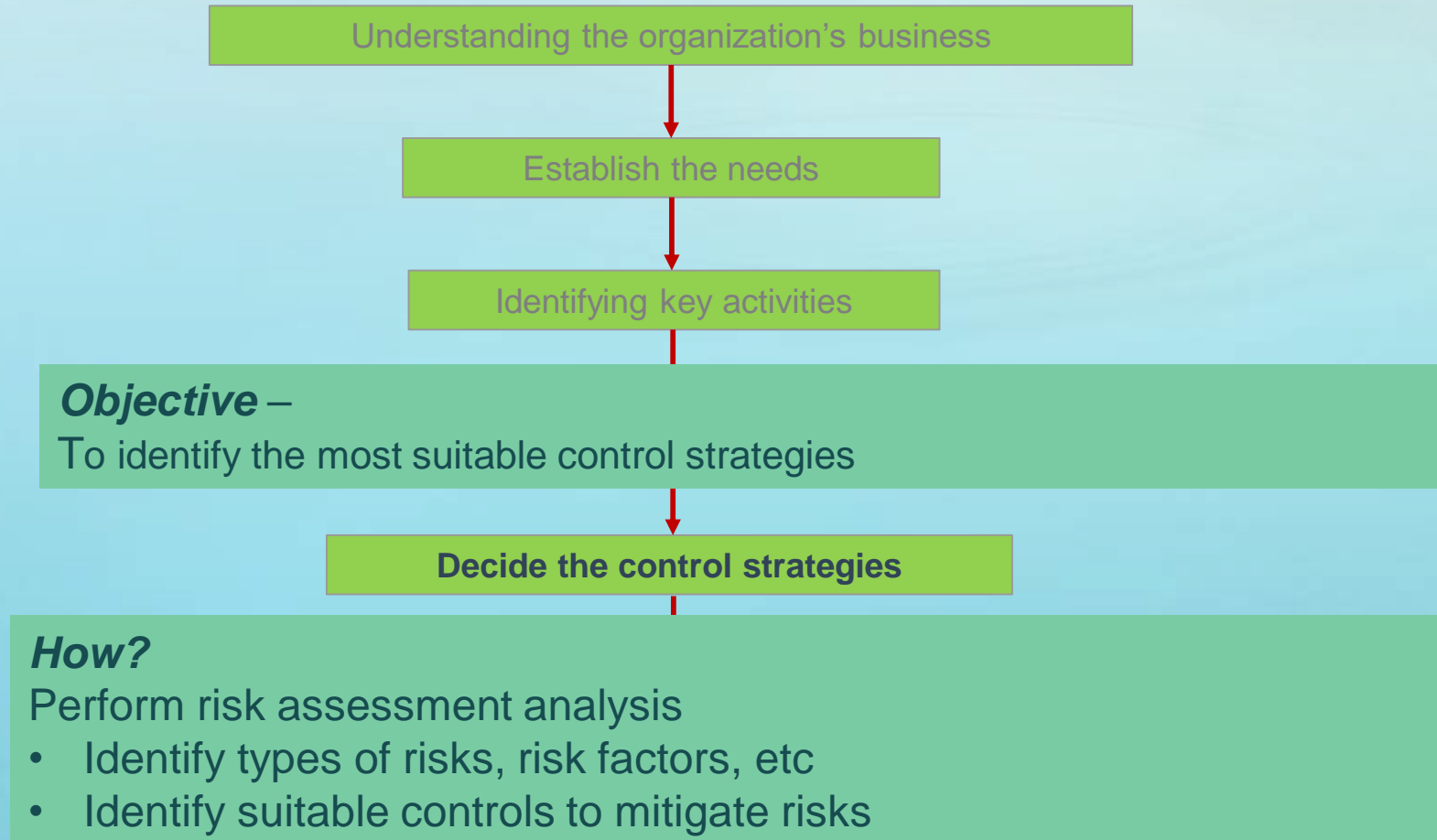
The impact of IT on organization

Management process



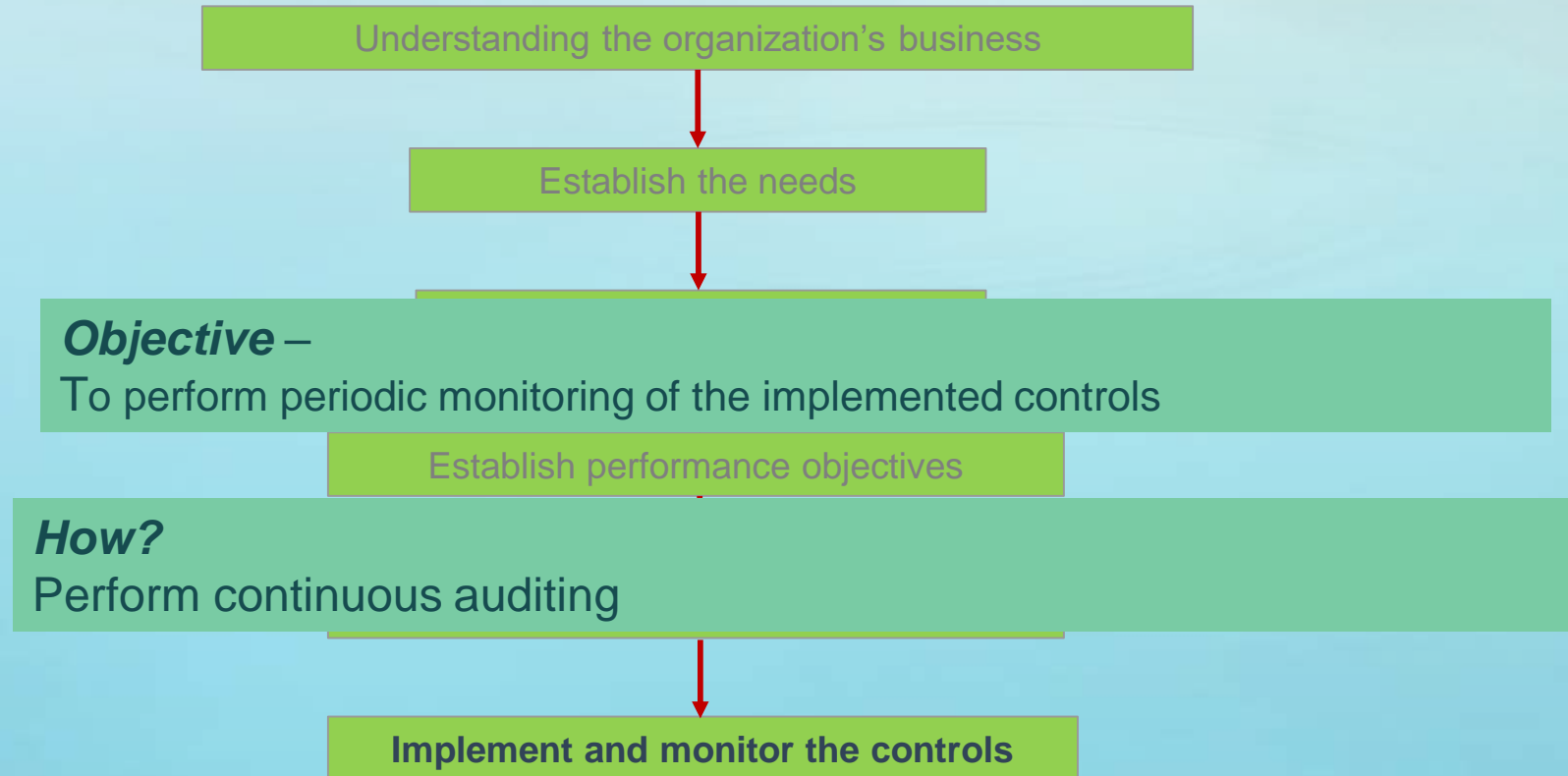
The impact of IT on organization

Management process



The impact of IT on organization

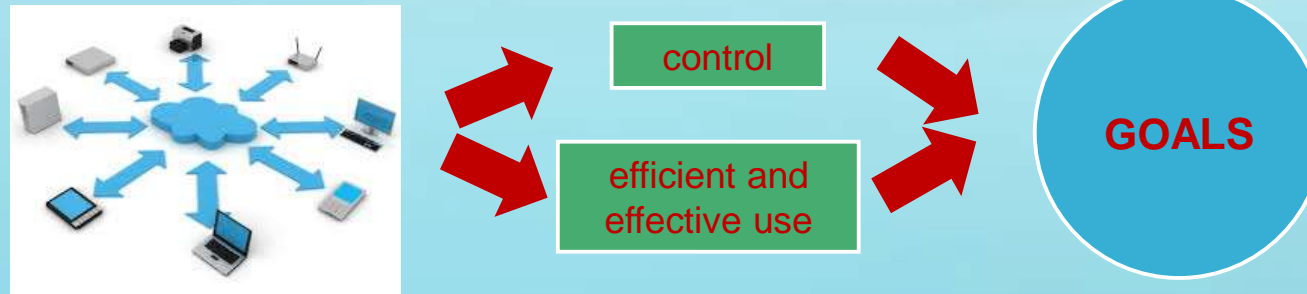
Management process



IT Governance

- The process of **controlling an organization's IT resources** and **ensuring effective and efficient use of IT** in enabling an organization to achieve its **business goals and strategies**

Adapted from Gartner Group



Audit

- **Independent** review and examination of records and activities to **assess** the **adequacy** of **internal controls**, to **ensure compliance** with established policies and operational procedures, and to **recommend necessary changes** in controls, policies, or procedures.

So what does it mean by independence?

Webster's: *"Not influenced or controlled by others."*

IIA's : *"..the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner"*

Thus, it means:

To provide value to all the stakeholders (management, executives, the board, the shareholders, the populace at large), auditors have to be able to carry out our responsibilities without worrying about being influenced or controlled by others.

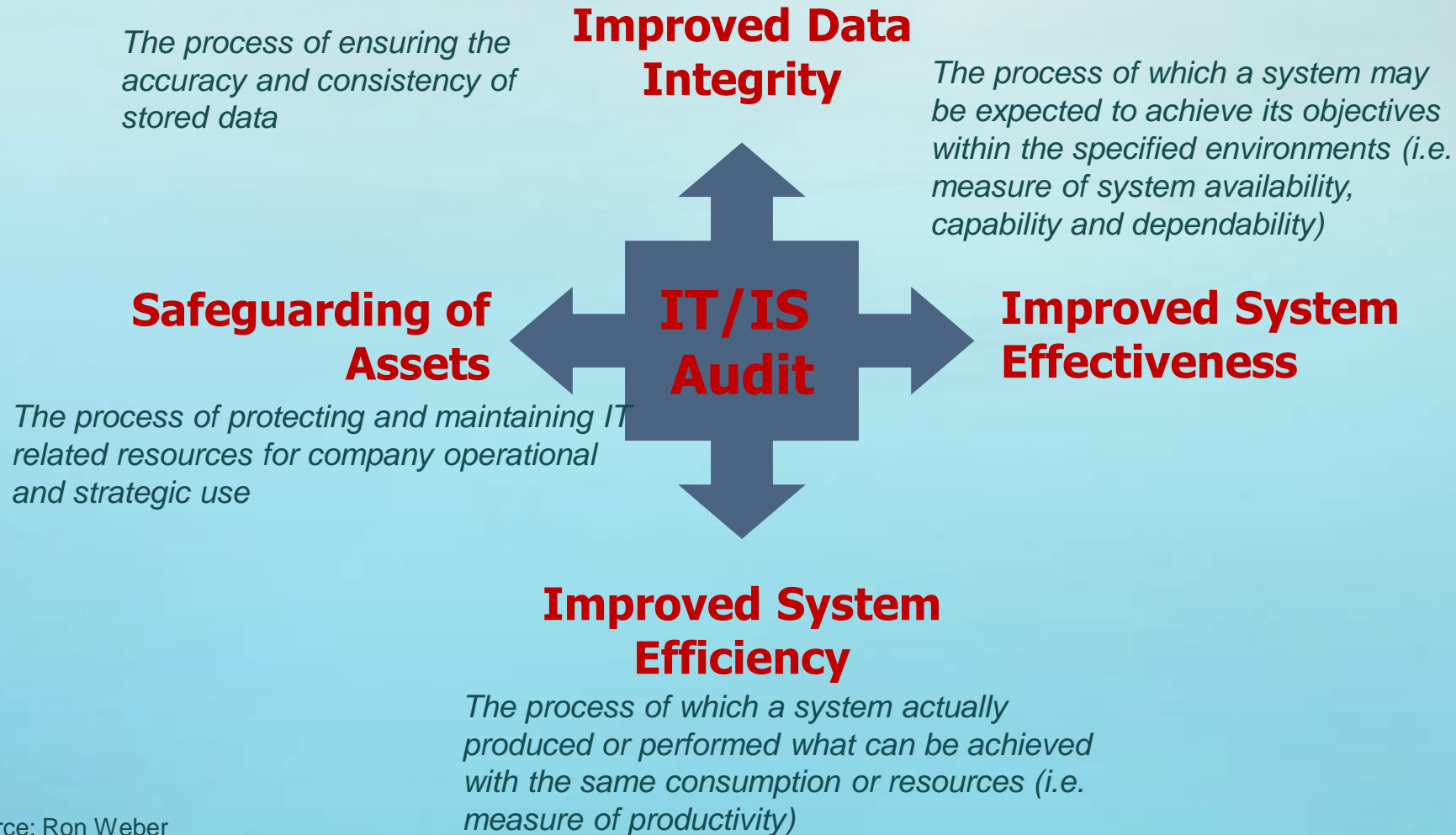
Source: Mike Jacka, IIA

IT Audit

- The process of collecting and evaluating evidence to determine whether computer system safeguards assets, maintain data integrity, achieves organisational goals effectively and consumes resources efficiently.

Source: Ron Weber

Objectives of IT Audit



IT Audit

- For most enterprises today, IT audit is not a single, unique function within an enterprise but a separate unit or component of the internal audit group, led by a Chief Audit Executive.
- Although a very important component of the internal audit function, IT audit generally follows the overall procedures and practices for the overall audit function.
- With IT functions so important to most enterprises today, there is almost always a need to have a specialized IT audit function or to have a regular financial or operational internal audit groups with strong IT-related technical skills.
- Every internal audit function should have at least one person on staff with strong skills in understanding and evaluating IT controls

Link between IT Governance and IT/IS Audit

Major focus areas of IT Governance

- Strategic alignment
- Value delivery
- Resource management
- Risk management
- Performance measure

IT/IS Audit

- IT Strategic Planning
- IT Project Management, Change Management
- IT Staffing function, Project Management
- Application Controls
- IT Strategic Planning

The impact of IT on organization

Management process



Types of IS Audit

#	Types of IS Audit	Category
1	IT General Controls Audit	General
2	Application Controls Audit	Information Systems
3	IT Governance Audit	IT Governance
4	IT Investment Audit	IT Governance
5	IT Risk Audit	IT Risk Management
6	Information Security Audit	Information Security
7	System Development Audit	Information Systems
8	Business Continuity Audit	Information Security
9	IT Performance Audit	IT Governance
10	Compliance Audit	IT Governance
11	Specialised Audit	Information Systems

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
3. Application Software
4. Application Development
5. Network Security
6. Business Continuity
7. Data Integrity

Elements IT/IS Audit

1. **Physical and Environmental**

2. System Administration

3. Application Software

4. Application Development

5. Network Security

6. Business Continuity

7. Data Integrity

Physical security

Power supply

Air conditioning

Humidity control

Other environmental factors

Elements IT/IS Audit

1. Physical and Environmental

2. System Administration

3. Application Software

4. Application Development

5. Network Security

6. Business Continuity

7. Data Integrity

Security review of the operating systems, database systems, and all other system administration procedures and compliances

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
- 3. Application Software**
4. Application Development
5. Network Security
6. Business Continuity
7. Data Integrity

Review of the access controls and authorizations, validations, error and exception handling, business process flows, manual controls and procedures of business applications

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
3. Application Software
- 4. Application Development**
5. Network Security
6. Business Continuity
7. Data Integrity

Review of the change management or project management of business applications

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
3. Application Software
4. Application Development

5. Network Security

6. Business Continuity
7. Data Integrity

Review of internal and external connections to the systems, perimeter security, firewall review, router access control lists, port scanning, intrusion detection systems

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
3. Application Software
4. Application Development
5. Network Security
- 6. Business Continuity**
7. Data Integrity

Review of areas related to the continuation of business operations in the event of disasters which include existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, documented and tested disaster recovery/ business continuity plan

Elements IT/IS Audit

1. Physical and Environmental
2. System Administration
3. Application Software
4. Application Development
5. Network Security
6. Business Continuity
7. **Data Integrity**

To verify the adequacy of controls and impact of weaknesses of live data (can be subset of the other types of reviews)

Internal vs External Audit Functions

- Audit function can be performed *internally* or *externally*
- **Internal audit** is “an independent, objective assurance and consulting activity designed to add value and improve organization’s operation. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance process”
- **External audit** is an independent opinion of an organization’s financial statements in determining whether the statements conform with Generally Accepted Accounting Principles (GAAP) and fairly presents the financial position of an organization; whether the results of operations for a given period of time are represented accurately; and whether the financial statements have been affected materially

(Source: Lal Balkaran, The Institute of Internal Auditor)

Internal vs External Audit

	External	Internal
Appointment by and reports to	Shareholders or members who are outside the organisations governance structure.	Organization's governance structure (usually the Audit Committee)
Objectives	To consider whether the annual accounts give a "true and fair view" and are in accordance with legal requirement <i>(i.e. defined by statute / legal requirements)</i>	To consider if business practices are helping the business manage its risks and meet its strategic objectives- it can cover operational as well as financial matters <i>(Usually defined by the Audit Committee)</i>
Focus	Historical events and data	Historical and future events
Coverage	Financial reports, financial reporting risks.	All categories of risk, their management, including reporting on them.
Responsibility f or improvement	None, however there is a duty to report problems	Improvement is fundamental to the purpose of internal auditing. But it is done by advising, coaching and facilitating in order to not undermine the responsibility of management
What happens after the audit?	There is no follow up requirement, until next year's audit; when in planning the audit, past issues should be considered.	Follow up to see whether recommendations have been implemented. Consultative help to guide management's implementation of recommendations.
Mandatory?	It depends on the legal requirements of governing body of the organization	No, internal audit is discretionary.

Internal vs External Audit

- Revision of the Institute of Internal Auditors (IIA) Standards in 2007 – inclusion of Attribute Standard 1312 on External Assessment:

1312 – External Assessments

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The form and frequency of external assessments; and
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

Internal Audit Reporting Structure

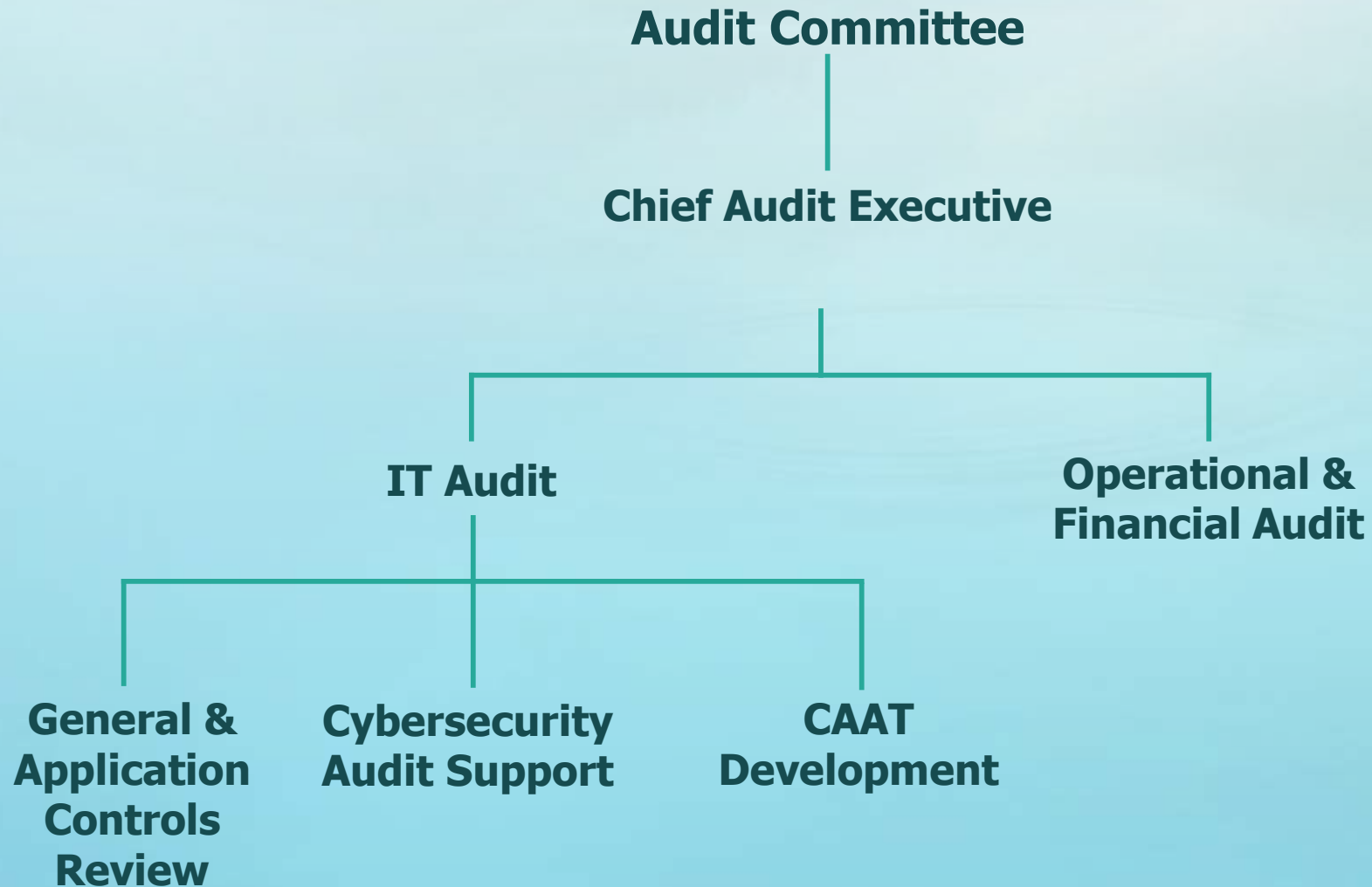
In defining the reporting structure of internal audit function of an organization, the organization must ensure:

Independence & Objectivity

a) **Standard 1100** - The internal audit activity must be *independent*, and internal auditors must be *objective* in performing their work.

b) **Standard 1110** - The Chief Audit Executive (CAE) **Independence** is the *freedom* from conditions that *threaten* the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. **Objectivity** is an *unbiased mental attitude* that allows internal auditors to perform engagements in such a manner that they *believe in their work product* and that *no quality compromises are made*. Objectivity requires that internal auditors *do not subordinate their judgment* on audit matters to others.

Internal Audit Organization Chart



Audit Committee

- The key component of a corporate board of directors with the responsibilities for internal controls and financial reporting oversight
- In requirement of SOx, audit committee:
 - must be **independent directors** with no connection to the enterprise management
 - composed of specially qualified groups of people who understand, monitor, coordinate and assess the internal controls environment and related financial activities for the entire board
- However, Audit Committee may invite members of the management to attend committee meetings and deliberations

Audit Committee Charter

1. Review the resources, plans, activities, staffing and organizational structure of IT audit (as part of enterprise internal audit)
2. Review the appointment, performance and replacement of Chief Audit Executive
3. Review all audits and reports prepared by internal audit together with the management's response
4. Review the management, the Chief Audit Executive, and the independent accountants the adequacy of financial reporting and internal control systems

Audit Committee Roles and Responsibilities

- Internal audit plans and budget
 - a) Should develop an overall understanding of the total audit needs of the enterprise
 - The annual audit plan is developed through internal audit risk analysis process and discussion with the senior management and audit committee
 - b) Review and approve high-level plans and budget of internal audit
- IT audit
 - a) Using Chief Audit Executive as the prime contact, IT audit needs to reach out to audit committee members to brief them on important and evolving IT-related internal control issues
- IT audit findings
 - a) Review and take action on significant audit findings that are reported to them by both internal and external auditors, management or other parties.

Chief Audit Executive Roles and Responsibilities

- Chief Audit Executive is the person responsible for all of internal audit, including the IT audit function
- Chief Audit Executive should have knowledge and understanding of these areas:
 - a) Enterprise operations and risks issues
 - b) Human resources and internal audit administration
 - c) Relationships with the audit committee and management
 - d) Corporate governance, accounting and regulatory issues
 - e) Internal audit team building and administration
 - f) Technology
 - g) Risk-based audit planning and process excellence
 - h) Negotiating skills and relationship management
 - i) Internal audit's assurance and consulting roles
 - j) Standards for the Professional Practice of Internal Auditing

What is IT Auditor?

- A professional that is assigned to assess *the adequacy of internal controls implementation* of an organization as well as *ensuring that IT related resources* are being utilized in *efficient and effective* manner to achieve the organizational goals
- Can be from within the organization (i.e. internal IT auditor) or outside the organization (i.e. external IT auditor)
- <http://itauditsecurity.wordpress.com/2012/10/02/top-10-it-auditor/>

Knowledge, Skills, Abilities and IT Auditor

- An IT auditor should be expected to have at least a high-level working knowledge of these areas:
 - a) Business application systems
 - b) Data management process
 - c) Systems development life cycle processes
 - d) Storage management and the importance of backup and recovery processes
 - e) Computer operating systems basic functions
 - f) Computer systems architectures
 - g) IT service operations processes
 - h) IT service design processes
 - i) Governance and service strategy processes
 - j) Programming or coding techniques
 - k) Ongoing interest and curiosity to understand and explore newer and evolving technology concept

Knowledge, Skills, Abilities and IT Auditor

- An IT auditor is expected to have also:
 - a) Interpersonal/human relation skills
 - b) Ability to exercise good judgment and objectivity
 - c) Ability to maintain confidentiality
 - d) Ability to use IT desktop office tools, vulnerability analysis tools, and other IT tools

Roles of IT Auditor

1. Ensuring IT governance of an organization by
 - a) Reviewing and assessing potential risks of an organization
 - b) Reviewing, assessing and monitoring organizational internal controls
2. Involved in the planning and execution of internal audit procedures and the creation of internal audit reports
3. Reporting to the governing body of the organization

*“IT auditors help organizations comply with legislation, making sure they keeping data and records secure. These auditors don't actually implement any fixes; they just offer an **independent review of the situation.**”*

(Source: Toni Bowers, <http://www.techrepublic.com/blog/career-management/it-auditor-one-of-the-fastest-growing-careers/>)

Professional IT auditor organizations and certifications

- ISACA (www.isaca.org)
An independent, nonprofit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems
 - a) *Certified Information Systems Auditor (CISA)*
 - b) *Certified Information Security Manager (CISM)*
- IIA (The Institute of Internal Auditors, <https://na.theiia.org/Pages/IIAHome.aspx>)
An international association that provides resources and education for internal audit professionals in the areas of internal auditing, risk management, governance, internal control, information technology audit and security.
 - a) *Certified Internal Auditor (CIA)*
- ACFE (Association of Certified Fraud Examiners, <http://www.acfe.com/>)
The world's largest anti-fraud organization and premier provider of anti-fraud training and education
 - a) *Certified Fraud Examiners (CFE)*
- AICPA (American Institute of Certified Public Accountants, <http://www.aicpa.org/>)
 - a) *Certified Information Technology Professional (CITP)*

Minimum Qualifications for IT Auditor

- Bachelor's degree in Computer Science, computer programming or accounting
- Certified Information Systems Auditor (CISA) credentials or candidate (preferred)
- Certified Internal Auditor credential (preferred)

Standards guidelines for the Professional Practice of Internal Auditing

- Why do internal auditors need a set of defined standards/guidelines?
 - Every profession requires a set of standard to govern its practices, general procedures, and ethics. Thus, it allows the specialists performing similar work to call themselves professional in their area of expertise.
- Three (3) main key players in defining standards for auditing and controls
 1. Institute of Internal Auditors (IIA)
 2. Information Systems Audit and Control Association (ISACA)
 3. Committee of Sponsoring Organization (COSO)

Standards guidelines for the Professional Practice of Internal Auditing

1. Institute of Internal Auditors (IIA)

Focuses on internal audit function of an organization

a) International Professional Practices Framework (IPPF)



Conformance with the principles set forth in mandatory guidance is **required and essential for the professional practice of internal auditing**.

Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input.

It describes practices for effective implementation of The IIA's Definition of Internal Auditing, Code of Ethics, and Standards.

Standards guidelines for the Professional Practice of Internal Auditing

International Standard fro the Professional Practice of Internal Auditing
Objectives:

- i. To delineate (define) basic principles for the practice of internal auditing
- ii. To provide a framework for performing and promoting an broad range of value-added internal audit activities
- iii. To establish the basis for the measurement of internal audit performance
- iv. To foster improved organizational processes and operations

This standard can be used as a guideline for the audit committee and management to measure the internal auditors, as well and for internal auditors to measure themselves

Standards guidelines for the Professional Practice of Internal Auditing

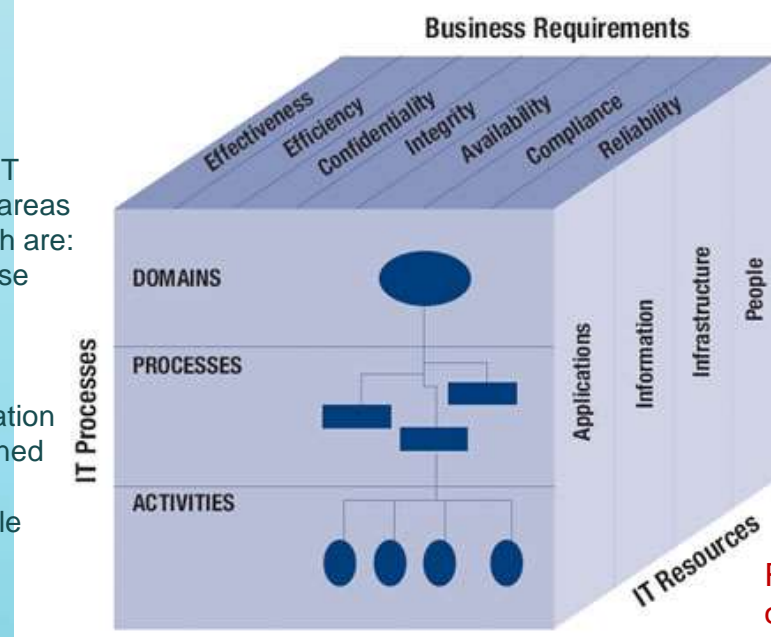
2. Information Systems Audit and Control Association (ISACA)

- Focuses more on IT auditing standards

- a) CobiT (Control Objectives for Information and related Technology)

These **seven (7) components** must should be considered when evaluating all business requirements

1. **Domain** – grouping of IT activities that match to areas of responsibilities, which are:
 - a) Planning & enterprise
 - b) Acquisition & implementation
 - c) Delivery & support
 - d) Monitoring & evaluation
2. **Process** – series of joined activities
3. **Activity** – has a life cycle



CobiT cube

1. **Application** – both automated and manual systems, or automated procedures to process information
2. **Information** – including input, output and processed data, for use by business processes
3. **Technology and infrastructure** – including hardware, OS, databases, networks and the environment that house and support them
4. **Key and specialized personnel** to plan, organize, acquire, implement, support, monitor and evaluate IT services

Represents all of an organization's IT assets

Standards guidelines for the Professional Practice of Internal Auditing

2. Information Systems Audit and Control Association (ISACA)

- Focuses more on IT auditing standards
 - b) Information Technology Assurance Framework (ITAF)
 - Objective – to establish standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills; and diligence, conduct and reporting requirements
 - ITAF IS audit and assurance are divided into three (3) parts:
 - a) Standards
 - b) Guidelines
 - c) Tools and techniques



Standards guidelines for the Professional Practice of Internal Auditing

1. ITAF IS audit and assurance **standards** are divided into:
 - a) **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
 - b) **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
 - c) **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated
2. ITAF IS audit and assurance **guidelines** are also divided into:
 - a) **General guidelines (2000 series)**
 - b) **Performance guidelines (2200 series)**
 - c) **Reporting guidelines (2400 series)**
3. Tools and techniques, section 3000, provide specific information on various methodologies, tools and templates—and provide direction in their application and use to operationalize the information provided in the guidance.

Standards guidelines for the Professional Practice of Internal Auditing

3. Committee of Sponsoring Organization (COSO)
 - Standard for measuring and evaluating internal accounting controls
 - Closely related to SOX 404 compliance
- a) Internal Control — Integrated Framework (2013)**

The 2013 Framework is expected to help organizations design and implement internal control in light of many changes in business and operating environments since the issuance of the original Framework, broaden the application of internal control in addressing operations and reporting objectives, and clarify the requirements for determining what constitutes effective internal control.

Standards guidelines for IT Auditing

- BS7799 and ISO17799
 - IT Security
- NIST Standard
 - Management Controls
 - Operational Controls
 - Technical Controls
- BSI Baselines
 - IT Security Management
 - IT Baseline Protection for Generic Components