*CA Final: Comprehensive Notes on*

# Information Systems Control and Audit (ISCA)

*Including past examination questions*

*For May 16 Exam*

# ISCA

*Sumit Shanker Dandowtiya*

*(FCA, DISA, CISA)*

*Course Duration: Two month / 48 Lectures Approx.*
*For new batch announcement check www.cafinal.com*

**www.cafinal.com**

**15.2 Edition**

# Where the mind is without fear

*Where the mind is without fear and the head is held high*
*Where knowledge is free*
*Where the world has not been broken up into fragments*
*By narrow domestic walls*
*Where words come out from the depth of truth*
*Where tireless striving stretches its arms towards perfection*
*Where the mind is led forward by thee*
*Into ever-widening thought and action*
*Into that heaven of freedom, my Father, let my country awake*

- Rabindranath Tagore

# ISCA Lecture Schedule

## (Total Duration: Two Months / 48 Lectures Approx.)

| Chapter | | Start Date | Finish Date | Duration<br>(48 Lectures) |
|---|---|---|---|---|
| Ch 1* | *Concepts of Governance and Management of Information Systems* | | | |
| Ch 2* | *Information Systems Concepts* | | | |
| Ch 3* | *Protection of Information Systems* | | | |
| Ch 4* | *Business Continuity and Disaster Recovery Planning* | | | |
| Ch 5* | *Acquisition, Development and Implementation of Information Systems* | | | |
| Ch 6* | *Auditing of Information Systems* | | | |
| Ch 7* | *Information Technology Regulatory Issues* | | | |
| Ch 8* | *Emerging Technologies* | | | |
| Reference | *Digital Signature* | | | |
| Glossary | *Glossary* | | | |

Morning batch: 10.15 – 11.30 AM (Apr-May, Aug-Sep, Dec-Jan)

Evening batch: 5.30 – 6.45 PM (Feb-Mar, Jun-Jul, Oct-Nov)

Address: 17, Luv-Kush Nagar (First),
Near JP Underpass, Sahakar Marg, Jaipur

Ph: 9314207273

* References – Final Course Study Material, Information Systems Control and Audit, ICAI.

# *Strategy for winning in ISCA*

1. *Consistency: Give time to this subject on regular basis, just 45 minutes, but daily. Do not leave this subject for last month preparation.*

2. *Keep Writing: Learn by writing bullet points again and again. Writing will make it easier to remember the points.*

3. *Revise: This subject requires repeated revision.*

4. *Conceptual Understanding: This subject requires both learning + conceptual understanding. Learning helps to answer the questions in exam but learning cannot be done without conceptual understanding.*

5. *Mock Test: Please appear for mock test one month before exam. This will help you to gauge your performance well in advance.*

6. *In Exam: Read the question very carefully in exam to identify and locate the correct chapter and paragraph. Misidentification is the major reason for securing less marks in this subject.*

***Wish you all the best***

***CA Sumit Shanker***

***17 Luv-Kush Nagar – I***
***Sahakar Marg,***
***Jaipur - 302015***

CHAPTER 1

# Concepts of Governance and Management of Information Systems

Key Topics:

1. Governance and Internal Control
2. IT Strategy Planning
3. Risk Management
4. COBIT 5 and IT Compliance Review

## ◙ Key concepts of Governance:

1. ***Governance*:** Governance means to steer or control any system. It includes everything that enables an organization to have an organized mechanism for running the business. Thus we can say that Governance means all the mechanism used for evaluation options, setting direction, monitoring compliance and performance.
2. ***Enterprise Governance*:** It means the set of responsibilities and practices used by the top management to provide strategic direction, to ensure objectives are achieved and ensuring that resources are used responsibly.
3. ***Corporate Governance*:** Corporate governance is defined as the system by which a company is directed and controlled so that it can increase shareholders value. It includes the structure and process for the direction and control of companies.

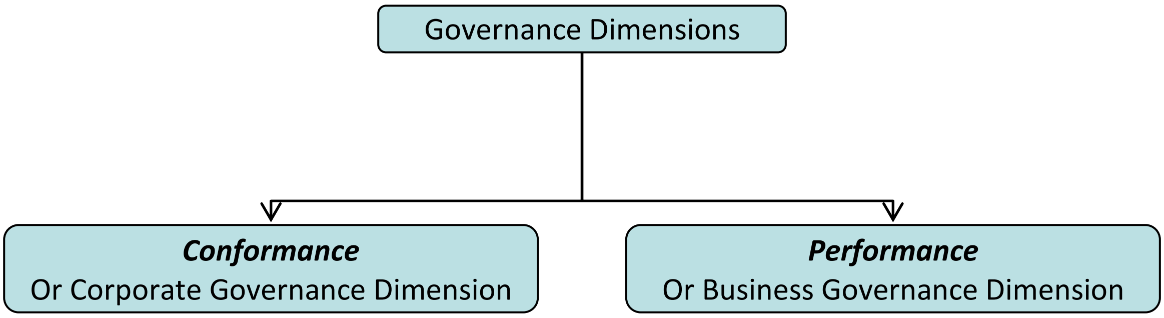
## ◙ Corporate Governance and IT Governance

***Benefits of Governance:*** Major benefits of governance can be summarized as follows:

i) *Achieving enterprise objectives* by ensuring that each element of the mission and strategy are assigned and managed with a *clearly understood and transparent decisions, rights and accountability* framework
ii) Defining and encouraging *desirable behavior in the use of IT* and in the execution of IT outsourcing arrangements
iii) Implementing and integrating the *desired business processes* into the enterprise
iv) *Providing stability* and overcoming the limitations of organizational structure
v) *Improving customer, business and internal relationships* and satisfaction, and reducing internal conflicts by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework
vi) Enabling *effective and strategically aligned decision making* for the IT Principles that define the role of IT, IT Architecture, IT Infrastructure, Application Portfolio and Frameworks, Service Portfolio, and IT Investment & Prioritization.

Based on the above, it can be seen that IT is an integral part of the governance. Let us discuss further the two distinct dimensions of governance to get a clarity on 'how governance is implemented in enterprises' and 'how does it impact enterprise'.

***Governance Dimensions***


Governance Dimensions
Conformance
Or Corporate Governance Dimension
Performance
Or Business Governance Dimension

***1) Conformance** or Corporate Governance Dimension*:

- The conformance dimension of governance provides a ***historic view*** of governance and ***focuses on regulatory requirements***.
- This covers corporate governance issues such as: ***Roles of the chairman and CEO, Role and composition of the board of directors, Board committees***, Controls assurance and Risk management for compliance.
- This also covers ***audit and assurance*** over compliance.
- There are ***established oversight mechanisms*** for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee, nominations committee and the remuneration committee. The Sarbanes Oxley Act of US and the listing requirements of SEBI also provides for such compliances.

2) ***Performance** or Business Governance Dimension*:

- Performance dimension of governance is ***pro-active*** in its approach. It is ***business oriented*** and takes a ***forward looking view***.
- This dimension focuses on ***strategy*** and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers.
- Conformance dimension is monitored by the audit committee. However, the performance dimension is the responsibility of the full board and there is ***no dedicated oversight mechanism***.
- Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. Thus there is an oversight gap in respect of strategy. One of the ways of dealing with this gap is to establish a strategy committee of similar status to the other board committees which will report to the board.

◙ **IT Governance and GEIT:** *[Although the terms IT Governance and Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro and broader in its scope of coverage.]*

***IT Governance***

IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT. It may be noticed that governance and IT governance are similar in their definition and approach except that in case of IT governance the focus is on IT and related areas.

***Key practices to determine status of IT Governance:***

*Some of the key practices, which determine the status of IT Governance in the enterprise, are:*

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

***Benefits of IT Governance***

- Increased *value* delivered through enterprise IT
- Increased *user satisfaction* with IT services
- Improved *agility* in supporting business needs
- Better *cost* performance of IT
- Improved management and mitigation of *IT-related business risk*
- IT becoming an *enabler for change* rather than hindrance
- Improved *transparency* and understanding of IT's contribution to the business
- Improved *compliance* with relevant laws, regulations and policies; and
- More *optimal utilization* of IT resources.

***Nov 2014*** *(6M) Q: What do you mean by IT Governance? Write any three benefits of IT Governance.*

*For every defined benefit, it is critical to ensure that:*

- Ownership is defined and agreed
- It is relevant and links to the business strategy
- The timing of its realization of benefit is realistic and documented
- The risks, assumptions and dependencies associated with the realization of the benefits are understood, correct and current
- An unambiguous measure has been identified; and
- Timely and accurate data for the measure is available or is easy to obtain.

### *Governance of Enterprise IT (GEIT)*

*The primary objective of GEIT is to analyze the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.*

### *Benefits of GEIT*

- It provides a consistent approach integrated and aligned with the enterprise governance approach
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives
- It ensures that IT-related processes are overseen effectively and transparently
- It confirms compliance with legal and regulatory requirements
- It ensures that the governance requirements for board members are met

### *Key governance practices of GEIT*

i) ***Evaluate** the Governance System:* Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;

ii) ***Direct** the Governance System:* Inform leadership and obtain their support and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and

iii) ***Monitor** the Governance System:* Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

### ◙ Corporate Governance, Enterprise Risk Management (ERM) and Internal Controls

Various prominent frauds committed by some large enterprises across the world including India in the last two decades have awakened regulators to the need of mandating the *implementation of corporate governance integrated with Enterprise Risk Management and Internal controls*.

As discussed earlier, Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.

*Some of the best practices of corporate governance are as follows:*

- *Clear assignment of responsibilities* and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors
- Establishment of a mechanism for the *interaction and cooperation* among the board of directors, senior management and the auditors
- Implementing *strong internal control systems*, including internal and external audit, risk management functions independent of business lines, and other checks and balances
- Special monitoring of risk exposures where *conflicts of interest* are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm
- Financial and managerial *incentives* to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate *information flows* internally and to the public.

## ERM: Enterprise Risk Management

In implementing controls, it is important to adapt a holistic and comprehensive approach. Before implementing controls it is important to consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise.
The Sarbanes Oxley Act (SOX) in the US, also focuses on the implementation and review of internal controls. In IT environment it is important to understand whether the relevant IT controls are implemented. How controls are implemented would be dependent on the overall risk management strategy and risk appetite of the management. SOX has used COSO framework as a guide for implementing risk management and internal controls. The Executive Summary of Enterprise Risk Management — Integrated Framework published by *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) highlights the need for management to implement a system of risk management at the enterprise level.

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows: *"Enterprise risk management is a process, effected by board of directors, management and other personnel, applied in strategy setting across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

**Internal Controls:** The *SEC final rules* define "*internal control over financial reporting*" as a "process designed by the company's principal executive or board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Relates to the maintenance of records of the transactions and assets of the company
- Provide reasonable assurance that transactions are recorded in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company
- Provide reasonable assurance regarding prevention or timely detection of unauthorized use of the company's assets that could have a material effect on the financial statements."

Under the *SEC final rules*, a company's annual report must include "an internal control report of management that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting
- Management's assessment of the effectiveness of the company's internal control over financial reporting, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management.
- A statement that the registered public accounting firm that audited the financial statements has issued an attestation report on management's assessment of the company's internal control over financial reporting."

***(a)*** ***Responsibility for Implementing Internal Controls:*** SOX made a major change in internal controls by holding Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) personally and criminally liable for the quality and effectiveness of their organization's internal controls. This is to ensure to the public that an organization's internal controls are effective. An organization must ensure that its financial statements comply with Financial Accounting Standards (FAS) and International Accounting Standards (IAS) or local rules.

***(b)*** ***Internal Controls as per COSO:*** According to COSO, Internal Control is comprised of five interrelated components: *(Details given in Ch 3, Pg 6)*

1. *Control Environment*
2. *Risk Assessment*
3. *Control Activities*
4. *Information and Communication*
5. *Monitoring*

***Nov 2014 (4M)*** *Q: Short Note – Internal Controls as per COSO*

***(c)*** Clause 49 of the listing agreements issued by SEBI in India is similar to SOX regulation and requires the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors. It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX.

___________x____________x____________