CA FINAL – ISCA
TEST PAPER
CF 16

Question 1 (4 Marks)

The 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. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. 2

The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. 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. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacuna is to establish a strategy committee with status similar to other board committees and which will report to the board. 2

Question 2 (5 marks)

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

1. Who makes directing, controlling and executing decisions? 1/2
2.How the decisions are made? 1/2
3. What information is required to make the decisions? 1/2
4. What decision-making mechanisms are required? 1/2
5. How exceptions are handled? 1/2
6. How the governance results are monitored and improved? 1/2

As per regulatory requirements and best practices frameworks of Governance of enterprise IT, it is important for the Board of Directors and senior management to play critical roles in evaluating; directing and monitoring IT Effectiveness of the IT governance structure and processes are directly dependent upon the level of involvement of the board and senior management. Different levels of the framework require different tools, techniques, and standards addressing specific needs of an effective IT governance structure, which consists of the organizational structure, leadership, and processes that ensure IT support of the organization’s strategies and objectives. 2

Question 3 (4 marks)

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. Part of the process is to attest to the public that an organization's internal controls are effective. Internal controls can be expected to provide only a reasonable assurance, not an absolute assurance, to an entity's management and board 2

An organization must ensure that its financial statements comply with Financial Accounting Standards (FAS) and International Accounting Standards (IAS) or local rules via policy enforcement and risk avoidance methodology called "Internal Control." There must be a system of checks and balances of defined processes that lead directly from actions and transactions reporting to an organization's owners, investors, and public hosts. 2

Question 4 (6 marks)

Steps in Information System Audit can be categorized into six stages as described below: 1

1. Scoping and pre-audit survey: Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

2. Planning and preparation: During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix. 1

3. Fieldwork: Gathering evidence by interviewing staff and managers, reviewing documents, and observing processes etc. 1

4. Analysis: This step involves desperately sorting out, reviewing and trying to make sense of and analysing all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis. 1

5. Reporting: Reporting to the management is done after analysis of evidence gathered and analyzed 1

6. Closure: Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits. 1

Question 5 (4 marks)

Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls.
This involves the following:
1. Risk assessment: The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
2. Controls assessment: The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
3. Planning for review of physical access controls: It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

Question 6 (4 marks)

Yes Mr A can be prosecuted under Sec 67 of ITAA 2008.	1
Section 67 says that Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees	3

Question 7 (8 marks)

1. Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.	1
The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. Service Design is not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels. It also provides guidance on the development of design capabilities for service management.	1
1. Service Catalogue Management: Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.	1/2

2. Service Level Management: Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs). Service-Level Management is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be; liaising with availability management, capacity management, incident management and problem management. 1/2

3. Availability Management: Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations. Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time 1

4. Capacity Management: Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modelling; capacity planning; resource management and performance management. 1

5. IT Service Continuity Management: IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs. 1

6. Information Security Management: A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability. 1/2

7. Supplier Management: The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination. 1/2

Question 8 (6 marks)

The cloud computing environment consists of multiple types of cloud based on their deployment and usage. 2

Different types of clouds are as follows:

• Public Clouds: They can be used by general public such as individuals, corporations, etc.
o They are administered by third parties or vendors over the internet
o Services are offered on 'Pay per use' basis
o These are also called as provider clouds
o Business models like SaaS and public clouds complement each other

o Advantages – Widely used in development, deployment and management of enterprise applications at affordable costs. Allows organizations to deliver highly scalable and reliable application rapidly.
o Limitations – Security and trust issues between clients and cloud providers. Assurance building is liable to happen but at a slow pace.

• Private Clouds: They reside within the boundaries of an organization and are used exclusively for its benefits. 2
o Also called as internal clouds
o They are built primarily by IT teams within enterprises who seek to optimize utilization of infrastructure resources
o They provide applications using concepts of grid and virtualization
o Advantages- Improve average server utilization. Allow usage of low cost hardware while providing higher efficiency and cost reduction. Reduction of operational costs and administrative overheads due to high levels of automation.
o Limitations- IT teams may have to invest in buying, building and managing clouds independently.

• Hybrid Clouds: It is a combination of both atleast one private and atleast one public cloud computing environment. 2
o Usually consists of infrastructure platforms and applications
o It is offered in two ways
§ A vendor has private cloud and forms partnership with public cloud provider or
§ Public cloud provider forms partnership with a vendor providing private cloud platform

Question 9 (6 marks)

Major categories of Social Networks are given below: 3

- Social contact networks: Formed to keep in touch with friends and family. These have become most popular today. Eg: Facebook & Twitter
- Study Circles: These are dedicated for students having areas for study topics, placement related queries, advanced research, etc. Eg: College tonight
- Networks for Socialist groups: Specifically designed for core field workers like doctors, scientists, engineers, etc. Eg: LinkedIn
- Network for Fine Arts: These are dedicated for people linked with music, painting and related arts.

- Police and Military Networks: These networks, though not in public domain, operate much like social networks on a private domain due to confidentiality of information. 3
- Sporting Networks: Dedicated to people of Sporting fraternity and have information related to this field
- Mixed networks: These are networks which have subscription of people from all above groups and are heterogeneous networks serving multiple types of social collaboration.
- Networks for inventors: These are networks for people who have invented concept of social networks. Eg: Technical forums and Mashups
- Shopping and utility networks: These are networks which analyse social behavious and send related information to respective marts and stores.

Question 9 (3 marks)

Green IT refers to the study and practice of establishing/using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them and the problems of disposing them at the end of their life cycle. 1 1/2

Green computing is the environmentally responsible use of computers and related resources. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

One of the earliest initiatives towards Green Computing in the US was the voluntary labeling program known as “Energy Star”. This label became a common sight especially in notebook computers and displays. Government regulation, however well-intentioned, is only part of an overall green computing philosophy.

The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following: 1 1/2

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
- Power-up and power-down energy-intensive peripherals such as laser printers according to need.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.
- Dispose of e-waste according to central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centers.

****