5.2 Related Terms

Various terminologies related to risk assessment are given as follows:

Asset: Asset means which carries some value for the organization; e.g., information in electronic or physical form, employee, etc.

Irrespective of the nature of the assets they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form part of organization's corporate identity, without which, the organization may be threatened.
- Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

Vulnerability: Vulnerability is the weakness in the system security that exposes the system to threats. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Missing safeguards often determine the level of vulnerability. To determine vulnerabilities, it involves evaluation of the system's security Including inspection of safeguards, testing, etc.

Simply, vulnerability is the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from weak software's design, defects in its implementation, or problems in its operation. Normally, vulnerability allows any of the following condition*:*

- Allows an attacker to execute programs as another user or
- Allows an attacker to access data which has specified access restrictions or
- Allows an attacker to pose as another entity.

Threat: Any circumstance or event which has the potential to cause harm to the software system through unauthorized access, destruction, modification, and/or denial of service is called a threat. A **threat** is an action, event or condition which can compromise the system in its quality and ability to inflict harm to the organization.

Threat attacks the system with the intent to cause harm to it. Threat should be analysed with a list of known threats and vulnerabilities found in similar systems. Every data is an asset to an organization and threat always prevail over the assets. Therefore, assets and threats are closely correlated. Threats can be minimised by applying some sort of protection to assets.

Attack: ***An attack is an attempt to gain unauthorized access into the system or to compromise the system's dependability. In software terms it means an intentional fault with the intent of exploiting vulnerability in the system.***
Attack is a set of actions designed to overcome confidentiality, integrity, availability of an information system.

Risk: Risk can be defined as the potential harm to a system if a particular threat materialize and risk analysis means the process of identifying risks to a system and determining their impact on an organization. Risk assessment includes the followings:

- ***Identification of threats and vulnerabilities in the system;***
- ***Potential harm to an enterprise operations or enterprise assets if threat exploits an identified vulnerability; and***
- ***The identification of security controls for the information system.***

5.3 Threats to the Computerized Environment

Any computerized environment is dependent on people. As a result threats emanate from people themselves. Threats also arise

on account of dependence on external agencies, various vendors and service providers, etc. Therefore it is necessary that IT team must deliver the system as per users' requirements. A few common threats to the computerized environment can be:

- **Theft or destruction of computing resources:** Since the computing equipments form the backbone any theft or destruction of the resource will results in damage to the organization.
- **Communication failure:** Failure of communication lines result in inability to transfer data which primarily would have travelled over communication lines. Eg., Call Centers.
- **Power failure:** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- **Fire, etc:** Fire may cause due to electric short circuit or due to riots, war or such other reasons which can cause irreversible damage to the IS infrastructure.
- **Disgruntled employees:** A disgruntled employee presents a threat since he can access sensitive information of the organization and can cause intentional harm to the organization.
- ***Errors and Omissions: Errors and omissions are important threats to data and system integrity. These errors are caused by all types of users, who create and edit data. Many programs lacks quality control measures and therefore they cannot detect all types of input errors or omissions. A sound awareness and training program can help an organization to reduce the number and severity of errors and omissions.***
- **Malicious code:** Malicious code such as viruses and worms which freely access through unprotected networks may affect organization and business networks.
- **Abuse of access privileges by employees:** The security policy of the company should authorize employees based on their job responsibilities to gain access and execute select functions in critical applications otherwise it will harm the organization.
- **Natural Disasters:** Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the Information System operations.

5.4 Threats Due to Cyber Crimes

Following are the major threats due to cyber crimes:

- **Embezzlement**: It is unlawful misappropriation of money or other things by the person to whom it was entrusted for his/her own use.
- **Fraud**: It occurs on account of intentional misrepresentation of information to deceive others, or the use of electronic means to transmit deceptive information, etc. Fraud may be committed by someone who is either inside or outside the company.
- **Theft of proprietary information**: means illegally obtaining of designs, plans, blueprints, codes, trade secrets, graphics, copyrighted material, data, files, lists, and personal or financial information usually by electronic copying by the competitors.
- **Computer virus**: A computer virus is a computer program that can harm a computer without the permission or knowledge of the user.
- **Other**: Threat includes several other cases such as intrusions, breaches of the computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained or not.
- **Denial of Service (DoS): An action which prevents access to the system or delays critical operations is termed as 'DoS'.** There can be disruption or degradation of service which is dependent on external sources. Eg: Problems may erupt through internet connection resulting in interruption of flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

5.6 Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information and helps in deciding countermeasures (safeguards and controls)to reduce risk to an acceptable level (i.e. residual risk), based on the value of the information.

An organization can also choose to reject risk by ignoring it, which can be dangerous depending upon the type of project. Normally, IS Auditor put a red flag on such conditions.

Risks may be classified as systematic and unsystematic risks:

Systematic Risk	**Unsystematic Risk**
Systematic risks are unavoidable risks.	Unsystematic risks are those risks which are peculiar to the specific applications or technology.
For example the probability of power outage is not dependant on the industry but is dependant on external factors.	For example one can use automatic mirroring to reduce the exposure of data loss in the event of failure of host computer.
No matter what technology is being used systematic risks would remain.	These risks can be generally mitigated by using an advanced technology or system.
Systematic risks can be reduced by designing management control process but does not involve any technological solutions. Thus there would not be any additional payment for technological solution to the problem.	Thus by making additional investment one can mitigate these unsystematic risk.

The management issue would be whether the additional payment to mitigate the risk is justifiable. The answer will be whether the overall risk exposure of the organization is coming down due to the additional investment.

Every business has its own inherent risk - the cost of running the business. The issue is how much risk is acceptable and what is the price to reduce a certain part of the risk. For this, measuring risk is essential through the process of risk and exposure measurement. Risk appetite of the organization should also be considered i.e., does it want to be risk aggressive or risk averter. For example, the risk appetite of risk aggressive bank may be far lower than that of a risk averse foreign exchange dealer.

5.9 Risk Mitigation

The purpose of risk identification and analysis is to prepare for risk mitigation. Risk Mitigation means a systematic reduction in exposure to a risk or likelihood of its occurrence. A causal understanding is required to manage and control risks. Knowing '*what causes what*' will give an understanding of risk and helps to implement the necessary controls. Simple cause and effect relationships are known from experience, but more complex situations cannot be handled through information at hand. Cause models help in the implementation of risk mitigation measures and identify the events and their impact on losses.

CA FINAL PAPER 6: ISCA

AMENDMENT APPLICABLE FOR NOV13

COMPLILED BY JIGNESH CHHEDA

8.3 ISO 27001 – Information Security Management Standard

ISO 27001 is the international best practice and standard for an Information Security Management System (ISMS). An ISMS is a systematic approach for managing confidential information so that it remains secure. It encompasses people, processes and IT systems.

ISO 27001 defines how to organise information security in any kind of organization and therefore different security should be prioritized to ensure overall effectiveness. ISO 27001 is for information security; the same thing that ISO 9001 is for quality.

Today ISO 27001is been taken as a basis for drawing up different regulations in various fields like personal data protection, protection of confidential information, protection of information systems, etc.

8.3.1 Four phases of ISMS: ISO 27001 prescribes 'how to manage information security through a system of information security management'. It consists of four phases which should be continuously implemented in order to minimise risks to the information.

These phases are given as follows:

- The Plan Phase – This phase plans basic requirement of information security, set objectives for information security and choose the appropriate security controls accordingly.
- The Do Phase – This phase carries out activity that was planned in the previous phase.
- The Check Phase – This phase monitors the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
- The Act Phase – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The detail description of all these afore mentioned phases is given as follows:

(i) The Plan phase

The Plan phase consists of the following steps:

- Determining the scope of the ISMS;
- Writing an ISMS Policy;
- Identifying the methodology for risk assessment and determining the criteria for risk acceptance;
- Identification of assets, vulnerabilities and threats;
- Evaluating the size of risks;
- Selection of controls for risk treatment;
- Obtaining management approval for residual risks;and
- Obtaining management approval for implementation of the ISMS;

(ii) The Do phase

This phase consists of the following activities:

- Writing a risk treatment plan which describes budget within which controls should be implemented;
- Implementing the risk treatment plan;
- Implementing applicable security controls;
- Determining how to measure the effectiveness of controls;
- Carrying out awareness programs and training of employees; and
- Implementation of procedures for detecting and managing security incidents.

(iii) The Check phase

This phase includes the following:

- Regular reviews of the effectiveness of the ISMS;
- Measuring the effectiveness of controls;
- Reviewing risk assessment at regular intervals;
- Reviewing internal audits at planned intervals;
- Management reviews to ensure that the ISMS is functioning properly and to identify opportunities for improvement; and
- Keeping records of activities and incidents that may affect the effectiveness of the ISMS.

(iv) The Act phase

This phase includes the following:

- Implementation of identified improvements in the ISMS;
- Taking corrective and preventive action;
- Communicating activities and improvements to all stakeholders; and
- Ensuring that improvements achieve the desired objectives.

8.4 Capability Maturity Model (CMM)

8.4.2 Five Levels of Software Process Maturity :

There are five levels defined along the continuum of the model:

- Initial - the starting point for use of a new or undocumented repeat process;
- Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted;
- Defined - the process is defined/confirmed as a standard business process;
- Managed'- the process is quantitatively managed in accordance with agreed-upon metrics; and
- Optimizing - process management includes deliberate process optimization/improvement.

(i) Level 1 - The Initial Level: Processes at this level are undocumented and tend to have dynamic change and thus gets negative reaction from the users. This provides an unstable environment for the processes.

(ii) Level 2 - The Repeatable Level: At this level some processes with consistent results are repeated. Process discipline is not likely to be same for all projects but where it is same then it may be helpful to ensure that existing processes are performed during times.

(iii) Level 3 - The Defined Level : At this level standard processes are defined and documented subject to some degree of improvement over time. These standard processes help consistent process performance across the organization.

(iv) Level 4 - The Managed Level : At this level management identifies ways to adjust and adapt the process for a particular projects without measuring deviations from specifications. Process Capability is established from this level.

(v) Level 5 - The Optimizing Level : At this level, focus is on continually improving process performance through both incremental and innovative technological improvements.

8.5 COBIT – IT Governance Model

COBIT is an IT governance framework that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout the organizations.

8.5.1 Need for Enterprises to Use COBIT 5: Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 addresses these critical business issues by creating optimal value for their information and thus provide tools to make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT;
- Reduced IT-related risks and compliance with laws, regulations and contractual requirements.
- The development of more business-focused IT solutions and services.
- Increased enterprise wide involvement in IT-related activities.

8.5.2 Benefits: COBIT 5 helps enterprises of all sizes to:

- maintain high-quality information to support business decisions;
- achieve strategic goals and realize business benefits through effective use of IT;
- achieve operational excellence through reliable, efficient application of technology;
- maintain IT-related risk at an acceptable level;
- optimize the cost of IT services and technology; and
- support compliance with relevant laws, regulations, contractual agreements and policies.

Customising COBIT as Per Need: COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture.

Because of its open design feature, it can be applied to meet needs related to:

- Information security,
- Risk management,
- Governance and management of enterprise IT,
- Assurance activities,
- Legislative and regulatory compliance, and
- Financial processing or CSR reporting.

Five Principles of COBIT 5: COBIT 5 simplifies governance challenges with just five principles and seven enablers. These five key principles builds an effective governance and management framework and these principles are as follows:

Principle 1: Meeting Stakeholder Needs

Enterprises goal is to create value for their stakeholders by maintaining a balance between the risks and benefits. Thus, COBIT 5 provides all required processes to support value creation goal through the use of IT. COBIT 5 can also be customized as per customer requirements.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 covers all functions and processes within the enterprise and does not focus only on the 'IT function', but also treats related technologies as an assets. It considers all IT related enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone—internal and external—which is relevant to enterprise information and related IT.

Principle 3: Applying a Single Integrated Framework

There are many IT-related standards and best practices, each providing their own guidance on IT activities. However, COBIT 5 is a single and integrated framework which also aligns with other latest relevant standards and frameworks, and thus provides a complete enterprise coverage to integrate effectively which other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach ie., it should also take several other components into account. COBIT 5 defines a set of enablers to support the implementation of a system for enterprise IT.

Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between **governance and management**.

- **Governance:** ensures that stakeholder needs are evaluated, enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance against set direction and objectives. In most enterprises, overall **governance is the responsibility of the board of directors.**
- **Management:** Management plans and monitors whether activities are in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management.

COBIT 5 Enablers: Enablers are factors that influence whether something will work in this case or not. Enablers are driven by the goals cascade, i.e., what the different enablers should achieve.

The COBIT 5 framework describes seven categories of enablers:

- **Principles, policies and frameworks** translates the desired behaviour into practical guidance for day-to-day management.
- **Processes** describe an organised set of practices and activities to achieve certain objectives and to derive output supporting overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, ethics and behaviour of individuals** and of the enterprise are very often underestimated as a success factor in governance and management activities.
- **Information is pervasive throughout organisation.** Further, information is required to keep organisation running, however at operational level, information is key product of the enterprise itself.
- **Services, infrastructure and applications** include the infrastructure, technology and applications which provides enterprise with information technology processing and services.
- **People, skills and competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

CoCo

The Criteria of Control (CoCo) model was published in 1995 by the Canadian Institute of Chartered Accountants. This model is build on COSO and therefore CoCo can be said to be a concise superset of COSO. CoCo is more concrete and

user-friendly. CoCo is a "guidance" which means that it is not intended as "minimum requirements" but rather as "useful in making judgments". As such CoCo can be seen as a model of controls for information assurance rather than a set of controls. CoCo's generality is one of its strengths. The objectives of COCO are:

- effectiveness and efficiency of operations,
- reliability of financial reporting,
- compliance with applicable laws and regulations.

objectives.

Four important concepts about "control" are as follows:

- Control is affected by the people throughout the organization including the board of directors, management and all other staff.
- People who are accountable for achieving objectives should also be accountable for the effectiveness of control.
- Organizations are constantly interacting and adapting.
- Control can be expected to provide only reasonable assurance, not absolute assurance.

ITIL (IT Infrastructure Library)

The Information Technology Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) which focuses on aligning IT services with business needs. ITIL is published in a series of five core publications in its current form which describes procedures, tasks and checklists those are not organization-specific for establishing a minimum level of competency. It also allows organization to establish a baseline from which it can plan, implement, and measure.
Today, IT services are more closely aligned and integrated with the business and therefore ITIL assists in establishing a business management approach and discipline to IT Service Management by providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services.

The 5 phases of ITIL are as follows:

- *Service Strategy,*
- *Service Design,*
- *Service Transition,*
- *Service Operation, and*
- *Continual Service Improvement.*

8.7.1 Details of the ITIL Framework: ***Details of these aforementioned volumes are given as follows:***

Service Strategy:

Service Strategy deals with the strategic management approach in respect of IT Service Management as well as strategic analysis, planning and implementation of service models, strategies, and strategic objectives. It provides guidance on how to improve service management capabilities to effectively deliver value to the customers and also illustrate value for service providers.

Service Design:

CA FINAL PAPER 6: ISCA

AMENDMENT APPLICABLE FOR NOV13

COMPLILED BY JIGNESH CHHEDA

Service Design translates strategic plans and objectives and creates the designs and specifications as per requirements for execution through service operations. It provides best feasible combination of infrastructure, applications, systems, and processes, along with suppliers for service offerings.

Service Transition:

Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.
Service Transition provides guidance on managing the complexity of changes to services and processes to prevent undesired consequences whilst permitting for innovation. It also provides guidance on transferring the control of services between customers and service providers.

Service Operation: Service Operation provides guidance on the management of a service for its day-to-day operation as well as for supporting operations through new models like shared services, web services mobile commerce, etc.
Service Operation provides detailed guidelines on processes, methods and tools in addressing the proactive and reactive control perspectives. Managers are provided with knowledge to enable them to make better informed decisions in areas such as managing the availability of services, optimizing capacity utilization, fixing problems, etc.

Continual Service Improvement: Continual Service Improvement measures the service performance through service life-cycle and suggests improvements to ensure that a service delivers the maximum benefit.
It combines methods from change management, quality management, and capability improvement to achieve significant improvements in service quality and business continuity.

SA 402 (Revised)

Audit Considerations Relating to an Entity using Service Organization, SA 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002. The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor.
This SA is effective for audits of financial statements w.e.f. April 1, 2010. Details of this standard are discussed in the study material of Advance Auditing paper at final level of CA Curriculum.