- **Issuer distinguished name :** The name of the entity issuing the certificate (usually a certificate authority).
- **Validity period of the certificate :** Start/end date and time.
- **Subject distinguished name :** The name of the identity the certificate is issued to.
- **Subject public key information :** The public key associated with the identity.
- Extensions (optional)

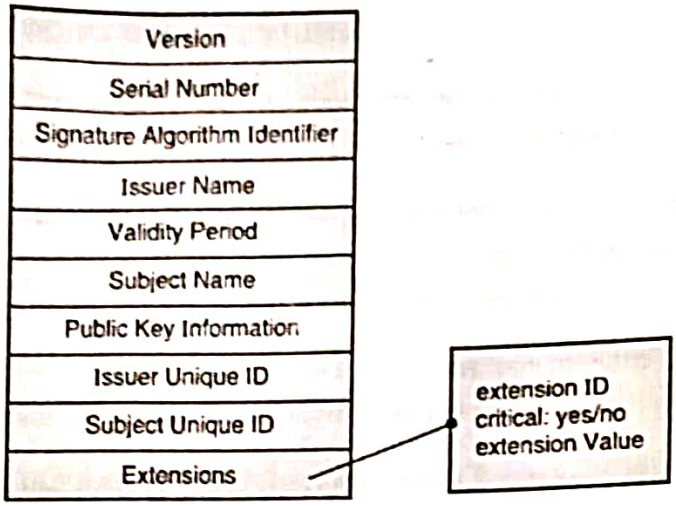

Fig. 5.4.3 : Certificate Format

5.5 Cyber Crime

MSBTE : S-17, W-17, S-18, W-18, S-19

Q.	Explain the process of cyber crime investigation.	**(S-17, S-19, 4 Marks)**
Q.	Describe in brief Cyber Crime. List different types of Cyber Crime.	**(W-17, S-18, 4 Marks)**
Q.	Define term Cyber crime.	**(W-18, 2 Marks)**

5.5.1 Introduction

- Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet and the worldwide web.
- **Cybercrime,** also known as **computer crime,** it uses a computer as an instrument for the further illegal things, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.
- Because of wide use of Internet, Cybercrime has grown in importance as the computer has become central to commerce, entertainment, and government.
- Mostly the cybercrime is an attack on data or information about individuals, corporations or governments. Generally the attacks do not take place on a physical body but it will be on the personal or corporate virtual body that means a set of informational attributes which define people and institutions etc. on the Internet.

- In the digital world any person's virtual identities are important elements-information about individuals can be used in multiple computer databases owned by governments and corporations.

- Cybercrime ranges across a variety of activities. At one end are crimes that involve fundamental violation of personal or corporate privacy, such as physical attacks on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual.

- Also at this end of the spectrum is the growing crime of identity theft. There are transaction based crimes like - fraud, pornography, digital piracy, money laundering, and counterfeiting.

- Some crimes are specific crimes with specific victims, but the criminal hides it in the relative anonymity which is provided by the Internet.

- Another part of this type of crime involves individuals within corporations or government organizations deliberately altering data for either profit or political objectives.

- There are other crimes that involve attempts to disrupt the actual workings of the Internet.

1. **Financial :** This crime disrupt businesses ability to conduct 'e-commerce'.
2. **Piracy :** This is related to the act of copying copyrighted material. The personal computer and the Internet both offer new way for an 'old' crime. Online theft is known as any type of piracy or private data that involves the use of the Internet to market or distribute creative works protected by copyright.
3. **Hacking :** This crime is related to the act of gaining illegal access to a computer system or network and some time making unauthorized use of such access. Also, it is the act by which other forms of cyber-crime like fraud, terrorism, etc. are committed.
4. **Cyber-terrorism :** The main outcome of acts of hacking is designed to cause terror. E-terrorism is the result of hacking which will cause violence against persons or property, or at least cause enough harm to generate fear like other conventional terrorism.
5. **Online Pornography :** There are laws against possessing or distributing child pornography. Distributing pornography of any form to a minor is illegal. The Internet is merely a new medium for this 'old' crime, but how best to regulate this global medium of communication across international boundaries and age groups has sparked a great deal of controversy and debate.
6. **Sabotage :** It is another type of hacking involves the hijacking of a government or corporation Web site. It means a purposeful destruction of property or slowing down of work with the intention of damaging a business or economic system or weakening a government or nation in a time of national emergency.

5.5.2 Hacking

MSBTE : S-17, W-17, S-18, W-18, S - 19

Q.	Define Hacking. Explain different types of Hackers.	(S - 17, 6 Marks)
Q.	State the meaning of Hacking.	(W-17, S-18, 2 Marks)
Q.	Explain the concept of hacking.	(W-18, S-19, 4 Marks)

- Hacking is one of the most well-known types of computer crime. A hacker is someone who find out and exploits the weaknesses of a computer system or network.
- It is refers to the unauthorized access of another's computer system. These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan Horses that can shutdown or destroy an entire computer network.
- Hacking is also carried out as a way to take credit card numbers, internet passwords, and other personal information.
- By accessing commercial databases, hackers are able to steal these types of items from millions of internet users all at once.

There are different types of hacker :

(i) **White Hat :** This type of hackers is someone who has non-malicious purpose whenever he breaks into security systems. In fact, a large number of white hat hackers are security experts themselves who want to push the boundaries of their own IT security ciphers and shields or even penetration testers specifically hired to test out how vulnerable or impenetrable (at the time) a present protective setup currently is. A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.

(ii) **Black Hat :** This type of hackers is also known as a cracker and he has a malicious purpose whenever he goes about breaking into computer security systems with the use of technology such as a network, telecommunication system, or computer and without authorization. His malicious purposes can range from all sorts cybercrimes such as piracy, identity theft, credit card fraud, damage, and so forth. He may or may not utilize questionable tactics such as deploying worms and malicious sites to meet his ends.

(iii) **Grey Hat :** A grey hat hacker is a combination of both white hats and black hats. This is the kind of hacker that is not a penetration tester but will go ahead and surf the Internet for vulnerable systems he could exploit. Like a white hat, he will inform the administrator of the website of the vulnerabilities he found after hacking through the site. Like a black hat and unlike a pen tester, he will hack any site freely and without any prompting or authorization from owners what so ever. He will even offer to repair the vulnerable site he exposed in the first place for a small fee.

(iv) **Elite Hacker :** As with any society, better than average people are rewarded for their talent and treated as special. This social status among the hacker underground, the elite are the hackers among hackers in this subculture of sorts. They are the masters of deception that have a solid reputation among their peers as the cream of the hacker crop.

(v) **Script Kiddie :** A script kiddie is basically an part-time or non-expert hacker, who breaks into people's computer systems not through his knowledge in IT security and the ins and outs of a given website, but through the prepackaged automated scripts (hence the name), tools, and software written by people who are real hackers, unlike him. He usually has little to know knowledge of the underlying concept behind how those scripts he has on hand works.

5.5.3 Digital Forgery

- Forgery has been defined as the crime of falsely altering or manipulating a document with the intension of misleading others. It may include the production of falsified documents or counterfeited items. Today, we live in the digital era, where digital technology has become predominant technology for creating, processing, transmitting, and storing information.
- Digital forgery is falsely altering digital contents such as pictures, images, documents, and music perhaps for economic gain. It may involve electronic forgery and identity theft. The majority of digital forgery occurs because digitally altered pictures often appeal to the viewer's eyes. And with the availability of powerful, affordable picture-processing software (such as Adobe Photoshop, Adobe Premiere, Corel Draw, or GIMP), one can alter almost anything in a photo. For example, images of children (child pornography) involved in sexually explicit conduct can be created from innocent images, or even without the involvement of an actual child.
- Digital techniques are notoriously more precise than conventional means of retouching because any area of the photo can be changed pixel by pixel. It is hard for humans to spot images that have been doctored in some way. Thus the common saying "seeing is believing" is no longer true in this digital age.
- It may involve electronic forgery and identity theft.
- The majority of digital forgery occurs because digitally altered pictures with the availability of powerful and affordable picture processing software (such as Adobe Photoshop, Adobe Premiere, Corel Draw, or GIMP).

5.5.4 Cyberstalking or Harassment

- Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities.
- This kind of cybercrime involves online harassment where the user is subjected to a use online messages and emails.
- Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear.
- Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety. Most of the victims of cyberstalking are women and children.

5.5.5 Cyber Pornography

MSBTE : S-17, W-18

Q. What is pornography ? **(S-17, W-18, 4 Marks)**

- The crime of child pornography includes the possession, production, distribution or sale of pornographic images or videos that exploit or portray children. In some cases writing can be considered a form of child pornography.
- Images of children involved in explicit sexual behaviour are, child pornography, but sexual activity does not have to be pictured for the images to be considered pornographic.
- In some rules, images depicting children nude or in erotic poses can be considered child pornography.

- In pornography where photographs of real children are altered to make it appear that, they are involved in sexual activity or photographs.

5.5.6 Identity Theft and Fraud

- **Identify theft** is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft and criminals can steal money.
- **Fraud** is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

5.5.7 Cyber Terrorism

- Cyber terrorism is any planned, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.
- Cyber terrorist attacks are explicitly designed to cause physical harm to individuals.
- Cyber terrorist will target the banking industry, military installations, power plants, air traffic control centers and water systems.
- Cyber terrorism can be carried out over private computer servers, against devices and networks visible through the public internet as well as against secured government networks or other restricted networks.
- Hackers who break into computer systems can introduce viruses to vulnerable networks, deface websites, launch denial-of-service attacks and/or make terroristic threats electronically.
- **For Examples :**
  - Global terror networks disrupting major websites to create public inconveniences or to stop traffic to websites that publish content the hackers disagree with.
  - International cyber terrorists accessing and disabling or modifying the signals that control military technology.
  - Cyber terrorists targeting critical infrastructure systems. For example, to disable a water treatment plant, cause a regional power outage, or disrupt a pipeline, oil refinery or fracking operation. This type of cyber attack could disrupt major cities, cause a public health crisis, endanger the public safety of millions of people as well as cause massive panic and fatalities.

5.5.8 Cyber Defamation

- The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person.
- The injury can be done by words oral or written, or by signs or by visible representations.

- The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public.
- **Cyber defamation** is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.
- The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world.
- Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published.
- The following are mediums by which cyber defamation can be committed :
  - World Wide Web
  - Discussion groups
  - Intranets
  - Mailing lists and bulletin boards
  - E-mail

5.6 Cyber Laws

5.6.1 Introduction and Need

- Cyber law is a term used to describe the legal issues related to use of communications technology.
- Cyber law is the rule which controls the conduct of the cyber activity and the security under the cyber space.
- Cyber law is the law related to the cyber space which includes computers, networks, software, data storage devices, the Internet, websites, emails and electronic devices like cell phones, ATM machines etc.
- It is less of a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction.
- In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet.
- The ITAct, 2000 is an act that has been made punishable. The main objective of this Act is to create a environment where Information Technology can be used safely.
- In India, The IT Act, 2000 as altered by The IT Act, 2008 is known as the Cyber law. It has a separate chapter entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

- Cyber law includes laws relating to :
  - Cyber Crimes
  - Intellectual Property
  - Data Protection and Privacy
  - Electronic and Digital Signatures

5.6.2 Categories

Cyber crimes can be divided into three major categories :

(i) Crime against Individual

These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

(ii) Government

When a cyber crime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

(iii) Property

Some online crimes occur against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.

5.7 Compliance Standards

- Information security plays an important role in protecting the data and assets of an organization. Hence organizations need to be fully aware of the need to devote more resources to the protection of information and its assets. Information security must become a top concern in government as well as business.
- To address the situation, a number of governments and organizations have set up benchmarks, standards and legal regulations on information security to help ensure an adequate level of security is maintained, resources are used in the right way, and the best security practices are adopted.
- Some industries like banking are regulated, and the guidelines or best practices put together as part of those regulations often become a de facto standard among members of these industries.
- Good practices can always help to generate an effective service management system for a service provider. These are nothing but the things that can be applied to work to achieve effectiveness. Such good practice can come from many various sources and frameworks like – ITIL, COBIT and CMMI, standards like ISO/IEC 20000 and ISO 9000, and by sufficient knowledge of people and organizations.

5.7.1 Implementing and Information Security Management System (ISMS)

- When the part of the management system dealing with information security it is referred to as the Information Security Management System (ISMS).
- An Information Security Management System (ISMS) is a set of policies and procedures which specifies the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security.
- The main objective of ISMS is to provide systematic approach for managing an organization's sensitive information in order to protect it.
- ISMS involves the following essential components :
  - Personal
  - Processes
  - Information
- The goal of ISMS is to minimize risk and make sure business continuity by pro-actively limiting the impact of a security breach.
- It addresses employee behaviour and processes as well as information and technology. It can be targeted towards a particular type of data, such as customer data or it can be implemented in a comprehensive way that becomes part of the company's culture.

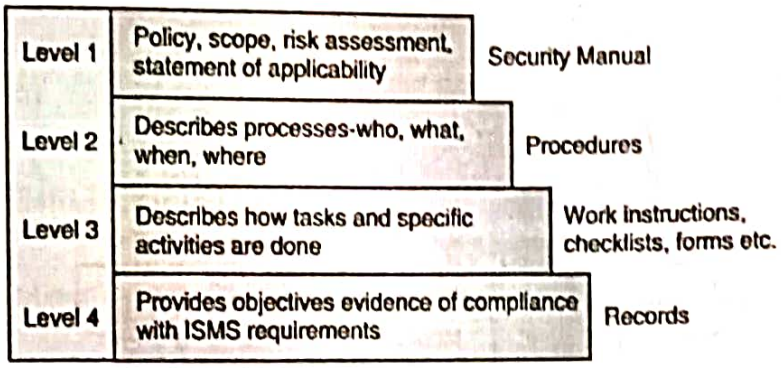

Fig. 5.7.1 : Four levels of documentation in ISMS

- Fig. 5.7.1 shows some basic measures that can be applied to achieve security of information system and threats to security should be controlled and managed by using broad security policy with the help of management.
- Organizations should identify the nature of possible threats to information system hence controls are used to ensure security of Information System.
- In organization, it is also necessary to ensure privacy, confidentiality of data stored in system; hence it is necessary to continually evaluate the controls by auditing process.

5.7.2 ISO 27001

MSBTE : W-17

Q. Describe ISO 27001. **(W-17, 4 Marks)**

The International Organization for Standard (ISO) is established in year 1997. It is non-governmental international body that collaborates with the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) on Information and Communication Technology (ICT) standards.

ISO 27001 describes following processes :

1. Definition of Information Security Policy
2. Definition of Scope of ISMS
3. Security Risk Assessment
4. Manage the identified risk
5. Select controls for implementation
6. Prepare SoA (Statement of Applicability)

ISO 27001 uses PDCA (Plan-Do-Check-Act) approach and this is used to improve the effectiveness of an organization.

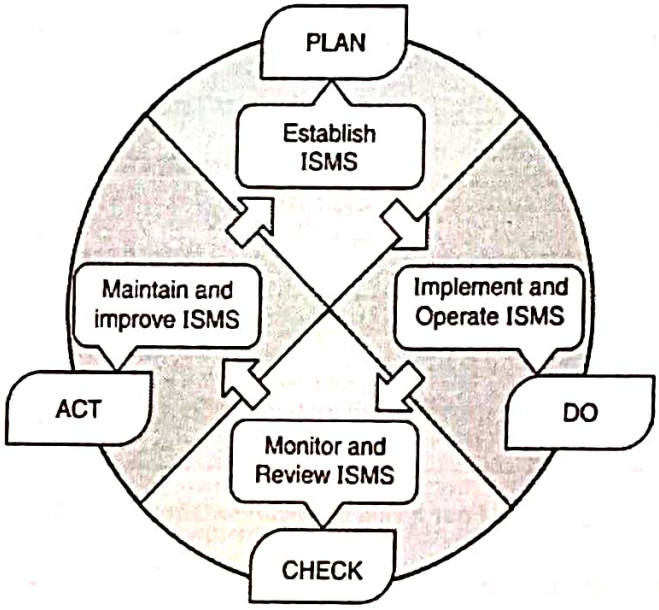

Fig. 5.7.2 : PDCA Model

1. **Plan :** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls.
   - Define the scope and policy of ISMS.
   - Identify the methodology for risk assessment and determine the criteria for risk acceptance.
   - Select controls for risk treatment.

2. **Do :** This phase includes carrying out everything that was planned during the previous phase.
   - Write and implement Risk treatment plan.
   - Implement applicable security controls.
3. **Check :** The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
   - Monitor different processes and take regular reviews of effectiveness of ISMS.
   - Conduct internal audits.
4. **Act :** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.
   - Implement identified improvements in ISMS.
   - Take corrective actions and preventive actions.
   - Communicate with stakeholders about activities and improvements.

ISO 27001 allows selection of objectives and controls of security which shows the unique security risks and requirements. This information is used to prepare SoA and then SoA is used to prepare Risk Treatment Plan. ISMS can be achieved by successful implementation of this plan.

5.7.3 ISO 20000

MSBTE : W-17

Q. Describe ISO 20000. **(W-17, 4 Marks)**

- ISO 20000 is an industry standard like ISO 9000/9001, and like ISO 9000/9001, ISO 20000 offers organizational certification.
- ISO 20000 standards shows IT how to manage and improve IT while establishing audit criteria. It also provides auditors with a documented standard to use for measuring IT compliance.
- The ITIL offers certifications for individuals but ISO 20000 is an organizational certification with international recognition.
- ISO 20000 was basically developed to use best practice guidance provided in ITIL framework. This standard was developed/ published in December 2005.
- ISO 20000 have two specifications.

o **ISO 20000-1** is the specification for Service Management. It defines the processes and provides assessment criteria and recommendations for those who are responsible for IT Service Management. Organizational certification uses this section.

- It includes following sections :
  1. Scope
  2. Terms and Definitions

3. Requirements for a Management System
4. Planning and Implementing Service Management
5. Planning and Implementing New or Changed Services
6. The Service Delivery Process
7. Relationship Processes
8. Resolution Processes
9. Release Process
10. Control Processes

- **ISO 20000-2** documents a "code of practice" that explains how to manage IT with regard to ISO 20000-1 audits.
- It includes all the sections from part 1 except requirements for a management system.
- Both ISO 20000-1 and ISO 20000-2 derive directly from the ITIL best practice.
- ISO 20000 groups the ITIL processes into following five core bundles :

Table 5.7.1 : ITIL processes

Service Delivery Processes	Relationship Processes	Resolution Processes	Control Processes	Release Process
Service Level Management Availability Management Capacity Management Continuity Management Budgeting Management Accounting/Financial Management Information Security Management	Business Relationship Management and Supplier Management	Incident Management Problem Management	Configuration Management Change Management	Release Management

Already, several governments have stated that ISO 20000 is a requirement for outsourced IT services. As the industry recognizes the value of ISO 20000, more and more companies will require their partners and vendors to reach ISO 20000 certification.

ISO 20000 also includes more than Service Delivery and Service Support. It includes sections on managing suppliers and the business; as well as Security Management.

ISO 20000 can assist the organization in benchmarking, its IT service management, improving its services, demonstrating an ability to meet customer requirements and create a framework for an independent assessment.

Some of the most common benefits of ISO 20000 certification for service providers are as follows :

1. It offers competitive differentiation by demonstrating reliability and high quality of service.
2. It gives access to key markets, as many organizations in the public sector mandate that their IT service providers demonstrate compliance with ISO/IEC 20000.
3. It provides assurance to clients that their service requirements will be fulfilled.
4. It enforces a measurable level of effectiveness and enforces a culture of continual improvement by enabling service providers to monitor measure and review their service management processes and services.
5. It drives down the costs of conformance to a large amount of system.
6. It helps leverage ITIL practices to optimize resources and processes.

5.7.4 BS 25999

- Business Continuity Management (BCM), the subject of British Standard BS 25999, is of real importance to organizations of all sizes, types, industry and location and to all staff members from Board directors, corporate executives and IT managers through to facilitate managers and business continuity professionals.
- Service disruptions, delays in responding to customer requests, the inability to process transactions in a timely manner, or being unable to resume business in the face of a disaster can all have significant impacts on an organization's effective operation.
- Natural disasters as well as terrorist activities have shown that an organization's resilience to disaster its ability to resume business quickly and efficiently were directly related to its preparedness to respond to unforeseen events.
- The BS 25999 standard is formed of two parts.
    - **BS 25999-1** is a Code of Practice for Business Continuity Management (BCM), took the form of general guidance on the processes, principles and terminology recommended for BCM. It was published by the British Standards Institution in December 2006.
    - **BS 25999-2** is a specification for a Management Scheme, specified a set of requirements for implementing, operating and improving a BCM System (BCMS). It was published in November 2007.

- Because of Part 2, organization can have their business continuity management arrangements independently certified by external auditors, thereby providing stakeholders, customers with a real degree of comfort.
- Both parts of the standard contributed significantly to the international standards that succeeded then and to the development of other national and international standards.
- Following are the benefits of implementation of a BCM in the organization :
  - Increased flexibility when faced with organizational threat.
  - Improved competence to maintain critical business services through action plan rehearsal.
  - Enhanced capability to handle disruption and protect brand reputation when integrated with business planning.
- For consumers it provides : Confidence and trust in the organization's brand because organization is using a consistent, standardized and robust method to assess, monitor and reduce the business risks.
- BS 25999 can be used by any organization that wants to ensure they are prepared to reduce and recover quickly from potential risks which may affect their business.

5.7.5 PCI DSS

- The Payment Card Industry Data Security Standard (PCI DSS) is administered by the PCI Security Standards Council.
- The purpose of the Standard is to decrease payment card fraud across the internet and increase credit card data security.
- Organizations that store transmit or process card holder data must comply with PCI DSS. Compliance is regulated and enforced by the 'acquiring bank' with which every organization must have a merchant account.
- The PCI DSS applies to any organization that processes, transmits or stores cardholder data.
  - **For Merchant :** The PCI DSS applies to Merchant. Even if merchant have subcontracted all PCI DSS activities to a third party, merchant have the responsibility for ensuring all the contracted parties are compliant with the standard.
  - **For Service Provider :** Including a software developer, the PCI DSS applies to service provider if he process, transmit or store cardholder data, or his activities affect the security of the cardholder data as it is being processed, transmitted or stored.
- IT Governance can advise on the applicability of the PCI DSS to the organization.
- The PCI DSS can apply across the whole of organization, or to a subset of the organization that transmits or stores the cardholder data away from the rest of the organization.
- It can apply to all people, processes and technologies that are involved in the processing, transmission or storage of cardholder data.
- It is not just the electronic systems but includes all systems including paper records such as receipts, mail order forms etc., and recordings of phone conversations if, they capture cardholder data being read out to call centre operators.

The Standard basically requires all applicable Merchants and Member Service Providers (MSPs) who are involved with the storage, processing or transmitting of cardholder data to.

1. Build the secure network using firewall etc and maintain it.
2. Protect the stored data of cardholder and transmission encryption to and from the data center across public networks.
3. Maintain a program for management of vulnerability using anti-virus software and using patches to secure system or application.
4. Implement strong access control by restricting the data access of cardholder, by using unique IDs and by Physical access restrictions to the data center and the managed servers.
5. Monitoring and testing networks on regular basis by logging and monitoring access to network resources / cardholder data and regular testing of security systems and processes.
6. There is a need for an up to date and detailed Information Security Policy hence maintains it.

5.7.6 ITIL Framework

MSBTE : S-17

Q. Describe ITIL framework. **(S - 17, 6 Marks)**

- In the early 1980s, the evolution of computing technology moved from mainframe-centric infrastructure and centralized IT organizations to distributed computing and geographically dispersed resources.
- While the ability to distribute technology provides more flexibility to the organizations, the side-effect was inconsistent application of processes for technology delivery and support.
- The UK government recognized that utilizing consistent practices for all aspects of an IT service lifecycle could assist in driving organizational effectiveness and efficiency, as well as achieving predictable service levels.
- It was this recognition that gave rise to ITIL, which has become a successful mechanism to drive consistency, efficiency and excellence into the business of managing IT services.
- ITIL is an approach to IT Service Management.
  - A **service** is something that provides value to customers. Services that customers can directly utilize or consume are known as business services.
  - **Service Management** is a set of specialized organizational capabilities for providing value to customers in the form of services.
- For example - Payroll is an IT service that is used to consolidate information, calculate compensation and generate pay cheque on a regular basis.
- In order for Payroll to run, it is supported by a number of technology or 'infrastructure' services. An infrastructure service does its work in the background, so that the business does not directly interact with it, but nevertheless this service is necessary as part of the overall value chain to the business service.

- 'Server administration', 'database administration' and 'storage administration' are all examples of infrastructure services required for the successful delivery of the Payroll business service.
- ITIL can be adapted and used in conjunction with other good practices such as :
  - COBIT (a framework for IT Governance and Controls)
  - Six Sigma (a quality methodology)
  - TOGAF (a framework for IT architecture)
  - ISO 27000 (a standard for IT security)
  - ISO/IEC 20000 (a standard for IT service management)
- IT organizations have traditionally focused on managing the infrastructure services and technology silos. ITIL suggests a more holistic approach to managing services from end to end.
- Managing the entire business service along with its underlying components in a cohesive manner ensures that every aspect of a service is considered so that the required functionality and service levels are delivered to the business customer.
- ITIL is organized around a service lifecycle which includes :

1. **Service strategy :** The lifecycle starts with service strategy, understanding who the IT customers are, the service offerings that are required to meet the customers' needs, the IT capabilities and resources that are required to develop these offerings, and the requirements for executing them successfully. Driven by strategy throughout the course of delivery and support for the service, the IT service provider must always try to ensure that the cost of delivery is consistent with the value delivered to the customer.
2. **Service design :** It ensures that new and changed services are designed effectively to meet customer expectations. The technology and architecture required to meet customer needs cost-effectively are an integral part of service design, as are the processes required to manage the services. Service management systems and tools to adequately monitor and support new or modified services must be considered, as well as mechanisms for measuring the service levels, the technology and the efficiency and effectiveness of processes.
3. **Service transition :** Through the service transition phase of the lifecycle the design is built, tested and moved into production to enable the business customer to achieve the desired value. This phase addresses managing changes - controlling the assets and configuration items (the underlying components such as hardware, software etc.) associated with the new and changed systems, service validation, and testing and transition planning to ensure that users, support personnel and the production environment have been prepared for the release to production.
4. **Service operation :** Once transitioned, service operation then delivers the service on an ongoing basis, overseeing the daily overall health of the service. This includes managing disruptions to service through rapid restoration after incidents; determining the root cause of problems and detecting trends associated with recurring issues; handling daily routine end-user requests and managing service access.
5. **Continual Service Improvement (CSI) :** CSI offers a mechanism for the IT organization to measure and improve the service levels, the technology and the efficiency and effectiveness of processes used in the overall management of services.

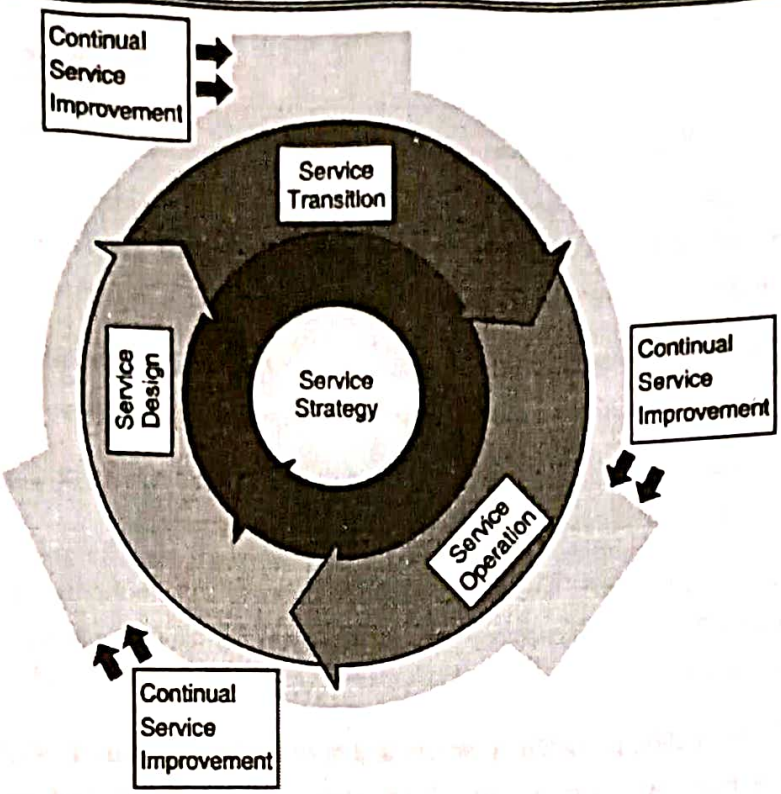

Fig. 5.7.3 : ITIL Service Life Cycle

- Following are the benefits to organization with ITIL framework :
  - Improve resource utilization
  - Be more competitive
  - Reduce re-work
  - Eliminate redundant work
  - Improve availability, reliability and security of business critical IT services.
  - Improve project deliverables and time-scales
  - Justify the cost of service quality
  - Provide services that meet or exceed business demands
- ITIL framework can be adopted by many types of companies like :
  - Large technological companies
  - Retailers
  - Financial Services Organizations
  - Entertainment
  - Manufacturing
  - Life Sciences companies etc.

5.7.7 COBIT Framework

MSBTE : S-17, W-17, S-18, W-18, S-19

Q. Describe COBIT framework with neat diagram. **(S-17, W-17, S-18, W-18, S-19, 6 Marks)**

- The Control Objectives for Information and related Technology (COBIT) is "a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered".
- COBIT is a framework developed by ISACA (Information System Audit and Control Association) in year 1996 for IT management and IT governance.
- COBIT is a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks.
- The main aim of COBIT is to research, develop, publicize and promote an authoritative, up to date, international set of generally accepted information technology control objectives for day to day use by business managers, IT professionals and assurance.
- In COBIT, a control is the policy, procedure, practices and organizational structures, which are designed to achieve reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
- Control objective is a statement of desired result or purpose to be achieved by implementing control procedures in a particular activity.

The COBIT framework is based on the following principle :

- To provide the information that the organization requires to achieve its objectives, the organization requires investing in and managing and controlling IT resources using a structured set of processes to provide the services which deliver the required enterprise information.

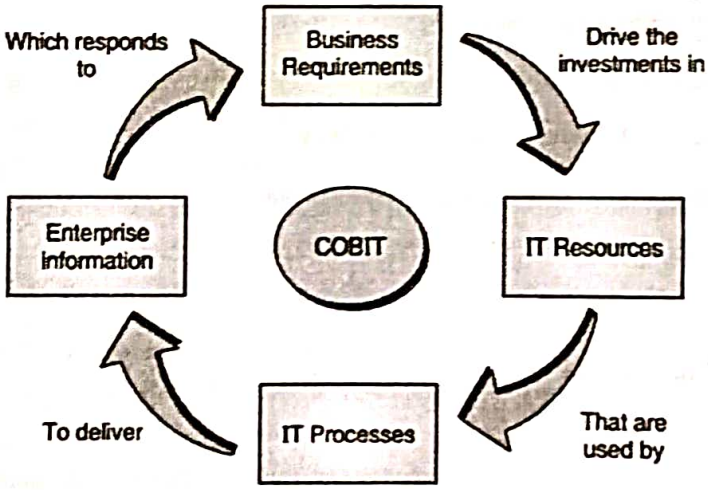

Fig. 5.7.4 : COBIT Framework Principles

- Managing and controlling information are at the heart of the COBIT framework and help to ensure alignment to business requirements.

Following are certain criteria that COBIT refers to as business requirements for information :

1. **Effectiveness :** It means that the information is relevant, timely, correct, consistent and applicable to the business process.
2. **Efficiency :** It means that the information is optimal for productive as well as economical use of resources.
3. **Confidentiality :** It means that the information is protected from unauthorized use.
4. **Integrity :** It means that the information is accurate and complete and valid for business.
5. **Availability :** It means that the information will be available whenever required by the business process.
6. **Compliance :** It means the information has fulfilled all laws, regulations and contractual arrangements, externally imposed business criteria as well as internal policies.
7. **Reliability :** It means that the information is appropriate for management to operate the entity and apply governance responsibilities.

- COBIT defines IT activities in a generic process model within four domains. These domains are 'Plan and Organize', 'Acquire and Implement', 'Deliver and Support', and 'Monitor and Evaluate'.
- The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities.
- The most necessary and early step towards good governance is use of an operational model and a common language for all different parts of the business in IT.
- COBIT will provide a structure to measure and monitor the performance of IT, communication with service providers and incorporation of best management practices.
- A process model encourages process ownership, enabling responsibilities and accountability to be defined.
- Following are the control objectives of COBIT which shows the requirements and resources of information :

(i) Quality control components show quality, cost as well as delivery of facility.

(ii) Fiduciary control components show efficiency, effectiveness and consistency of information as well as compliance.

(iii) Security control components shows security goals i.e. CIA.

To govern IT effectively, it is important to appreciate the activities and risks within it that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains are;

1. **Plan and Organize (PO) :** Provides direction to solution delivery (AI) and service delivery (DS). This domain typically addresses the following management questions;
   - Definition of strategic IT plan, Information architecture, IT organization and relationships.
   - Decide technology directions, assess the risks.
   - Manage IT investment, quality, project, HRs.
   - Make sure compliance with external requirements.
2. **Acquire and Implement (AI) :** Provides the solutions and passes them to be turned into services.
   - Recognize automated solutions.
   - Acquire and maintain application software and technology infrastructure.
   - Develop as well as maintain procedures and manage changes.
   - Install and credit the system.
3. **Deliver and Support (DS) :** Receives the solutions and makes them usable for end users.
   - Define service levels.
   - Manage service levels, third party services, performance, capacity, configurations, data, facilities, operations, problems and incidents.
   - Ensure security of system.
   - Educate and/or train the users, provide assistance and advise to users.
   - Recognize and allocate the cost.
4. **Monitor and Evaluate (ME) :** Monitors all processes to ensure that the direction provided is followed.
   - Monitor the process, assess internal control capability.
   - Find independent assurance.
   - Provide independent audit.

   COBIT supports IT governance by providing a framework to ensure that :

   (i) IT is aligned with the business.

   (ii) IT enables the business and maximizes benefits.

   (iii) IT resources are used responsibly.

   (iv) IT risks are managed appropriately.

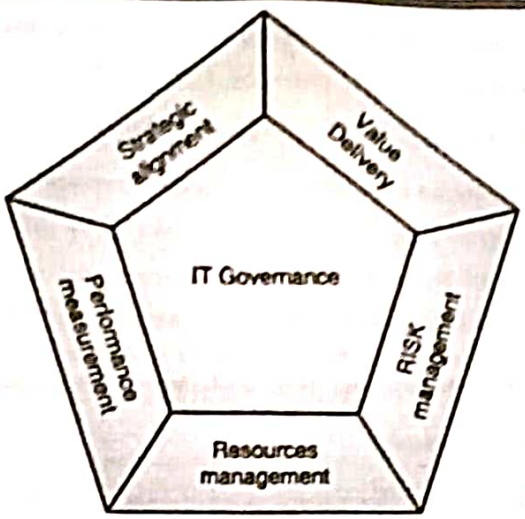

Fig. 5.7.5 : IT Governance domain

(i) **Strategic alignment :** It focuses on ensuring the connection of business and IT plans, defining and maintaining as well as validating the value of IT plans. It also focuses on aligning the operations between IT and enterprise.

(ii) **Value delivery :** It is related to the execution of the value plan during the delivery cycle. It also ensures that the IT delivers the assured benefits against the strategy. It concentrates on optimizing costs and proving the intrinsic IT value.

(iii) **Resource management :** It focuses on the best possible investments and the correct management for critical IT resources like applications, information, infrastructure and people.

(iv) **Risk management :** It focuses on risk awareness by senior management officers. It gives a clear understanding of risk of the enterprise. It focuses on compliance requirements, transparency of the major risks to the enterprise and implementation of risk management responsibilities into the organization.

(v) **Performance measurement :** It takes a follow up and monitors the strategic implementation, project completion, resource usage, process performance and service delivery.

- The most important part of IT governance which is supported by COBIT is Performance measurement. It contains setting and monitoring of measurable objectives like what is the requirement of IT processes to deliver and the way to deliver it.
- Many surveys have identified that the lack of transparency of IT's cost, value and risks is one of the most important drivers for IT governance. While the other focus areas contribute, transparency is primarily achieved through performance measurement.
- Operational management uses processes to organize and manage ongoing IT activities. COBIT provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model understandable to operational IT and business managers. The COBIT process model has been mapped to the IT governance focus areas providing a bridge between what operational managers need to execute and what executives wish to govern.

- To achieve effective governance, executives require that controls be implemented by operational managers within a defined control framework for all IT processes. COBIT's IT control objectives are organized by IT process therefore, the framework provides a clear link among IT governance requirements, IT processes and IT controls.
- COBIT is focused on what is required to achieve adequate management and control of IT, and is positioned at a high level. COBIT has been aligned and synchronized with other, more detailed, IT standards and good practices. COBIT acts as an integrator of these different guidance materials, summarizing key objectives under one umbrella framework that also links to governance and business requirements.
- The COBIT products have been organized into three levels designed to support :
  - Executive management and boards.
  - Business and IT management.
  - Governance, assurance, control and security professionals.
- Effective IT governance covers following key aspects :
  - WHAT type of decisions should be taken for effective management and use of IT?
  - WHO should take such type of decisions?
  - HOW to monitor the decisions taken?

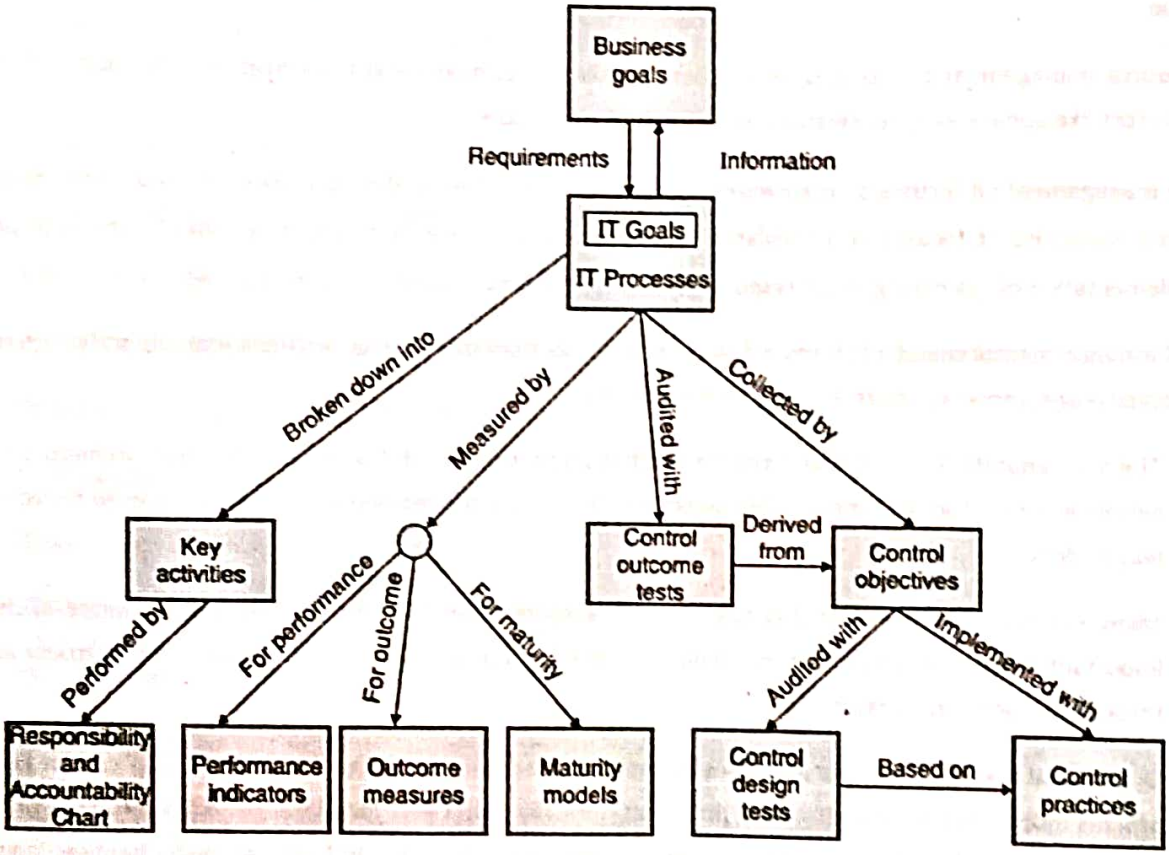

Fig. 5.7.6 : Inter relationship of COBIT components

- All of the COBIT components interrelate, providing support for the governance, management, control and assurance needs of the different audiences, as shown in Fig. 5.7.6.
- COBIT is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders.
- COBIT enables the development of clear policies and good practice for IT control throughout enterprises.
- COBIT is continuously kept up to date and harmonized with other standards and guidance. Hence, COBIT has become the integrator for IT good practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT.
- The process structure of COBIT and its high-level, business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT.
- The benefits of implementing COBIT as a governance framework over IT include :
  - Better alignment, based on a business focus.
  - A view, understandable to management, of what IT does.
  - Clear ownership and responsibilities, based on process orientation.
  - General acceptability with third parties and regulators.
  - Shared understanding amongst all stakeholders, based on a common language.
  - Fulfillment of the COSO requirements for the IT control environment.

Review Questions

Q. 1 What is Cybercrime? List different types of cyber crime.

Q. 2 Explain email security techniques (protocols).

Q. 3 What is IP Security ? Describe Authentication Header mode of IP Security.

Q. 4 How PGP is used for email security?

Q. 5 What is IP Security? Describe two modes of IP Security with suitable sketch showing modes.

Q. 6 How PEM is used for email security ?

Q. 7 Explain working of Kerberos with neat diagram.

Q. 8 Explain role of RA and CA in PKI.

Q. 9 Explain X.509 certificate format.

Q. 10 List and explain use of AS, TGS and SS in Kerberos.

Q. 11 Define following terms :

(a) Digital Forgery (b) Cyber Stalking

(c) Cyber Terrorism (d) Cyber Defamation

Q. 12 Describe various categories of cyber crime.

Q. 13 Explain, what is use of PCI DSS?

Q. 14 Explain ITIL framework in detail.

Q. 15 What are the four domains of the COBIT?

Q. 16 What is a control objective? Explain the structure of COBIT.

Q. 17 Explain ISO 27001 with PDCA approach.

Q. 18 Explain ISO 20000 with its two specifications.

Q. 19 Write a short note on BS25999.

□□□