CA Final ISCA

Super Summary 48 pages

alongwith marks allocation for last 5 attempts

By Aashish Mohtan

CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

1. Concepts of Governance
2. Risk Management
3. COBIT 5
4. Others

1. Concepts of Governance

① Governance
② Enterprise Governance
③ Benefits of Governance
④ IT Governance
⑤ GEIT
⑥ Corporate Governance, Enterprise Risk Mgt and Internal Controls.
⑦ IT steering Committee
⑧ IT strategy Planning.
⑨ Key Mgt. Practices for aligning IT strategy with enterprise strategy.
⑩ Business value from the use of IT.

① Governance:

Means & mechanisms
⇓ enable
multiple stakeholders
⇓
for
- evaluating options
- setting directions
- Monitoring (EDM)

compliance & performance.

② Enterprise Governance:

Responsibilities and practices
⇓ exercised by
The Board
- for providing strategic direction
- ascertaining that risks are managed appropriately
- verifying that the resources are used responsibly

Enterprise Governance has (two dimensions):

Corporate Governance (Conformance)

- system by which a co or enterprise is directed & controlled to achieve the objective of increasing shareholders wealth by enhancing economic performance
- it provides a historic view & focuses on regulatory requirements.

Business Governance (Performance)

- This dimension focuses on strategy and value creation for helping the board to make strategic decisions, understand risk appetite and key performance dimensions
- This performance dimension is pro-active & business oriented

③ Benefits of Governance:

AEIIOE

① Achieving enterprise Objectives
② Encouraging desirable behavior in the use of IT
③ Implementing & Integrating the desired process into the enterprise.
④ Improving business, customer, internal relationships.
⑤ Overcoming the limitations of organizational structure
⑥ Enabling strategically alligned decision making for the IT principles

④ IT Governance:

① Meaning
② Key practices to determine the status of IT Governance
③ Key benefits

① Meaning: Def: System in which directors evaluate, direct & monitor IT activities to ensure effectiveness, accountability & compliance of IT.

Objective: to achieve the strategic impact of IT.

② Key Practices to determine Status of IT Governance:

Decisions? — Who, How, What info, What mechanisms

How Exceptions handled?

How Governance results monitored?

Nov, 16 (4m)

③ Key benefits: Increased → user satisfaction with IT services.
→ value delivered through enterprise IT.

Improved → transparency.
→ compliance with relevant laws, regulations & policies.
→ agility in supporting business needs.
→ Mgt. and mitigation of IT related risk.

Nov, 15 (4m)

Nov, 14 (4m)

Nov, 16 (6m)

→ Better Cost performance of IT.
→ Optimal utilization of IT resources.
→ IT becoming an enabler for change rather than an inhibitor.

④ Governance of Enterprise IT (GEIT): ① Meaning ② Key Governance Practices ③ Key benefits

① Meaning Def: GEIT is a sub-set of corporate Governance and facilitates implementation of a framework of IS control within a enterprise.

Obj: to analyze and articulate the requirements of the governance of enterprise IT (GEIT).

② Key Governance Practices of GEIT: Evaluate, Direct, Monitor } Governance System

③ Key Benefits: ① Provides a consistent approach.
② Enables that IT related decisions are made in line with enterprise strategies & objectives.
③ Ensures that IT related processes are overseen effectively.
④ Confirms compliance with legal and regulatory requirements.
⑤ Ensures that Governance requirements for board members are met.

Provides, Confirms, Ensures — May 16 (4m)

⑥ Corporate Governance, Enterprise Risk Mgt and Internal Controls:

Best practices of Corporate Governance
① Clear assignment of responsibilities and decision making authorities
② Establishment of a mechanism for the interaction and cooperation among BOD, Senior mgt. & auditors
③ Implementing strong ICS
④ Financial and managerial incentives
⑤ Appropriate info flows internally and to the public

(ERM) → ERM is a process affected by an entity's BOD, Mgt and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite.

As per COSO, Internal control comp 5 Components
① Control Environment
② Control Activities
③ Risk Assessment
④ Info & Communicate
⑤ Monitoring

Nov 14 (6m)

⑦ IT steering Committee: Depending on the size and needs of the enterprise, the senior mgt may appoint a (high level committee) to provide appropriate direction to IT deployment and info system and to ensure that the IT deployment is in tune with the enterprise business goals and objectives. This committee is called IT-Steering Committee.

Functions:
① To ensure that the long and short range plans of the IT dept. are in tune with enterprise goals and objectives.
② To establish size and scope of the IT function and set priorities within the scope
③ To review and approve major IT deployment projects in all their stages.
④ To approve and monitor key projects by measuring result of IT projects in terms of return on invt.
⑤ To review the status of IS plans and budgets and overall IT performance
⑥ To review and approve stds, policies and procedures.
⑦ To make decisions on all key aspects of IT deployment and implementation.
⑧ To facilitate implementation of IT security within the enterprise.
⑨ To report to the BOD on IT activities on a regular basis.

ensure (establish), review & approve (monitor), review & approve (review), report to BOD, make decisions, facilitate implementation

⑧ IT strategy Planning: Planning is basically deciding in advance "what is to be done", "who is going to do" and "when it is to be done".

There are three levels of Managerial Activity in an enterprise:-
① Strategic Planning.
② Management Control.
③ Operational Control.

Nov, 15 (6m)

May, 16 RTP

① Key Mgt. Practices for Aligning IT strategy with Enterprise Strategy:

May 15 (6m) May, 16 (5m)

1. Understand Enterprise direction
   → Consider Current Enterprise Environment and Strategy & Future Objectives
2. Assess the Current Environment, Capabilities and Performance
3. Define target IT capabilities.
4. Conduct a gap analysis
5. Define the strategic plan and road map.
6. Communicate IT strategy and direction
   → ~~Stakeholders and Users~~

⑩ Business Value from use of IT:

Key Mgt Practices
1. Evaluate
2. Direct
3. Monitor
} Value Optimization

Key Metrices (% of)

IT enabled Invts.
→ where benefit realisation monitored through full economic life cycle.
→ where claimed benefits are met or exceeded.

IT services
→ where expected benefits realized
→ with clearly defined and approved operational costs and expected benefits

Invts Business
→ with clearly defined and approved ~~operational costs~~ and expected IT related costs and benefits.

2. Risk Management

1. Sources of Risk
2. Characteristics of Risk
3. Related Terms
4. Risk Mgt. Strategies.
5. Key Governance Practices of Risk Mgt.
6. Key Mgt. Practices of Risk Mgt.
7. Metrices of Risk Mgt.

① Sources of Risk: Commercial & legal relationships, Economic circumstances, Human behavior, Natural Events, Political Circumstances, Technology and technical issues, Mgt. activities and controls, Individual Activities.

② Characteristics of Risk: RTP Nov, 16
1. Loss potential that exists as the result of threat/vulnerability process
2. Uncertainty of loss expressed in terms of probability of such loss.
3. The probability/likelihood that a threat agent mounting a specific attack against a particular system.

③ Related Terms:
1. Asset: Something of value to the organization.
2. Vulnerability: Weakness in the system safeguards that exposes the system to threats. — May, 15 (4m)
3. Threats: Circumstance or event with the potential to harm the software system or component through its unauthorized access, destruction modification and/or denial of service is a threat.
4. Exposure: Extent of loss the organization has to face when a risk material ze.
5. Likelihood: ~~Likelihood of the threat occuring~~ is the estimation of the probability that the threat will succeed in achieving an undesirable event.
6. Attack: Attempt to gain unauthorized access to the systems services or to compromise the systems dependability. Also called malicious intention act.
7. Risk: Potential harm caused if a particular threat, exploits a particular vulnerability to cause damage to an asset.
8. Countermeasure: An action, procedure, technique or other measure that reduces the vulnerability of a component or system to a threat.
9. Residual Risk: Any risk still remaining after the counter measures are analyzed and implemented.

Vulnerability, Threat Risk — Nov, 14 (4m)

④ Risk Mgt. Strategies: May, 16 (4m)
1. Tolerate/accept the risk.
2. Terminate/Eliminate the risk.
3. Transfer/Share the risk.
4. Treat/mitigate the risk
5. Turn back (ignore the risk).

⑤. Key Governance Practices of Risk Mgt: Evaluate, Direct, Monitor } Risk Mgt.

⑥ Key Mgt. Practices of Risk Mgt:
1. Collect data
2. Analyze data
3. Maintain a risk profile
4. Articulate risk
5. Define a risk mgt. action portfolio
6. Respond a risk.

May, 15 (6m)

⑦. Metrices of Risk Mgt: ①. (%) of critical business processes, IT services and IT-enabled business programs covered by risk assessment.

Nov, 15 (4m)

② (%) of enterprise risk assessment including IT related risks.

③ No. of significant IT related incidents that weren't identified in risk assessment.

④. Frequency of updating the risk profile based on stakes of risk assessment.

3. COBIT-5
① Introduction
② Components in COBIT
③ Benefits of COBIT 5
④ FIVE Principles of COBIT 5
⑤. SEVEN Enablers of COBIT 5

① Introduction: Control Objectives for Info. and Related Technology (COBIT) is a set of best practices for Info. Technology Mgt. developed by Information Systems Audit & Control Association (ISACA) and IT Governance Institute in 1996.

② Components:
① Framework
② Process Description
③ Control Objectives
④ Mgt. Guidelines
⑤ Maturity Models.

③ Benefits of COBIT-5:
①. Enables enterprises in achieving their objectives for the governance and mgt. of enterprise IT.
② Helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
③. Enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.
④ Helps enterprises to manage IT related risks and ensure, compliances continuity, security and privacy.
⑤. Enables clear policy development & good practice for IT mgt. including increased business user satisfaction.
⑥. The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
⑦ COBIT-5 supports compliance with relevant laws, regulations, contractual agreements and policies.

COBIT 5 framework can be implemented in all sizes of enterprises.

④ FIVE Principles of COBIT 5: Principle 1 → Meeting Stakeholders needs.
Principle 2 → Covering the enterprise end-to-End.
Principle 3 → Applying a single integrated framework
Principle 4 → Enabling a holistic approach
Principle 5 → Separating Governance from mgt.

May, 15 (4m)

⑤ SEVEN Enablers of COBIT 5:
① Principles, policies and frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day mgt.
② Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
③ Organizational structures are the key decision-making entities in an enterprise.
④ Culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and mgt. activities.

PROCESS
Nov, 16 (5m)

⑤ Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Info. is req. for keeping the organization running and well governed, but at the operational level, info. is very often the key product of enterprise itself.

⑥ Services, infrastructure and applications include the infrastructure, technology & applications that provide the enterprise with info. technology processing and services.

⑦ Skills and Competencies are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective action

4. Others

- (A) Key Mgt. Practices of IT Compliance.
- (B) Key Metrices for Assessing Compliance Process.
- (C) Evaluating IT Governance Structure and Practices by Internal Auditors
- (D) Sample areas of GRC for Review by Internal Auditor
- (E) Sample areas of Review of Assessing and Managing Risks.
- (F) Key Mgt. Practices for evaluating and assessing the system of Internal Controls

(A) Key Mgt Practices of IT Compliance (provided by Cobit-5)

Nov 15 (4m)

[IOCO]

1. Identify external compliance requirements
2. Optimize response to external requirements.
3. Confirm external compliance.
4. Obtain assurance of external compliance.

(B) Key Metrices for Assessing Compliance Process:

Compliance with External Laws and Regulations

(Cost) (No) (Coverage)

1. Cost of IT non-compliance.
2. No. of IT non-compliance issues reported to board.
3. No. of non-compliance issues relating to contractual agreements with IT service providers.
4. Coverage of compliance assessments.

IT Compliance with Internal Policies (No) (%) (Frequency)

1. No. of incidents related to non-compliance to policy.
2. Percentage of stakeholders who understand policies (%)
3. Percentage of policies supported by effective stds. and (%) working practices.
4. Frequency of policies review and updates.

(C) Evaluating IT Governance Structure and Practices by Internal Auditors:

- Leadership
- Organizational Struct
- Processes
- Risks
- Controls
- Performance Measurement Monitoring

RTP May 16

(D) Sample areas of GRC for Review by Internal Auditor:

1. Scope
2. Governance
3. Evaluate Enterprise Ethics
4. Risk Mgt.
5. Interpretation
6. Risk Mgt. Process
7. Evaluate Risk Exposure
8. Evaluate fraud and fraud risk
9. Address adequacy of risk mgt. process.

(E) Sample areas of Review of Assessing and Managing Risks:

1. Risk Mgt. ownership and accountability.
2. Diff. kinds of IT risks
3. Defined and communicated risk tolerance profile.
4. Root cause analyses and risk mitigation measures.
5. Quantitative and/or qualitative risk measurement.
6. Risk assessment methodology, and
7. Risk action plans and Timely reassessment.

(F) Key Mgt Practices for (complying with Cobit-5) Evaluating and Assessing the system of Internal Controls:-

Nov, 14 (6m)

1. Monitor Internal Controls
2. Review Business Process Controls Effectiveness
3. Perform Control Self-assessment
4. Identify and Report Control Deficiencies
5. Ensure that assurance providers are independent and qualified
6. Plan Assurance Initiatives
7. Scope Assurance Initiatives.
8. Execute Assurance Initiatives.

Marks allocation

Nov, 14	May, 15	Nov, 15	May, 16	Nov, 16
16 m	15m	16m	9 m	12m

INFORMATION SYSTEM CONCEPTS

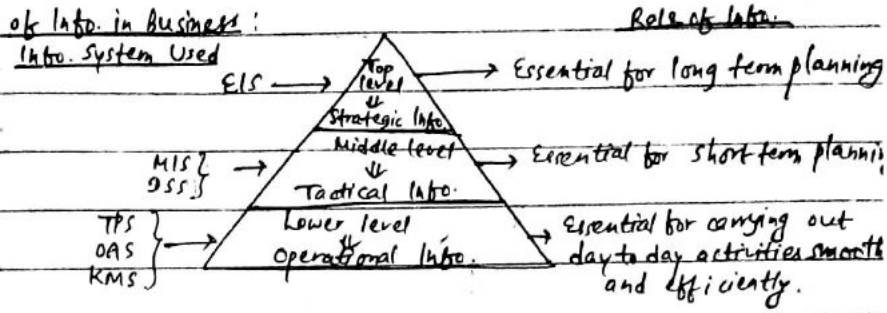
1. Information
2. System
3. Information System
4. Other Concepts

1. Information

Meaning: Processed data that have been put into a meaningful and useful conte
Mere collection of data is not info and mere collection of info is not knowledge.

Attributes: Availability, Purpose, Mode & format, Rate, Current/updated, Frequency, Completeness & Adequacy, Reliability, Validity, Quality, Transparen

Role of Info. in Business:



2. System

Meaning: Group of inter-connected components working towards the accomplishment of a common goal by accepting inputs in an orderly transformation process.

Classification:

(EIDW)

- Elements → Abstract / Physical
- Interactive Behavior → Open / Closed
- Degree of Human Intervention → Manual / Automated
- Working/Output → Deterministic / Probabilistic

3. Information System

Components: People, Computer System (Hardware, Software), Data, Network

Characteristics of Computer Based Info. System (CBIS) (5 points): Write abt General Syste and sub-system Concep

Major Areas of Computer Based Applications:
① Finance & A/cing
② Marketing & sales
③ Prod^{n}/Mfg.
④ Inventory Mgt.
⑤ HR Mgt.

4. Classification of Information System

- Operation Level System → (i) TPS
- Knowledge Level System → (ii) OAS, (iii) KMS
- Mgt. Level System → (iv) MIS, (v) DSS
- Strategic Level System → (vi) EIS/ESS

5. Specialized Systems

- (vii) Expert System (ES)
- (viii) Cross Functional Info. System, Eg. ERP (CFIS)
- (ix) Core Banking System (CBS)

(i) Transaction Processing System (TPS)

- **Meaning:** At the lowest level of mgt., TPS is an info. system that manipulates data from business transaction.
- **Major activities:** CPCP
  - Capturing → data to organize into files/database
  - Processing → files/databases using application software
  - Generating → info. in the form of reports
  - Processing → queries from various quarters of the organization
- **Components:** Input, Processing, Storage, Outputs
- **Features:** LABS
  - Large volume of data
  - Automation of basic operations.
  - Benefits are easily measurable.
  - Source of input for other systems.

(ii) Office Automation System (OAS)

- **Meaning:** Office Automation refers to the application of computer and communication technology to office functions. Eg: Microsoft office
- **Office Activities:**
  - Document capture
  - Document Creation
  - Receipts and Distribution
  - Filing search, retrieval and follow up
  - Calculations
  - Recording utilization of resources
- **Benefits of OAS:**
  - ① Improves communication by
    - ② Reduces cycle time
    - ③ Reduces the cost
  - ④ Ensures accuracy of info.

May, 15 (6m)

Classification of OAS

- Text Processing System → 4 Key Points
- Electronic Document Mgt. System (EDMS) → 4 Key Points
- Electronic Message Communication System (EMCS) → Components
  - Electronic Mail (E-Mail)
    - Features: EOBTPE
      - Electronic transmission
      - Online development and editing.
      - Broadcasting and rerouting.
      - Integration with other Info. Systems
      - Portability
      - Economical.
  - Facsimile (Fax)
  - Voice Mail
- Tele-Conferencing & Video-Conferencing System

(iii) Knowledge Mgt. System (KMS)

- **Meaning:** Knowledge Mgt. is the process of capturing, developing, sharing and effectively using organizational knowledge
- Explicit and Tacit are two types of Knowledge.
  - Explicit → Easily available across the organization and transferable knowledge → Online tutorials, policy, etc
  - Tacit → Personal, experimental and content specific. → Hand-on skills, special know how, employee experiences, etc.

(iv) Mgt. Info. System (MIS)

- **Meaning:** MIS is an integrated user machine system designed for providing information to support operational control, mgt. control and decision making functions in an organization. It is a computer based system that provides flexible and speedy access to accurate data.

Nov (1) (5m)

Characteristics of an effective MIS
- Mgt. Oriented
- Mgt. directed
- Integrated
- Common data flow
- Common database
- Computerized
- Heavy Planning Element
- Sub-system Concept.

(MICSH)

Misconceptions about MIS
- Any EDP is a MIS
- Any reporting system is MIS
- MIS is a mgt. technique.
- MIS is a bunch of technologies
- MIS is implementation of organizational systems and procedure
- study of MIS is abt. computer
- More data in reports generated is more info. to managers.
- Accuracy plays vital role in reporting.

Pre-requisites of an effective MIS
- Database
  - Characteristics
    - User oriented
    - capable of being used as a common data source to various users
    - available to authorized persons only.
    - controlled by a separate authority known as DBMS.
- Qualified System & Mgt. Staff.
  - System & Computer Experts
  - Mgt. Experts
- Support of Top Mgt.
  - Reasons
    - cannot be effectively controlled and may be delayed
    - Resources in CBIS are large.
    - To gain the support of top mgt., the officers should place before top mgt. all the supporting facts and state clearly the benefits.
- Control & Maintenance of MIS

Evaluation of MIS
- Examining enough flexibility
- Ascertaining abt. capabilities and deficiencies in system
- Guiding the appr. authority about steps to be taken to maintain effectiveness of MIS

Constraints in operating a MIS (talk abt. experts/staffs)
- Non-availability of expert
- Experts face problem which MIS sub-system to be installed first
- Approach of expert non-standardized
- Non-cooperation from staff

Limitations of MIS
- MIS is not substitute for effective mgt.
- MIS may not have requisite flexibility
- MIS can't provide tailor made info. packages.
- Takes into account mainly quantitative factors
- Less useful for non-programmed decisions

(v) Decision Support System (DSS):

Meaning: System that provides tools to managers to assist them in solving semi-structured and unstructured problem in their own, somewhat personalized way.

Planning languages used in DSS
- General Purpose Planning Language
  - that allow users to perform many routine tasks
- Special Purpose Planning Language
  - are more limited in what they can do, but usually do certain jobs better than general-purpose planning languages
  - Eg: SAS and SPSS

Characteristics of DSS
- How DSS helps?
  - supports decision making
  - can be used for solving structured problems.
- How DSS should be?
  - easy to use.
  - flexible (+) adaptable.
  - user friendly.
  - extensible (+) evolve over time.
  - used mainly for decision making rather than communicating decision.
  - focuses on decisions rather than data and info.

Components of DSS
- User → Manager, Staff Specialist (Analysts)
- Databases → Implementation at three levels (physical, logical, external).
- Model base
  - Brain of DSS as it performs data manipulations and computations.
- Planning Languages

Examples of DSS in A/cing.
1. Cost Accounting System
2. Capital budgeting System
3. Budget Variance Analysis System
4. General Decision Support System. (2 Costing, 1 FM)

(vi). Executive Information System (EIS):

Meaning: It is sometimes referred to as an Executive Support System (ESS). It serves the strategic level i.e. top level managers of the organization. It creates a generalized computing and communication environment.

Characteristics of EIS

How EIS helps?
- serves info. need of top executives.
- enables users to extract summary data
- rapid access to timely info. & direct access to mgt report
- provides extensive online analysis tool.
- capable of accessing both internal and external data.

Characteristics of types of Info. used in EIS

Nov 18 (6m)

1. Lack of structure
2. High degree of uncertainty.
3. Future orientation.
4. Informal source.
5. Low level of detail.

Contents of EIS

(Practical set of principles to guide the design of measures and indicators to be used/included in an EIS).

EIS measures must be
- easy to understand and collect.
- based on a balanced view of the organizations objective.
- must encourage mgt. and staff to share ownership of organizations objective
- must be available in the organization.
- must evolve to meet the changing needs of the organization.

(vii). Expert System (ES):

Meaning: An expert system is a highly developed DSS that utilizes knowledge generally possessed by an expert to solve a problem.

Business Applications of ES

(Main it helps in diff. areas)
1. Acing & finance
2. Marketing
3. Manufacturing.
4. Personnel.
5. General business.

Need for ES

1. Expert labour is expensive.
2. Expert can handle only a few factors at a time.
3. Both above limitations put a need for ES.

Benefits of ES

Nov 15 (6m)

1. ES preserve knowledge
2. ES put info. into an active form.
3. assist in thinking the way experienced professionals do.
4. ES are not subject to fatigue, being too busy or emotional.
5. ES can be effectively used in the areas of marketing products, cutting costs and improving products.

Properties that application should possess to quality for ES development:

Nov 14 (6m)

1. Availability.
2. Complexity.
3. Domain.
4. Expertise.
5. Structure.

(ACDES)

(viii). Cross Functional Information System (CFIS)

It is known as integrated info. system that combines most of info. systems and designed to produce info. and support decision making for diff levels of mgt and business functions.

Eg: ERP

Eg: ERP

ERP is a process mgt. software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources.

Nov 15 (6m)
May 16 (6m)

Components of ERP

1. Software Component
2. Process flow
3. Customer mindset
4. Change mgt.

Benefits of ERP

Main
1. Streamlining process with single integrated system.
2. Provide a consolidated picture of sales, inventory.

Reduces
1. Redundant data entry.
2. Inventory costs.

Improved
1. Workflow & efficiency.
2. Customer satisfaction.

(ix) Core Banking System (CBS):

Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank A/c and perform basic transactions from any of the member branch offices.

Elements of CBS

1. Making and servicing loans.
2. Opening new accounts.
3. Processing cash deposits and withdrawals.
4. Processing payments and cheques.
5. Calculating interest.
6. Customer Relationship Mgt (CRM) activities.
7. Managing Customer Accounts.
8. Establishing Int. Rates.
9. Maintaining records for all the bank transactions.

6. Other Concepts

① Application of IS in Enterprise Processes:

Info. systems perform following 3 vital roles:-

- Support business processes and operations.
- Support business decision making.
- Support strategic competitive advantage.

② Implication of IS in business:

May 15 (5m)

How Info. System helps?

- helps managers in efficient decision making.
- helps in making right decision at the right time.
- helps in generating innovative idea for solving critical problem.
- Knowledge gathered through IS may be utilized in unusual situations.
- IS is viewed as a process, it can be integrated to formulate a strategy of action or operation.

③ Knowledge req. by a human manager to operate IS effectively and efficiently:

includes operation, dev., and mgt. of H/w, S/w, data, network and other technologies. May 15 (4m)

comprises how end users and IS specialists develop and execute business/IT solns to problems

1. Foundation concepts → includes fundamental business & managerial concepts.
2. Information Technologies (IT) (5th Point)
3. Business Applications (4th Point) → includes major uses of IT in business steps.
4. Development Processes (1st)
5. Management Challenges → includes how the function and IT resources are maintained and utilized to attain top performance and build strategies.

④ Various types of Business Applications:

(Impact of IT on IS for diff. sectors)

RTP Nov. 16

1. E business
2. Financial service Sector
3. Wholesaling and Retailing.
4. Public sectors
5. Others

⑤ Underlying IT technologies:

1. Business Website
2. Internet and Intranet
3. Software and Packages
4. Business Intelligence (BI)
5. Computer Systems, Scanners, Laptops, Printer, Smart phone, etc.

May 16 (5m)

Nov. 14 (6m)

	DSS	Traditional MIS
⑥. Diff. bet^{n}:		
Philosophy:	① Providing integrated tools, data, models and languages to end users.	①. Providing structured info. to end users.
Orientation:	②. External Orientation	② Internal Orientation
Flexibility:	③ Highly flexible	③ Relatively flexible
Analytical Capability:	④ More analytical capability	④. Little analytical capability
System Analysis:	⑤. Emphasis on tools to be used in decision process.	⑤. Emphasis on info. req. analysis
System design:	⑥ Interactive process	⑥ System dev. based on static info. requirements.

	EIS	Traditional Info. System
⑦. Diff. bet^{n}:		
Level of Mgt.	①. For top or near top executives	①. For lower staffs.
Nature of Info. Access	②. Specific issues/problems and aggregate reports	②. Status reporting.
Nature of Info provided	③. Online tools and analysis	③. Offline status reporting.
Info. Sources	④. More external, less internal.	④. Internal.
Drill down facility	⑤. Available to go through details	⑤. Not available
Info. format	⑥. Text with graphics	⑥. Tabular
Nature of Interface	⑦. User friendly	⑦. Computer operator generated.

Marks Allocation

Nov 14	May 15	Nov 15	May 16	Nov 16
25m	23m	22m	18m	15m

PROTECTION OF INFORMATION SYSTEMS

1. Basics
2. IS Controls
3. Information Technology General Controls
4. Other Concepts

1. Basics

① Need for Protection of Is
② What Info. is sensitive?
③ Info. System Security and its objectives
④ Info. Security Policy and related issues
⑤ Components of Good Security Policy.

④ Hierarchy
⑤ Issues to address
⑥ Members of security Policy.

① **Need for Protection of Is**: Info. Security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive info. That is why protection of IS has become a need for organizations.

② **What Info. is sensitive**: strategic plans, Business operational data, Financial records.
[Critical Info. that each organization generates]

③ **Info. System security and its objectives**: Info. Security refers to the protection of valuable asset against loss, disclosure or damage.

Confidentiality, Integrity, Availability
[CIA]

④ **Info. Security Policy and related issues**: Info. Security Policy is the statement of intent by the mgt abt. how to protect a co's info. assets. It is a formal statement of the rules, which give access to people to an organizations technology and info. assets, and which they must abide by.

- Hierarchy
  - User Security Policy
    - User Security Policy
    - Acceptance Usage Policy
  - Organization Security Policy
    - Organizational Information Security Policy
    - Network & System Security Policy
    - Info. Classification Policy
  - Conditions of Connection

May 16 (6m) — Issues to address (def + reasons + exp):
① def of Info. Security.
② reasons why info. security is imp to organization
③ brief explanation of security policies, principles, stds, and compliance requirements.
④ def of all relevant info. security responsibilities
⑤ reference to supporting documentation.

Members of Security Policy
① Mgt. members
② Technical group
③ Legal experts

⑤ **Components of Good Security Policy**: Nov 15 (6m)
① Purpose and Scope of the Document and Intended audience.
② Security infrastructure.
③ Security policy document maintenance and compliance requirements.
④ Incident response mechanism and incident reporting.
⑤ Security Organization Structure
⑥ Inventory and classification of Assets.
⑦ Description of technologies and computing structure.
⑧ Physical and Environmental Security.
⑨ Identity Mgt. and access control.
⑩ IT operations mgt.
⑪ IT Communications
⑫ System Dev. and Maintenance Controls.
⑬ Business Continuity Planning (BCP)
⑭ Legal Compliances
⑮ Monitoring and Auditing Requirements.

2. IS Controls

① **Objectives of Controls:** Control is defined as [illegible] structure that are designed to provide [illegible] that business objectives will be achieved and [illegible] events are prevented, detected and corrected. ∴ The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss.

② **Components of Internal Controls:** ① Control Environment, ② Risk Assessment, ③ Control Activities, ④ Info. & Communication, ⑤ Monitoring

③ **Impact of Technology on Internal Controls:** ① Competent & Trustworthy Personnel, ② Segregation of Duties, ③ Authorization Procedures, ④ Adequate Documents and Records, ⑤ Physical Control over Assets and Records, ⑥ Adequate Mgt. Supervision, ⑦ Independent checks on performance, ⑧ Comparing recorded accountability with assets, ⑨ Delegation of authority and responsibility.

EXAMPLES — May 16 (4m)

④ **Classification of IS Controls**

- **Objective**
  - ① Preventive
  - ② Detective
  - ③ Corrective
  - ④ Compensatory
- **Nature of IS**
  - ⑤ Environmental
  - ⑥ Physical Access
  - ⑦ Logical Access
- **Function**
  - ⑧ Internal Acctg
  - ⑨ Operational
  - ⑩ Administrative
- **Audit**
  - ⑪ Managerial
  - ⑫ Application

①. Preventive Controls:

Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Eg: Use of password.

Characteristics: ① A clear cut understanding abt. the vulnerabilities of the asset ② Understanding probable threats, and ③ Provision of necessary controls to prevent probable threats from materializing.

Examples: ① Employ qualified personnel. ② Segregation of duties. ③ Access Control. ④ Vaccination against diseases. ⑤ Documentation. ⑥ Prescribing appropriate books for a course. ⑦ Training and retraining of staff. ⑧ Authorization of transaction. ⑨ Validation, edit checks in the application. ⑩ Firewalls. ⑪ Anti-virus software. ⑫ Passwords.

②. Detective Controls:

Controls designed to detect errors, omissions or malicious acts that occur and report the occurrence.

Characteristics: ① Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious etc. ② An established mechanism to refer the reported unlawful activities to the appropriate person or group. ③ Interaction with the preventive control to prevent such acts from occurring.

Examples: ① Hash totals. ② Check points in prod^n job. ③ Echo control in telecommunication. ④ Error message over tape labels. ⑤ Duplicate checking of cal^n. ⑥ Periodic performance reporting with variances. ⑦ Past due % report. ⑧ Internal Audit function. ⑨ Surprise checks by supervisor. ⑩ Intrusion detection system. (IDS) ⑪ Cash counts and bank reconciliation. ⑫ Monitoring exp. against budgeted amt.

Nov 16 (4m)

③. Corrective Controls:

Controls designed to reduce the impact or correct an error once it has been detected.

Characteristics: ① Minimizing the impact of the threat. ② Identifying the cause of the problem. ③ Providing remedy to the problems discovered by detective controls. ④ Getting feedback from preventive and detective controls. ⑤ Correcting error arising from a problem. ⑥ Modifying processing systems to minimize future occurrences of incidents.

Examples: ① Contingency planning. ② Rerun procedures. ③ Change input value to an application system. ④ Investigate budget variance and report violations.

May 15 (6m)

④. Compensatory Controls:

Controls designed to reduce the probability of threats which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control - keep in mind that the cost of the lock shouldn't be more than the cost of assets it protects.

⑤ Environmental Controls:

- Controls related to IT environment such as power, air-conditioning, UPS, smoke detection, fire extinguishers, dehumidifiers, etc.
- Environmental Issues and exposures: Environmental exposures are due to elements of nature. However with proper controls, exposures can be reduced.
  Eg: Fire, Earthquake, volcano, hurricane, tornado, power spike, e
- classification of IS resource from the perspective of Environmental Exposu
  1. Hardware & media
  2. Documentation
  3. IS supporting infrastructure or facilities
  4. supplies
  5. People.

Controls for Environmental Exposures:

1. Water detection
2. Hand-held fire extinguishers
3. Manual fire alarms
4. Smoke detectors.
5. Fire suppression system.
6. Strategically locating the computer room within the info. processing facility.
7. Regular inspection by fire dept.
8. Electrical surge protectors
9. Uninterruptible Power system (UPS)/Generator.
10. Power loads from two substations
11. Emergency power-off switch.
12. Prohibitions against eating, drinking and smoki
13. Fire resident office materials.

Nov, 15 (5m)

⑥ Physical Access Controls:

- Controls designed/related to physical security of the tangible IS resources and intangible resources stored on tangible media.
- Physical Access Issues and Exposures:
  - Possible perpetrators
    Perpetrations may be because of employees, who are:-
    1. Accidental ignorant
    2. Addicted to a substance/gambling
    3. Discontended.
    4. Experiencing financial or emotional problems
    5. Former employee
    6. Interested or informed outsiders
    7. Notified for their termination.
    8. on strike
    9. Threatened by disciplinary action or dismissal.
  - Facilities need to be protected from auditors perspective
    1. Communication channels.
    2. computer room.
    3. Control units.
    4. Dedicated telephones/telephone lines.
    5. Disposal sites.
    6. Input/Output devices.
    7. Local area networks (LANs)
    8. Micro and personal compute
    9. Off-site backup file storage facility.
    10. Portable equipment.
    11. Power sources
    12. Storage rooms and supplie
    13. Programming area

Controls for Physical Access Exposures

1. Locks on Doors
   - Cipher locks (Combination door locks)
   - Bolting door locks
   - Electronic door locks
   Map it (4m)
2. Physical Identification Medium
   - PIN
   - Plastic cards
   - Identification badges - special
3. Logging on facilities
   - Manual logging.
   - Electronic logging.
4. Other means of controlling physical access:
   1. Video Cameras.
   2. Security Guards.
   3. Controlled Visitor Access.
   4. Bonded Personnel.
   5. Dead Man Doors
   6. Computer Terminal Locks
   7. Controlled Single Entry Point.
   8. Alarm System.
   9. Perimeter Fencing.
   10. Control of out of hours of employee - employees.

⑦ Logical Access Controls:

- Controls relating to logical access to info system resources such as operating systems controls, application software boundary controls, networking controls, encryption controls, etc.
- Logical Access Paths:
  - Online Terminals
  - Dial-up Ports
  - Telecommunication Network.
- Logical Access Issues and Exposures: Access control mechanisms shou be applied not only to computer operators but also to end users programmers, security administrators, mgt. or any other authorized user/s. Access control mechanism should provide security to the following applications:
  1. Access Control Software
  2. Application Software
  3. Data
  4. Data dictionary/directory
  5. Dial-up lines
  6. Libraries
  7. Logging files.
  8. Procedure Libraries
  9. Spool queues.
  10. System software.
  11. Tape files.
  12. Telecommunication lines.
  13. Temporary disk files
  14. Utilities.

Issues related to Logical Access

- (i) Technical Exposures
- (ii) Computer Crime Exposures.
- (iii) Asynchronous Attacks.
- (iv) Ways to control Remote and distributed data processing applications.

Logical Access Controls

(i) Technical Exposures: (1) Data diddling (2) Bomb → time bomb, logic bomb (3) Trojan Horse (4) Worm (5) Rending down (6) Salami techniques

(ii) Computer Crime Exposures: (1) Financial Loss (2) Legal Responsibilities (3) Loss of credibility (4) [redacted] (5) sabotage (6) [redacted] (7) Disclosure of Confidential Sensitive or Embarrassing Info.

Norms (6m) — Sabotage, Espionage

(iii) Asynchronous Attacks:
(1) Data leakage
(2) Wire tapping
(3) Piggybacking
(4) Shutting down of the computer/Denial of service.

(iv) Ways to Control Remote and distributed data processing applications:

Mayls (5m)
(1) Remote access to computer and data files through the network should be implemented.
(2) Having a terminal lock can assure physical security to some extent
(3) Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
(4) Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
(5) In order to prevent unauthorized users from accessing the system, there should be proper control mechanism over system documentation and manuals.
(6) Data transmission over remote locations should be controlled
(7) When replicated copies of files exist at multiple location it must be ensured that all identical copies contain the same info.

Logical Access Controls (8)
(1) User Access Mgt.
(2) User Responsibilities.
(3) Network Access Control.
(4) Operating System Access Control.
(5) Application and Monitoring System Access Control.
(6) Mobile Computing.

(8) Internal A/cing Controls: Controls which are intended to safeguard the client's assets and ensure the reliability of the financial records.

(9) Operational Controls: Controls that deal with the day-to-day operations, functions and activities to ensure that the operational activities are contributing to business objectives

(10) Administrative Controls: These are concerned with ensuring efficiency and compliance with mgt policies, including the operational controls.

(11) Managerial Controls: Controls over managerial and controls that must be performed to ensure the development, implementation, operation and maintenance of info. system in a planned and controlled manner in an organization

- Top Mgt and IS Mgt Controls
  - The major functions that a senior mgr must perform:-
  - (1) Planning
  - (2) Organizing
  - (3) Leading
  - (4) Controlling
- System Dev. Mgt Controls
  - (1) System authorization activities
  - (2) User specification activities
  - (3) Technical Design activities
  - (4) Internal Auditor Participation.
  - (5) Program testing.
  - (6) User test and acceptance procedures.
- Programming Mgt. Controls
  - (1) Planning
  - (2) Control
  - (3) Design
  - (4) Coding
  - (5) Testing
  - (6) Operation & Maintenance.
- Data Resource Mgt Controls
  - (1) Def^n Controls
  - (2) Existence Controls
  - (3) Access Controls
  - (4) Update Controls
  - (5) Concurrency Controls
  - (6) Quality Controls.
- Quality Assurance Mgt. Controls
- Security Mgt. Controls
- Operating Mgt Controls
  - (1) Computer operations
  - (2) Network operations
  - (3) Data preparation & entry
  - (4) Prod^n control
  - (5) File library
  - (6) Documentation & Program library
  - (7) Help desk
  - (8) Capacity planning & performance monitoring

(2) Application Controls:

These include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.

Nov, 14 (6m)

- **Boundary Controls**
  - ① Cryptography
  - ② Passwords
  - ③ PIN
  - ④ Identification cards
  - ⑤ Biometric devices

  May, 15 (6m)
- **Input Controls**
  - ① Source Document Control
  - ② Data Coding Control
  - ③ Batch Control
  - ④ Validation Control

  Nov, 16 (6m)
- **Communication Controls**
  - ① Physical Component Controls
  - ② Line error Control
  - ③ Flow Controls
  - ④ Link Controls
  - ⑤ Topological Controls
  - ⑥ Channel Access Controls
  - ⑦ Interned working Controls
    - Devices
      - ① Bridge
      - ② Router
      - ③ Gateway.
- **Processing Controls**
  - ① Processor Controls
  - ② Real memory controls
  - ③ Virtual memory controls
  - ④ Data processing controls.
- **Database Controls**
  - Update Controls
    - ① Sequence check batch transaction & master files.
    - ② Ensure all records on files are processed
    - ③ Process multiple transactions for a single record in the correct order.
    - ④ Maintain a suspense a/c
  - Report Controls
    - ① Standing Data
    - ② Print run-to-run control totals
    - ③ Print suspense a/c entries
    - ④ Existence/Recovery controls
- **Output Controls**
  - ① Storage and logging of sensitive/critical forms
  - ② Logging of output program execution
  - ③ Spooling/queuing
  - ④ Controls over printing
  - ⑤ Report distribution & collection control
  - ⑥ Retention Control

3. Information Technology General Controls

ITGCs are the basic policies and procedures that ensure that an organization's info. systems are properly safeguarded, that application programs and data are secure and that computerized operations can be recovered in case of unexpected interruptions.

Most common ITGCs

① Logical access controls over infrastructure, applications and data.
② System dev. life cycle controls.
③ Program change mgt. controls.
④ Data center physical security controls.
⑤ System and data backup and recovery controls.
⑥ Computer operation controls.

4. Other Concepts

① Classification of Information
② Data security
③ Data Integrity ↔ Controls / Policies
④ Cyber frauds
⑤ Cyber-attacks
⑥ Impact of cyber frauds on Enterprises
⑦ Techniques to commit cyber frauds
⑧ Financial Controls
⑨ Personal Computer Controls

① Classification of Information

(TMI)

Nov, 15 (4m)

① Top Secret
② Highly Confidential
③ Proprietary
④ Internal Use only
⑤ Public Documents

② Data Security: Data Security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons as well as the prevention of unauthorized modification and deletion of the data.

As IS auditor is to [redacted] while [redacted] the [redacted] of [redacted]:-

{① Who is responsible for the [redacted] of data?}
{② Who is permitted to update data?}
{③ Who is permitted to read and use the data?
④ Who is responsible for determining who can read and update [redacted]?}
{⑤ Who controls the security of the data?}

③ Data Integrity Controls and Data Integrity Policies [VSD, QED]

The primary objective of data integrity controls techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific data processing program.

Categories
{① Source data control
② Input Validation Routines}
{③ Online-data entry controls.
④ Data processing and storage controls
⑤ Output Controls
⑥ Data transmission controls.}

Nov, 14 (5m)
① Virus - Signature Updating.
② Software Testing.
③ Division of Environments.
④ Offsite Backup Storage
⑤ Quarter-End and Year-End Backups
⑥ Disaster Recovery

④ Cyber Frauds: → Cyber fraud shall mean fraud committed by use of technology. It refers to any type of deliberate deception for unfair or unlawful gain that occurs online. Eg: Online credit card theft.

Types

Pure Cyber Frauds
Frauds, which exist only in cyber world. They are borne out of use of technology.
Eg: Website hacking.

Cyber Enabled Frauds
Frauds, which can be committed in physical world also, but with the use of technology.
Eg: Withdrawal of money from bank a/c by stealing PIN.

⑤ Cyber attacks: Major cyber attacks during year 2011.
① Phishing.
② Network scanning.
③ Virus/Malicious code.
④ Spam.
⑤ Website Compromise/Malware Propagation
⑥ Others (Cracking, Eavesdropping, E-mail forgery, E-mail threats, Scavenging)

⑥ Impact of Cyber Frauds on Enterprises:
Nov, 16 (5m)
Nov, 18 (4m)
① Financial loss
② Legal Repercussions
③ Loss of credibility a competitive Edge.
④ Disclosure of confidential, sensitive or embarrassing info.
⑤ Sabotage.

⑦ Techniques to Commit Cyber Frauds:
① Hacking
② Cracking
③ Data diddling
④ Data leakage
⑤ Denial of service (DOS) attacks
⑥ Internet terrorism.
⑦ Logic time bomb.
⑧ Password cracking.
⑨ Piggybacking.
⑩ Round down
⑪ Trap door.

⑧. Financial Controls:
① Authorization.
② Budgets.
③ Cancellation of documents.
④ Dual control.
⑤ Input/Output verification.
⑥ Safekeeping.
⑦ Sequentially numbered documents.

⑨ Personal Computers Controls:

PC/Pendrive
① Personal Computer are small in size and easy to connect and disconnect, so they are likely to be taken outside the org. for theft of info.
② Pen drives can be very conveniently transported from one place to another, so data theft may occur.
③ PC is basically a single user oriented machine and hence, doesn't provide inherent data safeguards. Problems can be caused by computer viruses and pirated software

Related risks

Nov, 14 (6m)

Staff
- Segregation of duty not possible
- Staff mobility higher
- not adequately trained

④ Segregation of duty is not possible, owing to limited no. of staff
⑤ Due to vast no. of installations, staff mobility is higher and hence becomes a source of leakage of info.
⑥ The operating staff may not be adequately trained.
⑦ Weak access control: Most of the log-on procedures become active only at the booting of the computer from the hard drive.

Security Measures to overcome above risks

① Physically locking the system.
② Proper logging of equipment shifting must be done.
③ Centralized purchase of hardware & software.
④ Stds. set for developing, testing and documenting.
⑤ Uses of antimalware software.
⑥ The use of personal computer and their peripheral must have controls, and.
⑦ Use of disc locks that prevent unauthorized access to the floppy disk or pen drive of a computer.

use of personal computer and their peripheral must have controls
- ① Physically locking
- ② Proper logging of eq. shifting
- ① Centralized purchase
- ② Stds. for developing, testing & documenting
- ① use of antimalware software
- ② use of disc locks

Marks Allocation

Nov.14	May.15	Nov.15	May.16	Nov.16
14m	13m	10m	11m	12m

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

1. Basics
2. Developing a BCP (8 phases)
3. Components of BCM Process
4. Others

1. Basics

① BCM Policy and its objectives
② BCP and its components
③ Objectives & Goals of BCP
④ Scope of Business Continuity.

① **BCM Policy** and its objectives: The main objective of a BCP is to minimize/eliminate the loss to enterprises business in terms of revenue loss, loss of reputation, loss of productivity and customers satisfaction.
This policy document is a high level document which shall be the guide to make a systematic approach for disaster recovery, to bring out awareness among the persons in scope about the business continuity aspects and its importance.

Objective of this policy is to provide a structure through which:-

① → critical services and activities undertaken by the enterprise operation for the customer will be identified
② → Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel IT and/or communication or failure within the supply and support chains.
③ → Invocation of incident mgt. and business continuity plans can be managed
④ → Planning and mgt responsibility are assigned to a member of the relevant senior mgt. team
⑤ → Incident Mgt Plan & BCP are subject to ongoing testing, revision & updation as required

① Critical services & activities → identified
② Plans → developed
③ Planning & Mgt resp. → assigned (Nov,14) (4m)
④ IMP & BCP → Invocation can be managed → subject to ongoing testing, revision & updation

② BCP and its components: BCP is the creation and validation of a practical logistics plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

Components
→ Business Resumption Planning
→ Disaster Recovery Planning
→ Crisis Mgt.

③ Objectives & Goals of BCP: The primary objective of a BCP is to minimize the loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations.

Key Objectives:
① Provide the safety and well being of people on the premises at the time of disaster.
② Continue critical business operations.
③ Minimize the duration of a serious disruptions to operations and resources (both info. processing & other resources)
④ Minimize immediate damage and losses
⑤ Establish mgt. succession and emergency powers
⑥ Identify critical lines of business and supporting functions.
⑦ Reduce the complexity of the recovery efforts.
⑧ Facilitate effective co-ordination of recovery tasks

Provide safety & well being of people.
Continue critical business operations.
Minimize duration of serious disruption → complexity of the recovery effort
immediate damage/losses
Identify critical lines of business and supporting functions.
Facilitate effective co-ordination of recovery tasks.
Establish mgt. succession & emergency plan.

∴ **Main Goals** of BCP should be to:
→ identify & know
→ minimize the duration of a serious disruption to business operations
→ facilitate effective co-ordination of recovery tasks
→ reduce the complexity of the recovery efforts.

④ Scope of Business Continuity: Top mgt of the enterprise needs to define the scope of the BCM program by identifying the key products and services that support the enterprises objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis.

Advantages of Business Continuity:-

→ the enterprise is able to proactively assess the threat scenario and potential risks.
→ the enterprise has planned response to disruptions which can contain the damage and minimize the impact on the enterprise, and
→ the enterprise is able to demonstrate a response through a process of regular testing and trainings.

2. Developing a BCP (8 phases)

→ **Methodology**: The methodology for developing a BCP can be sub-divided into 8 phases.

This methodology emphasises on the following:-

① Providing mgt with a comprehensive understanding of the total efforts req. to develop and maintain an effective recovery plan
② Obtaining commitment from appropriate mgt to participate & support in the effort.
③ Defining recovery requirements from the perspective of business function.
④ Documenting the impact of an extended loss of availability to operations and key business functions.
⑤ Focusing appropriately on disaster prevention and impact minimization as well as orderly recovery.
⑥ Selecting business continuity teams that ensure the proper balance required for plan development.
⑦ Developing a business continuity plan that is understandable easy to use and maintain.

8 phases:
- Pre-planning activities (Project initiation)
- Vulnerability Assessment and General defⁿ of req.
- Business Impact Analysis (BIA)
- Detailed defⁿ of Requirements
- Plan Development
- Testing Program
- Maintenance Program
- Initial Plan Testing and Plan Implementation.

Phase 1: Pre-Planning Activities (Project Initiation)

This phase is used to obtain an understanding of the existing and projected computing environment.

Deliverables:
→ A steering Committee should be established.
→ Development of a policy to support the recovery program.
→ An awareness program to educate mgt and senior individuals who will be required to participate in the projects.

Phase 2: Vulnerability Assessment and General Defⁿ of Requirements

→ A thorough Security Assessment should be conducted
→ The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
→ Identify vulnerabilities
→ Present findings and recommendations resulting from the activities of the Security Assessment to the steering Committee, so that corrective actions can be initiated
→ Define scope of the planning effort
→ Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
→ Develop a plan framework.
→ Assemble project team and conduct awareness sessions.

Phase 3: Business Impact Assessment (BIA)

→ Identify critical systems, processes and functions
→ Assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services & facilities

→ Assess the pain threshold" i.e the length of time business units can survive without access to systems services and facilities.

BIA report should be presented to the steering committee.

Phase 4: Detailed def^n of Requirements
During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies

Phase 5: Plan Development
During this phase, recovery plans components are defined and plans are documented

Phase 6: Testing/exercising Program
The plan testing/exercising program is developed during this phase. Testing/Exercising goals are established and alternative testing strategies are evaluated.

Phase 7: Maintenance Program
Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans

Phase 8: Initial Test Planning and Maintenance
Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results

Specific Activities in this phase include:-
→ Defining the test purpose/approach.
→ Identifying test teams.
→ structuring the test
→ conducting the test
→ Analyzing test results, and
→ Modifying the plans as appropriate.

3. Components of a BCM Process

① BCM Process
② Components of a BCM Process
① BCM, Info. Collection Process
② BCM - Strategy Process
③ BCM - Dev and Implementation Process
④ BCM - Testing & Maintenance Process
⑤ BCM - Training Process.

① BCM Process: BCM Process should be in place to address the policy and objectives as defined in the business Continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity mgt.

The BCM Process is mapped as follows:-

① Organization structure
The org. should nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation & maintenance

② Implementing Business Continuity in the Enterprise & Maintenance
↓
Major activities
① Defining the scope & context.
② Defining roles and responsibilities.
③ Engaging and involving all stakeholders.
④ Testing of program on regular basis.
⑤ Maintaining the currency & appropriateness of BCP program.
⑥ Reviewing, reworking and updating the business continuity capability, risk assessment (RA) and business impact analysis (BIA).
⑦ Managing costs and benefits awarded, and
⑧ Convert policies and strategies into actions.

③ BCM Documentation & Records
→ Business Continuity policy
→ BCM system
→ BIA report
→ Risk assessment Report
→ Aims & Objectives of each function
→ Activities undertaken by each function.
→ Business Continuity Strategy
→ Business Continuity Plans
→ Local Authority Risk Register
→ Exercise schedule and results
→ Incident Log
→ Training program.
→ Overall and specific incident mgt. plan.
→ Change control, preventative and corrective action control process

② Components of a BCM Process:

May 16 (5m)

① BCM - Info Collection Process: (May 15 (5m))
- Business Impact Analysis (BIA)
- Classification of Critical Activities
  - Business Categorization (Vital/Essential/Desirable)
  - Disaster Scenarios (Major/Minor/Trivial/Catastrophic)
- Risk Assessment.

② BCM - Strategy Process

③ BCM - Development and Implementation Process
- Incident Mgt. Plan (IMP)
- Business Continuity Plan (BCP)

④ BCM - Testing and Maintenance Process:

BCM Testing

⇓

Objectives of performing BCP tests are to ensure that:
1. the recovery procedures are complete and workable.
2. the competence of personnel in their performance of recovery procedures can be evaluated
3. There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
4. The manual recovery procedures and IT backup systems are current and can either be operational or restored.
5. The success or failure of the business continuity training program is monitored.

BCM Maintenance

⇓ Nov, 16 (4m)

Major maintenance tasks undertaken:-
1. Determine
   - ownership responsibility for maintaining the BCP strategies within the enterprise
   - maintenance regime to ensure that the plans remain up to date
   - maintenance processes to update the plan
2. Identify the BCP maintenance triggers.
3. Implement version control procedures to ensure that the plan is maintained up-to-date.

Reviewing BCM Arrangement (May 15 (4m))

Nov, 14 (5m) An audit or self-assessment of the enterprises' BCM program should verify that:-
1. All key products and services and their supporting critical activities and resources have been identified and included in the enterprises BCM strategy.
2. The enterprises BCM policy, strategies, framework and plans accurately reflect its priorities and requirements.
3. The enterprises BCM competence and its BCM capability are effective.
4. The enterprises BCM solutions are effective, up-to-date and fit-for-purpose
5. The enterprises BCM maintenance and exercising programs have been effectively implemented.
6. BCM strategies and plans incorporate improvements identified during incidents.
7. The enterprise has an ongoing program for BCP training & awareness.
8. BCM processes have been effectively communicated to relevant staff.
9. Change control processes are in place and operate effectively.

⑤ BCM - Training Process (Nov, 16 (4m))

4. Others
- ⑧ Types of Plans
- ⑨ Types of Back-ups
- ⑩ Alternate Processing Facility Arrangements
- ⑪ Third party site.
- ⑫ BCP Manual
- ⑬ Disaster Recovery Procedural Plan Document.
- ⑭ Audit of BCP/DRP

① Types of Plans: (Nov, 15 (6m))
- Emergency Plan
- Backup Plan
- Recovery Plan
- Test Plan

E-BRP

② Types of Back-Ups : Nov,14 (4m) Nov,16 (4m)

Full Backup
A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set.

Advantages
→ Restores are fast and easy to manage as the entire list of files and folders are in one backup set
→ Easy to maintain and restore diff. versions

Disadvantages
→ Backups can take very long as each file is backed up again every time the full backup is run.
→ Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

Incremental Backup
It captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup.

Advantages
→ Much faster backup
→ Efficient use of storage space as files are not duplicated.

Disadvantages
→ Restores are slower than with a full backup & differential backup
→ Restores are a little more complicated. All backup sets (first full backup & all incremental backups) are needed to perform a restore

Differential Backup
It falls in the middle of both full backup and incremental backup. It stores files that've changed since the last full backup. With diff. backups, one full backup is done first and subsequent backup runs save the changes made since the last full backup

Advantages
→ Much faster backup than full backup
→ More efficient use of storage space than full backup, since only files changed since the last full backup will be copied on each diff. backup run
→ Faster restores than incremental backup

Disadvantages
→ Backups are slower than incremental backup
→ Not as efficient use of storage space as compared to incremental backup
→ Restores are slower than with full backup
→ Restores are a little more complicated than full backup, but simpler than incremental backup.

Mirror Backup
Mirror backups are mirror of the source being backed up. With mirror backups when a file in the source is deleted, that file is eventually also deleted in the mirror backup.

Advantages
The backup is clean and doesn't contain old and obsolete files.

Disadvantages
There is a chance that files in the source deleted accidently, by sabotage or through a virus may also be deleted from the backup mirror

③ Alternate Processing Facility Arrangements (May,15 (4m))
→ Cold site
→ Hot site
→ Warm site
→ Reciprocal Agreement

④ Issues to be considered in Contract by Security Administrators, if a 3rd Party site is to be used for backup and recovery purposes:
(How soon) ← ① How soon the site will be made available subsequent to a disaster
(Concurrent use) ← ② The no. of organizations that will be allowed to use the site concurrently in the event of a disaster
③ The priority to be given to concurrent users of the site in the event of a common disaster.
(Nov,15 (4m)) (Period/conditions) ④ The period during which the site can be used
⑤ The conditions under which the site can be used
⑥ The facilities and services the site provider agrees to make available.
⑦ Procedures to ensure security of co's data from being accessed/damaged by another users of the facility and
⑧ What controls will be in place for working at the off-site facility.

→ Facilities/services
→ Procedures to ensure security
→ Controls for working at off-site facility

⑤ **BCP Manual**: A BCP Manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions.

⑥ **Disaster Recovery Procedural Plan Document**:

The disaster recovery procedural plan document may include the following areas:-

1. Conditions for activating the plans which describe the process to be followed before each plan is activated.
2. Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life.
3. Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations.
4. Resumption procedures, which describe the actions to be taken to return to normal business operations.
5. Maintenance schedule which specifies the process for maintaining the plan.
6. Awareness and education activities, which are designed to create an understanding of the disaster recovery process.
7. Contingency plan document distribution list.
8. Detailed description of the purpose and scope of the plan.
9. Contingency plan testing and recovery procedure.
10. List of phone numbers of employees in the event of an emergency.
11. Medical procedure to be followed in case of ~~ongoing~~ injury.
12. Back-up location contractual agreement 13. Emergency phone list for fire, police, H/W, S/W, 14. Insurance papers and claim forms supplier, customer.

⑦ **Audit of BCP/DRP**:

In a BCP Audit, the auditor is expected to evaluate the processes of developing and maintaining documented, communicated and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of a BCP Audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recovery time period.

Sample list of BCP Audit Steps are:-

1. Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology.
2. Determine if information backup procedures are sufficient to allow for recovery of critical data.
3. Determine if a test plan exists and to what extent the disaster recovery/business resumption plan tests has been tested.
4. Obtain and review the existing disaster recovery/business resumption plan.
5. Obtain and review the existing business impact analysis.
6. Gain an understanding of the methodology used to develop the existing disaster recovery/business resumption plan. Who participated in the development effort?

- Building, Utilities and Transportation
- Information Technology (IT)
- Administrative Procedures

Building Utilities & Transportation:

Does the Disaster Recovery/Business Resumption Plan
1. → have a provision for having a building engineer inspect the building and facilities soon after a disaster.
2. → consider the need for alternative shelter, if needed?
3. → consider the failure of electrical power, natural gas, toxic chemical
4. → consider the disruption of transportation containers and pipes? systems.
5. Review any agreements for use of backup facilities.
6. Are building safety features regularly inspected and tested?
7. Verify that the backup facilities are adequate based on projected needs. Will the site be secure?

Information Technology:

Determine if the plan
1. reflects the current IT environment.
2. includes prioritization of critical applications & systems.
3. includes time requirements for recovery/availability of each critical system and that they are reasonable.
4. Determine if a testing schedule exists and is adequate (at least annually).
5. Does the plan include arrangements for emergency telecommunications.
6. Is there a plan for alternate means of data transmission, if the computer network is interrupted? Has the security of alternate methods been considered?

Administrative Procedures:

Does the Disaster Recovery/Business Resumption Plan covers:
1. → administrative and mgt. aspects in addition to operations?
2. → procedures for disaster declaration, general shutdown and migration of operations to the backup facility.

Is there:
3. → a mgt. plan to maintain operations if the building is severely damaged?
4. → a designated emergency operations center where incident mgt. teams can coordinate response and recovery?
5. Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?
6. Are essential records separated from those that will not be needed immediately?

Marks Allocation

Nov, 14	May, 15	Nov, 15	May, 16	Nov, 16
15m	10m	16m	20m	16m

ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEMS

1. Basics
2. System Development Methodologies (6 Methodologies)
3. System Development Life Cycle (SDLC) (8 phases)
4. Others

1. Basics

① Business Process Design.
② System Development.
③ Achieving System Development Objectives.
④ Accountant's Involvement in Development Work

① **Business Process Design:** It means structuring or restructuring the tasks, functionalities and activities for improvising a business system.
Steps: ① Present Process Documentation
② Proposed Process Documentation
③ Implementation of New Process.

② **System Development:** It refers to the process of examining a business situation, with the intent of improving it through better procedures and methods.
Components: ① System Analysis
② System Design

③ **Achieving System Development Objectives:** (Why Org. fails to achieve their System Dev. Obj.)
① User Related Issues → Shifting user needs, Resistance to change, Lack of user participation, Inadequate testing and user training
② Developer related issues → Lack of std Project Mgt and System Dev Methodology, Overworked & under-trained Dev. staffs
③ Mgt. related issues → Lack of Senior Mgt support & involvement, Dev. of strategic systems.
④ New technologies

May, 15 (6m)

④ **Accountant's Involvement in Development Work:**
① Return on Invt. (ROI)
① Cost → Dev. Costs, Op. Costs, Intangible costs
② Benefits
② Computing cost of IT Implementation and Cost Benefits.
③ Skills expected from an Accountant.

2. System Development Methodologies (6 methodologies)

① Defn
② Characteristics
③ System Dev Methodologies
① Waterfall Model
② Prototyping Model
③ Incremental Model
④ Spiral Model
⑤ Rapid Application Dev. (RAD) Model
⑥ Agile Model.

① **Defn:** Formalized, standardized, well-organized and documented set of activities used to manage a system dev. project.

② **Characteristics:** ① Project is divided into a no. of identifiable processes.
② Specific reports & other documentation, called Deliverables must be produced
③ Users, managers and auditors are req. to participate in the project periodically.
④ System must be tested thoroughly prior to implementation.
⑤ A training plan is developed for those who will operate and use the new system.
⑥ Formal program change controls are established to preclude unauthorized changes.
⑦ A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system.

	Characteristics	Strengths	Weaknesses
① Waterfall Model	→ Traditional approach → each phase is carried out sequentially. → Used for recurring or frequently developed system. ① Divided into sequential phases so some splash back acceptable. ② Emphasis on planning, time schedule & implementation of an entire system at one time. ③ Tight control maintained. ↓ extensive written documentation Approval/sign off (+) by the user & Info. tech. mgt. at the end of most phases.	① Ideal for less experienced project teams & managers. ② ∵ orderly sequence ↓ ∴ quality, reliability, adequacy of software developed. ③ Progress is measurable. ④ Enables to conserve resources.	① ∴ tight controls, ∴ inflexible, slow, costly, cumbersome. ② Only slight movement backwards possible. ③ Little to iterate. ④ Depends on early identification and specification of requirements. ⑤ System performance cannot be tested until fully coded. ⑥ Gap bet' Users and Developers, clear division of responsibility.
② Prototyping Model May 18 (5m)	→ Develop a prototype of the system ↓ Users work with the Prototype & make suggestions ↓ These suggestions are incorporated in another prototype ↓ When prototype satisfies all user requirements, it is turned into a final system. → Used for New type of System, like DSS, MIS, etc. Generic phases: ① Identify Info. system req. ② Dev. the initial prototype. ③ Test & revise ④ Obtain user sign off of the approved prototype.	① User participation in System dev. ② Encourages innovative & flexible designs. ③ Quick implementation of an incomplete but functional application. ④ Potential exists for exploiting knowledge gained in earlier iteration in subsequent iteration. ⑤ Easy identification of confusing and missing functionality. ⑥ Better definition of user needs and requirements. ⑦ Errors are hopefully detected.	① Prototype may have not sufficient checks & balances. ② Prototype can only be successful, if users devote significant time in experimenting it & providing suggestions. ③ Prototype may cause behavioral problems with system users. ④ Requirements may change frequently.
③ Incremental Model (System is developed in parts) ↓ Increments	→ Method of System Development ↓ model is designed, implemented and tested incrementally, until the product is finished. → Combination of Waterfall and Iterative philosophy of prototyping. ① Mini Waterfall for small part of the system, before next increment. ② Overall req. are defined before proceeding to next mini-waterfall.	① Potential exists for exploiting knowledge gained in an earlier increment, as later increment developed. ② Moderate control, maintained through ↓ written documentation (+) approval/sign off by the user & Info. tech mgt. at major milestones. ③ More flexible and less costly to change scope. ④ Concrete evidence of project status throughout the life.	① Before moving into next increment in a series of mini-waterfall, lack of overall consideration of the business problem and technical requirement. ② Each phase of iteration is rigid. ③ Difficult to demonstrate early success to mgt. ④ Some modules completed earlier than other well defined interfaces required.
④ Spiral Model	→ Software development process ↓ combining elements of both design and prototyping-in-stages. → Combines features of the prototyping model and waterfall model. → For large, expensive and complicated projects. ① New System Req defined in much detail. ② Preliminary design from new system ↓ ③ 1st Prototype from Preliminary design. ↓ ④ 2nd Prototype by evaluating 1st prototype in terms of strengths, weaknesses and risks.	① Enhances risk abroidance. ② Optimal dev. of a given software with iterations based on project risk. ③ It can incorporate Waterfall, Prototyping and Incremental methodologies as special cases in the framework and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk.	① Challenging to determine the exact composition of development methodologies to use for each iteration around the Spiral. ② Quite complex and limits reusability. ③ Skilled and experienced project manager is required. ④ No established controls exist for moving from one cycle to another cycle. ⑤ There are no firm deadlines, cycles continue with no clear termination condition leading to inherent risk of not meeting budget or schedule.

5. Rapid Application Development (RAD) Model.

→ Software Dev Methodology uses minimal planning in favour of rapid prototyping.
→ The lack of extensive preplanning generally allows software to be written much faster, and makes it easier to change requirements.

① Fast development and delivery of a high quality system at a relatively low inv. cost.
② Reduces inherent project risk by breaking a project into smaller segments.
③ Emphasis is on fulfilling the business need, while technological or engineering excellence is of lesser importance.
④ If the project starts to slip, emphasis is on reducing requirements to fit the timebox
⑤ Active user involvement is imperative
⑥ Produces documentation necessary to facilitate future dev. and maintenance

① Operational version available much earlier than with Waterfall, Incremental or Spiral framework
② RAD produces system more quickly and to a business focus, so this approach tends to produce system at a lower cost.
③ Quick Initial reviews are possible.
④ Constant integration isolates problems and encourages customer feedback.
⑤ Concentrates on essential system elements from user viewpoint.
⑥ Provides for the ability to rapidly change system design as demanded by users.
⑦ It leads to a tighter fit bet^n user requirements and system specifications

① Fast speed and lower cost may adversely affect the system quality.
② The Project may end up with more requirements than needed.
③ Potential for feature creep when more and more features are added to the system over the course of development.
④ It may lead to inconsistent designs within and across systems
⑤ It may call for violation of programming stds related to inconsistent naming convention and inconsistent documentation.
⑥ It may call for lack of attention to later system administration needs built into system
⑦ Formal reviews and audits are more difficult to implement than for a complete system.
⑧ Since some modules will be completed much earlier than others, well-defined interfaces are req.

6. Agile Model.

→ Organized Set of Software Dev. methodologies based on the iterative and incremental development of requirements and solutions evolve through collaboration bet^n self-organizing cross functional teams
→ Promotes adaptive planning, evolutionary dev. and delivery, time-boxed iterative approach, and encourages rapid & flexible response to change

① Customer satisfaction by rapid delivery of useful software
② Welcomes changing requirements, even late in dev.
③ Working software is delivered frequently.
④ Working software is the principal measure of progress.
⑤ Sustainable dev. able to maintain a constant pace.
⑥ Face to face communication is the best form of communication
⑦ Simplicity
⑧ Self-organizing teams
⑨ Regular adaption to changing circumstances

① Has the concept of an adaptive team which enables to respond to changing requirements.
② The team doesn't have to invest time and efforts, and finally find that by the time they delivered the product, the requirement of the customer has changed.
③ Face to face communication and continuous inputs from customer representative leaves little space for guesswork
④ The documentation is crisp and to the point to save time
⑤ The end result is generally the high quality software in least possible time duration and satisfied customer

① In case of some software deliverds especially large ones it is difficult to assess the efforts required at the beginning of the SDLC
② There is lack of emphasis on necessary designing and documentation.
③ Agile increases potential threats to business continuity and knowledge transfer
④ By nature, agile projects are extremely light on documentation because the team focuses on verbal communication with the customer, rather than on documents or manuals.
⑤ The project can easily get taken off track, if the customer representative is not clear abt. the final outcome
⑥ Agile lacks attention to architectural Integration.
⑦ Agile requires more rework and due to lack of long term planning and light weight approach to architecture rework is often required on Agile projects, when the various components of the software are combined and forced to interact.

Agile Model → RTP Nov, 14

Nov, 14 (6m)

3. System Development Life Cycle (SDLC) (8 phases)

① Defⁿ/Meaning
② Advantages
③ Advantages from IS Audit Perspective
④ Anticipated risks & shortcomings associated with SDLC.
⑤ 8 phases:

① Def^n: SDLC provides System Designers and Developers to follow a sequence of activities. It contains a generic sequence of steps or phases in which each phase of the SDLC uses the result of the previous one.

Newly [1m]

② Advantages:
- Better planning and control by project manager
- Compliance to prescribed stds. ensuring better quality
- Documentation that SDLC stresses on, is an important measure of communication & control
- The phases are impt. milestones and help the project manager and the users for review and signoff

① Planning ② Control ③ Compliance ④ Documentation ⑤ Phases → milestones

③ Advantages from IS audit perspective:
The IS Auditor can have
- clear understanding of various phases of SDLC due to documentation
- on the basis of his/her examination can state in his/her report abt. the compliance by the IS mgt of the procedures.
- If auditor has technical and ability abt. diff. areas of SDLC, knowledge can be guide during diff. phases of SDLC.
- IS auditor can provide an evaluation of the methods and techniques used through the various dev. phases of the SDLC.

④ Anticipated risks and Shortcomings associated with SDLC:
① The dev. team may find it cumbersome
② The users may find that the end product is not visible for a long time.
③ Rigidity of the approach may prolong the duration of many projects.
④ It may not be suitable for small and medium sized projects.

⑤ 8 phases of SDLC:
① Preliminary Investigation
② System Requirement Analysis
③ System Design
④ System Acquisition
⑤ System Development
⑥ System Testing
⑦ System Implementation
⑧ Post Implementation Review and Maintenance.

① Preliminary Investigation:
It is predominantly aimed to determine and analyze the strategic benefits in implementing the system through evaluation and quantification of productivity gains, future cost avoidance, cost savings and intangible benefits.
The deliverable of this phase includes a report including feasibility study observations.

Steps/Activities
① Identification of Problem
② Identification of Objectives
③ Delineation of Scope:
- Dimensions to be covered: (Or IPCE fall) ① Functionality Req. ② Data to be processed ③ Control Req. ④ Performance Req. ⑤ Constraints ⑥ Interfaces ⑦ Reliability Req.
- Two primary methods: ① Reviewing Internal Documents ② Conducting Interviews

Aspects to be kept in mind while eliciting info to delineate scope:
① Diff. users may represent the problem and req. sol^n in diff. ways. The system developer should elicit the needs from the initiator of the project.
② While the initiator of the project may be a member of the senior mgt., the actual users may be from the operating levels in an organization. Understanding their profile.
③ The development org has to clearly quantify the economic benefits to the user organization.
④ It is also necessary to understand the impact of the sol^n on the organization - its structure, roles and responsibilities.
⑤ While economic benefits is a critical consideration when designing on a sol^n, there are several other factors that have to be given weightage too.

① Diff. users → problem → diff ways (sol^n) ∴ Elicit → need → initiator of project
② Initiator of project → member of senior mgt. Actual users → op. levels in an org
③ Dev. org. → quantity economic benefits → user org
④ Understand the impact of sol^n on org.
⑤ Economic benefits → critical consideration, but also consider several other factors
⑥ ① Feasibility Study ② Reporting results to mgt.

① Feasibility Study: Feasibility Stdy is evaluated under the following dimensions:

May 16 (Tue)

1. Technical → Is the technology needed available?
2. Financial → Is the sol^n viable financially?
3. Economic → Return on Investment?
4. Schedule/Time → Can the system be delivered on time?
5. Resources → Are human resources reluctant for the sol^n?
6. Operational → How will the sol^n work?
7. Behavioral → Is the sol^n going to bring any adverse effect on quality of work life?
8. Legal → Is the sol^n valid in legal terms?

[Rakhi Boyfriend Economical Last]

Technical feasibility

It is concerned with hardware & software. The analyst ascertains whether the proposed system is feasible with existing or expected computer hardware & software technology.

Technical issues raised:

- necessary technology exist ← → Does the necessary technology exist to do what is suggested (and can it be acquired)?
- proposed equipment ← → Does the proposed equipment have the technical capacity to hold the data required to run the new system?
- proposed system ← → Will the proposed system provide an adequate response to inquiries regardless of the number of location of users?
- can be expanded ← → Can the system be expanded, if developed?
- Technical guarantees ← → Are there technical guarantees of accuracy, reliability, ease of access, and data security?

Economic feasibility

It includes an evaluation of the incremental costs and benefits expected if the proposed system is implemented. This is the most difficult aspect of the study.

The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- → Cost of conducting a full system investigation.
- → Cost of hardware & software for the class of applications being considered.
- → The benefits in the form of reduced costs or fewer costly errors.
- → The cost if nothing changes (i.e the proposed system is not developed).

Operational Feasibility

It is concerned with ascertaining the views of workers, employees, customers and suppliers, abt the use of computer facility.

Some questions, helping in conducting the operational feasibility:

- → Is there sufficient support for the system from mgt. and users?
- → Are current business methods acceptable to users?
- → Have the users been involved in planning and dev. of project?
- → Will the proposed system cause harm? Will it produce poorer results in any respect or area?

② System Requirement Analysis:

This phase includes a thorough and detailed understanding of the current system, identification of the areas that need modification to solve the problem, determination of user/managerial requirements and to have fair idea abt various system dev. tools. Major deliverable is System Requirements Specification (SRS).

Process:

① Fact finding (Collection of info) [80-100] → Documents, Questionnaires, Interviews, Observation

② Analysis of Present System:

- → Reviewing Historical Aspects.
- → Analysing Inputs.
- → Reviewing Data files. (DFD from overall Procedure)
- → Reviewing Methods, Procedures and Data Communications.
- → Analysing Outputs
- → Reviewing Internal Controls
- → Modeling the Existing System.
- → Undertaking Overall analysis of the existing System.

Objectives:

1. Identify and consult the stake owners to determine their expectations and resolve their conflicts.
2. Analyze the requirements to detect and correct conflicts & determine priorities.
3. Gather data & find facts.
4. Verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable & traceable.
5. To Model activities such as developing models to document data Flow Diagrams, E-R diagrams, and
6. To document activities such as interview, questionnaires, reports etc and development of a system (data) dictionary to document the modeling activities.

③ System Analysis of Proposed system: The required system specifications should be in conformity with the project objectives and in accordance with the following:

- → Outputs are produced with great emphasis on timely managerial reports.
- → Input data is prepared directly from original source documents for processing by the computer system.
- → Methods and procedures that show the relationship of inputs and outputs to the database, utilize data communication as when and where deemed appropriate.
- → Work volumes and timings are carefully considered for present and future periods including peak periods.

④ System Dev. Tools: Many tools & techniques have been developed to improve current info. system and to develop new ones.
Such tools help end users and system analysts primarily for the following:-
① → To conceptualize, clarify, document and communicate the activities and resources in the org. and its info. system.
② → To analyze the present business operations, mgt. decision making and info. processing activities of the org., and.
③ → To propose and design new or improved info. systems to solve business problems or pursue business opportunities that have been identified.

Categories of System Dev. Tools based on system Features are;-

- System Components & flows
- User Interface
- Data attributes & relationships
- Detailed system processes.

Some Prominent Tools

Data Dictionary, Structured English, System Components Matrix, Flowcharts, CASE tools, Data flow diagrams, Decision Tree, Decision Table, User Interface Layout & Forms

Decision Table (4 parts):
① Condition stub
② Action stub
③ Condition entries
④ Action entries

Types:
① Layout form and screen Generator
② Menu Generator
③ Report Generator
④ Code Generator

⑤. System Specification:
At the end of the analysis phase, the system analyst prepares a document called System Requirement Specification (SRS).

Contents of SRS: ① Introduction
② Information description
③ Function description
④ Behavioral description
⑤ Validation Criteria.
⑥ Appendices.
⑦ SRS Review.

IDFCVAS

⑥ Roles Involved in SDLC: Steering Committee, Project Manager, Project Leader, System Analyst / Business Analyst, Module Leader/Team Leader, Programmer/Developer, etc.
Nov, 16 (6m)

Steering Committee: It is a special high power committee of experts to accord approvals for go-ahead and implementations

Functions:
① To provide overall directions and ensures appropriate representation of affected parties.
② To be responsible for all cost and timetables.
③ To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions
④ To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

⑦ System Design: → Key objective of this phase is to design an info. system that best satisfies user/managerial requirements. Major deliverables include a blueprint for the design with the necessary specifications.

Major activities
① Architectural Design
② Design of Data/Info Flow
③ Design of Database → activities → Conceptual Modeling, Data Modeling, Storage Structure Design, Physical Layout Design. (Nov, 14 (6m))
④ User Interface Design → factors affecting Input/output form design → Content, timeliness, format, media, form, Input Volume/Output Volume (Nov, 15 (6m))

⑧ Physical Design: General design principles to develop the design of typical info. system:-
① It is recommended procedure to design 2 or 3 alternatives and choose the best one on pre specified criteria
② Design should be based on analysis.
③ The software functions designed should be directly relevant to business activities.
④ The design should follow standards laid down.
⑤ The design should be modular, with high cohesion and low coupling

⑨ System Operating platform

④. System Acquisition: This phase relates to the acquisition of operating infrastructure including hardware, software & services.

Acquisition stds

Acquisition stds. should focus on the following:-

① Ensuring security, reliability, and functionality already built into a product
② Ensuring managers complete appropriate vendor contract, and licensing reviews and acquiring products compatible with existing systems.
③ Invitations to tender soliciting bids from vendors when acquiring hardware or integrated system and of H/w & S/w
④ Requests for proposals soliciting bids when acquiring off-the-shelf or third party developed software
⑤ Establishing acquisition stds.

Acquiring System Components from Vendors

① Vendor Selection.
② Geographical location of vendor
③ Presentation by Selected Vendor
④ Evaluation of Users Feedback

Besides these some specific considerations are:-

① The benchmark tests.
② Software considerations that can be current applications programs or new programs.
③ The benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.
④ If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible base for comparing all vendors' proposal.

Other Acquisition Aspects and Practices

① Hardware Acquisition
② Software Acquisition
③ Contracts, software licences and Copyright Violations.
④ Validation of Vendors Proposal

Factors to be considered
→ Performance capability of each proposed system in relation to co
May 16 (4m) → Costs & benefits of each proposed system
→ Maintainability of each proposed system
→ Compatibility of each proposed system with existing system
→ Vendor Support.

⑤ Methods of Validating the proposal:
→ Checklists
→ Point Scoring Analysis
→ Public Evaluation Reports
→ Benchmarking problems related Vendors' solutions
→ Testing problems

⑤. System Development:- This phase is supposed to convert the design specification into a functional system under the planned operating system environment.

Characteristics of a Good Coded Application & Program

Nov, 16 (6m) VR EFFE
① Reliability
② Robustness.
③ Accuracy
④ Efficiency
⑤ Usability.
⑥ Readability.

Other Related Aspects of this phase are:-

① Program Coding stds.
② Programming Language
③ Program debugging:
(Steps) → ① Giving input the source program to the compiler
② Letting the compiler to find errors in the program.
③ Correcting lines of code that are erroneous.
④ Resubmitting the corrected source program as input to the compiler
④ Testing the program
⑤ Program Documentation.
⑥ Program Maintenance.

⑥. System Testing: Testing is a process used to identify the correctness, completeness and quality of developed computer software.

Levels/facets of Testing

① Unit Testing → Functional Tests, Performance Tests, Stress Tests, Structural Tests, parallel Tests
② Integration Testing → Bottom-up Integration, Top-down Integration
③ Regression Testing
④ System Testing → Recovery testing, security testing, stress or Volume testing, Performance testing.
⑤ Final Acceptance Testing → Quality Assurance Testing, User Acceptance Testing → Alpha Testing, Beta Testing

Nov, 14 (5m) May 15 (4m) Nov, 15 (6m) Nov 16 (4m)

In terms of techniques:

Static testing
→ Desk test
→ Structured Walk through
→ Code Inspection

Dynamic Analysis Testing
→ Black box testing
→ White box testing
→ Grey box-testing.

7. System Implementation: It is a process of ensuring that the info. system is operational and then allowing users to take over its operation for use and evaluation. Implementation includes all those activities that take place to convert from the old system to the new.

↓ Activities.

1. Equipment installation → site preparation → Installation of new H/w / s/w. → Equipment Checkout.
2. Training Personnel.
3. System change over Strategies → Direct Implementation/abrupt changeover; → Phased Changeover; → Pilot changeover; → Parallel changeover.
4. System Technical Changeover or Conversion
   - → Procedure Conversion
   - → File Conversion
   - → System Conversion.
   - → Scheduling Personnel and Equipment.

8. Post Implementation Review and system Maintenance:

↓ Typical Evaluations
- → Development Evaluation
- → Operational Evaluation
- → Information Evaluation

↓ Types (Maybe (6m))
- → Scheduled Maintenance.
- → Rescue Maintenance.
- → Corrective Maintenance.
- → Adaptive Maintenance.
- → Preventive Maintenance.
- → Perfective Maintenance

4. Others:

Operation Manuals

It is a typical users' guide. Moreover, it may be a technical communication document intended to give assistance to people using a particular system. It is usually written by technical writers, although user guides are written by programmers, product or project managers, or other technical staff, particularly in smaller companies.

The section of an operation manual will includes the following:-

1. A Cover page, a title page and copyright page.
2. A preface, containing details of related documents and info. on how to navigate the user guide.
3. A contents page.
4. A guide on how to use (at least the main functions) of the system.
5. A FAQ (Frequently Asked Questions).
6. A glossary and, for larger documents an index.

Auditors Role in SDLC

The audit of systems under development is primarily aimed to provide an opinion on the efficiency, effectiveness and economy of the project mgt. An auditor's role is to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored.

Control considerations for an auditor:-
- → Documented policy & procedures.
- → Established project team with all infrastructure and facilities.
- → Developers/ MT managers are trained on the procedures.
- → Appropriate approvals are taken at identified mile stones.
- → Development is carried over as per stds, functional specifications.
- → Version control on programs.
- → Source code is properly secured.
- → Adequate audit trails are provided in the system.
- → Appropriateness of methodologies selected.
- → separate test environment for development/test/prod'n test plans.
- → Design norms and naming conventions are as per standards and are adhered to.
- → Business owner testing and approval before system going live.

[Cover ⊕ Preface ⊕ Contents ⊕ Guide ⊕ FAQ ⊕ Glossary]

Marks Allocation

Nov.14	May.15	Nov.15	May.16	Nov.16
10m	20m	20m	24m	22m

AUDITING OF INFORMATION SYSTEMS

1. Basics

① Need for Audit of IS (Why Control?) — Nov.15 (6m)
- ① Organizational Cost of Data loss
- ② Cost of Incorrect Decision Making
- ③ Cost of Computer Abuse
- ④ Cost of Computer Error
- ⑤ Value of Computer Hardware, Software & Personnel.
- ⑥ Maintenance of privacy.
- ⑦ Controlled evolution of computer use.

② Effects of Computer on Audit:

Changes to Evidence Collection — May.16 (6m)
- ① Data retention & storage.
- ② Absence of input documents.
- ③ Non-availability of audit trail.
- ④ Lack of availability of printed output.
- ⑤ Audit evidence.
- ⑥ Legal issues.

Changes to Evidence Evaluation
- ① System generated transactions
- ② Automated transaction processing system (TPS)
- ③ Systemic Error

Nov.14 (6m) / May.15 (4m)

2. IS Audit

① Meaning of IS Auditing
② objectives of IS Auditing
③ Skill set of IS Auditor
④ Functions of IS Auditor
⑤ Categories of IS Audit
⑥ Stages in IS Audit
⑦ Audit Stds. and Best Practices.
⑧ Steps in Performing IS Audit
⑨ Concurrent or Continuous Audit.
⑩ Audit Trail

① Meaning: The IS Audit of an Info. System environment may include one or both of the following:-
(a) Assessment of Internal Controls within the IS environment to assure validity, reliability and security of Info. and Info. System.
(b) Assessment of the efficiency and effectiveness of the IS environment.

② Objectives of IS Auditing: — Nov.15 (4m)
- Asset safeguarding objectives.
- Data Integrity objectives.
- System Effectiveness objectives.
- System Efficiency objectives.

③ Skill set of IS Auditor: — May.16 (6m)
- Knowledge → Business operation, practices, compliance requirements. → IT strategy, policy and procedural controls → Prof. Standards and best practices of IT controls & security
- Understanding → Info. risks & controls → Technical & manual controls relating to business continuity
- Posses Prof. Technical qualification and certifications
- ① Should possess the requisite professional, technical qualification and certifications
- ② Sound knowledge of business operations, practices and compliance requirements
- ③ Knowledge of IT strategies, policy and procedural controls
- ④ Good knowledge of Prof. stds and best practices of IT control and security.
- ⑤ Good understanding of Information risks and controls
- ⑥ Ability to understand technical and manual controls relating to business continuity.

④ Functions of IS Auditor: — Nov.14 (4m) / Nov.15 (5m)

IS Auditors (reviews risk) relating to IT systems and processes like:-
① Inadequate info. security controls
② Inefficient use of resources, or poor governance.
③ Ineffective IT strategies, policies and practices.
④ IT related frauds, (phishing, hacking, etc).

⑤ Categories of IS Audit: (Types) (SISTM)
① Systems and application
② Information processing facilities.
③ Systems Development
④ Mgt of IT and Enterprise Architecture.
⑤ Telecommunications, Internets and Extranets.

⑥ Stages in IS Audit: (Steps) (S-P-FAR-C)
① Scoping and pre-audit survey
② Planning and preparation.
③ Fieldwork
④ Analysis
⑤ Reporting.
⑥ Closure.
May, 15 (6m)

⑦ Audit Standards and Best Practices:
- ISACA → IS auditing standards, IS auditing guidelines, IS auditing procedures, COBIT
- ISO 27001
- Internal Audit Stds.
- Stds. on Internal Audit (issued by ICAI).
- ITIL

⑧ Steps in Performing IS Audit: → Basic Plan, → Preliminary Review

Basic Plan: Planning is the primary and important phase in an IS Audit, which ensures that the audit is performed in an effective manner.
Some imp. points:
① Extent of planning varies according to size of the entity, complexity of the audit & auditor experience
② Obtaining knowledge of the business.
③ Discuss with mgt., staff & Audit committee.
④ Develop and document overall audit plan.

Preliminary Review: It enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

Critical factors to be considered: (Nov, 16) (6m)

NCSC]
① Knowledge of Business
- General Economic factors (+)
- Nature of business, its products & services (+)
- General exposure to business (+)
- Clientele and vendors (+)
- Setup of IT dept (+)
- Level of competence of the Top Mgt. & IT Mgt.

② Understanding the Technology
- Analysis of business process & level of automation (+)
- Extent of dependence on IT to carry its businesses (+)
- Technology architecture (+)
- Knowledge of various technologies.
- Studying IT policies, Stds, guidelines and procedures.
May 15 (6m)

③ Understanding Internal Control System (ICS)

④ Legal Consideration and Audit Stds
- Evaluate Legal & Statutory implication on audit work (+)
- Audit, part of Statutory requirement, then consider related stipulations regulations and guidelines (+)
- Min. set of control objectives imposed by statute (+)
- Consider Audit Stds

⑤ Risk Assessment & Materiality
Nov, 16 (6m)
Steps for a risk-based approach:
① Inventory the IS in use and categorize them
② Determine which of the systems impact critical functions or assets.
③ Assess what risks affect these systems and the severity of impact on business.
④ Based on above assessment decide the audit priority, resources schedule & frequency.

Types of Risk → Inherent, Control, Detection.
Nov, 16 (6m)

⑨ Concurrent or Continuous Audit: Organizations produce info. on a real-time online basis. Real-time recordings need real-time auditing to provide continuous assurance abt the quality of the data. i.e. continuous auditing.

Types of Audit Tools (Continuous Audit Techniques)
→ (i) Snapshots
→ (ii) Integrated Test Facility (ITF)
→ (iii) System Control Audit Review File (SCARF)
→ (iv) Continuous and Intermittent Simulation (CIS)
→ (v) Audit Hooks

Advantages and Disadvantages of Continuous Audit Techniques.

(i) Snapshot: → Technique used to trace a transaction in a computerized system.
→ Snapshot software is built into the system
⇓
Takes images of the flow of any transaction as it moves through the application.
⇓
These images can be utilized to assess the authenticity, accuracy (aac) and completeness of the processing.

(ii) ITF: → Technique in which dummy entity is created in the application system files and the processing of the test data against the entity.

Method of entering Test Data
⇓
Transactions have to be tagged.

Method of removing the effects of ITF transactio
App. system may be programmed to recognize and ignore the ITF transactions.
Additional inputs that reverse the effects.

(iii) SCARF: → SCARF technique involves embedding audit software modules within a host application syst to provide continuous monitoring of the system's transactions. The info collected is written on a special audit file → the SCARF master files.
SCARF technique is like the snapshot technique in many ways, along with other data collection capabilities.

May, 16 (5m)

Info that can be collected using SCARF:
PSSSPPA
① Policy and Procedural Variances.
② System Exception.
③ Statistical Sample.
④ Snapshots and Extended Records
⑤ Profiling data.
⑥ Performance measurement.
⑦ Application System Errors.

(iv) CIS: → This is a variation of the SCARF continuous audit technique. This technique is used to trap exceptions whenever the app system uses a database mgt. system.
→ The DBMS reads an app system transaction. It is passed to CIS to determine whether to examine further or not
⇓
CIS replicates or simulates the app. system processing.
⇓
Every update to the database that arises from processing the selected transaction will be checked by CIS
⇓
Exceptions identified by CIS are written to a exception log file.

(v) Audit hooks: → Audit routines that flag suspicious transactions.

Continuous Audit Techniques

Advantages
① Timely, comprehensive and detailed auditing.
② Surprise Test Capability.
③ Info. to system staff on meeting of objectives
④ Training for new users.

Nov, 15 (5m)

Auditor should be able to
(i) → obtain resources req. from org.
(ii) → use continuous audit techniques, need knowledge of computer system, app system that is relatively stable.

Disadvantages
Continuous audit techniques are more likely to be used
(iii) → if auditors involved in dev. wor of new system.
(iv) → where audit trail is less visible.
(v) → Continuous audit techniques are unlikely to b effective unless they are implemented in an

(vi) Audit Trail: → Audit Trails are logs that can be designed to record activity at the system, application and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives.
→ Audit Trail Objectives:
① Detecting unauthorised access.
② Reconstructing Events.
③ Personal Accountability.

OR
Nov, 16 (6m)

3. Others
① Role of IS Auditor in Physical Access Controls → Risk Assessment, Control Assessment, Review of Documents.
② Audit of Environmental Controls.
③ Managerial Controls and their Audit Trails
④ Application Controls and their Audit Trails.
⑤ Audit of Application Security Controls.
⑥ Major tasks performed by Operating System: ① Scheduling jobs ② Managing resources hardware & software ③ Managing System Security ④ Enabling multiple user resource sharing ⑤ Handling Interr ⑥ Maintaining Usage Record

May, 16 (6m)

Scheduling jobs
Managing → H/w & S/w resources → System security
Enabling multiple user resource sharing
Maintaining
Handling interrupts
(4m)

Marks allocation				
Nov,14	May,15	Nov,15	May,16	Nov,16
10m	10m	8m	9m	15m

INFORMATION TECHNOLOGY AND REGULATORY ISSUES

1. Basics
2. IT Act
3. Requirements of Various Authorities for System Control & Audit
4. Othe

1. Basics

① Objectives of IT Act
② Key definitions.

(Amendment)
IT Act, 2008
IT Act, 2000

① Objectives of IT Act:

1. To grant legal recognition for transactions carried out by means of electronic data interchange. (EDI)
2. To give legal recognition to Digital Signatures for authentication of any info. or matter.
3. To facilitate electronic filing of documents with Govt. dept.
4. To facilitate electronic storage of data.
5. To facilitate and give legal sanction to electronic fund transfer. (EFT)
6. To give legal recognition for keeping of books of accounts by bankers in electronic for
7. To amend the Indian Penal Code, the Indian Evidence Act, 1872 and the Bankers' Book Evidence Act, 1891 and the RBI Act, 1934.

Grant Legal Recognition → ① EDI ② DS ③ EFT

Facilitate → ① Electronic filing ② Electronic storage of data

Amend → ⑦ IPC, IEA, BBEA, RBI

The IT Act extends to whole of India and also applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

② Key definitions:

1. Adjudicating officer: means adjudicating officer appointed u/s (1) of sec. 46.
2. Asymmetric Crypto System: means a system of a secure key pair consisting of a private ke for creating a digital signature and a public key to verify th digital signature.
3. Certifying Authority: means a person who has been granted a license to issue a Electronic Signature Certificate under section 24.
4. Digital Signature: means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of sec. 3.
5. Digital Signature Certificate: means a Digital signature Certificate issued under sec. 35(4).
6. Key pair: In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
7. Private key: means the key of a key pair used to create a digital signature
8. Public Key: means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
9. Electronic form: with reference to info., means any information generated, sent, receive or stored in media, magnetic, optical, computer memory, micro film computer generated micro fiche or similar device.

2. IT Act

Chapter II: Digital Signature & Electronic Signature

Sec 3: Authentication of Electronic Records
Sec 3A: Electronic Signature

Chapter III: Electronic Governance

Sec 4: Legal Recognition of Electronic Records
Sec 5: Legal Recognition of Electronic Signature
Sec 6: Use of Electronic Records and Electronic Signatures in Govt. and its agencies
Sec 6A: Delivery of services by Service Provider
Sec 7: Retention of Electronic Records. ← May,16 (4m)
Sec 7A: Audit of Documents maintained in electronic form
Sec 8: Publication of rules regulations in Electronic Gazette.
Sec 9: Sec 6,7,8 not to confer right to insist doc in electronic form.
Sec 10: Power to make rules by CG ← Nov,15 (4m)
Sec 10A: Validity of contracts formed through electronic means

Chapter IV: Secure Electronic Records & Secure Electronic Signatures.

Sec 14: Secure Electronic Record.
Sec 15: Secure Electronic Signature
Sec 16: Secure Procedures & Practices.

Chapter IX: Penalties, Compensation and Adjudication

Sec 43: Damages to computer
Sec 43A: Failure to protect data.
Sec 44: Failure to furnish info. return
Sec 45: Residuary penalty.

Chapter XI (Offences)

	Imprisonment upto	Fine upto	Both
Sec. 65: Tampering with Computer Source documents	3 yrs	2 L	(✓)
Sec. 66: Computer related offences	3 yrs	5 L	(✓)
Sec 66A: Sending Offensive messages through communication service	3 yrs	& fine	
Sec 66B: Dishonestly receiving stolen computer resource or communication device	3 yrs	1 L	(✓)
Sec. 66C: Identity theft	3 yrs	& 1 L	
Sec. 66D: Cheating by personation by using computer resource	3 yrs	& 1 L	
Sec. 66E: Violation of privacy	3 yrs	2 L	(✓)
Sec. 66F: Cyber terrorism	Imprisonment for life		
Sec 67: Publishing or transmitting obscene material in electronic form	3 yrs (5 yrs)	& 5 L (10 L)	
Sec. 67A: Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	5 yrs (7 yrs)	& 10 L	
Sec. 67B: Publishing or transmitting of material depicting children in sexually explicit act, in electronic form	〃	〃	〃

May, 15 (5m)

3. Requirements of Various Authorities for System Control & Audit

① IRDA
② RBI
③ SEBI

① IRDA

- ① Introduction → The Insurance Regulatory and Dev Authority of India (IRDA) is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India
- ② System Audit
- ③ System Controls
- ④ Preliminaries

② System Audit:
1. All insurers shall have their systems and procs audited at least once in 3 yrs by a CA Firm.
2. In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.
3. CA firm must be having a min of 3-4 yrs of experience of IT systems of banks or mutual funds or insurance companies.

③ System Controls: 1. There should be electronic trfs of Data without manual intervention. Audit Trail required at every Data point. All systems should be seamlessly integrated.
2. The auditor should comment upon the audit trail maintained in the system for various activities
3. The auditor shall also ascertain that the system has separate login for each user and maintains trail of every transaction w.r.t login ID, date and time for each data entry, authorization and modifications

④ Preliminaries: Before proceeding with the audit, the auditor is expected to obtain the following info:-
1. Previous audit reports (Internal Audit / Statutory Audit / IRDA Inspection)
2. Location(s) from where investment activity is conducted.
3. IT Application used to manage the insurers Invt. portfolio
4. Internal Circulars and guidelines of the Insurer.
5. Std. Operating Procedures (SOP)
6. IT security Policy
7. Business Continuity Plan (BCP)
8. Network security Reports pertaining to IT Assets.

Nov, 16 (5m)

② RBI

- ① Introduction → RBI is India's Central banking institution which formulates the monetary policy w.r.t the Indian Rupee. It was constituted:-
  - → to regulate the issue of banknotes.
  - → to maintain reserves with a view to securing monetary stability, and.
  - → to operate the credit and currency system of the country to its advantage.
- ② System Controls
- ③ System Audit

② System Controls:
1. Duties of system programmer/designer should not be assigned to person operating the systems
2. Contingency plans/procedures in case of system failure should be introduced/tested at periodic intervals.
3. An appropriate control measures should be devised and documented to protect the computer system from attacks of unscrupulous elements.
4. BOD and Senior Mgt. are responsible for ensuring that an institution's system of internal controls operates effectively.
5. There should be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
6. With a view to provide assurance to banks mgt. and regulators, banks are required to conduct a quality assurance (at least once every three years) on the banks Internal Audit including IS Audit.

May, 16 (5m)

⑤. System Audit :

① Banks require a separate IS Audit function within an Internal Audit dept. led by an IS Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE).

② As IS Audit is an integral part of the Internal Audit, auditors will also be required to be independent, competent and exercise due professional care.

③ The IS Audit should be independent of the auditee, both in attitude and appearance.

④ Additionally, to ensure independence for the IS Auditors, banks should make sure that: — ① Auditors have access to info. and applications and ② Auditors have right to conduct independent data inspection & analysis.

⑤. Competence: IS Auditors should be professionally competent having skills, knowledge, training and relevant experience.

⑥ IS Audits should also cover branches, with focus on large and medium branches, in areas of control of passwords, user ids, operating system security, segregation of duties, anti-malware, physical security, BCP policy and or testing.

⑦. IS Auditor should review the following additional areas:

→ IT Governance and info. security governance structures and practices implemented by the Bank.
→ Testing the controls on new development before implementing them in live environment.
→ Post implementation review of application controls to be carried out.
→ Detailed audit of SDLC process.
→ IS Auditors may validate IT risks before launching a product or service (identified by business-teams)

⑧. SEBI
① Introduction
② System Controls
③ System Audit
④ Audit Report Norms
⑤ Auditor Selection Norms.

① Introduction → ①. Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market :—
① Issuer of securities
② Investors
③ Intermediaries.
Market

② System Controls:

①. Along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying that the security and integrity of their IT systems

② A proper audit trail for upload/modification/downloads of KYC data to be maintained

③ Systems Audit :

① Audit should be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.

② Stock Exchange/Depository (Auditee) may negotiate & the board of Stock Exchange/Depository shall appoint the Auditors based on the prescribed Auditor selection Norms and TOR.
The auditors can perform a max. of 3 successive audits. The proposal from auditor must be submitted to SEBI for records.

③ Audit Schedule shall be submitted to SEBI at least 2 months in advance, along with scope of current audit & previous audit.

④ The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.

⑤. Audit has to be conducted and the Audit Report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement.

⑥ The Auditee must provide their comment abt. the Non-Conformities (NC) and observations. For each NC, specific time-bound (within 3m) corrective action must be taken and reported to SEBI. The report along with Mgt. Comments shall be submitted to SEBI within 1 month of completion of the audit.

Nov, 14 (Cm)

(4) Audit Report Norms:

① The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories.

② The Audit Report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or observations (or lack of it).

(5) Auditor selection Norms:

① Auditor must be min. 3 yrs of experience in IT audit of securities industry participants eg. stock exchanges, clearing houses, depositories, etc

② The auditor must have experience in/direct access to experienced resources in the areas covered under TOR.

May, 15 (4 yrs)

③ The auditor should've IT audit/governance frameworks and processes conforming to industry leading practices like COBIT.

④ The auditor should not have been engaged over the last 3 yrs in any consulting engagement with any dept/units of the entity being audited.

⑤ The auditor may not have any cases pending against its previous auditees which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

4. Others
   - ① National Cyber Security Policy 2013.
   - ② ISO 27001
   - ③ Information Technology Infrastructure Library (ITIL)

① National Cyber Security Policy 2013: Govt of India recently published the National Cyber Security Policy 2013, with the Vision "To build a secure and resilient cyberspace for citizens, business and Govt" and the Mission "To protect info. and info. infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and co-operation."

Objectives of this policy are:-

① To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

② To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security stds and best practices by way of conformity assessment.

③ To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

④ To enhance and create National and Sectoral level 24x7 mechanisms for obtaining strategic info. regarding threats of ICT infrastructure.

⑤ To enhance the protection and resilience of Nation's critical info. infrastructure by operating a 24x7 National Critical Info. Infrastructure Protection Centre (NCIIPC)

⑥ To create a workforce of 500,000 professional skilled in cyber security in the next 5 yrs through capacity building, skill development and training.

⑦ To provide fiscal benefits to businesses for adoption of standard security practices and processes.

⑧ To enable protection of info. while in process, handling, storage & transit so as to safeguard privacy of citizens' data and for reducing economic losses due to cybercrime or data theft.

⑨ To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention.

⑩ To create a culture of cyber security and privacy enabling responsible user behavior and actions through an effective communication and promotion strategy.

⑪ To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace. (eg: Reliance Metro)

⑫ To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

② ISO 27001: PDCA cycle (① The Plan Phase (Establishing the ISMS) ② The Do Phase (Implementing and working of ISMS) ③ The Check Phase (Monitoring and Review of ISMS) ④ The Act Phase (Update and improvement of ISMS).

Nov 14 (4m)

Benefits of ISO 27001:

① It can act as an extension of the current quality system to include security.
② It provides an opportunity to identify and manage risks to key info. and systems assets.
③ Provides confidence and assurance to trading partners and clients; acts as marketing tool
④ Allows an independent review and assurance to you on info. security ~~policies~~ practices

③ ITIL: ITIL is a set of practices for IT service Mgt. (ITSM) that focuses on aligning IT services with the needs of business. In its current form (ITIL V3 and ITIL 2011 edition) ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklist that ~~be not~~ organization-specific, used by an organization for establishing a minimum level of competency.

Although the UK Govt. originally created the ITIL, it has rapidly been adopted across the world as the std. for best practice in the provision of info. technology services.

ITIL Framework

① Service Strategy
- IT service Generation.
- Service Portfolio Mgt.
- Financial Mgt.
- Demand Mgt.
- Business Relationship Mgt.

Nov, 15 (4m)

② Service Design
- Service Catalogue Mgt.
- Service Level Mgt.
- Availability Mgt.
- Capacity Mgt.
- IT Service Continuity Mgt.
- Info. Security Mgt.
- Supplier Mgt.

Nov, 16 (6m)

③ Service Transition
- Service Transition Planning and Support.
- Change Mgt. & Evaluation
- Service Asset and Configuration Mgt.
- Release and Deployment Mgt.
- Service Validation and Testing
- Knowledge Mgt.

④ Service Operation
- Service Desk
- Application Mgt.
- IT Operations
- Incident Mgt.
- Request fulfillment
- Event mgt.

⑤ Continual Service Improvement.

Marks Allocation:

Nov,14	May,15	Nov,15	May,16	Nov,16
11m	9m	10m	16m	13m

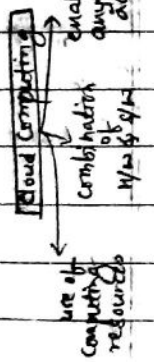
Emerging Technologies

1. Cloud Computing
2. Other Concepts

1. Cloud Computing
   1. Cloud Computing.
   2. Grid Computing.
   3. Goals of Cloud Computing
   4. Cloud Computing Architecture.
   5. Cloud Computing Environment.
   6. Cloud Computing Models
   7. Characteristics of Cloud Computing
   8. Advantages of Cloud Computing
   9. Issues relating to Cloud Computing

①. Cloud Computing:

① Cloud Computing simply means the use of computing resources as a service through networks, typically the internet. ② Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. ③ This model of IT enabled services enables anytime access to a shared pool of applications and resources.



②. Grid Computing:

Grid computing is a network of computing or processor machines managed with a kind of software such as middleware, in order to access and use the resources remotely. The managing activity of grid resources through the middleware is called Grid Services. Grid services provide access control, security, access to data including digital libraries and databases, and access to large-scale interactive and long-term storage facilities.

Grid computing is more popular due to following reasons.

→ ability to make use of unused computing power, thus cost-effective solution.

→ enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.

Cloud Computing V/s Grid Computing

Similarities

→ Cloud computing and Grid computing both are scalable.

→ Both computing types involve multi-tenancy and multi-tasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances.

Differences

→ While the storage computing in the grid is well suited for data-intensive storage it is not economically suited for storing objects as small as 1 byte. While in cloud computing we can store an object as low as 1 byte and as large as 5TB or even several terabytes.

→ A computational grid focuses on computationally intensive operations while cloud computing offers two types of instances; standard and high-CPU.

③. Goals of Cloud Computing: The core goal of utilizing a cloud-based IT ecosystem is to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used to make the services accessible and available from anywhere at any time.

(a) To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used.

(b) To access services and data from anywhere at any time.

(c) To consolidate IT infrastructure into a more integrated and manageable environment.

(d) To reduce the costs related to IT energy/power consumption.

(e) To enable or improve "Anywhere Access" (AA) for ever increasing users, and

(f) To enable rapid provision of resources as needed.

④ Cloud Computing Architecture → Front End Architecture. → Back End Architecture.

⑤ Cloud Computing Environment:

Private Cloud

This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organizations' benefit. Also called Internal Clouds.

Characteristics:
① → Secure
③ → Central Control
② → Weak Service Level Agreements (SLAs)

Advantages:
→ They improve average server utilization, allow usage of low-cost servers and hardware.
→ Provides a high level of security and privacy to the user.
→ Small in size and controlled and maintained by the organization.

Limitation:
→ IT teams in the org. may have to invest in buying, building and managing the clouds independently.
→ Budget is a constraint in private clouds and they also have (lose) SLAs.

Public Cloud

This environment can be used by the general public. Typically, these are administered by third parties or vendor over the Internet and the services are offered on pay-per-use basis. Also called Provider Clouds.

Characteristics:
③ → Highly scalable
⑤ → Affordable
① → Less Secure
④ → Highly available.
② → Stringent SLAs

Advantages:
→ Widely used in the dev., deployment & mgt of enterprise applications at affordable costs.
① → allows org. to deliver highly scalable and reliable applications rapidly and at more affordable costs.
→ no need for establishing Infrastructure for setting up and maintaining the cloud.
③ → Strict SLAs are followed.
④ → No limit for no. of users.

Limitation:
→ Security assurance.
→ Privacy and organizational autonomy not possible.

Hybrid Cloud

This is a combination of both at least one private (internal) and one public (external) cloud computing environments - usually consisting of infrastructure, platforms and applications. The usual method of using a hybrid cloud is to have a private cloud initially and then for additional resources, go for public cloud.

Characteristics:
③ → Scalable
① → Partially Secure
② → Stringent SLAs
④ → Complex Cloud Mgt.

Advantages:
→ Highly scalable and gives power of both private and public.
→ provides better security than public cloud.

Limitation:
→ The security features are not as good as the private cloud and complex to manage.

Community Cloud

It is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that've shared concerns. It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them. In this, a private cloud is shared b/t several organizations.

Characteristics:
② → Collaborative and Distributive maintenance.
① → Partially Secure.
③ → Cost effective

Advantages:
→ allows:
- establishing a low-cost private cloud
- collaborative work on the cloud.
- sharing responsibilities among the org.

→ has better security than the public cloud.

Limitation:
→ the autonomy of the org. is lost and
→ some of the security features are not as good as the private cloud.
→ It is not suitable in the cases where there is no collaboration.

⑥ Cloud Computing Models: (IPS) May16 (6m)

(1) Infrastructure as a Service (IaaS)

Services
- → Compute
- → Storage
- → Network
- → Load Balancers

Characteristics
- → Web access to the resources
- → Centralized mgt
- → Elasticity and dynamic scaling
- → Shared Infrastructure
- → Metered Services

Instances of IaaS
- → Network as a Service (NaaS)
- → Storage as a Service (STaaS)
- → Database as a Service (DBaaS)
- → Backend as a Service (BaaS)
- → Desktop as a Service (DTaaS)

DBD

(2) Platform as a Service (PaaS)

Services
- → Programming languages
- → Application frameworks
- → Database
- → Other tools

PAAS

Characteristics
- → All in One
- → Web access to the dev. platform
- → Off line access
- → Built in Scalability.
- → Collaborative Platform.
- → Diverse Client tools

(3) Software as a Service (SaaS)

Services
- → Business Services
- → Social Networks.
- → Document mgt.
- → Mail services

DBMS

Characteristics
- → One to many model
- → Web access
- → Centralized mgt.
- → Multi-device support.
- → Better scalability.
- → High availability
- → API Integration (Application Programming Interface)

Instances (TAE)
- → Testing as a Service (TaaS)
- → API as a Service (APIaaS)
- → Email as a Service (EaaS)

Other Cloud Service Models (IaaS)
- → Communication as a Service (CaaS)
- → Data as a Service (DaaS)
- → Security as a Service (SECaaS)
- → Identity as a Service (IDaaS)

⑦ Characteristics of Cloud Computing:

- → High Scalability.
- → Agility
- → High availability and reliability
- → Multi-sharing
- → Services in Pay-per-use mode
- → Virtualization
- → Performance
- → Maintenance.

High
- → Scability
- → Agility
- → Availability & Reliability

Multisharing
- → Services in Pay-per-use use

VPM
- → Virtualization
- → Performance
- → Maintenance

⑧ Advantages of Cloud Computing:

Nov15 (5m) [CA,BAEO]

- → Cost Efficiency
- → Almost unlimited Storage
- → Backup & recovery
- → Automatic software integration
- → Easy access to information
- → Quick deployment.

⑨ Issues relating to Cloud computing:

Security Issues

May15 (5m)

- → Confidentiality, Integrity, Availability — CIA
- → Governance
- → Trust
- → Legal issues and compliance
- → Privacy
- → Audit
- → Data Stealing
- → Architecture
- → Identity Mgt and Access Control
- → Incident Response
- → Software Isolation
- → Application Security

Implementation/Adaption Issues
- → Threshold policy
- → Interoperability
- → Hidden Costs
- → Unexpected behavior
- → Software development in cloud
- → Environmental friendly Cloud Computing

2. Other Concepts
- ① Mobile Computing.
- ② Bring Your Own Device (BYOD)
- ③ Social media and Web 2.0. and Web 3.0.
- ④ Green IT

① Mobile Computing:
- Def^n
- ② Components
- ③ How mobile computing works?
- ④ Benefits
- ⑤ Limitations
- ⑥ Issues

① Def^n: Mobile computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link.

② Components:
- Mobile Communication
- Mobile Hardware
- Mobile Software

③ How mobile computing works?
- ⓐ → The user enters or access data using the application on handheld computing device.
- ⓑ → Using one of several connecting technologies, the new data are transmitted from handheld to sites info. system where files are updated and the new data are accessible to other system user.
- ⓒ → Now, both systems (handheld and site's computer) have the same info. and are in sync.
- ⓓ → The process work the same way starting from the other direction.

④ Benefits of Mobile computing:
- Mobile workforce / Sales personnel → It provides mobile workforce with remote access to work order details. / It enables mobile sales personnel to update work order status in real time, facilitating excellent communication.
- Access to corporate services / Knowledgebase → It facilitates access to corporate services and info. at any time, from anywhere / It provides remote access to the corporate knowledgebase at the job location.
- Mgt effectiveness → It enables to improve mgt effectiveness by enhancing info. quality, info. flow and ability to control a mobile workforce.

May, 16 (6m)

⑤ Limitations:
- Insufficient bandwidth.
- Security stds.
- Power Consumption.
- Transmission interferences
- Potential health hazards
- Human interface with device.

Nov, 16 (5m)

⑥ Issues in Mobile Computing:
- → Security Issues
  - Confidentiality
  - Integrity
  - Availability
  - (CIA)
  - Legitimate
  - Accountability
  - (LA)
- → Bandwidth
- → Location Intelligence
- → Power Consumption
- → Revising the technical architecture.
- → Reliability, coverage, capacity and cost.
- → Integration with legacy mainframe and emerging client/server app^n
- → End-to-end design and performance.
- → Business Challenges.

② Bring Your Own Device (BYOD) → BYOD refers to business policy that allows employees to use their prefered computing devices like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smartphones, tablets, etc.) to connect to the corporate network to access info. and application.

Emerging BYOD threats
- → Network Risks
- → Device Risks
- → Application Risks
- → Implementation Risks.

Nov15 (5m) (NBAU)

Advantages of BYOD:
- → Happy Employees
- → Lower IT budgets.
- → IT reduces support requirement
- → Early adoption of new technologies.
- → Increased employee efficiency.

Nov16 (4m)

③. Social Media, Web 2.0, Web 3.0

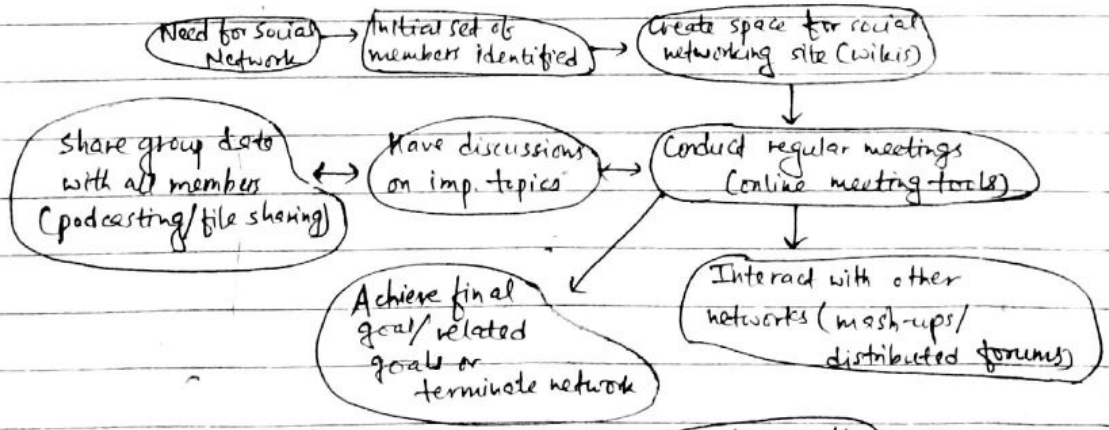
Social Media: A Social Network is usually created by a group of individuals who have a set of common interests and objectives

⇓

Types and Behavior of Social Networks
- → Social Contact Network (Eg. Facebook, twitter, etc).
- → Study Circles (College Tonight).
- → Social networks for Specialist Groups (Linked in)
- → Network for Fine Arts.
- → Police and Military Networks.
- → Sporting Networks
- → Mixed Networks
- → Social Networks for the 'Inventors'
- → Shopping and Utility Service Networks
- → others

⇓

Life Cycle of Social Networks



Web 2.0: Web 2.0 in the term given to describe a second generation of the World Wide Web, that is focussed on the ability for people to collaborate and share info. online. Web 2.0 basically refers to the transition from static HTML web pages to a more dynamic web that is more organized and is based on serving web application to users.
The two major contributors of Web 2.0 are the technological advances enabled by AJAX (Asynchronous JavaScript and XML) and other applications such as RSS (Really Simple Syndication) and Eclipse that support the user interaction and their empowerment in dealing with the web.

⇓

Components of Web 2.0 for Social Network
- → Communities
- → RSS-generated Syndication
- → Blogging
- → Wiki
- → Usage of Ajax and other new technologies
- → Folksonomy
- → File sharing/Podcasting
- → Mash-ups

May16 (4m)

Applications of Web 2.0

(SME) → Social Media
→ Marketing
→ Education.

Web 3.0: The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 is considered as the next Logical step in the evolution of the Internet and Web technologies.

Nov, 16 (4m)

Web 2.0 technologies allows the use of read/write web, blogs, interactive web applications, rich media, tagging or folksonomy while sharing content and also social networking sites focusing on communities. Web 3.0 technology uses the database technology. An eg of typical Web 3.0 application is the one that uses content mgt. systems along with artificial intelligence.

Components of Web 3.0

Semantic Web — Web Services

Q. Green IT :→ 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.

Green Computing Best Practices

Nov, 14 (5m) May, 15 (4m)

Develop a sustainable Green Computing plan

1. Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equip, govt guidelines and recommendations for purchasing green computer equipment in organizational policies and plans.
2. Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
3. Ongoing communication abt. and campus commitment to green IT best practices to produce notable results.
4. Include power usage, red^{n} of paper consumption as well as recommendations for new equip and recycling old m/c in organizational policies & plans.
5. Use cloud computing so that multiple organizations share the same computing resources.

Recycle

1. Dispose e-waste according to central, state or local regulations
2. Discard used or unwanted electronic eg. in a convenient & environmentally responsible manner.
3. Manufacturers must offer recycling options when product becomes unusable
4. Recycle computers through manufacturers' recycling services

Make environmentally sound purchase decisions

1. Purchase of desktop computers, notebooks and monitors based on environmental attributes.
2. Provide a clear, consistent set of performance criteria for the design of products.
3. Recognize manufacturers efforts to reduce the environmental impact of products
4. Use server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

Reduce Paper Consumption

1. Reduce paper consumption by use of e-mail and electronic archiving.
2. Use of 'track changes' feature in electronic documents rather than redline corrections on paper.
3. Use online marketing rather than paper based marketing.
4. While printing documents, make sure to use both sides of the paper.

Conserve Energy

1. Use LCD rather than CRT monitors (Liquid Crystal Display, Cathode Ray Tube).
2. Develop a thin-client strategy
3. Use notebook rather than desktop computers.
4. Power-down CPU and all peripherals during extended periods of inactivity.
5. Power up and power-down energy intensive peripherals according to need.
6. Adapt more of Web conferencing offers instead of travelling to meetings in order to go green & save energy.

Security Issues of Green IT (Short Note)

IT solutions providers are offering green security services in many ways. What to look in green security products, the challenges in the security services market and how security services fare in a recession. If administered properly with other green computing technologies, green security can be a cost-effective and lucrative green IT service for solution providers. The basic aim is to increase the customers energy savings through green security services and assess that "how sustainable computing technology can immediately help the environment." Green IT services present many benefits for clients as well as providers, but knowing "how to evaluate a client's infrastructure to accomodate green technology is really a vital issue."

Moreover, apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact.

Extra Questions:

Diff. bet^n On-Premise Private Cloud & Outsourced Private Cloud.

	On-Premise Private Cloud	Outsourced Private Cloud
Mgt	① Managed by the org. itself.	① Managed by the third party.
SLAs	② SLAs are defined between the organization and its users.	② SLAs are usually followed strictly as it is a third party organization.
Network	③ Network mgt. and network issue resolving are easier.	③ The cloud is fully deployed at the 3rd party site and organizations connect to the 3rd party by means of either a dedicated connection or through internet.
Security & data privacy	④ It is more resistant to attacks than any other cloud and the security attacks are possible from an internal user only.	④ Cloud is relatively less secure and the security threat is from a third party and the internal employee.
Location	⑤ The data is usually stored in the same geographical location where the cloud users are present.	⑤ The cloud is located off site and when there is a change of location, the data need to be transmitted through long distances.
Performance	⑥ Performance depends upon the network and resources and can be controlled by the network mgt. team.	⑥ The performance of the cloud depends on the third party that is outsourcing the cloud.