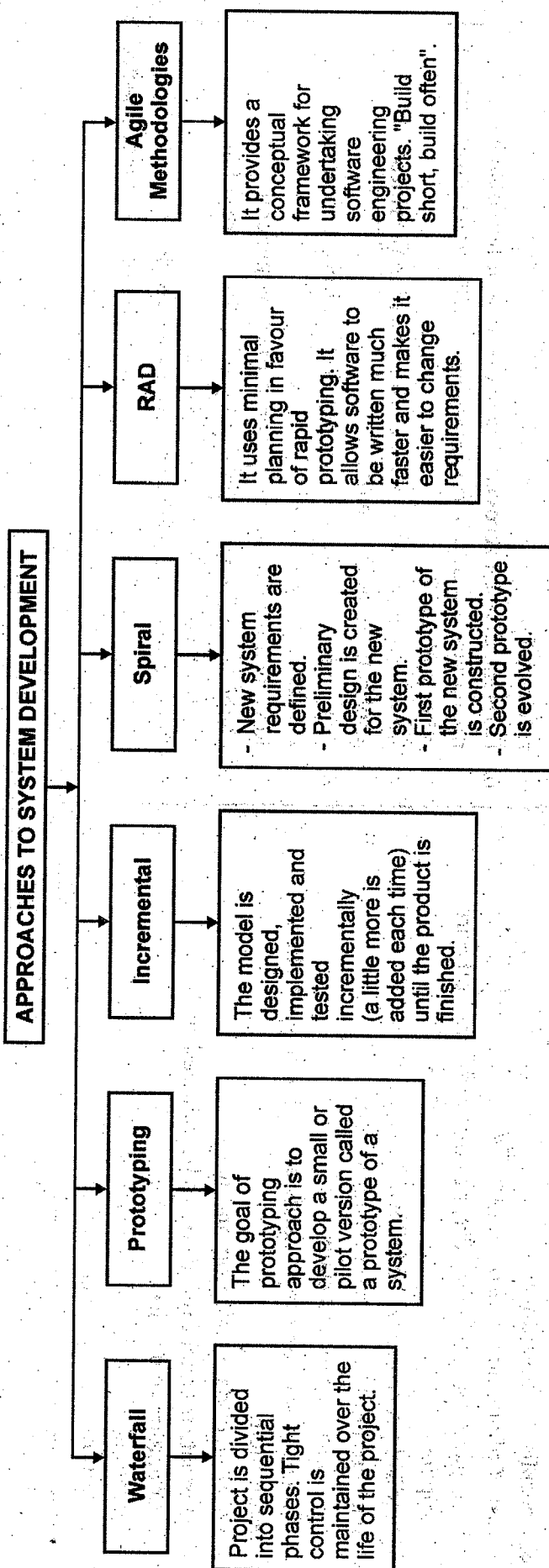


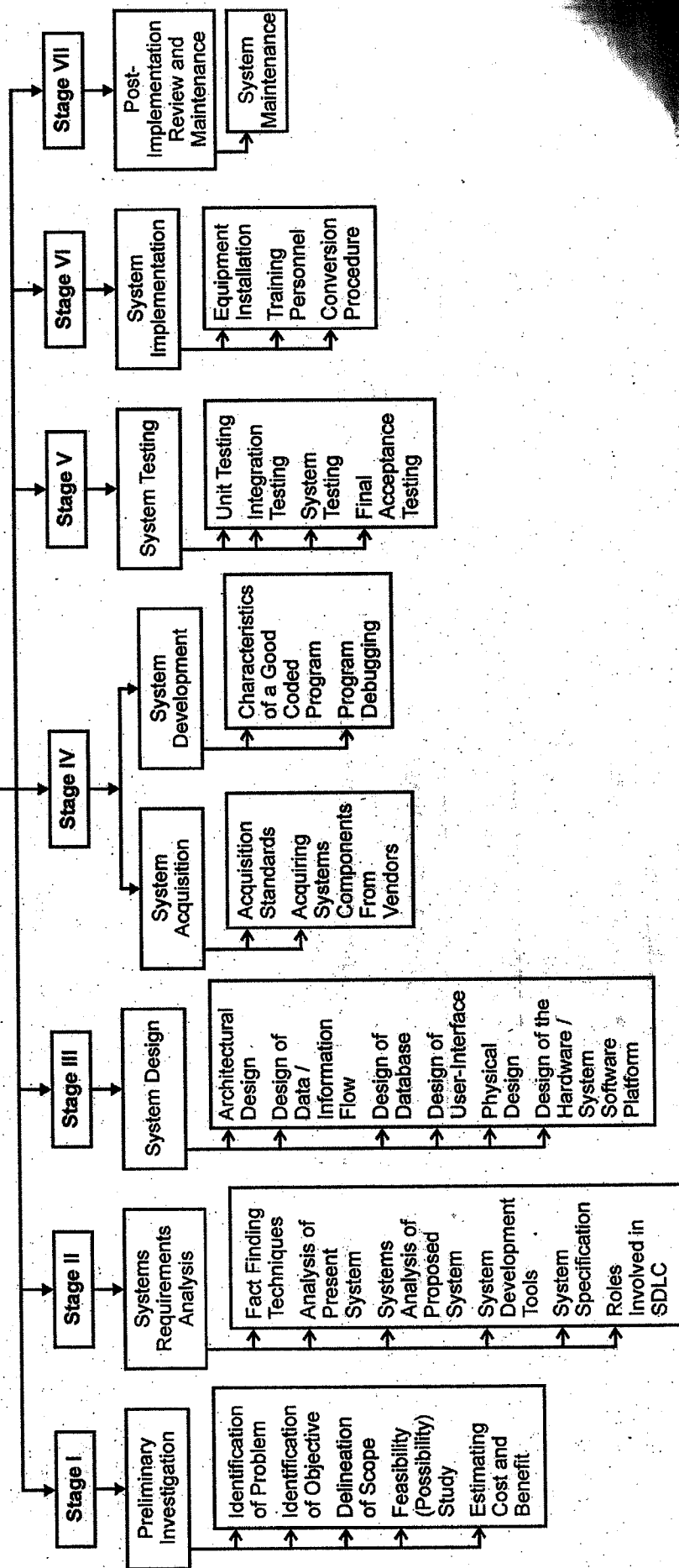
CHAPTER 5 : ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEMS

Flow Chart : 1



Flow Chart : 2

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)



SYSTEMS DEVELOPMENT PROCESS: Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods. • System Analysis • System Design	REASONS FOR FAILURE: • Lack of senior management support for and involvement in information systems development • Shifting user needs • Development of strategic systems • New technologies • Lack of standard project management and systems development methodologies • Overworked or under-trained development staff • Resistance to change • Lack of user participation • Inadequate testing and user training	THE CHARACTERISTICS OF SYSTEM DEVELOPMENT METHODOLOGY: • The project is divided into a number of identifiable processes • Deliverables must be produced • Users, managers, and auditors are required to participate in the project to provide sign-offs. • The system must be tested thoroughly • A training plan is developed • Formal program change controls are established • A post-implementation review of all developed systems must be performed
APPROACHES TO SYSTEM DEVELOPMENT • Waterfall: Linear framework type • Prototyping: Iterative framework type • Incremental: Combination of linear and iterative framework type • Spiral: Combination linear and iterative framework type • Rapid Application Development (RAD): Iterative Framework Type • Agile Methodologies	SYSTEM DEVELOPMENT LIFE CYCLE (SDLC): framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.	THE PHASES INVOLVED IN THE SDLC: (I Require A Design Developer To Implement and Maintain) • Preliminary Investigation • Systems Requirements Analysis • Systems Design • Systems Acquisition & Development • Systems Testing • Systems Implementation • Post Implementation Review and Maintenance

STAGE - I : PRELIMINARY INVESTIGATION - OBJECTIVES Objective: 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 like improvement in morale of employees. Document / Deliverable: A preliminary investigation report/ feasibility study for management.	1. IDENTIFICATION OF PROBLEM • Clarify and understand the project request • Determine the size of the project • Determine the technical and operational feasibility of alternative approaches • Assess costs and benefits of alternative approaches • Report findings to the management with recommendation outlining the acceptance or rejection of the proposal 2. IDENTIFICATION OF OBJECTIVE After the identification of the problem, it is easy to work out the objectives of the proposed solution.	3. DELINEATION OF SCOPE • Functionality requirements • Data to be processed • Control requirements • Performance requirements • Constraints • Interfaces • Reliability requirements Methods with the help of which the scope of the project can be analyzed are as follows: • Reviewing internal documents • Conducting Interviews
4. FEASIBILITY STUDY: (LOBSTER Fry) • <u>Legal</u> • <u>Operational</u> • <u>Behavioural</u> • <u>Schedule / Time</u> • <u>Technical</u> • <u>Economical</u> • <u>Resources</u> • <u>Financial</u>	ESTIMATING COST & BENEFIT COSTS: • Development • Operational • Intangible BENEFITS: • Tangible • Intangible	

STAGE - II : SYSTEMS REQUIREMENTS ANALYSIS FACT FINDING TECHNIQUES: (Doctor Interviews and Questions while Observation) • <u>D</u>ocuments • <u>I</u>nterviews • <u>Q</u>uestionnaires • <u>O</u>bservations	ANALYSIS OF PRESENT SYSTEM • Review <u>H</u>istorical Aspects • Analyze <u>I</u>nputs • Review Data Files Maintained • Review <u>M</u>ethods, Procedures & data Communications • Analyze <u>O</u>utput • Review <u>I</u>nternal Controls • <u>M</u>odel the Existing Physical & Logical System • Undertake <u>O</u>verall Analysis	SYSTEMS ANALYSIS OF PROPOSED SYSTEMS: After each functional area of the present information system has been carefully analysed, the proposed system specifications must be clearly defined.
SYSTEM DEVELOPMENT TOOLS: 1. System Components & Flows • System Flow Chart (SFC) • Data Flow Diagram (DFD) - Data Source & destination - Data Flows - Transformation Process - Data Stores • System Components Matrix • CASE Tools 2. User Interface 3. Data Attributes & Relationship 4. Detailed System Process	STRUCTURED ENGLISH: Structured English, also known as Program Design Language (PDL) or Pseudo Code, is the use of the English language with the syntax of structured programming. Thus, Structured English aims at getting the benefits of both the programming logic and natural language. Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages.	FLOWCHARTS: Flowcharting is a graphic technique that can be used by analysts to represent the inputs, outputs and processes of a business in a pictorial form. It is a common type of chart, that represents an algorithm or process showing the steps as boxes of various kinds, and their order by connecting these with arrows. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

TYPES OF FLOW CHARTS • Document flowchart • Data flowchart • System flowchart • Program flowchart	BENEFITS OF FLOWCHART: • Communication • Effective analysis • Proper documentation • Efficient Coding • Proper Debugging • Efficient Program Maintenance	LIMITATIONS OF USING FLOWCHARTS: • Complex logic • Alterations and Modifications • Reproduction • The essentials of what is done can easily be lost in the technical details of how it is done.
DECISION TREE: A Decision Tree (or tree diagram) is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. DECISION TABLE: A Decision Table is a table which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency. Condition Stub - which comprehensively lists the comparisons or conditions; • Condition Stub • Action Stub • Condition entries • Action entries	DATA DICTIONARY: It is a computer file that contains descriptive information about the data items in the files of a business information system. In other words, it is a computer file about data. <u>Uses:</u> • Aids in documentation - To Programmers & analysts • File Security • For Accountant - Planning flow of transaction data • For Auditors - Establish audit trail • Aids in investigation / documenting internal control procedures	<u>Data Dictionary Contains:</u> • Data item's length, type & range • Identify of source document used to create data item • Names of computer file storing data item • Names of computer programs that modify data item • Identity of individual permitted to access • Identity of individual not permitted to access

LAYOUT FORM AND SCREEN GENERATOR, MENU GENERATOR, REPORT GENERATOR, CODE GENERATOR • Layout form and Screen Generator • Menu Generator • Report Generator • Code Generator	SYSTEM SPECIFICATION At the end of the analysis phase, the systems analyst prepares a document called "Systems Requirement Specifications (SRS)", it contains: • Introduction • Information Description • Functional Description • Behavioural Description • Validation Criteria • Appendix • SRS Review	ROLES INVOLVED IN SDLC • Steering Committee • Project Manager • Project Leader • Systems Analyst / Business Analyst • Module Leader / Team Leader • Programmer / Coder / Developer • Database Administrator (DBA) • Quality Assurance • Tester • Domain Specialist • IS Auditor
STAGE - III: SYSTEM DESIGN System design involves first logical design and then physical construction of a system. Design specifications instruct programmers about what the system should do. The programmers, in turn, write the programs that accept input from users, process data, produce the reports, and store data in the files.	THE DESIGN PHASE INVOLVES: • Architectural Design • Design of the Data / Information Flow • Design of the Database • Design of the User-interface • Physical Design • Design and acquisition of the hardware/ system software platform	DESIGN OF DATABASE • Conceptual Modeling • Data Modeling • Storage Structure Design • Physical Layout Design

DESIGN OF USER-INTERFACE Output Objectives: • Convey info about past, current, future • Signal important events, opportunities, warnings • Trigger an action • Confirmation of action • Meets needs of organisation & users	Important factors in Input / Output design: (<u>CM's</u> <u>Fraud</u> on <u>TV</u>) • <u>C</u>ontent • <u>M</u>edia • <u>F</u>orm • <u>F</u>ormat • <u>T</u>imeliness • <u>V</u>olume	PHYSICAL DESIGN: Design Principles- • The recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria. • The design should be based on the analysis. • The software functions designed should be directly relevant to business activities. • The design should follow standards laid down. • The design should be modular.
STAGE - IV - Part 1: SYSTEM ACQUISITION Acquisition Standards • Ensuring security, reliability, and functionality already built into a product. • Ensuring managers complete appropriate vendor, contract, and licensing reviews. • Including invitations-to-tender and request-for-proposals. • Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.	ADVANTAGES OF APPLICATION SOFTWARE: (<u>Royal</u> <u>Challengers</u> <u>Quit</u> <u>League</u>) • <u>R</u>apid implementation • <u>C</u>ost • <u>Q</u>uality • <u>L</u>ow risk METHODS OF VALIDATING PROPOSAL • Checklists • Point Scoring Analysis • Public evaluation Reports • Benchmarking problem for vendor's proposal • Test problems	Validation of Vendors' proposals: (<u>Vice-Chairman</u> <u>Manages</u> <u>Company's</u> <u>Portfolio</u>) • <u>V</u>endor Support • <u>C</u>ompatibility with Existing Systems • <u>M</u>aintainability of the proposed system • <u>C</u>ost benefits of the proposed system • <u>P</u>erformance rating of the proposed system in relation to its cost

STAGE - IV - Part 2 : DEVELOPMENT (PROGRAMMING TECHNIQUES AND LANGUAGES) Objective: To convert the specification into a functioning system. Activities: Application programs are written, tested and documented, conduct system testing. Document/ Deliverable: A fully functional and documented system.	Characteristics Of A Good Coded Program: • Reliability • Robustness • Accuracy • Efficiency • Usability • Readability	Program Debugging Debugging refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. It consists of: • Inputting the source program to the compiler, • Letting the compiler find errors in the program, • Correcting lines of code that are erroneous, and • Resubmitting the corrected source program as input to the compiler.
STAGE - V: SYSTEM TESTING UNIT TESTING Categories of tests that a programmer typically performs on a program unit: (Pooja Patel Feeds Shrey Shah) • Performance Tests • Parallel Tests • Functional Tests • Stress Tests • Structural Tests	TYPES OF UNIT TESTING • Static Analysis Testing: - Desk Check - Structured walk-through - Code inspection • Dynamic Analysis Testing: - Black Box Testing - White Box Testing - Gray Box Testing	INTEGRATION TESTING • Bottom-up Integration • Top-down Integration • Regression Testing
SYSTEM TESTING • Recovery Testing • Security Testing • Stress or Volume Testing • Performance Testing	FINAL ACCEPTANCE TESTING • Quality Assurance Testing • User Acceptance Testing: - Alpha Testing - Beta Testing	

STAGE - VI : SYSTEM IMPLEMENTATION , EQUIPMENT INSTALLATION • Site Preparation • Installation of New Hardware/Software • Equipment Checkout TRAINING PERSONNEL • System Operators Training • Users Training	CONVERSION PROCEDURE: <u>Activities for successful conversion:</u> (Fifa Played in South Africa) • File conversion; • Procedure conversion • System conversion • Scheduling personnel and equipment • Alternative plans in case of equipment failure	<u>System Implementation Conversion Strategies:</u> • Direct Implementation / Abrupt change-over • Phased implementation • Pilot implementation • Parallel running implementation
STAGE - VII : POST-IMPLEMENTATION REVIEW & MAINTENANCE • Development Evaluation • Operation Evaluation • Information Evaluation	SYSTEM MAINTENANCE • Scheduled maintenance • Rescue maintenance • Corrective maintenance • Adaptive maintenance • Perfective maintenance • Preventive maintenance	OPERATION MANUALS • A cover page, a title page and copyright page; • A preface and information on how to navigate the user guide; • A contents page; • A guide on how to use at least the main functions of the system; • A troubleshooting section; • A FAQ (Frequently Asked Questions); • Where to find further help, and contact details; • A glossary and an index.

CHAPTER 6 : AUDIT OF INFORMATION SYSTEMS

NEED FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS • Organisational Costs of Data Loss • Incorrect Decision Making • Costs of Computer Abuse • Value of Computer Hardware, Software and Personnel • Maintenance of Privacy • Controlled Evolution of Computer Use • System Effectiveness Objectives • System Efficiency Objectives	EFFECT OF COMPUTERS ON AUDIT 1. Changes to evidence collection/ in the audit trail/ audit evidence • Data retention and storage • Audit Evidence • Lack of Visible output • Lack of a Visible audit trail • Absence of Input documents • Legal issues	2. Changes to Evidence Evaluation / New causes and sources of error: • System generated transactions • Systematic Error	RESPONSIBILITY OF IS AUDITOR • Sound knowledge of business operations • Technical qualification and certifications • Understanding of information Risks and Controls • Knowledge of IT strategies, policy and procedure controls • Knowledge of Professional Standards and Best practices • Ability to understand technical and manual controls relating to business continuity.
FUNCTIONS OF IS AUDITOR (i) Inadequate information security (ii) Inefficient use of corporate resources, or poor governance (iii) Ineffective IT strategies, policies and practices (iv) IT-related frauds	CATEGORIES OF IS AUDITS : (MISS Telephone) (i) Management of IT and Enterprise Architecture (ii) Information Processing Facilities (iii) Systems and Applications (iv) Systems Development (v) Telecommunications, Intranets, and Extranets	STEPS IN INFORMATION TECHNOLOGY AUDIT (i) Scoping and pre-audit survey (ii) Planning and preparation (iii) Fieldwork (iv) Analysis (v) Reporting (vi) Closure	AUDIT TRAILS Objectives of Audit Trail : (DR. Audit) 1. Detecting Unauthorized Access 2. Reconstructing Events 3. Personal Accountability

PERFORMING IS AUDIT Audit Planning (i) Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures. (ii) Materiality and significance include both quantitative and qualitative factors	BASIC PLAN The objective of audit planning is to optimize the use of audit resources. Important points are given as follows : • The extent of planning will vary according to the size of the entity • Obtaining knowledge of the business • The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff • The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. • The audit should be guided by an overall audit plan and underlying audit program and methodology.	PRELIMINARY REVIEW The following are some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review. (i) Knowledge of the Business (ii) Understanding the Technology (iii) Understanding Internal Control Systems (iv) Legal Considerations and Audit Standards (v) Risk Assessment and Materiality
Risks are categorised as follows : • Inherent Risk • Control Risk • Detection Risk	DOCUMENTATION BY AUDITOR As per (SA 200) "Overall Objectives of An Independent Auditor and Conduct of An Audit in Accordance With Standards of Auditing", any opinion formed by the auditor is subject to inherent limitations of an audit, which include : • The nature of financial reporting; • The nature of audit procedures; • The need for the audit to be conducted within a reasonable period of time and at a reasonable cost. • The matter of difficulty, time, or cost involved. • Fraud, particularly fraud involving senior management or collusion. • The existence and completeness of related party relationships and transactions. • The occurrence of non-compliance with laws and regulations. • Future events or conditions that may cause an entity to cease to continue as a going concern.	CONCURRENT OR CONTINUOUS AUDIT AND EMBEDDED AUDIT MODULES : (She Is Smart and Cool but Arrogant) 1. Snapshots 2. Integrated Test Facility (ITF) 3. System Control Audit Review File (SCARF) 4. Continuous and Intermittent Simulation (CIS) 5. Audit Hooks

ADVANTAGES	DISADVANTAGES	UNDERSTANDING THE LAYERS AND RELATED AUDIT ISSUES	AUDIT TRAIL FOR APPLICATION CONTROLS
• Timely, comprehensive and detailed auditing • Surprise test capability • Information to system staff on meeting of objectives • Training for new users	• Auditors should be able to obtain resources • More likely to be used if auditors are involved in the development • Auditors need the knowledge and experience of working with computer systems • Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.	BOUNDARY CONTROLS • Audit trail includes • Identify would be user of system. • Authentication Information supplied. • Resources requested. • Action privileges requested. • Start and finish time. • Number of sign on attempts. • Log in and log out time. • Action privileges allowed / denied.	BOUNDARY CONTROLS • Identify would be user of system. • Authentication Information supplied. • Resources requested. • Action privileges requested. • Start and finish time. • Number of sign on attempts. • Log in and log out time. • Action privileges allowed / denied.
Input Controls • Identity of person who was source of data. • Identity of person who entered the data into the system. • Time and date when data was captured. • Physical device used to enter data into system. • The record to be updated by the transaction. • Standing data to be updated. • Detail of the transaction. • Physical or logical batch used for processing. • Number of keying errors. • Number of data coding errors.	Processing Controls • To trace the processing performed on data item. • Comprehensive log on hardware consumption - CPU usage time, storage space used and communication facilities used. • Comprehensive log on software consumption. • Compilers used, file management systems used and communication software used.	ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS 1. Risk assessment 2. Controls assessment 3. Planning for review of physical access controls	Output Controls • What output was presented to users. • Who received the output. • When the output was received. • What actions were taken with the output.

Data-Base Controls ● To attach unique time stamp to all transaction. ● To attach before and after images of data. ● Any modifications or corrections to audit trail transaction accomodating the change that occur within an application system. ● To maintain a chronology of resource consumption events that affects the data base.	Communication Controls ● Unique identifier of the source. ● Time and date at which message was received by the source. ● Time and date at which node in the network was transversed by the message. ● Message sequence number and the image of the message received at each node traversed in the network. ● Log of system restarts. ● Message transit times. ● Queue length at each node.	
---	---	--

CHAPTER 7 : INFORMATION TECHNOLOGY REGULATORY ISSUES

REQUIREMENTS OF IRDA FOR SYSTEM CONTROLS AND AUDIT (i) System Audit (ii) Preliminaries (iii) System Controls • There should be Electronic transfer of Data without manual intervention. • The auditor should comment on the audit trail maintained in the system for various activities. • The auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorisation and modifications.	REQUIREMENTS OF RBI FOR SYSTEM CONTROLS AND AUDIT (i) System Controls • Duties of system designer should be assigned to persons operating the system and there should be separate persons dedicated to system design. • Contingency plans in case of failure of system should be introduced and tested at periodic intervals. • An appropriate control measure should be devised. • Uniformity of software used by various branches / offices. • Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively. • Annual review of IS Audit Policy. • Quality assurance, at least once every three years. (ii) System Audit
REQUIREMENTS OF SEBI FOR SYSTEM CONTROLS AND AUDIT (i) Systems Audit (ii) Audit Report Norms (iii) Auditor Selection Norms (iv) System Controls : • Further, along with the audit report, Stock Exchanges / Depositories are advised to submit a declaration from the MD / CEO certifying the security and integrity of their IT Systems. • A proper audit trail for upload / modifications / downloads of KYC data to be maintained.	

SECURITY STANDARDS Major objectives of this policy are given as follows :- • To create a secure cyber ecosystem • To create an assurance framework • To strengthen the Regulatory framework • To enhance and create National and Sectorial level 24*7 mechanisms • To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information • To develop suitable indigenous security technologies • To improve visibility of the integrity of ICT products and services • To create a workforce of 5,00,000 professional skilled in cyber security • To provide fiscal benefits to businesses • To enable protection of information while in process, handling, storage and transit • To enable effective prevention, investigation and prosecution of cybercrime; • To create a culture of cyber security and privacy enabling responsible user behaviour and actions; • To develop effective public private partnerships; • To enhance global cooperation.	ISO 27001 - INFORMATION SECURITY MANAGEMENT STANDARD (ISMS) These phases are given as follows : (I <u>P</u>lan to <u>D</u>o <u>C</u>heck-up <u>A</u>ctually) • The <u>P</u>lan Phase • The <u>D</u>o Phase • The <u>C</u>heck Phase • The <u>A</u>ct Phase	
	BENEFITS • Extension of the current quality • Opportunity to identify and manage risks • Provides confidence and assurance • An independent review and assurance	ITIL (IT INFRASTRUCTURE LIBRARY) • Service Strategy • Service Design • Service Transition • Service Operation • Continual Service Improvement
HOW STANDARD WORKS ISO 27001 requires that management - • Systematically examine organisation information security risk. threats, vulnerabilities and impacts) • Design and implement comprehensive security controls and/or other form of risk treatment. • Adopt management process to ensure that information security controls continue to meet organisation information security need.	Structure of ISO 27001 Clause 1 : Scope Clause 2 : Normative references Clause 3 : Terms of Definitions Clause 4 : Context of organisation Clause 5 : Leadership Clause 6 : Planning Clause 7 : Support Clause 8 : Operation Clause 9 : Performance evaluation Clause 10 : Improvement	

CHAPTER 8 : EMERGING TECHNOLOGIES

CLOUD VS GRID COMPUTING • Scalability • Multi-tasking • Storage • Focus	GOALS OF CLOUD COMPUTING : (I Saw CAR being Created in front of my Eyes) 1. "Anywhere Access" (AA) 2. To scale the IT ecosystem quickly, easily and cost-effectively. 3. To consolidate IT infrastructure into a more integrated and manageable environment. 4. To access services and data from anywhere at anytime. 5. To reduce costs related to IT energy/power consumption. 6. To create a highly efficient IT ecosystem. 7. To enable rapidly provision resources as needed.	CLOUD COMPUTING ARCHITECTURE • Front End Architecture • Back End Architecture • Middleware
CLOUD COMPUTING ENVIRONMENT (a) Public Clouds (b) Private Clouds (c) Hybrid Clouds (d) Community Clouds	CLOUD COMPUTING MODELS 1. <u>I</u>nfrast<u>r</u>ucture as a Service (<u>I</u>aaS) Services • Storage • Network • Compute • Load • Balances Characteristics • Web Access • Scalable • Centralised • Shared Infrastructure • Metered Services (Pay per use) Instances • NaaS • STaaS • DBaaS • BaaS • DTaaS	2. <u>P</u>latform as a Service (<u>P</u>aaS) Services • Programming Languages • Framework/Templates • Database (For Software Development) • Other Tools Characteristics • Web Access • Scalable • Offline • All in One • Collaborative 3. <u>S</u>oftware as a Service (<u>S</u>aaS) Services • Business Services • Social Network • Document Management • Mail Services Characteristics • Web access • Scalable • High Availability • Centralised • One to Many • Multidevice Support • API Integration Instances • TaaS • APIaaS • EaaS 4. <u>N</u>etwork as a Service (<u>N</u>aaS) 5. <u>C</u>ommunication as a Service (<u>C</u>aaS)

CHARACTERISTICS OF CLOUD COMPUTING : (Multiple Services Should be Performed and Maintained by ARAV)

1. Multi-Sharing
2. Services in Pay-Per-Use Mode
3. High Scalability
4. Performance
5. Maintenance
6. High Availability and Reliability
7. Agility
8. Virtualisation

ADVANTAGES OF CLOUD COMPUTING : (Efficient Iphone Quickly Stores and Back-up's Automatically)

1. Cost Efficiency
2. Easy Access to Information
3. Quick Deployment
4. Almost Unlimited Storage
5. Backup and Recovery
6. Automatic Software Integration

CHALLENGES RELATING TO CLOUD COMPUTING :

(CIA Guys Talks A Lot About Data Privacy but Manages Several Incidents Apathetically)

1. Confidentiality
2. Integrity
3. Availability
4. Governance
5. Trust
6. Audit
7. Legal Issues and Compliance
8. Application Security
9. Data Stealing
10. Privacy
11. Identify Management and Access Control
12. Software Isolation
13. Incident Response
14. Architecture

PERTINENT ISSUES : (Teach Emraan SUSHI)

1. Threshold Policy
2. Environment Friendly Cloud Computing
3. Security Issues
4. Unexpected Behaviour
5. Software Development in Cloud
6. Hidden Costs
7. Interoperability

MOBILE COMPUTING

1. Mobile Computing Benefits

- It provides mobile workforce with remote access to work order details
- It enables mobile sales personnel to update work order
- It facilitates access to corporate services
- It provides remote access to the corporate knowledgebase
- It enables to improve management effectiveness

2. Components of Mobile Computing

- Mobile Hardware
- Mobile Software
- Mobile Communication

3. Limitations of Mobile Computing

- Security
- Power Consumption
- Health Hazards
- Insufficient Bandwidth
- Transmission Inferences
- Human Intervention with Device

4. Issues in Mobile Computing • Security Issues - Confidentiality - Integrity - Availability - Legitimacy - Accountability • Bandwidth • Location Intelligence • Power Consumption • Revising the Technical Architecture • Reliability, Coverage, Capacity and Cost • Integration with Legacy Mainframe and Emerging Client/Server Applications • Business Challenges	BENEFITS AND CHALLENGES FOR SOCIAL NETWORKS USING WEB 2.0 Benefits 1. It provides a platform 2. No new knowledge skills are required. 3. Web 2.0 techniques are very people centric activities 4. People are coming much closer to another 5. Using Web 2.0 also increases the social collaboration to a very high degree Number of challenges 1. Data security and privacy 2. Privacy of individual users also arises 3. A majority of the social networks are offline 4. This becomes more viable in the areas of the world that are developing	BYOD Risks can be classified into four areas as outlined below : (I Need <u>Apple Devices</u>) 1. <u>I</u> mplementation Risks 2. <u>N</u>etwork Risks 3. <u>A</u>pplication Risks 4. <u>D</u>evice Risks
ADVANTAGES/BENEFITS OF BYOD 1. Happy Employees 2. Lower IT Budgets 3. Reduced/Lower IT Support Requirement 4. Early Adoption of New Technologies 5. Increase Employee Efficiency	TYPES AND BEHAVIOUR OF SOCIAL NETWORKS • Social Contract Networks • Study Circles • Social Networks for Specialist Groups • Networks for Fine Arts • Police and Military Networks • Sporting Networks • Mixed Networks • Social Networks for the 'Inventors' • Shopping and Utility Service Networks • Others SOCIAL MEDIA AND WEB 2.0 Components of Web 2.0 for Social Networks • Communities • Blogging • Wikis • Folksonomy • File Sharing/Podcasting • Mashups • Ajax • RSS - Generates Syndication	APPLICATION OF WEB 2.0 1. Social Media 2. Marketing 3. Education APPLICATION OF WEB 3.0 1. Semantic Web 2. Web Services GREEN COMPUTING BEST PRACTICES • Develop a Sustainable Green Computing Plan • Recycle • Make Environmentally Sound Purchase Decisions • Reduce Paper Consumption • Conserve Energy