

CHAPTER 1 : CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

KEY CONCEPTS OF GOVERNANCE • Governance • Enterprise Governance • Corporate Governance	BENEFITS OF GOVERNANCE : (Afterwards Deffy and I Provided Improvised Decision) 1. <u>A</u>chieving enterprise objectives 2. <u>D</u>efining and encouraging desirable behaviour in the use of IT 3. <u>I</u>mplementing and integrating the desired business processes 4. <u>P</u>roviding stability 5. <u>I</u>mproving customer, business and internal relationships 6. <u>E</u>nable effective and strategically aligned decision making for the IT	GOVERNANCE DIMENSIONS • Conformance or Corporate Governance Dimension • Performance or Business Governance Dimension
BENEFITS OF IT GOVERNANCE • Increased value delivered through enterprise IT • Increased user satisfaction • Improved agility • Better cost performance • Improved management • IT becoming an enabler • Improved transparency • Improved compliance • More optimal utilisation of IT resources	KEY PRACTICES TO DETERMINE STATUS OF IT GOVERNANCE • Who makes directing, controlling and executing decisions ? • How the decisions are made ? • What information is required to make the decisions ? • What decision-making mechanisms are required ? • How exceptions are handled ? • How the governance results are monitored and improved ?	KEY GOVERNANCE PRACTICES OF GEIT : (Electronic Dance Music) 1. <u>E</u>valuate the Governance System 2. <u>D</u>irect the Governance System 3. <u>M</u>onitor the Governance System
	BENEFITS OF GEIT • It provides a consistent approach. • IT-related decisions are made in line with the enterprise's strategies and objectives. • IT-related processes are overseen effectively. • Compliance with legal and regulatory requirements. • Governance requirements for board members are met.	

BEST PRACTICES OF CORPORATE GOVERNANCE : (SAIF AND FARHAN CLEARLY EXERCISE IN GYM) 1. <u>S</u>pecial monitoring 2. <u>A</u>ppropriate information flows internally and to the public 3. <u>F</u>inancial and managerial incentives 4. <u>C</u>lear assignment of responsibilities 5. <u>E</u>stablishment of a mechanism for the interaction and co-operation among the board of directors, senior management and the auditors 6. <u>I</u>mplementing strong internal control systems	INTERNAL CONTROLS : (MAP) The SEC's final rules define "internal control over financial reporting" : 1. Pertain to the <u>m</u>aintenance of records 2. Provide reasonable <u>a</u>ssurance that transactions are recorded as necessary to permit preparation of financial statements 3. Provide reasonable assurance regarding <u>p</u>revention of timely detection of unauthorised acquisition, use, or disposition of the company's assets	
INTERNAL CONTROLS AS PER COSO : (ERA of Communalism was Monitored) 1. <u>C</u>ontrol <u>E</u>nvironment 2. <u>R</u>isk Assessment 3. <u>C</u>ontrol <u>A</u>ctivities 4. <u>I</u>nformation and <u>C</u>ommunication 5. <u>M</u>onitoring	IT STEERING COMMITTEE The role and responsibility of the IT Steering Committee : • To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives • To establish size and scope of IT • To review and approve major IT deployment projects • To approve and monitor key projects • To review the status of IS plans • To review and approve standards, policies and procedures • To make decisions on all key aspects of IT • To facilitate implementation of IT security • To facilitate and resolve conflicts in deployment of IT • To report to the Board of Directors on IT activities on a regular basis	STRATEGIC PLANNING There are three levels of managerial activity in an enterprise : • Strategic Planning • Management Control • Operational Control
IT strategy planning in an enterprise could be broadly classified into the following categories : • Enterprise Strategic Plan • Information Systems Strategic Plan • Information Systems Requirements Plan • Information Systems Applications and Facilities Plan		

KEY MANAGEMENT PRACTICES FOR ALIGNING IT STRATEGY WITH ENTERPRISE STRATEGY : (U Are The Greatest Show Conductor) 1. <u>U</u>nderstand enterprise direction 2. <u>A</u>ssess the current environment, capabilities and performance 3. Define the target IT capabilities 4. Conduct a gap analysis 5. Define the strategic plan and road map 6. <u>C</u>ommunicate the IT strategy and direction	BUSINESS VALUE FROM USE OF IT : (Electronic Dance Music) 1. <u>E</u>valuate Value Optimisation 2. <u>D</u>irect Value Optimisation 3. <u>M</u>onitor Value Optimisation	SOURCES OF RISK : (Mainly HNI Causes Political and Economical Tension) 1. <u>M</u>anagement activities and controls 2. <u>H</u>uman behaviour 3. <u>N</u>atural events 4. <u>I</u>ndividual activities 5. <u>C</u>ommercial and Legal relationships 6. <u>P</u>olitical circumstances 7. <u>E</u>conomic circumstances 8. <u>T</u>echnology and Technical issues
RELATED TERMS 1. Asset : Asset can be defined as something of value to the organisation; e.g. information in electronic or physical form, software systems, employees. 2. Vulnerability is the weakness in the system safeguards that exposes the system to threats. 3. Threat : Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorised access, destruction, modification, and / or denial of service is called a threat. 4. Likelihood : Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. 5. Attack : An attack is an attempt to gain unauthorised access to the system's services or to compromise the system's dependability. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by: • Widespread use of technology. • Interconnectivity of systems. • Elimination of distance, time and space as constraints. • Unevenness of technological changes. • Devolution of management and control. • External factors such as legislative, legal and regulatory requirements or technological developments. Countermeasure : An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure. Residual Risk: Any risk still remaining after the counter measures are analysed and implemented is called residual risk.		

RISK MANAGEMENT STRATEGIES : (5T) • <u>T</u>olerate/ Accept the risk • <u>T</u>erminate/ Eliminate the risk • <u>T</u>ransfer/ Share the risk • <u>T</u>reat/ Mitigate the risk • <u>T</u>urn back	KEY GOVERNANCE PRACTICES OF RISK MANAGEMENT : (Electronic Dance Music) 1. <u>E</u>valuate Risk Management 2. <u>D</u>irect Risk Management 3. <u>M</u>onitor Risk Management	KEY MANAGEMENT PRACTICES OF RISK MANAGEMENT : (CA and MAD about Results) 1. <u>C</u>ollect Data 2. <u>A</u>nalys^e Risk 3. <u>M</u>aintain a Risk Profile 4. <u>A</u>rticulate Risk 5. <u>D</u>efine a Risk Management Action Portfolio 6. <u>R</u>espond to Risk	KEY MANAGEMENT PRACTICES OF IT COMPLIANCE : (I Owe Company an Apology) 1. <u>I</u>dentify external compliance requirements 2. <u>O</u>ptimise response to external requirements 3. <u>C</u>onfirm external compliance 4. <u>O</u>btain assurance of external compliance
COBIT 5 - A GEIT FRAMEWORK : NEED FOR ENTERPRISES TO USE COBIT 5 1. Increased value creation from use of IT. 2. User satisfaction with IT engagement and services. 3. Reduced IT-related risks and compliance with laws, regulations and contractual requirements. 4. The development of more business-focused IT solutions and services. 5. Increased enterprise wide involvement in IT-related activities.	CUSTOMISING COBIT AS PER NEED : (I Regularly Go and Ask For Leave) 1. <u>I</u>nformation security 2. <u>R</u>isk management 3. <u>G</u>overnance and management of enterprise IT 4. <u>A</u>ssurance activities 5. <u>F</u>inancial processing or CSR reporting 6. <u>L</u>egislative and regulatory compliance	FIVE PRINCIPLES OF COBIT 5 : (Municipal Corporation of Ahmedabad Ensures Safety) Principle 1 : <u>M</u>eeting Stakeholder Needs Principle 2 : <u>C</u>overing the Enterprise End-to-End Principle 3 : <u>A</u>pplying a Single Integrated Framework Principle 4 : <u>E</u>nabling a Holistic Approach Principle 5 : <u>S</u>eparating Governance from Management	COBIT 5 ENABLERS : (Principal Informs us about the Organisation, Processes, Culture and Services rendered to People) 1. <u>P</u>rinciples, policies and frameworks 2. <u>I</u>nformation 3. <u>O</u>rganisational structures 4. <u>P</u>rocesses 5. <u>C</u>ulture, ethics and behaviour 6. <u>S</u>ervices, infrastructure and applications 7. <u>P</u>eople, skills and competencies

COMPONENTS OF COBIT 5: 1. Control Objective 2. Framework 3. Process Descriptions 4. Management Guidelines	EVALUATING IT GOVERNANCE STRUCTURE AND PRACTICES BY INTERNAL AUDITORS: (Organisational Leaders Perform to Process Risky Controls) 1. Organisational Structure 2. Leadership 3. Performance Measurement/Monitoring 4. Processes 5. Risks 6. Controls	The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows : (Play Station Is Ensured to be Exchanged on MRP) 1. Plan assurance initiatives 2. Scope assurance initiatives 3. Identify and report control deficiencies 4. Ensure that assurance providers are independent and qualified 5. Execute assurance initiatives 6. Monitor internal controls 7. Review business process controls effectiveness 8. Perform control self-assessment
--	--	---

CHAPTER 2 : INFORMATION SYSTEMS CONCEPTS

CLASSIFICATION OF SYSTEM	CHARACTERISTICS OF INFORMATION : (CAR has <u>MRF Tyres</u> and <u>Voice Recorder</u>)	COMPONENT OF INFORMATION SYSTEM	CHARACTERISTICS OF A BUSINESS SYSTEM / COMPUTER-BASED INFORMATION SYSTEM (CBIS)
1. Elements • Abstract System • Physical System 2. Interactive Behaviour • Closed System • Open System • Relatively Closed System 3. Degree of Human Intervention • Manual System • Automated System 4. Working / Output • Deterministic System • Probabilistic System	1. Completeness 2. Cost Benefit Analysis 3. Accuracy and Quality 4. Relevance and Purpose 5. Mode and Format 6. Redundancy 7. Frequency 8. Timeliness 9. Validity 10. Reliability	• People • Computer System • Data • Network	• All systems work for predetermined objectives • No subsystem can function in isolation • If one subsystem or component of a system fails, then in most cases the whole system does not work. • The way a subsystem works with another subsystem is called interaction. • The work done by an individual subsystem is integrated to achieve the central goal of the system.
MAJOR AREAS OF COMPUTER BASED APPLICATIONS	TYPES OF INFORMATION SYSTEMS		TRANSACTION PROCESSING SYSTEM (TPS)
1. Finance and Accounting 2. Marketing and Sales 3. Production and Manufacturing 4. Inventory / Stores Management 5. Human Resource Management	• Operational Level IS - Transaction Processing Systems (TPS) • Management Level IS - Management Information Systems (MIS) - Decision Support Systems (DSS) • Strategic Level IS - Executive Information Systems (EIS) • Knowledge Base IS - Knowledge Management Systems (KMS) - Office Automation Systems (OAS)		• Capturing data to organize in files or databases • Processing of files / databases • Generating information • Handling of queries from various quarters of the organization.

TPS COMPONENTS • <u>I</u>ntputs • <u>P</u>rocessing • <u>S</u>torage • <u>O</u>utputs	FEATURES OF TPS : (LABS) • <u>L</u>arge volume of data • <u>A</u>utomation of basic operations • <u>B</u>enefits are easily measurable • <u>S</u>ource of input for other systems	MANAGEMENT INFORMATION SYSTEM (MIS) Characteristics of an Effective MIS : (MICS is a History) 1. <u>M</u>anagement Oriented 2. <u>M</u>anagement Directed 3. <u>I</u>ntegrated 4. <u>C</u>ommon Database 5. <u>C</u>omputerised 6. <u>S</u>ub system concept 7. <u>H</u>eavy Planning Element	MISCONCEPTIONS ABOUT MIS • Any computer based information system is a MIS. • Any reporting system is MIS. • MIS is a management technique. • MIS is a bunch of technologies. • It is a file structure. • The study of MIS is about use of computers. • More data is generated reports refers more information to managers. • Accuracy plays vital role in reporting.
PRE-REQUISITES OF AN MIS : (D - CESS) 1. <u>D</u>atabase 2. <u>C</u>ontrol and Maintenance of MIS 3. <u>E</u>valuation of MIS 4. <u>S</u>ystem and Management Staff should be qualified 5. <u>S</u>upport of Top Management	CONSTRAINS IN OPERATING A MIS : (QUEST) 1. <u>Q</u>ualified staff not available 2. <u>Q</u>uantifying the benefits of MIS is difficult 3. <u>E</u>xpert's turnover is high 4. <u>S</u>election of Sub system of MIS 5. <u>S</u>tandardised approach not possible 6. <u>S</u>taff's Cooperation not available	LIMITATIONS OF THE MANAGEMENT INFORMATION SYSTEM : (LIMITATION) 1. <u>L</u>ess useful for unstructured data 2. <u>I</u>nternal information is taken into consideration 3. <u>M</u>anagement keeps changing so does their goals 4. <u>I</u>ntputs and processing quality determines the quality of outputs of MIS 5. <u>T</u>ransaction processing system's limitations still exist in MIS 6. <u>A</u>d-hoc reporting is not possible 7. <u>T</u>he Attitudes and moral (non-quantitative factors) are ignored in MIS 8. <u>I</u>ntegration is lacking 9. <u>H</u>oarding of information and not sharing with others exists and hence reduces the effectiveness of MIS 10. <u>N</u>ot a substitute for effective management.	

CHARACTERISTICS OF DSS 1. This supports decision making 2. It should be able to help group making decisions. 3. It should be flexible 4. DSS focuses on decision rather than data and information. 5. It should be easy to use. 6. DSS can be used for structured problems. 7. DSS should be user-friendly. 8. DSS should be extensible and evolve overtime. 9. DSSs are used mainly for decision making rather than communicating decisions and training purposes. 10. The impact of DSS should be on decision where the manager's judgement is essential	COMPONENTS OF A DSS • The User • Databases • A planning language • Model Base	EXAMPLES OF DSS IN ACCOUNTING 1. Cost Accounting System 2. Capital Budgeting System 3. Budget Variance Analysis System 4. General Decision Support System
CHARACTERISTICS OF EIS • EIS is a Computer-based-information system • EIS enables users to extract summary data • EIS provides rapid access to timely information • EIS is capable of accessing both internal and external data • EIS provides extensive online analysis tool • EIS can easily be given a DSS support for decision making	CHARACTERISTICS OF THE TYPES OF INFORMATION USED IN EXECUTIVE DECISION-MAKING : (SUFI Level) 1. <u>S</u>tructure is lacking 2. High degree of <u>U</u>ncertainty 3. <u>F</u>uture orientation 4. <u>I</u>nformal source 5. Low <u>L</u>evel of detail	
PRINCIPLES TO BE FOLLOWED WHILE DESIGNING AN EIS • Easy to understand and collect. • Based on a balanced view of the organisation's objectives. • Reflecting everyone's contribution in a fair and consistent way. • Encouraging for the management and staff to share ownership of the organisation's objectives. • Available to everyone in the organization. • Evolving to meet the changing needs of the organization.		KNOWLEDGE MANAGEMENT SYSTEMS (KMS) Types of Knowledge • Explicit Knowledge • Tacit Knowledge

Different office activities can be broadly grouped into the following types of operations: (<u>F</u>iles are <u>C</u>reated, <u>C</u>aptured, <u>C</u>alculated & <u>R</u>ecorded before <u>D</u>istribution) • <u>F</u>illing, Search, Retrieval and Follow up • Document <u>C</u>reation • Document <u>C</u>apture • <u>C</u>alculations • <u>R</u>ecording Utilization of Resources • Receipts and <u>D</u>istribution	BENEFITS OF OFFICE AUTOMATION SYSTEMS (i) Improve communication (ii) Reduce the cycle time (iii) Reduce the costs (iv) Ensure accuracy	CATEGORIES OF COMPUTER BASED OFFICE AUTOMATION SYSTEMS 1. Text Processing Systems 2. Electronic Document Management Systems 3. Electronic Message Communication Systems 4. Teleconferencing and Videoconferencing Systems
BUSINESS APPLICATIONS OF EXPERT SYSTEM 1. Accounting and Finance 2. Marketing 3. Manufacturing 4. Personnel 5. General Business	BENEFITS OF EXPERT SYSTEMS (i) Expert Systems preserve knowledge (ii) Expert Systems put information into an active-form (iii) Expert Systems assist novices in thinking (iv) Expert Systems are not subject to such human fallings (v) Expert Systems can be effectively used as a strategic tool	The Properties That Potential Applications Should Posses to Qualify For Expert System Development are : (Due to <u>D</u>omain <u>S</u>tructure <u>C</u>omplexity <u>E</u>xpertise is <u>A</u>vailable) (i) <u>D</u>omain (ii) <u>S</u>tructure (iii) <u>C</u>omplexity (iv) <u>E</u>xpertise (v) <u>A</u>vailability
ENTERPRISE RESOURCE PLANNING (ERP) A. <u>C</u>omponents of <u>ERP/Methodology for Implementing ERP Model</u> • Software • Process Flow • Customer Mindset • Change Management	B. Benefits of ERP • Streamline processes into single integrated system. • Improves workflow and efficiency. • Reduced duplication in data entry. • Establish uniform process for sharing information. • Inventory - Reduced inventory cost from better planning. • Improved customer satisfaction. • Faster collection based on better visibility of accounts. • Prepares consolidated picture for organisation.	

CORE BANKING SYSTEM (CBS)**Elements of CBS:**

- (a) Opening a new account
- (b) Process cash deposit and withdrawal
- (c) Processing payments and cheques
- (d) Making loans
- (e) Calculating interest
- (f) Managing CRM
- (g) Establishing minimum balance criteria
- (h) Maintaining records of all activities

INFORMATION SYSTEM AND ITS ROLE IN MANAGEMENT

- Aids in decision-making
- Gain competitive edge
- Innovative ideas
- Knowledge
- It can be integrated to formulate a strategy of action or operation

Information systems perform following three vital roles in business firms:

1. "Support an organization's business processes and operations"
2. "Support business decision-making"
3. "Support Strategic Competitive Advantage"

To operate information systems (IS) effectively and efficiently a business manager should have following knowledge about it :

- Foundation Concepts
- Information Technologies (IT)
- Business Applications
- Development Processes
- Management Challenges

The impact of IT on information systems for different sectors is explained below :

1. E-business
2. Financial Service Sector
3. Wholesaling and Retailing
4. Public Sectors
5. Others

CHAPTER 3 : PROTECTION OF INFORMATION ASSETS

SECURITY OBJECTIVE • <u>C</u>onfidentiality • <u>I</u>ntegrity • <u>A</u>vailability	WHAT INFORMATION IS SENSITIVE ? • Strategic Plans • Business Operations • Finances	TOOLS TO IMPLEMENT POLICY Standards, Guidelines and Procedures	ISSUES TO ADDRESS • A definition of information security. • Reasons why information security. • A brief explanation of the security policies, principles, standards and compliance requirements. • Definition of all relevant information security responsibilities. • Reference to supporting documentation.
MEMBERS OF SECURITY POLICY • Management members • Technical group • Legal experts	TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY : (<u>U</u> And <u>I</u> Can <u>O</u>bviously <u>N</u>ail <u>I</u>t) 1. <u>U</u>ser Security Policy 2. <u>A</u>cceptable Usage Policy 3. <u>I</u>nformation Security Policy 4. <u>C</u>onditions of Connection 5. <u>O</u>rganisational Information Security Policy 6. <u>N</u>etwork and System Security Policy 7. <u>I</u>nformation Classification Policy		
EFFECT OF COMPUTERS ON INTERNAL CONTROLS : (<u>R</u>AM'S <u>P</u>ersonal <u>A</u>ssistant) • <u>R</u>ecord keeping • <u>A</u>ccess to assets and records • <u>M</u>anagement supervision and review • <u>S</u>egregation of duties • <u>P</u>ersonnel • <u>A</u>uthorisation procedures	Internal Controls used within an Organisation comprise of the following five Interrelated Components : (<u>E</u>nvironment <u>I</u>nformation <u>R</u>equires <u>M</u>onitoring <u>A</u>ctivities) • <u>C</u>ontrol <u>E</u>nvironment • <u>I</u>nformation and <u>C</u>ommunication • <u>R</u>isk <u>A</u>ssessment • <u>M</u>onitoring • <u>C</u>ontrol <u>A</u>ctivities	BASED ON OBJECTIVE 1. Preventive Controls 2. Detective Control 3. Corrective Controls 4. Compensatory Controls	Another Classification of Controls is based on the Nature of such Controls with regard to the Nature of IS Resources to which they are applied : (i) <u>E</u>nvironmental Controls (ii) <u>P</u>hysical Access Controls (iii) <u>L</u>ogical Access Controls

BASED ON AUDIT FUNCTION (a) Managerial Control (b) Application Control	INFORMATION CLASSIFICATION : (TCP/IP) • Top Secret • Highly Confidential • Proprietary • Internal Use only • Public Documents	ACCESS CONTROL MECHANISMS 1. Identification 2. Authentication 3. Authorisation	LOGICAL ACCESS PATHS : (D BOOT) 1. Dial-up Ports 2. Online Terminals 3. Operator Console 4. Telecommunication Network
TECHNICAL EXPOSURES (TECHNICAL RISKS) : (Worms Destroyed D Horse by Throwing Bombs) (a) Worms (b) Data Diddling (c) Rounding Down (d) Trojan Horse (e) Salami Techniques (f) Bombs	ASYNCHRONOUS ATTACKS : (Pig LTD) (a) Piggybacking (b) Data Leakage (c) Wire-Tapping (d) Shut Down of the Computer/Denial of Service	COMPUTER CRIME EXPOSURES : (Free DISCS) (a) Financial Loss (b) Legal Repercussions (c) Disclosure of Confidential, Sensitive or Embarrassing Information (d) Industrial Espionage/Blackmail (e) Sabotage (f) Loss of Credibility/Competitive Edge (g) Spoofing	USER CONTROLS 1. Boundary Control 2. Input Control 3. Processing Control 4. Output Control 5. Database Control 6. Communication Control
BOUNDARY CONTROL TECHNIQUES ARE • Personal Identification Numbers (PIN) • Passwords • Cryptography • Identification Cards • Biometric Devices	INPUT CONTROLS (a) Source Document Controls • Use pre-numbered source document • Use source documents in sequence • Periodically audit source documents	(b) Data Coding Controls • Transcription Errors - Addition - Truncation - Substitution • Transposition Errors - Single transposition - Multiple transposition	(c) Validation Controls • Field interrogation • Record interrogation • File interrogation

FIELD INTERROGATION • Limit Check • Picture Check • Valid Code Checks • Check Digit • Arithmetic Checks • Cross Checks	RECORD INTERROGATION • Reasonableness Check • Valid Sign • Sequence Check	FILE INTERROGATION • Version Usage • Internal and External Labeling • Data File Security • Before and after Image and Logging • File Updating and Maintenance Authorisation • Parity Check	PROCESSING CONTROLS 1. Processor Control (i) Error detection and correction (ii) Multiple execution states (iii) Timing controls (iv) Component replication 2. Real Memory Control 3. Virtual Memory Control 4. Data Processing Control : (REFER) • <u>R</u>un-to-run totals • <u>E</u>dit checks • <u>F</u>ield initialization • <u>E</u>xception reports • <u>R</u>easonableness verification • <u>E</u>xistence and Recovery Control
OUTPUT CONTROLS : (Spoon and Log Require Retaining, Storing, Reporting & Printing) • <u>S</u>pooling/Queuing • <u>L</u>ogging of output program executions • <u>R</u>ecovery Controls • <u>R</u>etention controls • <u>S</u>torage of sensitive critical forms • <u>R</u>eport distribution and collection controls • <u>P</u>rinting Controls	DATABASE CONTROLS The update controls are: • Sequence Check Transaction and Master Files • Ensure All Records on Files are processed • Process multiple transactions for a single record in the correct order • Maintain a suspense account The Report controls are: (Standard Print Recovery) • <u>S</u>tanding Data • <u>P</u>rint Run-to-Run control Totals • <u>P</u>rint Suspense Account Entries • <u>E</u>xistence/<u>R</u>ecovery Controls	COMMUNICATION CONTROL (a) Physical Component Control (b) Line Error Control (c) Flow Control (d) Link Control (e) Topology Control (f) Internet Working Control	
		MANAGERIAL CONTROLS 1. Top Management and Information Systems Management Controls 2. Systems Development Management Controls 3. Programming Management Controls 4. Data Resource Management Controls 5. Quality Assurance Management Controls 6. Security Management Controls 7. Operations Management Controls	

DATA INTEGRITY : (SID) is on the POT) • Source data control • Input validation routines • On-line Data Entry Controls • Data Processing and Storage Controls • Output Controls • Data Transmission Controls	DATA INTEGRITY POLICIES • Virus-Signature Updating • Software Testing • Division of Environments • Offsite Backup Storage • Quarter-End and Year-End Backups • Disaster Recovery	DATA SECURITY An IS auditor is responsible to evaluate the following when reviewing the adequacy of data security controls: • Who is responsible for the accuracy of the data? • Who is permitted to update data? • Who is permitted to read and use the data? • Who is responsible for determining who can read and update the data? • Who controls the security of the data? • If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data? • Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
FINANCIAL CONTROL TECHNIQUES • Authorization • Budgets • Cancellation of documents • Documentation • Dual control • Input/ output verification • Supervisory review	PERSONAL COMPUTERS CONTROLS Related risks • Easy to connect and disconnect • Pen drives can be very conveniently transported • Does not provide inherent data safeguards • Segregation of duty is not possible • The staff mobility is higher • The operating staff may not be adequately trained	CONTROL The Security Measures that could be exercised to overcome these aforementioned risks are given as follows : • Physically locking the system • Proper logging of equipment shifting must be done • Centralised purchase of hardware and software • Standards set for developing, testing and documenting • Uses of antimalware software • The use of personal computer and their peripheral must be controls.

REMOTE AND DISTRIBUTED DATA PROCESSING APPLICATIONS CAN BE CONTROLLED IN MANY WAYS

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently.
- There should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled.
- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

LOGICAL ACCESS CONTROL ACROSS THE SYSTEM

- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application and monitoring system access control
- Mobile computing

PHYSICAL ACCESS ISSUES AND EXPOSURES

The following points elucidate the results due to accidental or intentional violation of the access paths:

- Abuse of data processing resources.
- Blackmail
- Embezzlement
- Damage, vandalism or theft to equipments or documents.
- Modification of semester equipment and information.
- Public disclosure of sensitive information.
- Unauthenticated entry

PHYSICAL ACCESS CONTROLS	CONTROLS FOR ENVIRONMENTAL EXPOSURES	CYBER FRAUDS	CYBER ATTACKS
- Locks on Doors - Cipher locks (Combination Door Locks) - Bolting Door Locks - Electronic Door Locks - Biometric Door Locks - Physical identification medium - Personal Identification numbers (PIN) - Plastic Cards - Cryptographic Control - Identification Badges - Logging on utilities - Manual Logging - Electronic Logging - Other means of controlling Physical Access - Video Cameras - Security Guards - Controlled Visitor Access - Bonded Personnel - Dead man Doors - Non-exposure of Sensitive Facilities - Computer Terminal Locks - Controlled Single Entry Point - Alarm System - Perimeter Fencing	- Hand-Held Fire Extinguishers - Manual Fire Alarms - Fire Suppression Systems - Dry-Pipe sprinkling systems - Water based systems - Halon systems - Regular Inspection by Fire Department - Water Detectors - Smoke Detectors - Strategically Locating the Computer Room - Fireproof Walls, Floors and Ceilings surrounding the Computer Room - Electrical Surge Protectors - Uninterruptible Power Supply (UPS) / Generator - Power Leads from Two Substations - Emergency Power-Off Switch - Wiring Placed in Electrical Panels and Conduit - Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility - Documented and Tested Emergency Evacuation Plans	CYBER FRAUDS Two types: - Pure Cyber Frauds - Cyber Enabled Frauds IMPACT OF CYBER FRAUDS ON ENTERPRISES - Financial Loss - Legal Repercussions - Loss of Credibility or Competitive Edge - Disclosure of Confidential, Sensitive or Embarrassing Information - Sabotage TECHNIQUES TO COMMIT CYBER FRAUDS - Hacking - Cracking - Data Diddling - Data Leakage - Denial of Service (DoS) Attack - Internet Terrorism - Logic Time Bombs - Masquerading or Impersonation - Password Cracking - Piggybacking - Round Down - Scavenging or Dumpster Diving - Social Engineering Techniques - Super Zapping - Trap Door	CYBER ATTACKS The major cyber-attacks during the year 2011 are discussed as follows: - Phishing - Network Scanning - Virus/Malicious Code - Spam - Website Compromise / Malware Propagation - Others - Cracking - Eavesdropping - E-mail Forgery - E-mail Threats - Scavenging

CHAPTER 4 : BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

NEED FOR BUSINESS CONTINUITY MANAGEMENT (BCM) Some key terms related to BCM : 1. Business Contingency 2. BCP Process 3. Business Continuity Planning (BCP)	ADVANTAGE OF BUSINESS CONTINUITY 1. is able to proactively assess the threat scenario and potential risks; 2. has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and 3. is able to demonstrate a response through a process of regular testing and trainings.	BCM POLICY The objective of this policy is to provide a structure through which: • Critical services and activities undertaken by the enterprise operation for the customer will be identified. • Plans will be developed to ensure continuity of key service delivery. • Invocation of incident management and business continuity plans can be managed. • Incident Management Plans and Business Continuity Plans are subject to ongoing testing, revision and updation as required. • Planning and management responsibility are assigned to a member of the relevant senior management team.	BUSINESS CONTINUITY PLANNING Business continuity covers the following areas: • Business resumption planning • Disaster recovery planning • Crisis management
OBJECTIVES AND GOALS OF BUSINESS CONTINUITY PLANNING The key objectives of the contingency plan should be to: • Provide for the safety and well-being of people on the premises at the time of disaster. • Continue critical business operations. • Minimise the duration of a serious disruption. • Minimise immediate damage and losses. • Establish management succession and emergency powers. • Identify critical lines of business and supporting functions. The goals of the business continuity plan should be to: • Identify weaknesses and implement a disaster prevention program. • Minimise the duration of a serious disruption to business operations. • Facilitate effective co-ordination of recovery tasks. Reduce the complexity of the recovery effort.			PHASES OF BUSINESS CONTINUITY PLANNING : (Pakistan Vs Bangladesh Delayed Playing Their Match In India) The eight phases are described in detail in the following: 1. <u>P</u>re-Planning Activities 2. <u>V</u>ulnerability Assessment and General Definition of Requirements 3. <u>B</u>usiness Impact Analysis 4. <u>D</u>etailed Definition of Requirements 5. <u>P</u>lan Development 6. <u>T</u>esting Program 7. <u>M</u>aintenance Program 8. <u>I</u>nitial Plan Testing and Plan Implementation

COMPONENTS OF BCM PROCESS • BCM - Management Process • BCM - Information Collection Process • BCM - Strategy Process • BCM - Development and Implementation Process • BCM Testing and Maintenance Process • BCM Training Process	BCM DOCUMENTATION AND RECORDS The following documents (representative only) are classified as being part of the business continuity management system : • The business continuity policy; • The business continuity management system; • The business impact analysis report; • The risk assessment report; • The aims and objectives of each function; • The activities undertaken by each function; • The business continuity strategies; • The overall and specific incident management plans; • The business continuity plans; • Change control, preventative action, corrective action, document control and record control processes; • Local Authority Risk Register; • Exercise schedule and results; • Incident log; and • Training program.	BUSINESS IMPACT ANALYSIS (BIA) For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should : • assess the impacts that would occur if the activity was disrupted over a period of time; • identify the maximum time period after the start of a disruption within which the activity needs to be resumed; • identify critical business processes; • assess the minimum level at which the activity needs to be performed on its resumption; • identify the length of time within which normal levels of operation need to be resumed; and • identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.	BCM TESTING In case of Development of BCP, the objectives of performing BCP tests are to ensure that: • The recovery procedures are complete and workable. • The competence of personnel in their performance of recovery procedures can be evaluated. • The resources such as business processes, IS systems, personnel, facilities and data are obtainable. • The manual recovery procedures and IT backup system/s are current and can either be operational or restored. • The success or failure of the business continuity training program is monitored.
--	--	---	---

MAINTENANCE PROGRAM • Determine the ownership and responsibility. • Identify the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel. • Determine the maintenance regime to ensure the plan remains up-to-date. • Determine the maintenance processes to update the plan. • Implement version control procedures to ensure that the plan is maintained up-to-date.	REVIEWING BCM ARRANGEMENT An audit or self-assessment of the enterprise's BCM program should verify that : • All key products and services and their supporting critical activities and resources have been identified • The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities • The enterprise's BCM competence • The enterprise's BCM solutions are effective • The enterprise's BCM maintenance and exercising programs • BCM strategies and plans incorporate improvements • The enterprises has an ongoing program for BCM training and awareness • BCM procedures have been effectively communicated to relevant staff • Change control processes are in place and operate effectively
TRAINING, AWARENESS AND COMPETENCY • Actively listens to others, their ideas, views and opinions; • Provides support in difficult or challenging circumstances; • Responds constructively to difficult circumstances; • Adapts leadership style appropriately to match the circumstances; • Promotes and positive culture of health, safety and the environment; • Recognizes and acknowledges the contribution of colleagues; • Encourages the taking of calculated risks; • Encourages and actively responds to new ideas; • Consults and involves team members to resolve problems; • Demonstrates personal integrity; and • Challenges established ways of doing things to identify improvement opportunities.	SOFTWARE AND DATA BACK-UP TECHNIQUES - TYPES OF BACK-UPS : (1 Managed to Draw a Flower) 1. <u>I</u>ncremental Backup 2. <u>M</u>irror back-up 3. <u>D</u>ifferential Backup 4. <u>F</u>ull Backup TYPES OF PLANS : (Boys Entered the Room) 1. <u>B</u>ack-up Plan 2. <u>E</u>mergency Plan 3. <u>R</u>ecovery Plan 4. <u>T</u>est Plan ALTERNATE PROCESSING FACILITY ARRANGEMENTS • <u>C</u>old site • <u>H</u>ot site • <u>W</u>arm site • <u>R</u>eciprocal agreement: • <u>T</u>hird party site

DISASTER RECOVERY PROCEDURAL PLAN

- The conditions for activating the plans
- Emergency procedures
- Fallback procedures
- Resumption procedures
- A maintenance schedule
- Awareness and education activities
- The responsibilities of individuals
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organisation
- Checklist for inventory
- List of phone numbers of employees
- Emergency phone list for fire, police, hardware, software, suppliers
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement
- Insurance papers and claim forms.
- Primary computer centre hardware, software, peripheral equipment
- Location of data and program files
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation
- Details of airlines, hotels and transport arrangements.

AUDIT OF THE DISASTER RECOVERY / BUSINESS RESUMPTION PLAN

1. Determine if a disaster recovery plan exists
2. Determine if resources have been made available to maintain the disaster recovery/business resumption plan and keep it current.
3. Gain an understanding of the methodology used to develop the existing disaster recovery/business resumption plan.
4. Interview functional area managers or key employees to determine their understanding of the disaster recovery/business resumption plan.
5. Is there a designated emergency operations center where incident management teams can co-ordinate response and recovery ?
6. Does the disaster recovery/business resumption plan include the names and numbers of suppliers of essential equipment and other material ?
7. Determine if the plan includes prioritisation of critical applications and systems.
8. Determine if the plan includes time requirements for recovery/availability of each critical system.
9. Review information backup procedures in general.
10. Determine if information backup procedures are sufficient to allow for recovery of critical data.
11. Review any agreements for use of backup files.
12. Verify that the backup facilities are adequate based on projected needs.