3.2 need for protection of information system

Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information & executive management has a responsibility to ensure this needs.

3.5.2 Impact of Technology on Internal Controls

Personnel: should have knowledge of IT systems working to discharge their duty.
Segregation of duties: key control. The staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.
Authorization procedures: written evidence may be replaced by computerized authorization controls.
Access to assets and records: Client's financial data and computer programs are vulnerable to unauthorized amendment.
Concentration of programs and data:
Data may be in the access of large number of users and outsiders through the network.

Gap between need to protect & Degree of protection

Components of internal control:
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring

3.6.1 Categories of Controls

Based on Objectives of Controls	Based Nature of IS Resource	Based on Functional Nature
Preventive	Environment	Internal Accounting
Detective	Physical Access	Operational
Corrective	Logical Access	Administrative
Compensatory	IS Operational	
	IS Management	
	SDLC	

3.8.1 Data Integrity

Controls	Policies
Source Document	Virus-Signature Updating
Input Validation	Software Testing
Online data entry	Division of Environments
Data Processing & Storage	Offsite Backup Storage
Output	Quarter-End and Year-End Backups
Data Transmission	Disaster Recovery

Chapter 3-Protection of Information System (Students may note that this summary notes will be helpful to you only if you are reading my full notes) – CA Bhinang Tejani 9898054244 (Bhinang.tejani@gmail.com)

3.3 IS security(I.e. protection of valuable asset)
Objectives:-CIA(DMW)
Confidentiality-Disclosure
Integrity- Modification
Availability-Withholding

3.6.1(Continued) Control Techniques

Organizational Control	Management Control	Financial Control	Data Processing Environment Control	Physical Access Control	Logical Access Control	SDLC Control	BCP Control	Application Control
•Reporting Responsibility & Authority of Each Function •Policy & Procedures •Job Descriptions •Segregation of Duties		•Authorization •Budgets •Cancellation of documents •Documentation •Dual control •Safekeeping •Sequentially numbered documents •Supervisory review						

3.9 Logical Access Control

Access Paths	Exposures			Access Controls
	Technical	Computer Crime	Asynchronous	
•Online Terminal & Operator Console •Dial Up Ports •Telecommunication Link				•User Access Management •User Responsibilities •Network access control •Operating System access control •Application System access control •Mobile Computing

3.3.1 What information are sensitive
Strategic Plans: Critical for success
Business Operations: consist of an organization's process and procedures
Finances: Financial information, such as salaries and wages

3.7 User Controls

Boundary Controls	Input Control	Processing Control	Output Control	Database Control: Update Control	Database Control: Report Control
•Cryptography •Passwords •PIN •Identification Cards •Biometric Devices				•Sequence Check •Ensure all records are processed •Processing multiple transaction for single record •Maintain Suspense A/c	•Standing data control •Print run to run total •Print Suspense A/c •Recovery Controls

Exposures (Heading 3.9 continued)

Technical	Computer Crime	Asynchronous
Data Dibbling, Bombs, Trojan Horse, Worms, Rounding Down, Salami Technique, Trap Door	Financial Loss, Legal Repercussions Loss of Credibility, Blackmail, Sabotage, Disclosure of confidential Information, Spoofing	Data Leakage Wire Tapping Piggy backing Denial of Service

3.4 Information Security Policy (Formal statement of the rules.)
Statement of intent about how to protect a company's information assets.

3.10 Physical Access Controls

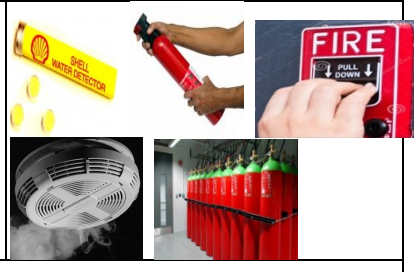
Locks on Doors	Physical Identification	Logging on	Others
		Manual Electronic	

3.4.1 Tools to Implement Policy
Standards specify technologies and methodologies to be used to secure systems. (specify uniform use of specific technologies)
Guidelines help in smooth implementation of information security policy. (assist in effectively securing their systems)
Procedures are more detailed steps to be followed to accomplish particular security related tasks. (Assist in implementing applicable information security Policy.)

3.4.2 Issues to address In security policy
definition of security
definition of all relevant responsibilities
explanation of policies, principles, standards and compliance requirements,
goals and principles,
reasons why security is important
Reference to supporting documentation.

3.5 Information Systems Control
Control means Policies, procedures, practices and enterprise structure designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented, detected and corrected.

3.11 Environmental Control

Resources	Exposures
Hardware and Media Information Systems Supporting Infrastructure or Facilities Documentation Supplies People	

3.4.3 Members of Policy
Management members who have budget and policy authority,
Technical group who know what can and cannot be supported,(Engineer) and
Legal experts who know the legal ramifications of various policy charges.(Advocate)

3.12 Cyber Frauds: Two Types
1. Pure Cyber Fraud
2. Cyber Enabled Fraud

3.4.4 Types of Policy
Information Security Policy: provides definition of Information Security, its objective and importance.
User Security Policy: sets out the responsibilities and requirements.
Acceptable Usage Policy: acceptable use of email and Internet services
Organizational Information Security Policy: main IT security policy. Sets out the Group policy for the security of its information and systems processing this information.
Network & System Security Policy: policy for system and network security.
Information Classification Policy: policy for the classification.

3.12.1 Cyber Attack

	Other categories of attack are:
Phishing Network Scanning Virus/Malicious Code Website Compromise/ Malware Propagation	Cracking Eavesdropping E-mail Forgery E-mail Threats Scavenging

3.4.5 Purpose and Scope of the Document and the intended audience;

Impact of Cyber Crime

Techniques of Cyber Crime

Components of the Security Policy:	Security Infrastructure; Security organization Structure; Incident response mechanism and incident reporting; Inventory and Classification of assets; Physical and Environmental Security; Identity Management and access control; IT Operations management; IT Communications; System Development and Maintenance Controls Business Continuity Planning Legal Compliances	Financial Loss, Legal Repercussions, Loss of credibility or Competitive Edge, Disclosure of Confidential, Sensitive or Embarrassing Information, Sabotage.	Hacking Cracking Data Diddling Data Leakage Denial of Service (DoS) Attack Internet Terrorism Logic Time Bombs Masquerading	Password Cracking Piggybacking Round Down Scavenging or Dumpster Diving Social Engineering Techniques Super Zapping