Information Systems Control and Audit - Ch 6

NO.	QUESTIONS	MNEMONICS	ANSWERS
1	Need for Audit of Information Systems	COST - 4	Organizational **costs** of data loss **Cost** of computer abuse High **costs** of computer error **Costs** of incorrect decision making Maintenance of privacy Value of hardware, software personnel Controlled evolution of computer use
2	Objectives of IS Audit	DAS	**Data Integrity** Objectives **Asset Safeguarding** Objectives **System Effectiveness** Objectives **System Efficiency** Objectives
3	Effect of Computers on Internal Audit		(i) Changes to Evidence Collection (ii) Changes to Evidence Evaluation
4	Changes to Evidence Collection	AND ALL	Absence of input documents Non-availability of audit trail Data retention and storage Audit evidence Lack of availability of output Legal issues
5	Changes to Evidence Evaluation	SAS	System generated transactions Automated transaction processing Systemic Error
6	Functions of IS Auditor	IS Auditors review risks relating to IT systems and processes; some of them are:	Inadequate information **security controls** Inefficient use of **resources, or poor governance** Ineffective **IT strategies, policies and practices** IT-related **frauds**
7	Categories (TYPES) of IS Audits : 5	MIS	Management of IT and Enterprise Architecture Information Processing Facilities Intranets,Extranets & Telecommunications Systems and Application Systems Development
8	Steps in IS Audit		Scoping and pre-audit survey Planning and preparation Fieldwork Analysis Reporting Closure
9	Audit Standards and Best Practices		IS auditing standards IS auditing guidelines IS auditing procedures COBIT ISO 27001 Internal Audit Standards Standards on Internal Audit

Information Systems Control and Audit - Ch 6

10	Types of Audit Tools	SISCA (LED)	Snapshots Integrated Test Facility (ITF) System Control Audit Review File (SCARF) Continuous and Intermittent Simulation (CIS) Audit Hooks

11	Types of Info - SCARF	SAP	Snapshots and Extended Records System Exception Statistical Sample Application System Errors Policy and Procedural Variances Performance Measurement (of an application system) Profiling Data (Profiles of system users)
12	Advantages of continuous audit techniques (CAT)	SIT	Surprise test capability Information to system staff on meeting of objectives Timely, Comprehensive and Detailed Auditing Training for new users
13	Limitations of continuous audit techniques (CAT)		Auditors are involved in the development work Auditors need the knowledge and experience Auditors should be able to obtain resources required Audit trail is less visible Application system that is relatively stable
14	Audit Trail Objectives	DRP	Detecting unauthorized access to the system Reconstruction of events Promoting personal accountability
15	Application Controls and their Audit Trail Audit Trails : 2	IPO BCD	Input Controls Processing Controls Output Controls Boundary Controls Communication Controls Database Controls A/c ing Operational
16	Managerial Controls and their Audit Trails	STOPS DQ	System Development Top Management and IS Operations Programming Security Data Resource Quality Assurance
17	Understanding of the technology env. (How to unders. Tech. Env.)		Studying IT policies, standards, guidelines & procedures Studying network diagrams Analysis of business processes Assessing the extent of dependence on IT Knowledge of various technologies Understanding technology architecture Understanding extended enterprise architecture
18	KEY STEPS : Risk-based approach to make an audit plan		Inventory (Make list of) the IS in use Determine which of the systems impact CBO Assess what risks affect these systems Decide the audit priority, resources, schedule and frequency
19	Application Security Audit - 3 Layers	Operational Layer Tactical Layer Strategic Layer	User Accounts & Access Rights Password Control Segregation of duties Timely updates to user profiles Audit Logging & Monitoring IT Risk Mgt Interface Security