Module 13 · Information Systems Security Audit P17 · 13.1–13.4

SM pp. 580–602, exercise 603–608. **45 marks in 7 papers. Q7(a), 7 marks, was an IS-audit question in every paper from Jun'24 to Dec'25** (Dec'23 had it as Q6(b), Jun'23 as Q7(b)); Jun'26 gave Q7(a) to corporate image instead. Answers are SM headings in SM order; the PTP answer copies SM 586.

Paper	Question	Paper	Question
Jun'23	Q7(b) **disruption of operations + business continuity planning** (8) · MCQ security in IS design	Jun'25	Q7(a) **role of cyber security in protecting data** (= PTP Q7(a) word for word)
Dec'23	Q6(b) **cyber security and computer forensics: the difference**	Dec'25	Q7(a) **steps in an IT security audit**
Jun'24	Q7(a) **IS audit approaches**	Jun'26	(Q7(a) went to corporate image, Module 12)
Dec'24	Q7(a) **IS auditor of a bank: maintaining data integrity**	Dec'26?	postal Q9(a) **pitfalls of inadequate security controls** (never asked) · postal: auditing with a computer

DEC'26 PREDICTION · Q7(a), 7 MARKS · ABOUT 70% IT IS IS AUDIT

- By the slot model: cyber security / forensics (13.3) 25% · IS audit in banks, approaches, BCP (13.4) 20% · security framework, pitfalls of weak controls (13.2) 15% · IT security audit steps (13.1) 10%. The other 30%: corporate image or ESG (Module 12).
- Write-first list: **pitfalls of inadequate controls** (postal, never asked) · **objectives of IS audit** · **IS audit methodology (5 steps)** · **business continuity plan + cold / warm / hot sites** · **RBI cyber security framework**.
- MCQ facts: three approaches · around = inputs vs outputs · audit trail localises the source of an error · firewall stops hackers · ACL · 90% of network problems are cable-related · effectiveness > 100%.

MAP OF THE MODULE

13.1 IT SECURITY AUDIT
5 steps: objectives → plan → perform → report → act

↓

13.2 COMPLIANCE FRAMEWORK
RBI: top-down governance, CSITE cell, baseline controls, levels 1–4

↓

13.3 CYBER SECURITY vs FORENSICS
prevention vs reaction

↓

13.4 IS AUDIT (BANKS)
4 objectives · 3 approaches · CAATs · 5-step method · framework A–F · BCP · KYC case

13.1 IT security audit · Dec'25 Q7(a)

- SM WORDS An IT security audit is a **comprehensive examination and assessment of an enterprise's information security system**; regular audits identify **weak spots and vulnerabilities**, verify security controls, ensure **regulatory compliance**. It verifies the security of hardware, software, services, networks and data centres. [SM 580]
- It answers: any weak spots? any tools that serve no security purpose? can we fend off threats and **recover after an outage or breach**? what action for the flaws found? Many laws require it for collection, use, retention and destruction of personal data. A **compliance audit** is done by a certified auditor of the regulator or an independent third party; staff may do an internal one. [SM 580]
- **Security audit vs risk assessment** (timing and scope): a **risk assessment** comes at the **start of an IT initiative**, before tools are deployed, and whenever the threat landscape changes (ransomware rise, remote working); it looks **outward**, to decide how to build the infrastructure. A **security audit** tests the **existing** infrastructure, at regular intervals. [SM 582]
- **Best practices**: clear objectives and scope; **buy-in from key stakeholders** (CSO, CIO, management sponsorship);

THE FIVE STEPS (THE DEC'25 ANSWER)

1. **Define the objectives**: goals with their business value, aligned to the company's goals. Which systems and services? Digital infrastructure, physical equipment, or both? Disaster recovery? A particular regulation?
2. **Plan the audit**: roles of management and IT administrators; schedule and methodology; tools for identifying, monitoring, reporting and **data classification**; logistics (taking equipment offline); **document and circulate** the plan.
3. **Perform the auditing work** per the plan: **scans** of file-sharing services, database servers, SaaS (e.g. Office 365) for network security, data access levels, **user access rights**, configurations; **physically inspect the data centre** for fire, flood, power surges; **interview employees outside IT** on security awareness and policy.
4. **Report the results**: formal report to management or the regulator: risks and vulnerabilities found + recommended mitigation.
5. **Take necessary action**: **remediation** of flaws; **training** in security compliance and awareness; best practices for sensitive data, **malware and phishing**; new technologies and regular monitoring.

clear **action items** from the results; audit the whole portfolio on a schedule. [SM 582]

[SM 580–581]

13.2 Compliance and security framework (RBI for banks) · pitfalls of weak controls

- Banking relies on electronic platforms, so **RBI expects banks to assess their cyber security preparedness**, with a **top-to-down approach** in information security governance: Board → IT and IS committee → down the hierarchy. Banks report to the **CSITE Cell** (Cyber Security and Information Technology Examination) of the Department of Banking Supervision: (1) **gap analysis** against the Cyber Security / Resilience Framework; (2) information security controls; (3) their **effectiveness**; (4) plan of action to mitigate risks; (5) role of the **CISO**. [SM 583]
- **How RBI audit is done**: in-depth technical assessment; information security process audit; applicability of cyber controls; **evidence and logs on servers**; all RBI technical norms. **Report**: detailed **gap analysis**; who must do what to comply, by which team or person. [SM 583]
- **Baseline controls** (selection): inventory of IT assets; preventing unauthorised software; application security life cycle; **patch, vulnerability and change management**; vendor risk; removable media; **audit logs**; network security; **user access control**; customer authentication; anti-phishing; **VAPT**; red team exercises; **incident response**; awareness; secure configuration; secure mail; **data leak prevention**; risk-based transaction monitoring. [SM 583–584]
- **By level**: Level 1 = baseline + vendor / outsourcing risk; Level 2 adds network, configuration, ASLC, change management, periodic testing, access, anti-phishing, DLP, logs, incidents; Level 3 adds advanced real-time threat defence and risk-based monitoring; **Level 4 = a Cyber Security Operation Centre (C-SOC)**, cyber drills, forensics and metrics, IT strategy, IS governance, CISO, Information Security Committee, **Audit Committee of Board**. [SM 584–585]

⚠ NOT IN THE SM: PITFALLS OF INADEQUATE SECURITY CONTROLS (POSTAL Q9(a), SM ESSAY Q7)

- **Unauthorised access** to data and programs (weak user IDs, passwords, access rights).
- **Loss or corruption of data** (no backup, untested restoration, virus attack, disk crash).
- **Fraud** at data entry and through **patch programs** that leave no audit trail.
- **Business disruption** with no business continuity plan; poor recovery.
- **Non-compliance** with laws and regulators (RBI framework, data protection) → penalties.
- **Loss of confidentiality** of customer data → reputation and competitive loss.
- Unreliable output (**GIGO**), wrong decisions; undetected errors with no audit trail.
- Policies not defined or not followed: controls "exist on paper" only (e.g. weekly password change not happening, SM 593).

Built from SM 589, 593, 597–598 and the SM's own MCQ 15 (protect against disasters, disgruntled or poorly trained employees, hackers, spies, data-entry operators).

*Jun'23 MCQ: security in the design of IS is used to **protect data and programs from accidental or intentional loss** (SM MCQ 14).* [SM 606, SM 608]

13.3 Cyber security and computer forensics · Dec'23 Q6(b), Jun'25 Q7(a), PTP Q7(a)

- SM WORDS **Computer forensics focuses on uncovering and preserving encrypted or lost data, while cyber security is about preventing data loss or cybercrimes from occurring. In short, one is reactionary while the other is preventative.** [SM 586]
- **Cyber security**: a professional discipline of **defensive measures against cyber attacks**; skills in programming, operating systems, networking; goal: a network **impossible to breach**. It is **almost entirely about prevention** (even ethical hackers only test and improve). Protocols: **user permissions**, **file transfer protocols (FTP)**, **secure, frequently changing passwords**; everyone must practise safe computer use. [SM 586]
- **Computer forensics**: **recovering data from a device**, often to uncover evidence of crime; **reactionary**, after the incident. Two purposes: **assist an investigation** (access to a suspect's laptop or phone; recover data in a way that does not violate the suspect's rights, so it is **admissible in court**) or **recover lost data** for a company (same processes, court rules not needed); may also identify the perpetrator. [SM 586]

	Cyber security	Computer forensics
Focus	**prevention**	**recovery and reaction**
When	before an attack	after an incident
Think of it as	a **security company**	**investigators**
Specialisations	systems architecture, software security, access management, ethical hacking, vulnerability assessment	criminal investigations; data recovery (also breach evidence)
Common aim	both protect data, programs, networks, digital assets; forensics also identifies the culprit	

SM 587. The ICMAI PTP answer to "role of cyber security in protecting data" = the SM 586 paragraph + **cyber hygiene**: strong passwords, software updates, user permissions, FTP, **multi-factor authentication**, training staff not to click suspicious links, **data backups**, **incident management**, VPNs, firewalls, **Zero Trust**.

MODEL ANSWER FRAME · JUN'25 Q7(a) "ROLE OF CYBER SECURITY IN PROTECTING DATA"

1. Definition: protecting systems, networks and data from unauthorised access, use, disclosure, disruption, modification; keeps operations running, protects sensitive data, prevents financial and reputational damage.
2. A discipline of **defensive measures**; almost entirely **prevention**.
3. **Access**: user permissions, strong and frequently changed passwords, MFA.
4. **Transfer**: secure FTP, VPN, firewalls, Zero Trust.
5. **Resilience**: backups, incident management.
6. **People**: everyone trained (phishing links); it is not one person's job.
7. Contrast in one line with computer forensics (after the event).

13.4 IT audit in the banking sector · objectives · Dec'24 Q7(a) data integrity

- SM WORDS IS audit identifies the **risks an organisation is exposed to in the computerised environment**, evaluates the adequacy of security controls and informs management; it is an **independent subset** of the normal audit, whose objectives do not change. **Four major objectives: (a) safeguarding IS assets, (b) data integrity, (c) system effectiveness, (d) system efficiency.** [SM 588]
- **(a) Safeguarding assets**: hardware, software, facilities, people (knowledge), data files, documentation, supplies; review physical security, systems software security, internal controls; hazards are **accidental** (fire, flood, power failure) or **intentional**. [SM 588]
- **(b) Data integrity** = safeguarding information against **unauthorised addition, deletion, modification or alteration** (records, backups, documentation). Eight features must not be compromised: **Accuracy, Confidentiality, Completeness, Up-to-date status, Reliability, Availability, Timeliness, Effectiveness**. Poor integrity = loss of true representation and competitive advantage. [SM 588–589]
- **(c) System effectiveness** = **actual output ÷ standard (budgeted) output**; above **100%** = effective. Goals: improved task accomplishment, improved quality, operational, technical and **economic effectiveness** (benefits exceed cost). [SM 589]
- **(d) System efficiency** = **output ÷ input**: minimum resources for the objectives; matters once there is no excess capacity. [SM 590]
- **Other objectives**: prioritise risks; IT per the Board-approved **Security Policy**; procedures adhered to; duties of system administrators; minimise computer abuse; improve controls; advise management; ethics and standards. **Scope**: all computerised offices; evidence on safeguarding, integrity, availability, effectiveness, efficiency; planning and monitoring of IS; IS staff. [SM 590]

MODEL ANSWER FRAME · DEC'24 Q7(a) "IS AUDITOR OF XYZ BANK: DATA INTEGRITY"

1. **Meaning**: safeguard data against unauthorised addition, deletion, modification, alteration; accurate data, securely transmitted. [SM 588]
2. **Check the eight features**: accuracy, confidentiality, completeness, up-to-date, reliability, availability, timeliness, effectiveness. [SM 589]
3. **Data input controls**: the most error-prone and fraud-prone area (routine work); evaluate minutely; control scanners and external media. [SM 597]
4. **Data processing controls**: only authorised officers run **start-of-day**; **day-end** with prescribed reports; authenticated record of database corrections. [SM 597]
5. **Patch programs**: bypass menu controls, **leave no audit trail**; only approved programs loaded (file name, size, date and time of compilation match the approved list); a record of each patch with reasons. [SM 597]
6. **Purging**: full backup first; never purge master data; purged media stored chronologically, in safe custody; manual record; access restricted. [SM 597]
7. **Backup and restoration**: regular; one set **off-site**; tested by restoring; labelled and numbered; restoration shows the data as at a date (detects tampering). [SM 597–598]
8. **Output and audit trail reports** (user ID of the operator and the authorising official for every change), **exception reports**, **version control** (licensed, listed programs), **virus protection**. [SM 598–599]

KYC solved case (CBS): data request for SB customer master (branch, customer and account ID, holders, address, PAN, mobile, phones, mode, balance) as text → import into **GAS** → **duplicate key test** (same PAN / mobile / address, different customer IDs) → check account-opening forms → **SOUNDEX** test on names (phonetic code: "Prasanna Iyer" = "P Alyer") → **de-dup**: several SB accounts of one customer in one branch = **red flag**. [SM 600]

13.4 IS audit approaches · CAATs · methodology · Jun'24 Q7(a)

THREE APPROACHES (THE JUN'24 ANSWER)

- **Around the computer**: check the **output against the input** without the processing details (SM MCQ 7); used when the auditor lacks technical skill, reliance is on **user (procedural) controls**, the system is **simple with a clear audit trail** (exception reports, batch input, low inherent risk, rarely modified), or a **well-tested generalised package** from a reputed vendor (not modified). Simple, but says nothing about coping with change; **not for complex systems**. [SM 591]
- **Through the computer**: the **programs and data are the target**; compliance and substantive tests on the OS, application and data; the computer tests logic and controls. Needs knowledge of the OS, hardware and systems development; **increases confidence** in the evidence but is **time-consuming**. [SM 591]

IS AUDIT METHODOLOGY: FIVE STEPS

1. **Planning**: understand the auditee and its processes, objectives, background, staff by skill, **areas of risk** (risk analysis: critical information, number and value of transactions); understand internal controls (previous reports, interviews, observation, documentation).
2. **Tests of controls** (management and application controls): **identification, implementation, existence** (e.g. weekly password change on paper but not done), **adequacy, documentation, maintenance** (fire extinguishers, UPS kept working), **monitoring** (supervision, surprise checks).
3. **Tests of transactions**: material misstatement from wrong transactions; objective = **data integrity**; trace journal entries to source, price files, computation, transaction log.
4. **Tests of balances**: final judgment on losses: confirm receivables, count inventory, **recalculate depreciation**; GAS prints confirmations.

- **With the computer**: the computer and its programs are **tools** for **substantive tests**; auditee data retrieved into an **independent environment** and interrogated with special programs. Used where (a) **large volumes** of input and output, (b) **complex logic**, (c) **substantial gaps in the visible trail**. [SM 591–592]

TOOLS (CAATs)

- **CAATs**: audit system files and evaluate internal controls where information is only on magnetic media; their papers kept **separate**; documentation describes the CAAT. **Audit software**, three types: **package programs**, **special purpose programs**, **utility programs** (sort, create, print). **Test data**: sample transactions entered, results compared with predetermined results. **General Audit Software**: most widely used, limited by staff skill; **ACL (Audit Command Language)**: flexible reports, auditor independent of IT experts, more coverage, saves time, money and effort, confidence in results. [SM 592]

5. **Completion**: opinion with findings and recommendations; **exit conference** with the auditee; draft report; final report after the auditee's responses; organised **work papers**.

[SM 593–594]

- Manual, computer-assisted and fully automated procedures, often combined; CAATs let the auditor test **every record** instead of samples. [SM 593]
- **Sub-system factoring**: break a complex system into sub-systems small enough to understand; evaluate each one's controls and its effect on the whole. **Management systems**: top-level, IS, systems development, programming, data administration, quality assurance, security administration, operations. **Application systems**: **boundary, input, communication, processing, database, output**. [SM 595–596]

13.4 Framework for IS audit · business continuity · Jun'23 Q7(b)

A. SAFEGUARDING ASSETS: WHAT THE AUDITOR INSPECTS

- **Environmental security**: server room strategically located, not easily accessible, for the server only. **UPS**: conditioned power, battery when electricity fails, maintained. **Electrical lines**: separate earthing for the dedicated line. **Data cabling**: experts estimate **90 percent** of network problems are **cable-related**; cable map; data and electrical cables must not cross. **Fire protection**: alarms, smoke detectors, extinguishers (water, carbon dioxide, Halon; gas replaces oxygen; water dangerous near live equipment; **no dry powder or foam**, they leave deposits). **Insurance**. **AMC** renewed in time, with a maintenance record. [SM 596]
- **Logical security**: user ID and password at OS and application level; check secrecy, access levels, creation and termination of maintenance users, login status reports, **dummy user IDs**. [SM 597]

B–F. THE OTHER CONCERNS

- **B. Data integrity** (input, processing, patch, purging, backup, restoration: see the Dec'24 frame). **Output reports: GIGO** (garbage in, garbage out); scrutinise reports on a sample basis; **audit trail report** with the operator's and authoriser's IDs; exception reports. **Version control**: licensed copies, complete list of programs. **Virus protection**: updated anti-virus, scan external media. [SM 598–599]
- **D. System effectiveness**: does it achieve the goals of computerisation, user-friendly? **E. Efficiency**: every asset used to maximum capacity. **F. Organisation and administration**: placement by aptitude and skill; **segregation of duties**, job descriptions, training, **dual control**, a system administrator with back-up; records of work, rotation, logins. [SM 599]

Vodafone (VOIS) case: to keep **PCI DSS** compliance for UK customer card data, VOIS needed **File Integrity Monitoring (FIM) and change control**; a first vendor's proof of concept failed after **2 months**; NNT's Change Tracker flagged harmful and unapproved changes without "change noise", giving continuous compliance and a faster audit. [SM 601–602]

C. BUSINESS CONTINUITY PLANNING (THE JUN'23 ANSWER)

- **Yes, disruption can occur**, from two types of problems: (1) **minor**: power failure, UPS failure, server failure, unreadable backups, cable fault; (2) **calamities**: natural (fire, flood, building collapse) or man-made (bomb blast, radiation, **virus attack**, induced data loss). [SM 598]
- A **BCP** is prepared to recover from such interruptions: **anticipating any disastrous event and planning for the business to live through it**. The auditor verifies its **existence and operability**, staff **awareness** of executing it, and comments on its effectiveness; it must be **documented and tested at regular intervals**. [SM 598]
- **Recovery horizons**: short term = essential systems and services restored; medium term = systems recovered temporarily; long term = **total recovery** of the processing environment. [SM 598]
- **Recovery sites**: **cold** = a room where equipment can be installed when needed; **warm** = room with equipment, software to be loaded; **hot** = the original installation **duplicated and ready**. [SM 598]
- The BCP sets out: responsibilities for recovery, how to reproduce media, location of backups, **priorities for recovery**, sources of replacement hardware and software, alternative communication. **Backup** is itself a BCP measure. [SM 598]

SM EXERCISE KEYS (SM 608)

1 **controls** ensure the system processes data as designed, results reliable · 2 (i) and (ii) · 3 (i), (ii), (iii) · 4 two-way check: (ii) and (iv) · 5 check-point: breaks programs into portions · 6 **audit**: inspect it is built as per specifications · 7 around = inputs vs outputs · 8 audit trail **localises the source of an error** · 9 with = auditing programs check a system · 10 testing = performing as per specifications · 11 **parallel runs** when first implemented · 12 viruses: (i) and (ii) · 13 **firewall** stops hackers · 14 **security** protects data and programs from loss (= Jun'23 MCQ) · 15 all six. [SM 608]