



ITSEC — Certificate Examination in IT Security

Complete Book | Table of Contents | 20 chapters + 9 sections

Module A — IT Security Overview

CH-1	Introduction to Information Security	2
CH-2	Corporate IT Security	5
CH-3	Organisational Security and Risk Management	8
CH-4	Security Governance	11
CH-5	Physical and Environmental Security	15
CH-6	Hardware Security	18
CH-7	Software and Operational Security	21
CH-8	Security Standards and Best Practices	25

Module B — IT Security Controls

CH-9	Asset Classification and Controls	29
CH-10	Physical and Environmental Security Controls	32
CH-11	Software Security Controls	35
CH-12	Network Controls	39
CH-13	Controls in Software Development and Maintenance	43

Module C — IT Security Threats

CH-14	IT Security Threats	47
CH-15	Software Attacks - Virus and Malwares	51
CH-16	Incident Management	54
CH-17	Fault Tolerant System	57
CH-18	Business Continuity and Disaster Recovery Management	60

Module D — IS Audit and Regulatory Compliance

CH-19	Information Systems Audit	64
CH-20	Regulatory Mechanism in Indian Banks	68

Additional Resources

—	Case Studies — Module A: IT Security Overview	72
—	Case Studies — Module B: IT Security Controls	80
—	Case Studies — Module C: IT Security Threats	85
—	Case Studies — Module D: IS Audit and Regulatory Compliance	91
—	Mega Tests — Mega Test 1 — 100 Questions (Full Syllabus)	93
—	Mega Tests — Mega Test 2 — 100 Questions (Full Syllabus)	101
—	Mega Tests — Mega Test 3 — 100 Questions (Full Syllabus)	109
—	Mega Tests — Mega Test 4 — 100 Questions (Full Syllabus)	117
—	Mega Tests — Mega Test 5 — 100 Questions (Full Syllabus)	126

CH-1

Introduction to Information Security

Topic 1 — Data, Information and Information Asset

Term	What it is	Key point
Data	Raw facts, figures and statistics that are unorganised	Little meaning on its own; must be processed, interpreted and organised
Information	Data that has been processed, organised and interpreted	Meaningful and useful; in a format that can be easily understood and applied
Information asset	Information plus the resources that store, process or transmit it	Its loss, misuse or unavailability can harm business operations

Forms of an information asset

- **Hardware gadget** — A network device, hard disk, storage device, pen drive or print-out can hold information.
- **Software** — Software where information lies is also an information asset.
- **Communication channel** — A channel through which information only traverses is an asset, even though it is **not stored** there.

Topic 2 — Threats to Information Assets

Source of threat	Examples	Possible result
External factors or events	Hackers, cybercriminals, competitors trying to gain unauthorised access	Data breach, theft of sensitive information, disruption of services
Insider threats	Intentional or unintentional action or negligence of employees, contractors, business partners	Misuse or leakage from within
Human error	Sending data to the wrong recipient, misconfigured security settings, falling for social engineering	Significant risk to information assets
Systemic failures	Failure of hardware (servers, storage); bugs, glitches or vulnerabilities in software	Data loss, service interruption, exploitation by attackers
Factors beyond the organisation's control	Earthquake, flood, fire, other natural disasters	Physical damage to infrastructure, data loss, disruption

Topic 3 — Parties Associated with an Information Asset

Party	Who	Role
Owner	Person or entity who created or acquired the asset, or its legal owner; usually a senior-level person (department head, manager, executive)	Determines the value and criticality of the asset; sets access controls and usage policies
Custodian	Individual or group, often IT professionals or administrators	Day-to-day care, maintenance and protection; implements the security measures defined by the Owner — secure storage, regular backup , proper access controls
User	Any individual or system accessing the asset — employees, contractors, customers, automated processes	Uses the asset for assigned roles; subject to the access controls and usage policies set by the Owner

Remember this

- **Owner decides, Custodian implements, User complies.**

Topic 4 — Information Classification

Information is classified so that the level of protection matches its importance. Three bases are used: **criticality**, **confidentiality** and **availability**.

Basis	Highest level	Middle level	Lowest level
Criticality	Most critical — vital, difficult to recreate, crucial for functioning	Critical — important, somewhat replaceable, still of significant value	Least critical / insignificant — public domain, easily recreated, not highly valuable
Confidentiality	Most confidential — highly sensitive, restricted to a specific group or individual	Confidential — needs protection, may be shared with specific authorised groups	Least confidential / low — lower sensitivity, broader accessibility
Availability	Topmost critical — unavailability seriously disrupts operations; a single copy is a major resilience risk	Critical — disruption tolerable for a limited time	Least critical — unavailability has little operational effect

Topic 5 — Need to Know

- **Meaning** — Employees get only the particular information and facts required to perform their role in the organisation.
- **Wider link** — It encompasses other basic principles: **access control, access privileges, availability and authentication.**

Topic 6 — Information Security and its Pillars

- **Meaning** — Information security protects information from unauthorised **access, disclosure, alteration, destruction and disruption**.
- **Goal** — It ensures the **confidentiality, integrity and availability (CIA)** of information.

Pillar	Assurance given	Guards against
Confidentiality	Information is accessible only to those with proper authorisation	Unauthorised disclosure
Integrity	Information stays accurate and reliable	Unauthorised or unintended alteration, corruption, tampering
Availability	Information is accessible and usable when needed	Disruption of access

Additional pillars:

Pillar	Meaning	Key point
Non-repudiation	Evidence of origin, delivery or an action that others can verify	Helps resolve disputes about responsibility; a handwritten signature is evidence of authorship, but its authenticity and surrounding evidence must be evaluated if the signer disputes it
Accountability	Actions can be linked to the responsible individual or system	Presupposes proper identity of authorised users, their records and protected audit trails
Authenticity	Information or an entity is what it claims to be ; a message or transaction is from the source it claims	Involves proof of identity ; supports confidence in origin but does not guarantee factual truth

Remember this

- **CIA** = Confidentiality–Integrity–Availability; add-ons **NAA** = Non-repudiation, Accountability, Authenticity.

Topic 7 — Physical Security and Intrusion Detection

- **What it protects** — Physical security protects **hardware, software, networks and data**.
- **Against what** — Physical actions and events causing serious loss or damage: **fire, flood, natural disasters, burglary, theft, vandalism and terrorism**.
- **See** — Ch 5 (p. 15) for physical threat groups and the steps in physical security.

Intrusion detection mechanism	How it works
Disturbance sensors	Discrete detection of vibration or movement of a fence or other structure; alarm when the disturbance meets a predefined threshold
Barrier detectors	Send a continuous beam of energy ; a break in the beam indicates intruder penetration

Intrusion detection mechanism	How it works
Buried-line sensors	Underground cables or instruments sensing pressure, seismic and magnetic signals
Surveillance	Through radar or Closed-Circuit TV (CCTV)

Topic 8 — Logical Security and Software Access Controls

- **Meaning** — Logical security uses **software and systems** to control and limit access to information.
- **Tools** — These include user identification and password access, authentication, access rights and authority levels.
- **Access controls** — They prevent, or limit the likelihood of, unauthorised access to data files or programs.

Control	Key features
Password	Set of characters allocated to a person, terminal or facility ; keyed in before further access is permitted; can protect data files and program files
Personal Identification Number (PIN)	A secret used to authenticate a user; the user name or account identifier identifies the user
Encryption	Converts information into a secret code that hides its true meaning
Authentication	Verifies a claimed identity or the origin of a message
Authorisation	Separately decides which resources or actions are permitted

Remember this

- **Identification** = who you claim to be; **Authentication** = proving it; **Authorisation** = what you may do.

Topic 9 — Information Security Programme

Aspect	Points
Advantages	Protects business information, supports reliable customer services, assigns clear responsibilities; coordinated controls help prevent incidents, detect problems and recover operations
Disadvantages and costs	Controls need money, staff time and maintenance; excessive restrictions slow work and inconvenience users
Control selection	Choose proportionate controls through risk assessment ; security does not eliminate every risk
Goals	Protect CIA while supporting business needs; define measurable objectives, accountable owners and regular review

Topic 10 — Information Security Services

Group	Service	What it does
Core	Authentication	Checks a claimed identity or origin
Core	Access control	Enforces permissions
Core	Confidentiality	Safeguards data from unauthorised disclosure
Core	Integrity	Detects or prevents improper changes
Supporting	Non-repudiation	Supplies verifiable evidence for disputed actions
Supporting	Accountability	Links activity to an identifiable actor
Supporting	Availability	Resilience, recovery and timely access to authorised information

Example: A payment system **authenticates** the customer, checks **transaction permissions**, **protects messages**, records a reliable **audit trail** and maintains **service continuity**. These controls work together — a password alone cannot provide all services.

- **Basis** — These concepts follow internationally accepted information security principles and **risk-based control selection**.
- **Not a substitute** — They do not replace Indian banking requirements, such as the RBI's cybersecurity and IT risk directions for banks.

ITSEC | Module A | CH-1 | MCQs

Q1. A bank's customer database is kept on a server, copied nightly to tape and sent over a leased line to the DR site. Which of these is an information asset? [Ref: Topic 1, p. 2]

- (a) Only the database file
- (b) Only the server and the tape
- (c) The database, the server, the tape and the leased line
- (d) Only the leased line, because data passes through it

Q2. Raw transaction logs are summarised into a branch-wise overdue report used by management. The report is best described as: [Ref: Topic 1, p. 2]

- (a) Information
- (b) Data
- (c) Metadata only
- (d) An information asset owner

Q3. An officer emails a borrower list to the wrong external address. This threat is classified as: [Ref: Topic 2, p. 2]

- (a) External event
- (b) Systemic failure
- (c) Factor beyond control
- (d) Human error

Q4. A flood damages the server room and causes data loss. This threat falls under: [Ref: Topic 2, p. 2]

- (a) Insider threat
- (b) Factors beyond the control of the organisation
- (c) Social engineering
- (d) Software vulnerability

Q5. Who determines the value and criticality of an information asset? [Ref: Topic 3, p. 2]

- (a) Custodian
- (b) User
- (c) Owner
- (d) External auditor

Q6. The database administrator who takes regular backups and configures access rights as directed by the department head acts as the: [Ref: Topic 3, p. 2]

- (a) Custodian
- (b) Owner
- (c) User
- (d) Intermediary

Q7. Information that is readily available in the public domain and easily recreated is classified on criticality as: [Ref: Topic 4, p. 2]

- (a) Most critical
- (b) Critical
- (c) Topmost critical
- (d) Least critical or insignificant

Q8. A clerk handling loan disbursement is denied access to treasury dealing data. The principle applied is: [Ref: Topic 5, p. 2]

- (a) Non-repudiation
- (b) Need to know
- (c) Availability
- (d) Authenticity

Q9. A hacker alters the interest rate field in a deposit record without being detected. Which pillar is directly violated? [Ref: Topic 6, p. 3]

- (a) Confidentiality
- (b) Availability
- (c) Integrity
- (d) Accountability

Q10. A customer denies initiating a fund transfer, but the bank produces a digitally signed and logged instruction. The property relied on is: [Ref: Topic 6, p. 3]

- (a) Non-repudiation
- (b) Availability
- (c) Need to know
- (d) Custodianship

Q11. Which intrusion detection mechanism raises an alarm when a continuous beam of energy is broken? [Ref: Topic 7, p. 3]

- (a) Disturbance sensor
- (b) Buried-line sensor
- (c) Barrier detector
- (d) Radar surveillance

Q12. After a user's identity is verified with a PIN, the system checks whether she may approve a ₹5 lakh transfer. This second check is: [Ref: Topic 8, p. 3]

- (a) Authentication
- (b) Authorisation
- (c) Encryption
- (d) Identification

Q13. Which statement on an information security programme is correct? [Ref: Topic 9, p. 3]

- (a) It eliminates every risk once fully implemented
- (b) Controls should be as restrictive as possible regardless of cost
- (c) It needs no review once objectives are set
- (d) Controls should be proportionate and selected through risk assessment

Q14. Which information security service links an activity to an identifiable actor through protected audit trails? [Ref: Topic 10, p. 4]

- (a) Accountability
- (b) Confidentiality
- (c) Availability
- (d) Encryption

Answer key

Q	Ans	Q	Ans	Q	Ans	Q	Ans	Q	Ans
1	c	4	b	7	d	10	a	13	d
2	a	5	c	8	b	11	c	14	a
3	d	6	a	9	c	12	b		

CH-2 Corporate IT Security

Topic 1 — Corporate IT Security and the Need for a Policy

- **Meaning** — Corporate IT security is a set of **practices, policies and technologies**.
- **What it safeguards** — The organisation's digital assets, information and technology infrastructure.
- **Against what** — Unauthorised access, data breaches, cyber threats and other risks.
- **Aim** — It protects the **confidentiality, integrity and availability** of corporate information systems.

Need	Why a policy is required
Protection of critical assets	Information and technology assets are among the most critical; the policy protects hardware, software, networks and sensitive data
Prevention of unauthorised access	Defines protocols for user authentication, access controls and data encryption
Organisational impact	IT security is not only the IT department's concern ; benefits of IT spending extend to the whole organisation
Risk mitigation	Covers vulnerability management, incident response and disaster recovery planning
Legal and regulatory compliance	Supports compliance with data protection and security laws; effective implementation and monitoring are still needed to manage legal risk
Responsibility and accountability	Defines roles so everyone understands their part in maintaining security

Topic 2 — Legal Requirements

Information Technology Act, 2000

- **Legal recognition** — The **Information Technology Act, 2000** gave **legal recognition to electronic records**.
- **Electronic records** — It paved the way for keeping records electronically and highlighted the value of information assets.
- **Scope** — It regulates electronic transactions, offences and **intermediary** responsibilities.
- **Bank as intermediary** — A bank is an intermediary **only** for activities within the statutory definition.
- **2008 amendment** — The **IT (Amendment) Act, 2008** addressed detailed **due diligence** and duties of employees and service providers.

Provision	Rule	Current status
Section 43A (inserted 2008)	A body corporate handling sensitive personal data is liable to pay compensation if negligence in reasonable security practices causes wrongful loss or gain	Still in force ; DPDP Act s. 44(2) omits it only from the date notified — 18 months after the commencement notification of 13 Nov 2025

Provision	Rule	Current status
Section 79 (substituted 2008)	Conditional safe harbour : an intermediary is not liable for third-party information it handles	Subject to due diligence and statutory exceptions

DPDP Act, 2023 and DPDP Rules, 2025 — phased commencement

- **Phase 1** — Definitions, the **Data Protection Board** and the penalty framework apply from **13 Nov 2025**.
- **Phase 2** — Certain provisions apply after **12 months**.
- **Phase 3** — The core obligations of **data fiduciaries** apply after **18 months**.
- **Penalty** — Penalties go up to **₹250 crore** per breach.
- **Practical check** — Before treating a safeguard, reporting duty or penalty as operational, identify the provision, its **commencement date** and the organisation's role.

Remember this

- **43A** = compensation for negligent security of sensitive personal data; **79** = intermediary safe harbour with due diligence.

Topic 3 — Essential Features: Preamble and Document Control

Element	Content
Need for the policy	States the reasons and objectives for establishing the IT security policy
Version and document ownership	Version of the document and who owns it, so responsibility for updates and maintenance is clear
Document control	Procedure for reviewing, adding, deleting or modifying the policy and the authority responsible for each action

Topic 4 — Information Security Committee and the CISO

RBI Directions, 2026 for commercial banks

- **Governing rules** — The **Reserve Bank of India (Commercial Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026** set the governance structure.
- **ITSC** — Board-level, with **at least 3 directors**; chaired by an independent director with **at least 7 years'** experience in information systems or technology/cybersecurity; meets **at least quarterly**.
- **ISC and CISO** — The ISC works under ITSC oversight and is headed from the **risk management vertical**; the CISO, preferably **General Manager** rank, reports to the **ED overseeing risk**, never to the Head of IT, has **no business targets** and is a **permanent invitee** to the ITSC and IT Steering Committee.
- **See** — Ch 4 (p. 11) for the full Board, committee, ISC and CISO requirements, the banks excluded from coverage and the position of foreign banks.
- **Component policies** — The corporate IT security policy is made up of several component policies.
- **Who runs them** — The respective **functional heads** implement and maintain each component policy.
- **Oversight** — The information system security set-up supervises, guides and monitors them, with the **CISO at the top**.