Module 10 · Cyber Security and Data Privacy

P13 · Section B · topics 10.1–10.3

SM pp. 385–400 (16 pages). **53.5 marks in 7 papers.** A 7-mark long question in 6 of 7 papers (usually Q6(b)); **business intelligence** alone has had three. An MCQ in every paper except Dec'25. Section numbers the SM does not print are taken from the Act.

Paper	What was asked	Marks
Jun'23	MCQ: **trespass** (= SM MCQ 10) · Q7(b)(ii) list **5 cyber crimes under the IPC** and special laws	2 + 3
Dec'23	MCQ: e-governance PPP for grievances, land records and services = **Lokvani (UP)**, not in the SM · Q6(b) **how the BI process works**	2 + 7
Jun'24	MCQ: **embedded BI** (= SM fill-in 7) · Q6(a) **business intelligence**: meaning and benefits	2 + 7
Dec'24	MCQ: Cyber Appellate Tribunal → **High Court** (= SM MCQ 6) · Q3(b) **data protection** under the IT Act and the law in India today	2 + 7
Jun'25	MCQ: **not an IT Act crime**: threatening e-mail (= SM MCQ 8) · Q5(b)(i) **cyber crimes against persons**	2 + 3.5
Dec'25	Q6(b) **how the BI process works** (repeat of Dec'23)	7
Jun'26	MCQ: offences on **unauthorised access** · Q6(b) **identity theft and cheating by personation**; adjudication and penalties (not in the SM)	2 + 7

HOW IT IS EXAMINED · DEC'26 PREDICTION

- **Q6(b), 7 marks**: (1) **BI process + benefits** (asked 3 times, in the PTP; about 45%); (2) **data protection / SPDI Rules** (25%); (3) **s.43 compensation** (ICMAI MQP Q6(b), not in the SM; see the ⚠ box); (4) cyber crimes (20%).
- MCQs come from the SM exercise; the Dec'26 supplementary adds **synthetically generated information** (MCQ material).

MAP

1. IT Act: objects, CCA, offences, appeals ★★
2. Data protection: s.43A, s.72A, SPDI Rules ★★★
3. ⚠ DPDP Act 2023; s.43, 66C, 66D ★★
4. Business intelligence: process, benefits, tools ★★★
5. Cyber crimes: persons, property, Government ★★
6. Model answers · SM exercise

10.1 Information Technology Act, 2000 · Dec'24 MCQ

OBJECTS · RECORDS · CCA

- **Objects**: (i) **legal recognition of electronic transactions** through digital signatures, including electronic publication of rules and gazette notifications; (ii) **electronic filing** and retention of documents with Government (the public cannot be forced to use only the electronic mode); (iii) consequential amendments to other Acts; (iv) set up the **licensing, monitoring and certifying authority**. [SM 387]
- **Dispatch** occurs when a record enters a resource outside the originator's control; **receipt** when it enters the addressee's designated computer resource (or when retrieved, if none is designated); place of business is the place of dispatch and receipt. [SM 387]
- **Controller of Certifying Authorities** (CCA), appointed by the CG: recognises, **licenses**, regulates and supervises **certifying authorities**, which **issue digital signature certificates** (SM MCQ 1 and a fill-in). The CG/Controller may intercept information for security and declare **protected systems**. [SM 387]

OFFENCES · DISPUTES

- Applies to any offence by anyone, anywhere, if it involves a **computer, system or network located in India**. [SM 387]
- Offences: (a) **tampering with computer source documents**; (b) **hacking** (destroying, deleting or altering data with intent to cause damage); (c) **misrepresentation** to the Controller or a CA; (d) **breach of confidentiality and privacy**; (e) **publishing false digital signature certificates**. [SM 387]
- **Disputes**: the CG appoints **adjudicating officers** with IT and legal knowledge. Appeal against the Controller or an adjudicating officer to the **Cyber Appellate Tribunal within 45 days**; its decision may be appealed to the **High Court within 60 days** (the SM prints "6o") (Dec'24 MCQ = SM MCQ 6). **Civil courts have no jurisdiction.** [SM 388] ⚠ Since 2017 the Cyber Appellate Tribunal's work is done by the TDSAT.

10.1.2 Data protection: s.43A, s.72A and the SPDI Rules, 2011 · Dec'24 Q3(b)

WHAT IT IS · THE LAW (SM)

SM WORDS **Data protection** refers to the set of privacy laws, policies and procedures that aim to **minimise intrusion into one's privacy** caused by the **collection, storage and dissemination of personal data**. Personal data is information

SPDI RULES, 2011 (NOTIFIED 11 APRIL 2011) · SM ESSAY 3, 4

1. Apply only to **bodies corporate and persons located in India** (SM MCQ 7). [SM 388]
2. **Rule 3**: sensitive personal data includes **passwords**, **card details**, **biometrics** (DNA, fingerprints, voice patterns),

relating to a person who can be **identified** from it, whether collected by Government or a private body. [SM 388]

- The IT Act came into force on **17 Oct 2000** without data-protection provisions; the **2008 Amendment** (in force **27 Oct 2009**) inserted **s.43A**, and the CG notified the **2011 Rules**. Privacy became a **fundamental right** on **24 Aug 2017** (an SM fill-in). [SM 388]
- **s.43A**: a body corporate that holds **sensitive personal data** and is **negligent in maintaining reasonable security**, causing wrongful loss or gain, is **liable to pay damages** to those affected. [SM 388]
- **s.72A**: disclosing information **in breach of a lawful contract**: imprisonment up to **three years**, or fine up to **five lakh rupees**, or both. [SM 388]

physical, physiological and **mental health**. Information freely available in the public domain is not sensitive. [SM 388]

3. **Rule 4**: a **privacy policy**, published on the website: what is collected, why, and the security practices. [SM 389]
4. **Rule 5**, duties when collecting: **consent**; collect only for a **lawful, necessary purpose**, use only for it and do not keep it longer than needed; tell the person the purpose, recipients and who holds it; let them **review and correct** it; keep it **secure**; appoint a **Grievance Officer** named on the website. [SM 389]
5. **Prior permission** of the provider before disclosing to a **third party**. [SM 389]
6. **Rule 8**: reasonable security practices, e.g. **IS/ISO/IEC 27001**; an **audit at least once a year** or on a significant upgrade. [SM 389]

⚠ "THE LAW AS PREVALENT IN INDIA TODAY": DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NOT IN SM)

The SM says India has no separate data-protection law; that is out of date. The **DPDP Act, 2023** (assent 11 Aug 2023) applies to **digital personal data** processed in India, and abroad when offering goods or services to people in India. Personal data may be processed only for a lawful purpose with the person's **consent** (after a notice), or for certain **legitimate uses**. **Data fiduciaries** must keep data accurate, take **security safeguards**, report **breaches**, and **erase** data once the purpose is served. **Data principals** have rights to **access, correction and erasure**, grievance redressal and to nominate. A child's data needs **verifiable parental consent**. **Significant data fiduciaries** appoint a DPO and conduct audits. The **Data Protection Board of India** adjudicates; penalties go up to **₹250 crore**. The DPDP Rules were notified in Nov 2025, with most duties applying after 18 months; s.43A and the SPDI Rules are to be replaced by it. In the answer: **write the SM part first**, then this paragraph.

⚠ IT Act sections the SM leaves out · ICMAI MQP Q6(b), Jun'26 Q6(b)

s.43 · ACTS THAT ATTRACT COMPENSATION (MQP)

If any person, **without permission** of the owner or person in charge of a computer, system or network: (a) **accesses** it; (b) **downloads or copies** data; (c) introduces a **virus**; (d) **damages** it or its data; (e) **disrupts** it; (f) **denies access** to an authorised person; (g) **helps** another to access it in breach of the Act; (h) **charges** services used by one person to another's account; (i) **destroys, deletes or alters** information or reduces its value; (j) **steals or alters source code**: he is liable to pay **damages by way of compensation** to the person affected. Doing any of these **dishonestly or fraudulently** is the offence under **s.66** (up to 3 years or fine up to ₹5 lakh, or both).

s.66C, 66D · ADJUDICATION (JUN'26 Q6(b))

- **s.66C identity theft**: fraudulently or dishonestly using another person's **electronic signature, password or other unique identification**: imprisonment up to **3 years** and fine up to **₹1 lakh**.
- **s.66D cheating by personation** using a computer resource or communication device: imprisonment up to **3 years** and fine up to **₹1 lakh**.
- **Adjudication (s.46)**: the CG appoints an **adjudicating officer** (a Government officer of at least Director rank) who holds an inquiry after a reasonable opportunity of hearing, for claims up to **₹5 crore**; above that, the **civil court**. Factors (s.47): unfair gain, loss caused, repetitive nature. Appeals: Tribunal in **45 days** → High Court in **60 days** (as in the SM).
- Others: **s.65** tampering with source code: 3 years or ₹2 lakh; **s.67** obscene material: 3 years and ₹5 lakh (first conviction); **s.72** breach of confidentiality by an official: 2 years or ₹1 lakh.

SUPPLEMENTARIES

Dec'26: synthetically generated information (SGI): IT (Intermediary Guidelines and Digital Media Ethics Code) Rules amended (notified **10 Feb 2026**, effective **20 Feb 2026**). SGI = audio, visual or audio-visual content **generated or altered by technology so that it appears authentic** or represents a real person, event or fact. Intermediaries must **label** it clearly, embed **technical or provenance information** (prescribed intermediaries), and act to **remove or restrict unlawful SGI**. [Supp Dec'26 p.9] **Jun'26:** the RBI required scheduled banks to move to the **".bank.in"** internet domain by **31 Oct 2025**. [Supp Jun'26]

10.2 Business intelligence · Dec'23 Q6(b), Jun'24 Q6(a), Dec'25 Q6(b), PTP Q6(b)

SM WORDS **Business Intelligence (BI)** is a **technology-driven process for analyzing data and delivering actionable information** that helps executives, managers and workers make **informed business decisions**. Organisations **collect** data from internal systems and external sources, **prepare** it, **run queries**, and create **visualizations, dashboards and reports** for operational decisions and strategic planning. The goal: **better decisions** that increase revenue, improve efficiency and give a **competitive advantage**. [SM 390]

HOW THE BI PROCESS WORKS (ASKED TWICE)

- **Architecture**: data is stored in an enterprise **data warehouse** or smaller departmental **data marts**; it may be **historical or real-time**, so BI supports strategic and tactical decisions. [SM 390]
- Raw data from different sources is **integrated, consolidated and cleansed** with data-integration and data-quality tools so that analysis is accurate and consistent. [SM 390]

(a) Data preparation organise and model data sets → **(b) Analytical querying** of the prepared data → **(c) Distribution** of KPIs and findings → **(d) Use** to drive decisions

- **Self-service BI**: business users now query data and build dashboards themselves. **Advanced analytics** (data mining, predictive analytics, text mining, statistics, big data; e.g. what-if modelling) is usually done by data scientists. [SM 390]
- **Why it matters**: without BI, decisions rest on experience, intuition and "gut feelings", which risk errors. [SM 391]

BENEFITS (JUN'24)

Managers **monitor performance continuously**; customer analysis improves marketing, sales and service; **supply-chain bottlenecks** are found early; HR tracks productivity and labour cost. Key benefits: [SM 391]

1. **faster, better decision-making**
2. **optimised internal processes**
3. higher **operational efficiency and productivity**
4. spotting **business problems**
5. identifying **emerging business and market trends**
6. stronger **business strategies**
7. higher **sales and new revenues**
8. a **competitive edge** over rivals

Also: tracking projects; **competitive intelligence**; IT teams analyse their own operations (SM MCQ 5: all of the above). [SM 391]

BI tool	Meaning (SM)
Ad hoc analysis	writing and running queries on a specific business issue, on a casual or temporary basis [SM 391]
OLAP (online analytical processing)	analysis along **multiple dimensions**; complex queries and calculations
Mobile BI	dashboards on smartphones and tablets, showing two or three visualisations and KPIs
Real-time BI · **operational intelligence**	data analysed as it is created (credit scoring, stock trading, targeted offers) · real-time analytics for frontline workers [SM 391–392]
Open source BI (OSBI)	a free community edition and a paid commercial version with vendor support (SM MCQ 4)
Embedded BI ★	puts BI and data-visualisation functions **directly into business applications** (Jun'24 MCQ = SM fill-in 7)
Collaborative BI	BI plus collaboration tools: users annotate and share analysis
Location intelligence	geospatial data on maps: store sites, location-based marketing, logistics [SM 392]

Platforms: visualisation software; dashboards, reports and scorecards; **data storytelling**; usage monitoring and security. **Uses**: performance monitoring, decisions and planning, process improvement, operational information, trends and patterns. By industry: banks and insurers (risk analysis, cross-selling), retail (campaigns, inventory), manufacturing (plant operations), airlines and hotels (capacity, pricing), healthcare, education. **Trends**: BI teams (architects, developers, analysts) and **Agile BI** replacing waterfall development. [SM 392–393]

10.3 Cyber crime: meaning, types, laws · Jun'23 Q7(b)(ii), Jun'25 Q5(b)(i)

SM WORDS **Cybercrime** is criminal activity in which **computers or computer networks are a tool, a target, or a place** of criminal activity: phishing, credit-card fraud, illegal downloading, industrial espionage, child pornography, scams, cyber terrorism, viruses. It has **no geographical boundaries** and the criminals are unknown. [SM 394]

A. AGAINST PERSONS (JUN'25 Q5(b)(i))

- **Cyber-stalking**: creating fear of physical threat through internet, e-mail, phones, texts, webcams or websites. [SM 394]
- **Obscenity**: indecent exposure, pornography (especially child pornography), hosting such sites.
- **Defamation**: lowering a person's dignity, e.g. hacking his mail and sending vulgar mails (SM fill-in 6).
- **Hacking**: unauthorised control or access over a computer system. **Cracking**: breaking in and tampering with confidential data. [SM 394–395]
- **Spoofing**: e-mail or SMS that misrepresents its origin. **Carding**: false ATM, debit or credit cards. **Fraud**: stealing

B. AGAINST PROPERTY · C. AGAINST GOVERNMENT

- **Property**: IPR violation (software piracy, copyright, trade marks); **squatting** (two persons claiming the same domain name); **vandalism** (destroying data or disrupting a network); hacking; **viruses and worms**; **trespass**: accessing a computer without authority but **not disturbing, altering or damaging** it, e.g. over wireless internet (Jun'23 MCQ = SM MCQ 10). [SM 395]
- **Government**: **cyber terrorism** (DDoS, hate sites, attacks on sensitive networks); **warfare** (politically motivated hacking and spying); **piracy**; **unauthorised information**. [SM 395–396]

passwords and data with a guilty mind. **Threat**: threatening life through e-mail, videos or phones. [SM 395]

Under the IT Act (SM ESSAY 2; SM MCQ 8)	Under the IPC (Jun'23 Q7(b)(ii): any 5) and special laws
(i) tampering with computer source documents: **s.65** (ii) hacking, data alteration: **s.66** (iii) publishing obscene information: **s.67** (iv) unauthorised access to a protected system: **s.70** (v) breach of confidentiality and privacy: **s.72** (vi) publishing false digital signature certificates: **s.73** [SM 396]	(i) threatening e-mail: **s.503** · (ii) defamatory e-mail: **s.499** · (iii) forgery of electronic records: **s.463** · (iv) bogus websites, cyber frauds: **s.420** · (v) e-mail spoofing: **s.463** · (vi) web-jacking: **s.383** · (vii) e-mail abuse: **s.500**. **Special Acts**: online sale of drugs (NDPS Act); online sale of arms (Arms Act). [SM 396] ⚠ The IPC was replaced by the Bharatiya Nyaya Sanhita from 1 July 2024 (e.g. cheating 420 → BNS 318; forgery 463 → 336; intimidation 503 → 351; defamation 499 → 356; extortion 383 → 308). Quote the SM's IPC numbers and add "now BNS".

Jun'25 MCQ: "threatening messages by e-mail" is an IPC crime, not an IT Act one (A). Jun'26 MCQ: the SM groups s.65, 66 and 72 together under "unauthorised information", which points to (D) all of the above.

M Model answers

MODEL ANSWER 1 · HOW BI WORKS AND ITS BENEFITS (DEC'23, DEC'25 Q6(b); JUN'24 Q6(a); PTP) · 7 MARKS

(1) **Definition** in the SM's words (above). (2) **Architecture**: data warehouse and data marts; historical and real-time data; integrate, consolidate and cleanse. (3) **Four steps**: data preparation → analytical querying → distribution of KPIs → use in decisions. (4) **Self-service BI** and **advanced analytics**. (5) **Benefits**: the eight points. (6) A line on **tools** (OLAP, embedded, mobile, real-time). For "BI in the context of cyber security" (Jun'24): add that BI needs **secure, accurate data**; data-protection duties (SPDI Rules) apply to the data it uses. [SM 390–392]

MODEL ANSWER 2 · DATA PROTECTION UNDER THE IT ACT AND IN INDIA TODAY (DEC'24 Q3(b)) · 7 MARKS

(1) Meaning of data protection (SM words). (2) **Background**: IT Act 2000; 2008 Amendment inserted **s.43A**; SPDI Rules 2011; privacy a fundamental right (24 Aug 2017). (3) **s.43A** damages and **s.72A** punishment (3 years / ₹5 lakh). (4) **SPDI Rules**: who they apply to; sensitive data (Rule 3); privacy policy (Rule 4); collection duties (Rule 5); third-party disclosure; security and annual audit (Rule 8). (5) **Today**: the DPDP Act 2023 (⚠ box). [SM 388–389]

The SM's own exercise for Cyber and Data (SM 397–400)

1 CAs licensed by	**Controller of Certifying Authorities**	6 Cyber Appellate Tribunal → ★	**High Court**
2 not an IT Act offence	**making a faulty contract**	7 SPDI Rules apply to	**bodies corporate and persons in India**
3 SPDI Rules notified in	**2011**	8 not an IT Act crime ★	**threatening e-mail**
4 OSBI	**open source business intelligence**	9 not a cyber offence to the public	**data alteration**
5 BI benefits	**all of the above**	10 access without altering ★	**trespass**

True/False: tampering with source documents is not an offence **F** · the CCA issues digital signature certificates **F** (certifying authorities do) · appeal to the Cyber Appellate Tribunal **T** · unauthorised access without damage = trespass, an offence **T** · BI facilitates analytical querying **T**. **Fill-ins:** CCA = **Controller of Certifying Authorities** · appeal from the adjudicating officer to the **Cyber Appellate Tribunal** · rules preserving privacy = **data protection** · KPI = **key performance indicators** · OLAP = **online analytical processing** · **defamation** · **embedded BI** ★ · certificates issued by the **certifying authority** · SPDI Rules **2011** · privacy a fundamental right in **2017**.

R Revision: numbers

Rule	Number	Rule	Number
IT Act in force / 2008 amendment in force	17 Oct 2000 / 27 Oct 2009	appeal to Tribunal / High Court	45 / 60 days
SPDI Rules notified	11 Apr 2011	s.72A	3 yrs or ₹5 lakh
privacy a fundamental right	24 Aug 2017	security audit (Rule 8)	at least once a year
s.66C / s.66D (Act)	3 yrs + ₹1 lakh each	adjudicating officer up to (Act)	₹5 crore
SGI rules notified / effective	10 / 20 Feb 2026	DPDP penalty up to (Act)	₹250 crore