544

Roll No. ..... **OPEN BOOK EXAMINATION**

Time allowed : 3 hours ***Maximum marks : 100***

Total number of questions : 4 ***Total number of printed pages : 15***

NOTE : *Answer* ***ALL*** *Questions.*

1. TechSecure Innovations Pvt. Ltd., headquartered in Bangalore, is a fast-growring IT and cybersecurity solutions provider specializing in AI-driven security systems, digital compliance, and OTT platform support services. Its client base spans across banks, healthcare providers, e-commerce platform, and digital streaming services, making the company an integral part of India's ongoing digital transformation journey. However, the company operates in an environment where new cybersecurity challenges, evolving digital laws, and stricter regulatory frameworks are forcing it to rethink strategies and realign operations. TechSecure now faces multiple situations that test its technical capacity, legal awareness, and strategic decision-making.

TechSecure recently launched an AI-based Intrusion Detection System (IDS) that processes and analyzes millions of data points every second to detect anomalies and potential threats. The positive impact is that the system has drastically reduced the number of cyberattacks targeting client networks but challenge is that it sometimes produces false positives, creating unnecessary panic and diverting resources. Some clients also fear that over-reliance on AI could compromise decision-making if human oversight is minimized and this raises the issue of how TechSecure can strike a balance between automation and human expertise in cybersecurity.

India's National Cybersecurity Policy 2013 emphasizes the promotion of indigeneous research and development in cybersecurity. Currently, TechSecure imports several tools from foreign vendors. The CEO is considering investing in an in-house R&D lab in Bangalore to build homegrown AI-based security products, but this requires substantial resources and skilled manpower. The decision could either make TechSecure a leader in indigenous innovation or become a financial burden if not executed well.

Recently, a ransomware attack bypassed TechSecure's automated defenses and was detected only through manual log analysis after damage had been done. This exposed the need for a proactive threat hunting team that can identify suspicious activity before it escalates. Management is debating whether to train its current workforce in advanced threat hunting techniques or hire specialized cybersecurity hunters to proactively seek anomalies and neutralize threats before they escalate. The decision will affect both the cost structure and the effectiveness of future cybersecurity strategies.

One of TechSecure's OTT clients faced regulatory warnings from the Ministry of Information & Broadcasting (MIB) under the Digital Media Ethics Code 2021 for hosting "sensitive content." The OTT platform asked TechSecure to build an AI-driven compliance monitoring system. This raises a dilemma : should TechSecure stick to being a technology enabler or also act as a compliance partner by advising clients on ethical content management. This situation raises concerns about role boundaries, business diversification, and ethical responsibilities in the digital ecosystem.

The Digital India Act 2023, which seeks to replace the outdated IT Act 2000, will impose new rules and obligations on digital companies. This act is expected to bring stricter cybersecurity accountability, AI governance rules, and higher penalties for data misuse. TechSecure anticipates increased compliance costs, legal liabilities, and operational challenges in adapting existing frameworks to align with new legal requirements. TechSecure must now prepare for a future where compliance is not optional but a core business strategy.

In the above case scenario, answer the following questions :

(*a*) TechSecure operating online, adopted AI tools for cybersecurity, customer experience, and compliance. Being technical head in TechSecure, experience with AI-based intrusion detection system analysis, how would you justify the usefulness of AI for their online operations ?

(5 marks)

(*b*) The aim of National Cyber Security Policy-2013 is to create a Cybersecurity framework by collaboration of government and non-government entities that strengthen India's position as a global cybersecurity hub. According to you what strategies, of TechSecure in promotion of research and development in cybersecurity, contribute to building long-term national resilience against evolving digital threats ?

(5 marks)

(*c*) TechSecure faced concerns about role boundaries, business diversification, and ethical responsibilities in the digital ecosystem. In this context, what guidelines should TechSecure follow relating to social media administered by the Ministry of Electronics and IT of the Intermediary Guidelines and Digital Media Ethics Code, for regulating social media platforms.

(5 marks)

(*d*) Considering TechSecure's role in AI-driven cybersecurity and OTT compliance, what way forward strategies should the company adopt to successfully adapt to the provisions of the Digital India Act ?

(*5 marks*)

(*e*) In the context of TechSecure's ransomeware incident, how could a structured threat hunting investigation have helped detect the attack earlier and reduce its impact ?

(5 marks)

2. TechNova Digital Solutions Pvt. Ltd. is a globally recognized leader in the Information Technology industry, renowned for its cutting-edge innovations and extensive digital ecosystem. The company operates a diverse range of online services, including an Online Content Platform that hosts a wide array of digital content such as news, current affairs, blogs, and audio-visual materials, and attracts millions of daily active users from various regions worldwide. It's social media platform VibeNest enables users to connect, share posts, exchange multimedia content, and participate in live discussions. It also offers secure and user-friendly email services to individuals and organizations that support integration with third-party applications and cloud storage for seamless communication. Headquartered in India, with operational offices in Europe, North America, and Southeast Asia, and serves a global user base exceeding 10 million registered accounts across all its platforms. Known for its technological advancements, but recently under scrutiny for challenges in data privacy, misinformation control, and timely grievance redressal. TechNova manages an Aadhaar-based identity authentication service integrated with its digital content platform but concerns arose regarding the collection, storage, and use of biometric and demographic data without explicit consent safeguards.

TechNova's online content platform is facing increasing criticism for being a hub of fake news, hate speech, and illegal content. During the recent state elections, several unverified posts spread rapidly across the platform, shaping voter perceptions and sparking public unrest. In another instance, a false rumor about a health emergency went viral, leading to panic buying and street-level protests. These incidents exposed serious vulnerabilities in TechNova's content moderation processes, fact-checking mechanisms, and overall responsiveness to user grievances.

TechNova's popular social media platform, "VibeNest" faced an incident where a flaw in its popular media platform integration feature "View As" was exploited, allowing hackers unauthorized access to the million-user accounts, including third-party apps linked through social login. This led to the theft of access tokens for thousands of accounts, exposure of personal information as name, email/phone numbers of 20 thousand users, and additional sensitive details like gender, religion, and location leaked for 30 thousand accounts. The company taken technological safeguards and patch and upgrade the "View As" feature with multi-layer authentication and role-based access control and implement end-to-end encryption for access tokens and sensitive data.

TechNova suffered a sophisticated cyberattack on its centralized database that managed client credentials, financial transactions, and personal information. Hackers exploited a vulnerability in the company's web application to gain unauthorized access to its servers. They tampered with computer source code, altering transaction logs and misdirecting payments. Attackers used advanced techniques to erase traces of their intrusion, making it difficult for the incident response team to trace their activities.

This breach compromised over 500,000 user accounts. To strengthen the Company's defensive perimeter, the configuration and performance of the firewalls across all data centres were evaluated. They saw them not as passive barriers but as active components of threat management. The latest generation of firewalls in use had intrusion prevention systems capable of identifying malicious patterns in network traffic and blocking them before damage occurred. However, they found that the firewall policies in some regional facilities were overly permissive, allowing unnecessary inbound connections. This was promptly rectified, with tighter rules and regular review schedules introduced to ensure that only essential traffic passed through.

A legal challenge emerged when certain politically sensitive posts were taken down without court orders, leading to accusations of violating citizens' free speech rights online on social media platforms. It would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.

TechNova faced major challenges in data privacy, cybersecurity, and content moderation, including unauthorized access, misuse of Aadhaar data, and fake news proliferation. These incidents exposed gaps in grievance redressal, consent management, and compliance with IT regulations. While corrective measures were adopted, a proactive privacy-by-design appraoch and stronger adherence to IT Rules 2021 are essential to restore user trust and regulatory compliance.

In the above case scenario, answer the following questions :

(*a*) TechNova's Aadhaar-based identity authentication raised concerns over collecting and using biometric and demographic data without proper consent safeguards.

— What is the Supreme Court's stance in the 2018's Aadhaar judgement concenrning the Right to Privacy ?

— How does the case illustrate the balance between technological innovation (AI-driven biometric systems) and individual privacy rights in India ?

(5 marks)

(*b*) A viral rumor threatens to spoil TechNova's fame in the digital media world.

— How the Information Technology rules apply to TechNova in this scenario ?

— What key monthly compliance requirements must TechNova fulfill as a large digital platform ?

— How do these rules aim to enhance accountability, grievance redressal, and proactive content regulations ?

(*5 marks*)

(*c*) TechNova Digital Solutions Pvt. Ltd. has recently faced multiple cybersecurity breaches, including unauthorized access to Aadhaar-based identity data, fake news propagation during elections, and exploitation of its social media platform 'VibeNest'. Such vulnerabilities in major IT platforms can be leveraged for cyber terrorism activities in India.

In support of your answer, analyze the real-life cases of cyber terrorism attacks reported in the country over the past decade.

(*5 marks*)

(*d*) You have been asked for consultation in TechNova Digital Solutions Pvt. Ltd to suggest a device that exclude unwanted and undesirable network traffic from entering the organization's system.

Critically evaluate the role of the suggested device, including next-generation capabilities, in an organisation's network defence strategy.

(5 marks)

(*e*) "It would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not'.

In light of the above statement, how can a legal framework be established for accusations of violating citizens free speech rights in judicial proceedings ?

(5 marks)

3. Arun is the CEO of SecureNext E-Commerce Pvt. Ltd., one of India's fastest-growing online platforms. The company specializes in providing engineering equipment, industrial solutions, and services to industries across the country. Its rapid expansion has made it a crucial player in India's industrial supply chain, handling thousands to customer transactions everyday.

The transactions involve sensitive payment information, vendor agreements, employee data, and proprietary product designs. This combination of intellectual property, financial records, and personal data makes SecureNext an attractive target for cybercriminals. As the business grows, the volume of data and the complexity of its IT infrastructure have also expanded, creating new cybersecurity challenges.

Recently, SecureNext has been facing serious software security issues in its internal network. Unauthorized logins, SQL injection attempts, and ransomware alerts have created concern for both Arun and regulators. These events have alarmed not only Arun and his leadership team but also regulators and stakeholders. The Board of Directors has formally directed Arun to strengthen cybersecurity compliance and align reporting mechanisms with statutory requirements under the Information Technology Act, 2000, Digital Personal Data Protection (DPDP) Act, 2023, Sectoral advisories from CERT-In and the Reserve Bank of India (RBI), particularly for handling financial transactions.

The first major crisis struck when SecureNext's application servers were targeted by a ransomware attempt. Investigations revealed the root causes are weak access controls, unpatched open-source libraries, and a lack of multi-factor authentication. The RBI and CERT-In advisories mandate regular patch management, encryption of sensitive data, and multifactor authentication for payment systems. To meet these requirements, Arun must institutionalize secure coding practices, roll out access control policies, and ensure detailed logging of user activity, while also filing timely compliance reports to regulators.

To overcome scalability and resilience challenges, the company's member of advisory board, Mr. Deepak suggested adopting a cloud computing model where a provider delivers on-demand computing resources like servers, storage, and networking over the internet for flexibility and scalability, and offers benefits such as cost efficiency and disaster recovery, shared responsibility matrices, and provider responsibilities with hardware security, hypervisor patching and Customer responsibilities in application security, data protection, identity management. Before migration, SecureNext must prepare a compliance roadmap, demonstrating how security responsibilities will be divided between the cloud provider and the company. Arun realizes this decision requires deep knowledge of cloud architectue, statutory obligations, and forensic readiness.

A troubling insider attack revealed further gaps in SecureNext's security posture. During foresnic investigations, it was discovered that the incident response team had failed to capture volatile evidence (RAM data such as session keys, temporary files, and unsaved logs) before the compromised system was rebooted. Since volatile evidence disappears once a system is powered down, this failure raised serious concerns. To fix this, Arun must ensure that forensic policies mandate the order of the volatility principle and use tools like FTK Imager and registry viewer, and establish standard operating procedures (SOPs) for handling live evidence during incident response.

During the festival season, SecureNext faced a DDoS attack that temporarily crippled its main database, but operations were restored using remote recovery. As part of its cloud strategy, the company is conducting Disaster Recovery (DR) testing with geo-redundant backups and high-availability architecture. Meanwhile, an employee accused of data theft formatted his workstation to erase evidence. Forensic investigators recovered deleted files from unallocated disk space, but during legal proceedings, the defense challenged the evidence due to improper chain of custody, missing hash verification logs, and incomplete documentation. CEO Arun must now ensure robust cybersecurity measures, proper forensic protocols, and compliance with Indian regulations to strengthen resilience and maintain the admissibility of digital evidence in future incidents.

From the above scenario, answer the following questions :

(*a*) SecureNext's servers were compromised due to weak access controls and unpatched software libraries. Software security is a continuous process that starts at design and development and continues through the lifecycle with regular updates and patches to address vulnerabilities. In this context, what best practices would you suggest, being a consultant, be adopted to strengthen software security and prevent such attacks ?

(5 marks)

(*b*) Mr. Deepak recommended migrating to a cloud service platform, where computing, networking, and storage resources are made available to users on demand over the internet on a pay on use basis. Which cloud service model will meet SecureNext's requirements, and what advantages can the company gain from utilizing this service ?

(5 marks)

(*c*) SecureNext found a suspect's unauthorized data transfer from one of its servers. As a forensic investigator, you perform Live Forensics to capture volatile data.

— Analyze, why Live Forensics is the preferred method in this situation ?

— Describe the order of volatility you would follow during evidence collection, and

— Evalaute the potential risks if the live data is not collected immediately.

(5 marks)

(*d*) During the festival season, SecureNext successfully utilized remote recovery capabilities to restore operations after a Distributed Denial-of-Service (DDoS) attack. Analyze the importance of implementing remote recovery as part of the company's cloud disaster recovery strategy.

(5 marks)

(*e*) During a data theft investigation at SecureNext, forensic analysts retrieved deleted files from unallocated disk space using specialized tools.

— What are the capabilities of digital investigation software that it maintains the admissibility of such evidence in court ?

— How do tools like Forensic Toolkit and EnCase ensure data integrity during this process ?

(5 marks)

4. In the first quarter of 2025, Pragati Bank Ltd., a mid-sized private sector bank in India, began to feel the pressure of rising competition from nimble fintech players. These new-age companies were offering real-time payments, decentralized investment products and seamless user experiences that traditional banks struggled to match. Pragati Bank, with its legacy systems and centralized databases, often found itself dealing with reconciliation delays, operational bottlenecks, and increasing customer complaints about transparency. It was against this backdrop that the Board of Directors initiated a discussion on adopting blockchain technology as part of the bank's long-term digital transformation agenda.

The bank's management recognized that blockchain, though popularly associated with cryptocurrencies, offered much broader applications. The directors were also keen on the promise of reducing dependence on third-party auditors and intermediaries, which not only raised costs but also left scope for human errors. To justify the investment, the Board asked the executive team to present a clear business case. The team highlighted three areas of concern.

First, the time and effort spent reconciling inter-branch and inter-bank transactions consumed enormous resources and affected service delivery.

Second, customers were increasingly demanding quicker settlements and transparent systems where they could track their transactions instantly.

Third, the bank was facing heightened risks from cyber threats, making it necessary to adopt a system that ensured confidentiality, integrity and availability of data. Blockchain, they argued, could provide a framework that addressed all these concerns, provided it was implemented correctly.

The bank did not want to adopt the technology blindly. The technology committee studied global practices and found that leading banks in Europe and Singapore had already begun using blockchain for trade finance and settlements. Some institutions had also experimented with decentralized finance applications that enabled peer-to-peer lending without involving traditional intermediaries. Non-fungible tokens, although popularly known in the art world, were also being used to certify ownership of digital contracts and documents, a use case highly relevant to loan agreements and property papers. Encouraged by these developments, Pragati Bank began exploring potential vendors who could deliver blockchain solutions adapted to its needs. Three vendors were shortlisted and invited to present their products through a structured request for proposal process.

There was also the larger issue of aligning the bank's management information system, which handled everything from customer databases to HR processes, with the distributed design of blockchain. Pragati Bank's prime service that is offered in the banking industry is to solve the financial problems that the customers of the bank are facing. The MIS in a bank must be designed in such a manner that it is able to provide differentiated services to the varied service requests of the customers. The key factors which Pragati Bank Ltd should consider while designing a Banking Information System may be Customer Database; Service to the Account Holders; Service for Business Promotions; Index Monitoring System; Human Resource Upgrade.

The Company Secretary reminded the Board that under the Companies Act, the responsibility of maintaining statutory books of accounts remained unchanged, regardless of the medium or technology used. Blockchain, therefore, could complement but not replace legal and regulatory obligations.

Despite these concerns, the bank approved a pilot project with one of the vendors. Blockchain was introduced in trade finance, where letters of credit and cross-border remittances were recorded on the distributed ledger, and in payroll management, where salary payments and vendor bills were validated through smart contracts. The early results were encouraging, transaction times reduced significantly, reconciliation errors dropped, and customers appreciated the enhanced transparency. However, new risks soon surfaced. A coding flaw in one smart contract led to an overpayment to a supplier, and because blockchain entires were irreversible, the error could not be corrected. Regulators also expressed apprehensions that peer-to-peer lending platforms modelled on decentralized finance could undermine established safeguards designed to protect depositors.

The Chief Information Security Officer emphasized that any system must guarantee secure and reliable information access, while the Committee stressed the need for staff training in blockchain, smart contracts, and cryptographic protocols. The Company Secretary proposed a phased approach. Instead of rolling out blockchain across all functions, the bank should first consolidate its success in internal operations such as vendor management and cross-border payments, while keeping experimental projects like decentralized lending within a controlled sandbox environment. He recommended drawing up a comprehensive compliance framework mapping blockchain transactions to statutory obligations, negotiating robust vendor contracts with clear liability clauses, and conducting independent audits of smart contracts. The Board accepted this advice and also resolved to publish an annual Blockchain Governance Report to communicate its approach transparently to shareholders, regulators and customers.

While immutability, decentralization, and efficiency offered by the technology were compelling, the risks of coding errors, legal uncertainties, and regulatory pushback could not be ignored. The case highlighted the fact that blockchain was not merely a technological shift but a tansformation with deep legal, ethical, and governance implications. For traditional banks, the challenge lies not in jumping on the blockchain bandwagon but in carefully aligning innovation with fiduciary duties, compliance requirements, and the trust that underpinned their relationship with customers.

Based on the facts, answer the following questions :

(*a*) Pragati Bank, with its legacy systems and centralized databases, often found itself dealing with reconciliation delays, operational bottlenecks, and increasing customer complaints about transparency. Why do you think Board of Directors initiated a dicussion on adopting blockchain technology as part of the bank's long-term digital transformation agenda ?

(*5 marks*)

(*b*) What governance safeguards and legal reviews should Pragati Bank Ltd. undertake before finalizing a blockchain vendor contract to ensure value and minimize risks ?

(*5 marks*)

(*c*) The prime service that is offered in the banking industry is to solve the financial problems that the customers of the bank are facing. The MIS in a bank must be designed in such a manner that it is able to provide differentiated services to the varied service requests of the customers. Outline the key factors which Pragati Bank Ltd should consider while designing a Banking Information System.

(*5 marks*)

(*d*) "There was also the larger issue of aligning the bank's management information system, which handled everything from customer databases to HR processes, with the distributed design of blockchain." Elucidate the essential elements required for the effective implementation of a complete information system in an organisation.

(*5 marks*)

(*e*) Technology is a huge part of business, so managing corporate and customer data is top priority for companies. As this intervention of technology in banking becomes most essential to keep data secured and make policies related to data security, what are the factors chief information security officer should adhere in safeguarding information security in banks ?

(*5 marks*)

———— o ————