SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

III SEMESTER

PMC303 - DATA SECURITY AND PRIVACY

Regulation – 2024

Academic Year 2025 – 2026(Odd Semester)

Prepared by

P.Pandi Deepa

Assistant Professor
Department of Computer Applications

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur-603 203
DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

SUBJECT : PMC303 - DATA SECURITY AND PRIVACY
SEM/YEAR: III / II

UNIT - I: ATTACKS AND PRIVACY

Attacks: Analyzing common attack vectors – Data Security – Probabilistic reasoning about attacks –Data security mitigations. Privacy aware Machine learning and Data Science: Privacy preserving techniques in ML - Open-source libraries for PPML Architecting privacy in Data and ML projects

UNIT - I: PART – A

Q. No	Question	BT Level	Competence	Course Outcome
1	Define **attack vector** with an example.	BTL-1	Remember	CO1
2	What is a **brute-force attack** in cybersecurity?	BTL-1	Remember	CO1
3	List any two types of **social engineering attacks**.	BTL-1	Remember	CO1
4	What is the difference between **passive** and **active attacks**?	BTL-1	Remember	CO1
5	Define **data confidentiality** and **data integrity**.	BTL-1	Remember	CO1
6	What do you mean by **probabilistic reasoning** in the context of attacks?	BTL-1	Remember	CO1
7	Give any two examples of **data security breaches**.	BTL-1	Remember	CO1
8	What is a **zero-day attack**?	BTL-1	Remember	CO1
9	Explain how a **phishing attack** works with a real-time example.	BTL-2	Understand	CO1
10	How does **encryption** help in data security?	BTL-2	Understand	CO1
11	Describe the role of **threat modeling** in identifying attack vectors.	BTL-2	Understand	CO1
12	Explain **probabilistic reasoning** with respect to analyzing attack likelihood.	BTL-2	Understand	CO1
13	List any two **data security mitigation techniques**.	BTL-1	Remember	CO1
14	What is the purpose of **access control mechanisms**?	BTL-1	Remember	CO1
15	Define **firewall** and its use in network security.	BTL-1	Remember	CO1
16	What is a **hashing algorithm**?	BTL-1	Remember	CO1
17	What is the difference between **symmetric** and **asymmetric encryption**.	BTL-2	Understand	CO1
18	How does **multi-factor authentication (MFA)** enhance data security?	BTL-2	Understand	CO1

19	Discuss how **regular software updates** help mitigate vulnerabilities.	BTL-2	Understand	CO1
20	Describe how **intrusion detection systems (IDS)** work.	BTL-2	Understand	CO1
21	What is **Privacy-Preserving Machine Learning (PPML)**?	BTL-1	Remember	CO1
22	Name any two **open-source libraries** used for PPML.	BTL-1	Remember	CO1
23	What is **differential privacy**?	BTL-1	Remember	CO1
24	Define **federated learning** in ML.	BTL-1	Remember	CO1

UNIT - I: PART – B

CO1

Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	Illustrate various **common attack vectors** (e.g., phishing, malware, MITM) with suitable examples. Design a simple attack scenario involving two of these vectors.	16	BTL-3	Apply	CO1
2	Analyze the working of a **SQL Injection attack** and suggest a mitigation strategy by examining its vulnerabilities.	16	BTL-4	Analyze	CO1
3	Compare **phishing and spear-phishing** attacks with real-world examples. What makes spear-phishing harder to detect?	16	BTL-4	Analyze	CO1
4	Evaluate the impact of Advanced Persistent Threats (APTs) on enterprise security. Justify your answer with at least one case study.	16	BTL-5	Evaluate	CO1
5	Apply the concept of probabilistic reasoning to estimate the likelihood of a ransomware attack on a banking system. Use basic probabilities to model and explain.	16	BTL-3	Apply	CO1
6	Analyze the relationship between **data confidentiality, integrity, and availability (CIA)** with respect to data breach incidents.	16	BTL-4	Analyze	CO1
7	Examine how **attack trees** and **Bayesian models** help in understanding and predicting cyber attacks.	16	BTL-4	Analyze	CO1
8	Critically evaluate the use of probabilistic reasoning models in cybersecurity risk assessment. What are the limitations?	16	BTL-5	Evaluate	CO1
9	Design a basic Bayesian Network model to analyze a security incident involving multiple attack paths (e.g., phishing, malware, insider threat).	16	BTL-3	Apply	CO1
10	Implement a data security plan for an educational institution. Apply techniques like access control, encryption, and backup planning.	16	BTL-3	Apply	CO1
11	Analyze and compare the effectiveness of **firewalls, IDS, and antivirus software** in protecting against external threats.	16	BTL-4	Analyze	CO1
12	Differentiate **preventive, detective, and corrective** security controls using real-time examples.	16	BTL-4	Analyze	CO1

13	Evaluate the effectiveness of multi-layered security architecture (defense-in-depth) in enterprise systems.	16	BTL-5	Evaluate	CO1
14	Evaluate the benefits and trade-offs of differential privacy vs. federated learning in real-time ML applications.	16	BTL-5	Evaluate	CO1
15	Analyze the privacy risks involved in ML-based healthcare applications. What can go wrong if privacy isn't preserved?	16	BTL-4	Analyze	CO1
16	Design a privacy-preserving ML pipeline using federated learning and differential privacy techniques. Include tools and libraries used.	16	BTL-6	Create	CO1
17	Create an architecture for a privacy-preserving data analytics platform for a retail company. Include data minimization, anonymization, and compliance aspects (e.g., GDPR).	16	BTL-6	Create	CO1

UNIT II ENCRYPTED COMPUTATION

Encrypted computation – Types of encrypted computation: Secure Multi-party computation – Homomorphic encryption. Real-world encrypted computation: Private set intersection – Private join and compute – Secure Aggregation – Encrypted Machine Learning. PSI and Moose.

UNIT II PART – A

Q. No	Questions	BT Level	Competence	Course Outcome
1	Define **encrypted computation**.	BTL-1	Remember	CO2
2	What is **Secure Multi-party Computation (SMPC)**?	BTL-1	Remember	CO2
3	Define **homomorphic encryption**.	BTL-1	Remember	CO2
4	Name any two types of **homomorphic encryption** schemes.	BTL-1	Remember	CO2
5	List any two **applications** of encrypted computation.	BTL-1	Remember	CO2
6	What do you mean by **semi-honest adversary** in SMPC?	BTL-1	Remember	CO2
7	Name two cryptographic techniques used in **SMPC**.	BTL-1	Remember	CO2
8	State the difference between **partially** and **fully homomorphic encryption**.	BTL-1	Remember	CO2
9	Explain how **homomorphic encryption** allows computation on encrypted data.	BTL-2	Understand	CO2
10	Compare **SMPC** and **homomorphic encryption** in terms of privacy and computation.	BTL-2	Understand	CO2
11	Illustrate the need for **encrypted computation** in cloud environments.	BTL-2	Understand	CO2
12	Explain the term **"computation over encrypted data"** with an example.	BTL-2	Understand	CO2
13	What is **Private Set Intersection (PSI)**?	BTL-1	Remember	CO2
14	Define **Private Join and Compute (PJC)**.	BTL-1	Remember	CO2
15	What is **Secure Aggregation**?	BTL-1	Remember	CO2
16	Mention one **real-world application** of PSI.	BTL-1	Remember	CO2
17	What does the term **privacy-preserving aggregation** mean?	BTL-1	Remember	CO2

18	Name any two organizations using Secure Aggregation in production.	BTL-1	Remember	CO2
19	Describe the process of **Private Set Intersection** with an example scenario.	BTL-2	Understand	CO2
20	Explain how **Secure Aggregation** ensures data privacy in federated learning.	BTL-2	Understand	CO2
21	Compare **Private Join and Compute** with PSI.	BTL-2	Understand	CO2
22	+Discuss the use of **encrypted machine learning** in healthcare or finance.	BTL-2	Understand	CO2
23	What is **Moose** in the context of encrypted computation?	BTL-2	Understand	CO2
24	List one difference between **PSI** and **Moose**.	BTL-1	Remember	CO2

UNIT II PART – B

Q. No	Question	Mark	BT Level	Competence	Course Outcome
1	**Design a scenario** in which encrypted computation is necessary. Show how either **homomorphic encryption** or **SMPC** can be applied to solve it.	16	BTL-3	Apply	CO2
2	Apply **partially homomorphic encryption** to compute the sum of encrypted data without decrypting it. Explain step by step.	16	BTL-3	Apply	CO2
3	Construct a real-world application where **SMPC** is used to compute a function collaboratively without revealing individual inputs.	16	BTL-3	Apply	CO2
4	Analyze the trade-offs between **homomorphic encryption** and **secure multi-party computation** in terms of computational cost and privacy.	16	BTL-4	Analyze	CO2
5	Compare and contrast **fully**, **partially**, and **somewhat** homomorphic encryption with examples.	16	BTL-4	Analyze	CO2
6	Analyze the limitations of using **encrypted computation** in large-scale cloud data processing.	16	BTL-4	Analyze	CO2
7	Explain how the choice of encrypted computation technique depends on the **threat model** (e.g., honest-but-curious vs malicious adversaries).	16	BTL-4	Analyze	CO2
8	Evaluate the effectiveness of **SMPC protocols** (like Yao's Garbled Circuits or GMW) in financial use cases such as joint fraud detection.	16	BTL-5	Evaluate	CO2
9	Assess the suitability of **homomorphic encryption** in a healthcare data analytics system. What are the privacy and performance implications?	16	BTL-5	Evaluate	CO2
10	Compare the **usability, performance, and security guarantees** of SMPC and homomorphic encryption in the context of secure elections.	16	BTL-5	Evaluate	CO2
11	Analyze the challenges in implementing **encrypted machine learning** and how real-world frameworks attempt to overcome them.	16	BTL-4	Analyze	CO2
12	Discuss how **Private Join and Compute** balances computation cost	16	BTL-4	Analyze	CO2

	and data confidentiality when working across datasets.				
13	Apply **Private Set Intersection (PSI)** in a contact tracing scenario where privacy of individuals is preserved.	16	BTL-3	Apply	CO2
14	Demonstrate the use of **Private Join and Compute** in ad conversion tracking with encrypted user identifiers.	16	BTL-3	Apply	CO2
15	Illustrate how **Secure Aggregation** works in federated learning. Show how client updates are encrypted and aggregated.	16	BTL-3	Apply	CO2
16	Evaluate the impact of using **encrypted computation** techniques on model accuracy and system performance in ML pipelines.	16	BTL-5	Evaluate	CO2
17	Design a secure application using Moose and PSI to allow hospitals to compute common patient statistics across institutions without revealing raw data.	16	BTL-6	Create	CO2

UNIT – III DATA GOVERNANCE AND PRIVACY APPROACHES

Data Governance – Identifying sensitive data – Documenting data for use - Basic Privacy – Anonymization – Differential privacy – Privacy loss – Differential privacy with Laplace mechanism – Gaussian noise for differential privacy – Sensitivity and Privacy units – kAnonymity – Building Privacy into Data Pipelines.

Q. No	**Questions**	**BT Level**	**Competence**	**Course Outcome**
	UNIT III PART – A			
1	Define **data governance**.	BTL-1	Remember	CO3
2	What is meant by **sensitive data**?	BTL-1	Remember	CO3
3	List any two examples of **personally identifiable information (PII)**.	BTL-1	Remember	CO3
4	What do you mean by **data documentation**?	BTL-1	Remember	CO3
5	Define the term **metadata** in the context of data governance.	BTL-1	Remember	CO3
6	State two key objectives of **data governance policies**.	BTL-1	Remember	CO3
7	Explain why it is important to **identify and label sensitive data**.	BTL-2	Understand	CO3
8	Describe how **data documentation** supports transparency in data usage.	BTL-2	Understand	CO3
9	Differentiate between **sensitive** and **non-sensitive data** with examples.	BTL-2	Understand	CO3
10	Explain the relationship between **data governance** and **compliance requirements** (e.g., GDPR, HIPAA).	BTL-2	Understand	CO3
11	What is **basic data privacy**?	BTL-1	Remember	CO3
12	Define **anonymization**.	BTL-1	Remember	CO3
13	What is **k-anonymity**?	BTL-1	Remember	CO3
14	List two techniques used for **anonymization** of data.	BTL-1	Remember	CO3
15	What is a **quasi-identifier**?	BTL-1	Remember	CO3
16	Define **re-identification risk**.	BTL-1	Remember	CO3
17	Explain the concept of **k-anonymity** with a simple example.	BTL-2	Understand	CO3
18	Discuss the limitations of **basic anonymization techniques**.	BTL-2	Understand	CO3
19	Differentiate between **anonymization** and **pseudonymization**.	BTL-2	Understand	CO3
20	Why is **k-anonymity** considered insufficient for high-risk datasets?	BTL-2	Understand	CO3
21	Define differential privacy.	BTL-1	Remember	CO3

22	What is the **Laplace mechanism** in differential privacy?	BTL-1	Remember	CO3
23	What is meant by **sensitivity** in differential privacy?	BTL-1	Remember	CO3
24	What is the role of **Gaussian noise** in privacy preservation?	BTL-1	Remember	CO3

UNIT III PART – B

Q. No	Question	Mark	BT Level	Competence	Course Outcome
1	Apply the principles of **data governance** to design a data access policy for a healthcare institution.	16	BTL-3	Apply	CO3
2	Demonstrate how to **identify sensitive data** in a banking dataset using data classification techniques.	16	BTL-3	Apply	CO3
3	Create a data documentation plan for a dataset used in a **machine learning project**, including metadata and data lineage.	16	BTL-3	Apply	CO3
4	Analyze the **challenges in identifying sensitive data** in a large enterprise environment with structured and unstructured data.	16	BTL-4	Analyze	CO3
5	Compare and contrast different **data documentation approaches** and explain their impact on privacy compliance and auditability.	16	BTL-4	Analyze	CO3
6	Apply **anonymization techniques** to transform a sample dataset while retaining its analytical value.	16	BTL-3	Apply	CO3
7	Use a real-life example to explain how **k-anonymity** can protect user identities in a public dataset.	16	BTL-3	Apply	CO3
8	Analyze the risks of **re-identification** in anonymized datasets and explain how **quasi-identifiers** contribute to the problem.	16	BTL-4	Analyze	CO3
9	Compare **k-anonymity, l-diversity, and t-closeness**. In which scenarios is each more effective?	16	BTL-4	Analyze	CO3
10	Evaluate the effectiveness of **traditional anonymization techniques** versus **modern privacy-preserving methods** (like differential privacy) in the context of e-commerce data.	16	BTL-5	Evaluate	CO3
11	Use a numerical example to demonstrate the working of **Gaussian noise** in differential privacy.	16	BTL-3	Apply	CO3
12	Analyze how **privacy loss** is calculated and managed in differential privacy. What does the privacy budget represent?	16	BTL-4	Analyze	CO3
13	Differentiate between **Laplace mechanism and Gaussian mechanism** with their mathematical formulation and use cases.	16	BTL-4	Analyze	CO3
14	Design a **data pipeline** that incorporates privacy-preserving steps such as encryption, access control, and anonymization.	16	BTL-3	Apply	CO3
15	Implement a privacy-aware data flow in a **real-time analytics pipeline** using tools like Apache Kafka or Spark.	16	BTL-3	Apply	CO3
16	Propose an architecture to embed **differential privacy mechanisms** directly into an ML training pipeline.	16	BTL-6	Create	CO3
17	Create a complete privacy governance framework for a company that handles user behavioral data for targeted advertising.	16	BTL-6	Create	CO3

UNIT – IV FEDERATED LEARNING AND DATA SCIENCE

Distributed data – Distributed Optimization - Federated learning – Architecting federated systems – Open-source federated libraries – Federated data science				
Q. No	**Questions**	**BT Level**	**Competence**	**Course Outcome**
	UNIT IV PART – A			
1	Define **distributed data**.	BTL-1	Remember	CO4
2	What is **data partitioning** in distributed systems?	BTL-1	Remember	CO4
3	List two examples of **distributed data storage systems**.	BTL-1	Remember	CO4
4	What is meant by **data locality**?	BTL-1	Remember	CO4
5	Define **distributed optimization**.	BTL-1	Remember	CO4
6	Name any two techniques used in **distributed optimization**.	BTL-1	Remember	CO4
7	What is a **parameter server** in distributed learning?	BTL-1	Remember	CO4
8	Mention any two challenges in handling distributed data.	BTL-1	Remember	CO4
9	What is **federated learning**?	BTL-1	Remember	CO4
10	List two advantages of federated learning.	BTL-1	Remember	CO4
11	What is a **federated averaging algorithm (FedAvg)**?	BTL-1	Remember	CO4
12	Define **client drift** in federated learning.	BTL-1	Remember	CO4
13	Name any two devices where federated learning is commonly used.	BTL-1	Remember	CO4
14	What is **model aggregation** in federated systems?	BTL-1	Remember	CO4
15	Explain the difference between **federated learning** and **centralized learning**.	BTL-2	Understand	CO4
16	Describe the concept of **on-device learning** in federated environments.	BTL-2	Understand	CO4
17	Discuss how **privacy** is maintained in federated learning.	BTL-2	Understand	CO4
18	Explain how **federated learning supports personalization** of models.	BTL-2	Understand	CO4
19	Identify key components of a **federated learning architecture** (e.g., client, server, aggregator).	BTL-2	Understand	CO4
20	Describe the challenges of **communication efficiency** in federated systems.	BTL-2	Understand	CO4
21	**Discuss** any two key features of PySyft and how they support federated learning.	BTL-2	Understand	CO4
22	**Explain** the concept of federated data science in your own words.	BTL-2	Understand	CO4
23	**Describe** two real-world applications of federated data science and how they benefit from data privacy.	BTL-2	Understand	CO4
24	**Interpret** two commonly used metrics to evaluate performance in federated learning environments.	BTL-2	Understand	CO4

	UNIT IV PART – B				
Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	Apply a **distributed data architecture** for a multinational company managing real-time analytics across geolocations.	16	BTL-3	Apply	CO4
2	Demonstrate how **gradient descent** can be adapted to work in a distributed environment.	16	BTL-3	Apply	CO4
3	Illustrate the role of **parameter servers** in distributed optimization with a case study from a large-scale ML training scenario.	16	BTL-3	Apply	CO4
4	Construct a federated learning scenario involving mobile devices	16	BTL-3	Apply	CO4

	using FedAvg and explain the step-by-step flow**.**				
5	Analyze the impact of **data partitioning strategies** (horizontal vs. vertical) on performance and fault tolerance.	16	BTL-4	Analyze	CO4
6	Compare and contrast **synchronous vs. asynchronous distributed optimization** with respect to convergence and scalability.	16	BTL-4	Analyze	CO4
7	Examine the trade-offs between **data consistency and scalability** in distributed data systems.	16	BTL-4	Analyze	CO4
8	Apply federated learning to a healthcare application involving multiple hospitals with patient data privacy constraints.	16	BTL-3	Apply	CO4
9	Analyze the problem of **client drift** and its impact on model convergence in non-IID federated data.	16	BTL-4	Analyze	CO4
10	Compare **federated learning** and **traditional centralized learning** in terms of privacy, latency, and model performance.	16	BTL-4	Analyze	CO4
11	Discuss the challenges of **handling stragglers and dropped clients** in federated learning environments	16	BTL-4	Analyze	CO4
12	Break down the stages of a federated learning system pipeline, highlighting where architectural optimizations can be made.	16	BTL-4	Analyze	CO4
13	Design a high-level architecture for a federated system used in real-time predictive maintenance in manufacturing.	16	BTL-3	Apply	CO4
14	Assess the benefits and limitations of using **open-source libraries** for deploying federated learning at scale.	16	BTL-5	Evaluate	CO4
15	Compare the **deployment flexibility, scalability, and community support** among federated libraries like FATE, OpenFL, and Flower.	16	BTL-5	Evaluate	CO4
16	Propose a federated data science workflow for a **collaborative fraud detection system** across multiple financial institutions without sharing raw data.	16	BTL-6	Create	CO4
17	Design a complete **federated learning architecture** with edge devices, model server, aggregator, and privacy-preserving techniques for a smart city application.	16	BTL-6	Create	CO4

UNIT – V LEGALITY OF PRIVACY

GDPR – CCPA – HIPAA - LGPD - PIPL- Internal policies and contracts – Adhering to contract agreements and law – Interpreting Data protection regulations – Data governance 2.0 - Indian Data Protection Framework - Use case analysis.

Q. No	Questions	BT Level	Competence	Course Outcome
	UNIT V PART – A			
1	Define **GDPR**.	BTL-1	Remember	CO5
2	List two key rights provided to individuals under GDPR.	BTL-1	Remember	CO5
3	What is the purpose of a **Data Protection Impact Assessment (DPIA)** under GDPR?	BTL-1	Remember	CO5
4	Describe the concept of **consent** under GDPR.	BTL-1	Remember	CO5
5	Explain the role of a **Data Protection Officer (DPO)** as per GDPR.	BTL-1	Remember	CO5

6	Define **CCPA** and mention one of its main objectives.	BTL-1	Remember	CO5
7	What are two rights given to consumers under the CCPA?	BTL-1	Remember	CO5
8	Differentiate between **GDPR and CCPA** in terms of scope and applicability.	BTL-1	Remember	CO5
9	What is the primary goal of **HIPAA**?	BTL-1	Remember	CO5
10	List two types of entities covered under HIPAA.	BTL-1	Remember	CO5
11	Define **Protected Health Information (PHI)**.	BTL-1	Remember	CO5
12	What is **LGPD**?	BTL-1	Remember	CO5
13	Mention two similarities between **LGPD** and **GDPR**.	BTL-1	Remember	CO5
14	Describe the term **data subject rights** under LGPD.	BTL-2	Understand	CO5
15	What is **PIPL**?	BTL-2	Understand	CO5
16	List two key principles of data protection under PIPL.	BTL-2	Understand	CO5
17	Explain how **user consent** is handled in PIPL.	BTL-2	Understand	CO5
18	Describe the role of **data localization** under PIPL.	BTL-2	Understand	CO5
19	Compare **PIPL and GDPR** in terms of enforcement.	BTL-2	Understand	CO5
20	Define **internal data policy** in the context of data protection.	BTL-2	Understand	CO5
21	Mention two reasons why **contract compliance** is important in data privacy.	BTL-2	Understand	CO5
22	Explain the need for **interpreting data protection regulations** accurately.	BTL-2	Understand	CO5
23	Describe how organizations can **adhere to data sharing contracts**.	BTL-2	Understand	CO5
24	What is **Data Governance 2.0** and how does it differ from traditional data governance?	BTL-2	Understand	CO5

UNIT V PART – B

Q. No	**Question**	**Mark**	**BT Level**	**Competence**	**Course Outcome**
1	Apply the key principles of **GDPR** to design a privacy-compliant data handling system for a European e-commerce platform.	16	BTL-3	Apply	CO5
2	Demonstrate how a **healthcare application** should be designed to comply with **HIPAA** regulations.	16	BTL-3	Apply	CO5
3	Illustrate how a company based in California must handle user data to comply with **CCPA**.	16	BTL-3	Apply	CO5
4	Implement the **Indian Data Protection Bill** principles in the development of a local fintech app.	16	BTL-3	Apply	CO5
5	Show how **internal privacy policies and contracts** can be aligned with global data protection laws in a multinational organization.	16	BTL-3	Apply	CO5
6	Analyze the similarities and differences between **GDPR**, **CCPA**, and **PIPL** in terms of consent, user rights, and enforcement.	16	BTL-4	Analyze	CO5
7	Examine the impact of **LGPD** on Brazilian startups handling personal data of EU and non-EU citizens.	16	BTL-4	Analyze	CO5
8	Compare **HIPAA** and **GDPR** in the context of healthcare data privacy and cross-border data flow.	16	BTL-4	Analyze	CO5
9	Analyze a **real-world data breach** case and evaluate the failure of adherence to data privacy laws.	16	BTL-4	Analyze	CO5
10	Break down the key elements of **Data Governance 2.0** and how it improves upon traditional governance practices.	16	BTL-4	Analyze	CO5

11	Analyze the key components of Data Governance 2.0 and explain how each can contribute to improved transparency and compliance in a government data portal.	16	BTL-4	Analyze	CO5
12	Design a data privacy framework that integrates GDPR, HIPAA, and Indian data protection laws for a multinational healthtech company**.**	16	BTL-6	Create	CO5
13	**Demonstrate** how a unified policy structure can be implemented to manage internal contracts and data sharing in compliance with local laws.	16	BTL-3	Apply	CO5
14	**Illustrate** how a financial services app operating in California and Brazil can meet the data privacy requirements of both CCPA and LGPD.	16	BTL-3	Apply	CO5
15	Justify whether the **Personal Data Protection Bill (India)** sufficiently addresses privacy concerns for citizens and tech companies.	16	BTL-5	Evaluate	CO5
16	Critically assess the role of **Data Protection Officers (DPOs)** under different privacy regulations like GDPR and PIPL.	16	BTL-5	Evaluate	CO5
17	Create a compliance checklist for an Indian startup handling EU, US, and Chinese citizen data.	16	BTL-6	Create	CO5