Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 05/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CDV3416 **Course Name:** DevSecOps in Financial Services

Semester: Seventh Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	46	44

ANSWER KEY

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	A Secure SDLC is a software development lifecycle in which security activities are included in requirements, design, coding, testing, deployment, and maintenance.	2	CO1	BT2
2	Access control ensures that only authorized users or systems can access applications, data, infrastructure, or functions according to defined permissions.	2	CO1	BT2
3	GDPR mainly protects the personal data and privacy rights of individuals.	2	CO1	BT2
4	DAST, or Dynamic Application Security Testing, tests a running application to find vulnerabilities visible during runtime.	2	CO2	BT4
5	Hardcoded secrets can be exposed through source code, repositories, builds, or logs. This may allow unauthorized access to systems and data.	2	CO2	BT4

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Suggested points: Point / Marks Financial applications handle money, transactions, personal data, and sensitive credentials / 2 Identity and access management/least privilege / 1 Multi-factor authentication / 1 Encryption of data at rest and in transit / 1 Secure coding and security testing / 1 Secret management / 1 Logging, monitoring, and incident response / 1 Vulnerability management and patching / 1 Compliance with PCI DSS, GDPR, RBI, or SOX as applicable / 1	10	CO1	BT2
7	Threat / Expected Explanation Phishing / Attackers trick users into revealing credentials or OTPs Malware/ransomware / Malicious software steals, encrypts, or disrupts data and systems Data breach / Unauthorized disclosure of customer or financial information Insider threat / Authorized employees misuse access intentionally or accidentally Account takeover / Attackers use stolen credentials to access customer accounts DDoS attack / Attackers overload services and affect availability API attack / Weak APIs are exploited to access data or perform unauthorized transactions Supply-chain attack / A third-party package, tool, or vendor is compromised	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT

PTO (Please Turn Over)

8	Suggested points: Point / Marks GDPR protects personal data and privacy of individuals — 2 Financial apps process sensitive data such as identity, account, and transaction-related information — 1 Collect only necessary data and use it for a lawful purpose — 1 Obtain valid consent where required and provide transparency — 1 Protect data through access controls and encryption — 1 Support data-subject rights such as access, correction, and deletion where applicable — 1 Report/manage personal-data breaches according to requirements — 1 Maintain records, governance, and accountability — 1 Reduce legal, reputational, and compliance risk — 1	10	CO1	BT2
9	Suggested points: Point / Marks RBI guidelines provide cybersecurity expectations for regulated banking and financial entities — 2 They support protection of digital banking services and customer data — 1 Strong governance and defined security responsibilities — 1 Risk assessment and security controls — 1 Monitoring, logging, and incident detection — 1 Incident response and reporting processes — 1 Secure access management and authentication — 1 Vulnerability management, testing, and patching — 1 Improved resilience, trust, and regulatory compliance — 1	10	CO1	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	NA	10	CO2	BT4
11	Suggested points: Point / Marks Vulnerable code may reach production — 2 Secrets, insecure dependencies, or misconfigurations may remain undetected — 2 Add SAST for source-code security analysis — 1 Add dependency/SCA scanning for open-source libraries — 1 Add secret scanning for credentials and tokens — 1 Add DAST in a test or staging environment — 1 Add container image scanning where containers are used — 1 Define security quality gates that block high-severity findings — 1	10	CO2	BT4

PART E: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
12	NA	10	CO2	BT4
13	Suggested points: Point / Marks Confirm the affected component, version, and application exposure using the SBOM — 2 Assess severity, exploitability, and impact on customer data or transactions — 2 Upgrade, patch, remove, or replace the vulnerable dependency — 2 Rebuild, test, scan, and redeploy the application through the CI/CD pipeline — 1 Monitor logs and investigate possible exploitation — 1 Document the incident and update dependency-management procedures — 1 Use dependency scanning and security gates to reduce recurrence — 1	10	CO2	BT4

ANSWER KEY