LTIMindtree | EduTech | Joint PG Courses

Syllabus for M.Tech (Cyber Security)

Document Version / Details: Ver. 0.3 / 20-06-2024

Course Overview

Digital transformations bring along tremendous benefits, but not without threats to the privacy and security of crucial enterprise data. In present times, cyberattacks are rampant, and new-age cyber threats require dexterous strategies. Therefore, enterprises need to develop cyber defense resilience to counter such incidents.

The global Cyber Security market size was estimated at $222 billion in 2023 and is projected to reach over $500 billion by 2030, with a growth of 12% CAGR annually. With respect to India, the Cyber Security market stands at around $4.5 billion in 2024, with a growth of 18% CAGR annually to reach over $18 billion. This reflects the increased importance and priority given by organizations to secure and protect their digitalization initiatives and implementations, third-party collaborations, unified threat detection and response, OT/IoT management, GenAI, Digital Forensics etc.

The rise in cyberattacks has prompted governments and organizations to focus more on data security, privacy, governance and compliance.

We offer MTech Cybersecurity course which is a specially designed two-year post-graduate program for engineers to leverage the advantages of emerging trends in market and get them skilled to do their job as soon as they complete their Postgraduate in any of the following roles:

1. Security Operations Engineer
2. Network Security Engineer
3. Application Security Engineer
4. Identity & Access Management Specialist
5. Cloud Security Engineer
6. GRC Specialist
7. Data Security Engineer
8. Endpoint Security Engineer

This course covers topics such as Computer System & Network Security (SecOps & SecMon), Application Security & Infrastructure Vulnerability Management, Risk Controls & Compliance, OT & IOT, Data Security, Cloud Security, Identity & Access Management (IAM). Students learn to implement Cyber Security concepts in real-world scenarios through hands-on projects, proof-of-concepts and case studies. Elective topics such as API Security, Digital Forensics, Data Privacy, BCP/DR are also included.

The curriculum and syllabus are designed and developed by LTIMindtree Industry practitioners, chief architects, and experts who have more than 2 decades of experience in this field with rich technical and domain knowledge to help students get industry exposure while learning.
During the 1st year, the students will take these courses within their respective universities and for the 2nd year they will be given an opportunity to work at LTIM locations for internship and hands on projects.

The outcome of this course is to shape a student's career in emerging technologies in Cybersecurity and implementing secure and safe solutions to real world problems/ requirements.

The total program consists of theory, theory + integrated lab, exclusive laboratory, soft skills, internship and projects.

Course Structure

Joint PG Course - MTech (Cyber Security)

Semester I						
Subject	**Hours**	**Type**	**L**	**T**	**P**	**Credits**
Network Security	60	C	4	0	0	4
Cyber Threat Management	45	C	3	0	0	3
Application & Infrastructure Vulnerability Management	75	C	3	0	2	4
Professional Elective – I	45	E	3	0	0	3
Professional Skills – I	30	A	0	0	2	1
Professional Elective – II	30	E	2	0	0	2
Network Security Lab	60	P	0	0	4	2
Data Security Lab	60	P	0	0	4	2
Total	405					21
Professional Elective – I: Data Privacy / Digital Forensics						
Professional Elective – II: Data Security (Mandate) / CS60306						

Semester II						
Subject	**Hours**	**Type**	**L**	**T**	**P**	**Credits**
Risk, Controls and Compliance	45	C	3	0	0	3
Identity and Access Management	75	C	3	0	2	4
Cloud Security	45	C	3	0	0	3
Professional Elective – III	30	E	2	0	0	2
Professional Soft Skills – II	30	A	0	0	2	1
Professional Elective – IV	45	E	3	0	0	3
Security & Compliance Lab	60	P	0	0	4	2
Operational Technology (OT) and IoT Lab	60	P	0	0	4	2
Total	390					20
Professional Elective – III: BCP / API Security Testing						
Professional Elective – IV: Operational Technology (OT) & IoT (Mandate) / CS60304						

Semester III					
Subject	**Type**	**L**	**T**	**P (Hours)**	**Credits**
Professional Elective – III: Certification	C	3	0	0	3
Project – I	P	-	-	-	16
Total					19

Semester IV					
Subject	**Type**	**L**	**T**	**P**	**Credits**
Project – II	P	-	-	-	20
Total					20

C-Core, E-Elective, A-Audit, O-Open elective, P-Practical, L-Lecture, T-Tutorial

Semester – I

Title	Network Security	Code	
Prerequisite	Basic understanding of networks and IT concepts.	Credits | Total Hours	4-0-0 [4] | 60

Course Objective:

1. To understand and apply fundamental network security principles.
2. To grasp and implement basic cryptographic techniques.
3. To implement and manage network security tools effectively.
4. To administer and secure system endpoints and services.
5. To design and deploy SASE architecture and services.

Course Outcome:

CO1: Evaluate and mitigate network threats and vulnerabilities.
CO2: Analyze and apply cryptographic methods for data protection and authentication techniques.
CO3: Secure and manage network access and communications.
CO4: Configure and maintain robust endpoint and server security.
CO5: Implement and manage SASE for enhanced network security.

Unit 1: Security Principles and Standards 12

Networking Concepts: Network Models, Network Protocols, Network Types, IP Addressing. Security Fundamentals: Threats and Vulnerabilities, CIA Triad, Defense in Depth, Types of Malware, Least Privilege, Security Models. Attacks in OSI and TCP/IP Models: Physical Layer Attacks, Data Link Layer Attacks, Network Layer Attacks, Transport Layer Attacks, Session Layer Attacks, Presentation Layer Attacks, Application Layer Attacks. Vulnerable Protocols: FTP, NTP, ICMP, DNS, HTTP, SMTP. Zero Trust Concepts: Zero Trust Architecture, Principles, Use Cases, Benefits. Cloud Networking and Security: Cloud Networking Fundamentals, Cloud Security Fundamentals, Cloud Security Services, Network Security Management in the Cloud.

Unit 2: Cryptography 12

Introduction to Cryptography: Definition and Importance, Basic Concepts, Cryptographic Goals. Symmetric Encryption: Introduction, Block Ciphers, Stream ciphers, Key Management. Public Key Encryption: Introduction, RSA Algorithm, Elliptic Curve Cryptography, Key Exchange Algorithms. Hash Functions and Message Integrity: Introduction, Common Hash Algorithms: MD5, SHA, Message Authentication Codes, Digital Signatures. Cryptographic Implementations: Cryptography in Secure Communications and Data Protection, Common Attacks and Countermeasures, Post-Quantum Cryptography, Blockchain and Cryptographic Innovations.

Unit 3: Network Security Applications 12

Access Management: Authentication, Access Management, Auditing, Key Vendors and Solutions. Network Management Security: Introduction, Network Access Control, Security Controls and Best Practices. Firewall Management: Understanding Firewalls, Types of Firewalls, Firewall Controls, Configuring Firewall Rules. Intrusion Detection and Prevention Systems, Key Vendors and Solutions. Email Security: Social Engineering, Common Email Threats, Email Security Protocols, Examples of Key Vendors. Web Security: Web Threats, Web Security Gateways and Proxies, Examples of Key Vendors, Security Controls. IP Security: Introduction, Configuring and Managing VPNs, IPsec Policies and Tunnels, Key Vendors and Solutions. Application Security: Common Application Vulnerabilities, OWASP, Secure SDLC, Application Security Controls, Key Vendors and Solutions.

Unit 4: System Security 12

Patching and Vulnerability Management: Introduction, Impact of Unpatched Systems on Security, Server and Endpoint Patch Management, Vulnerability Tracking and Reporting. Endpoint Security: Endpoint Protection Platforms, Endpoint Detection and Response, Examples of Key Vendors. Proxy Management: Proxy Servers, Types of Proxy Servers, Proxy Server Configuration, Proxy Vendors and Solutions. Linux: Introduction, Distributions and FAQs, Setting up the Laboratory for Linux, Shells, Linux Signs, Linux Desktop Environments, Linux GUI, Basic Commands. Linux File Systems: Linux File Hierarchy, File Permissions. Network Settings: Display Network, Leasing New IP from DHCP Server. Services, User Management in Linux, Process Management, Package Management, System Monitoring.

Unit 5: Secure Access Service Edge 12

Introduction to SASE: Definition of SASE, History and evolution of SASE, Benefits of SASE, Use cases for SASE. SASE Components & Architecture: SASE Architecture and Components, SASE Edge Services, SASE Security Services, SASE Management Services, SASE Use Cases, ZTNA, Remote Access, Secure Web Gateway, Firewall as a Service, Cloud Access Security Broker, DLP, Sandboxing, ATP, SD-WAN. SASE Design and Deployment: SASE Design Best Practices, SASE Deployment Options and Considerations, SASE Integration with Existing Network and Security Infrastructure. SASE Operations and Management: SASE Service Monitoring and Troubleshooting, SASE Service Level Agreements, SASE Policies and Configuration Management, Emerging SASE Technologies and Services, Future of SASE in Networking and Security.

Reference Books:

1. William Stallings, Network Security Essentials: Applications and Standards 6th Edition– By Pearson Education (2018)
2. Omar Santos, John Stuppi, Cisco CCNA Security book 1st Edition – By Cisco Press (2015)

Reference Links:

1. Linux for Beginners: Linux for Beginners: Linux Basics
2. Networking Fundamentals: https://app.pluralsight.com/paths/skill/networking-fundamentals
3. Network Security Basics: https://app.pluralsight.com/library/courses/network-security-basics-cert/table-of-contents

Title	Cyber Threat Management	**Code**	
Prerequisite	Computer and Network Security, Linux OS	**Credits |Total Hours**	3-0-0 [3] | 45

Course Objective:

1. Understand and utilize SOC tools and processes.
2. Analyze network traffic for security threats.
3. Defend endpoints and analyze security logs.
4. Triage security alerts and investigate incidents.
5. Enhance SOC operations through automation.

Course Outcome:

CO1: Implement and manage SOC functions effectively.
CO2: Analyze network traffic for security threats.
CO3: Identify and respond to endpoint threats.
CO4: Prioritize and analyze security alerts efficiently.
CO5: Improve threat detection and SOC processes.

Unit 1: Security Operations Teams and Tools 9

SOC Foundations: SOC Organization and Functions, SOC Data Collection, Incident Management. An Introduction to SIEM: SIEM/Splunk Architecture, Alert Generation and Processing, Building SIEM Queries, SIEM Visualizations and Dashboards. Threat Intelligence Platforms: Understanding and examples of Platforms available like Splunk. SOAR: Understanding and Examples of Platforms available like Cortex XSOAR- IBM Qradar SOAR.

Unit 2: Network Traffic Analysis 9

Network Architecture and Traffic: Network Architecture Foundations, Role of Understanding the Architecture from Threat Management Standpoint, Traffic Capture and Analysis, Basics of Identifying Breach and Attacks from Network Traffic Analysis. TCP/IP: TCP/IP Architecture and Security Features in The Default Protocol Stack. Understanding DNS: DNS Protocol and Functional Architecture, DNS Traffic Analysis and DNS attacks. Understanding HTTP: HTTP(S) protocol and functional architecture, HTTP(S) traffic analysis and attacks, Working of HTTP/2 and HTTP/3, Analyzing Encrypted Traffic for Suspicious Activity. Management protocols: SSH, ICMP, RDP, SNMP Architecture, Traffic Analysis and Attacks

Unit 3: Endpoint Defense, Security Logging, and Malware 9

Common Endpoint Attack Tactics: Antivirus Evasion, Registry Modification, RDP Exploit etc. Endpoint Defense in Depth: Architecture, Controls Relating to Antivirus, EDR etc., Best Practices. Logging: Working of Windows & Linux Logging, Interpreting Security, Critical Log Events, Other Logging. Making Logs Usable: Log Collection, Parsing, And Normalization. Identifying Potentially Malicious Files, Dissecting Commonly Weaponized File Type, Fast Identification and Safe Handling of Malicious Files.

Unit 4: Efficient Alert Triage and case Studies 9

Alert triage and analysis theory: Collecting Alerts, Categorizing Alerts, Prioritizing Alerts, Analyzing Alerts, Response. Incident Documentation, Closing and Investigation Quality. Triaging A Malware Incident: Detecting Malware Penetration Activity, Segregating Genuine Activity and Real Malware Infection. Triaging an Email Incident: Detecting Malicious Emails Through Email Header Analysis (SPF - DKIM - DMARC and more), Email Content, URL and Attachment Analysis. Further steps beyond triage

Unit 5: Continuous Improvement, Analytics, and Automation 9

Setting up a Resilient Threat Detection Operation: Process, People and Technology Foundations. Threat Detection Enterprise Coverage Foundations: Coverage Mapping, Tracking & Improvement. False Positive Reduction: Analytic Features and the Importance of Log Enrichment, Noise Reduction using AI. Alert Tuning Methodology: SOC Automation and Orchestration (with and without SOAR), Automation Short Case Study - Improving Analyst Efficiency and Workflow. Mandatory Operational Processes: RACI Matrix, Communications Management, Feedback Management, Root Cause Analysis. Skill and Career Development for SOC: Trainings and Certifications. SOC Team Load and Burnout Reduction: Role of Efficient Processes, Communication, Organization Wide Top-Down Strategy, AI and Automation.

Reading Materials:

1. Mike O'Leary, Cyber Operations: Building, Defending, and Attacking Modern Computer Networks 1st Edition - By Springer Nature (2016)
2. Arun E Thomas, Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence - By Arun E Thomas (2018)

3. Ashish M Kothekar, Building a Next-Gen SOC with IBM QRadar: Accelerate your security operations and detect cyber threats effectively 1st Edition - By Packt Publishing (2023)
4. Constance S. Uthoff, Cyber Intelligence - By Lynne Rienner Publishers Inc (2021)
5. Izzat Alsmadi, Chuck Easttom, Lo'ai Tawalbeh, The NICE Cyber Security Framework 1st Edition - By Springer (2020)
6. Alexander Kott (Editor), Cliff Wang (Editor), Robert F. Erbacher (Editor), Cyber Defense and Situational Awareness: (Advances in Information Security) 1st Edition – By Springer International Publishing AG (2016)
7. Daniel Moore, Offensive Cyber Operations: Understanding Intangible Warfare - By Oxford Univ Press (2022)

Reference Links:

1. Security Operations Analyst Associate - SC-200: Shoshin School (ltimindtree.com)
2. IBM -Security Orchestration and Response (SOAR) : Course: QRadar SOAR for Technical Sales Level 3 (ibm.com)
3. QRadar Security Information and Event Management (SIEM) : https://learn.ibm.com/course/view.php?id=11834
4. Microsoft Defender: Implementing and Managing Microsoft Defender XDR Path | Pluralsight

Title	Application & Infrastructure Vulnerability Management	**Code**	
Prerequisite	Basic knowledge in cyber security concepts	**Credits | Total Hours**	3-0-2 [4] | 75

Course Objective:

1. Understand and manage infrastructure and application vulnerabilities.
2. Implement and optimize application security testing methodologies.
3. Employ advanced security testing and governance practices.
4. Conduct thorough infrastructure vulnerability assessments.
5. Develop and enforce comprehensive vulnerability management policies.

Course Outcome:

CO1: Conduct comprehensive security testing and vulnerability management.
CO2: Identify and remediate application vulnerabilities effectively.
CO3: Integrate security into SDLC and manage application security.
CO4: Prioritize and mitigate infrastructure security risks.
CO5: Develop and enforce comprehensive vulnerability management policies.

Unit 1: Introduction to Security Testing 10

Introduction to security testing: CIA Triad, Hacking Categories, Type of Vulnerabilities. Infrastructure Vulnerability Management: Types of Infrastructure Vulnerability Testing, Tools and Technologies, Attack Landscape, CVE, CWE. Application vulnerability management: Types of Application Testing, Application Testing Across SDLC, Common Application Vulnerabilities and Best Practices, Security Standards and Frameworks

Unit 2: Application Security Testing 6

Introduction to Threat Modeling: Methodology and Best Practices, Tools and Technologies. Introduction to Static Application Security Testing (SAST), Methodology and Best Practices, Tools and Technologies, False Positive Elimination, Reporting. Introduction to Software Composition Analysis (SCA) & SBOM: Methodology and Best Practices, Tools and Technologies, False Positive Elimination, Reporting. Introduction to Dynamic Application Security

Testing (DAST) & Application Programming Interface (API): Methodology and Best Practices, Tools and Technologies, False positive elimination, Reporting.

Unit 3: Advanced Application Security & Governance 6

Interactive Application Security Testing (IAST) and Runtime Application Self-Protection (RASP): Introduction, Tools and Techniques, Implementation. Application Penetration Testing: Testing Methodology, Significance in SDLC - Best Practices - Tools and Technologies, Manual Techniques. DevSecOps Implementation. Best Practices Implementation (OWASP, SAN, NIST). Automation & Program Governance: Ticketing and Tracking automation, Report Presentation, Stakeholder communication

Unit 4: Infrastructure Security Testing 12

Introduction to Infrastructure Vulnerability Management: Key Concepts and Objectives, Tool Architecture: Different tools, Setup and Configuration, Implementation. Prioritization: Vulnerabilities Prioritization factors, Risk scoring, Manual Analysis techniques. Automation & Program Governance – Ticketing and Tracking Automation - Report Presentation - Stakeholder Communication

Unit 5: Vulnerability Management 11

Application Landscape: Understanding Application Technology landscape (COTS, Thick client, custom etc.), Risk Based Classification of Application based on business requirements. Infrastructure Landscape: Understanding Infrastructure Technology landscape (Servers, End Points, Network Devices), Defining and Implementing Vulnerability Management Policies and Process, Tool Identification and Recommendation, Industry best practices adoption - Compliance mandates and process implementation.

Practical 30

1. Installing Fortify SSC on the testing environment. Activate the license for SSC - WebInspect, Fortify-SAST and SCA-Sonatype Nexus IQ.
2. Configuring the applications for DAST, SAST and SCA scans by providing URL with credentials, source code path and open-source library files.
3. Perform a test scan on the application to validate the configurations.
4. Create or setup schedule or on-demand scans to perform application security assessment.
5. Analyze identified vulnerabilities. Manual analysis and false positive validation.
6. Create reporting templates, schedule them to generate reports after every scan, get on-demand assessment reports and generate remediation reports
7. Installing Qualys VMDR agents on target assets. Get sensors from portal, activate the agent, and verify it has installed.
8. Install Qualys VMDR scanner on localhost, activate it with license and verify it is reachable to all target systems
9. Create asset groups based on use cases & impact. Provide IP details, DNS, NetBIOS, Domains, Scanner Appliance
10. Create or setup schedule or on-demand scans to perform vulnerability assessment. Create scan profiles, setup target host, select scanner appliance
11. Analyze identified vulnerabilities. Validate manually ransomware vulnerabilities, public exploit vulnerabilities, active attacks, etc.
12. Create reporting templates, schedule them to generate reports after every scan, get on-demand assessment reports and generate remediation reports

13. Download and install Metasploit Framework (MSF) Community edition, configure & connect Postgres database to MSF, create various MSF environments.
14. Download & install Metasploitable2 on localhost, login and check for network connectivity, check MSF is reachable to this host
15. Perform auxiliary scanning via MSF to identify open ports, service, versions, DNS details, etc. and maintain the record of all the results
16. Perform Remote Code Execution attacks via MSF to take control over the system. Setup exploits, payloads, host details, etc.
17. Perform client-side attacks via MSF. Create evasive payloads via MSFVenom, deploy the payloads to target host, execute to gain access
18. Perform post-exploitation activities via MSF. Dump hashes, take screenshot, exfiltrate data, deploy backdoors, etc.
19. Create custom reports that includes, vulnerability details, affected service, severity score, impact score, POC (Screenshots), remediation details.

Reading Materials:

1. Park Foreman, Vulnerability Management 2nd edition – By Taylor & Francis Ltd (2022)
2. Andrew Magnusson, Practical vulnerability management: A strategic approach to managing cyber risk - By No Starch Press (6 October 2020)
3. Simon Parkinson, Andrew Crampton, Richard Hill, Guide to vulnerability analysis for computer networks and systems 1st edition - By Springer Nature Switzerland AG (2018)
4. Tanya Janca, Alice and bob learn application security 1st edition - By Wiley (2020)
5. Mark Dowd, John McDonald, Justin Schuh, the art of software security assessment - identifying and preventing software vulnerabilities 1st edition - By Addison-Wesley Professional (2006)
6. Richa Gupta, Hands-on penetration testing for web applications: run web security testing on modern applications using nmap - burp suite and wireshark 1st edition - By BPB Publications (2021)
7. Andrew Hoffman, Web application security: exploitation and countermeasures for modern web applications 2nd edition - By Shroff/O'Reilly (2024)

Reference Links:

1. Fundamentals of DevSecOps: PluralSight Pathway: https://app.pluralsight.com/paths/skill/fundamentals-of-devsecops
2. Microsoft Azure Solutions Architect: Implement an Application Security Strategy https://app.pluralsight.com/library/courses/microsoft-azure-solutions-architect-implement-application-security-strategy/table-of-contents
3. Red Team Operations: Target and Capability Development https://app.pluralsight.com/library/courses/red-team-operations-target-capability-development/table-of-contents
4. Red Team Tools for Emulated Adversary Techniques with MITRE ATT&CK https://app.pluralsight.com/library/courses/red-team-tools-adversary-techniques-mitre-attack/table-of-contents
5. Conducting Network Vulnerability Analysis https://app.pluralsight.com/library/courses/network-vulnerability-analysis-conducting/table-of-contents
6. Discover Network Weaknesses with Nessus https://app.pluralsight.com/library/courses/discover-network-weaknesses-nessus/table-of-contents
7. Vulnerability Analysis with Nessus https://app.pluralsight.com/library/courses/nessus-vulnerability-analysis/table-of-contents
8. DevSecOps: The Big Picture https://app.pluralsight.com/library/courses/devsecops-big-picture-2023/table-of-contents

9. Web Security Testing with Burp Suite https://app.pluralsight.com/paths/skill/web-security-testing-with-burp-suite

Title	Data Privacy	Code	
Prerequisite		Credits |Total Hours	3-0-0 [3] | 45

Course Objective:

1. Understand core principles of privacy and data protection.
2. Comprehend and comply with major data protection regulations.
3. Apply privacy principles in data processing systems design.
4. Utilize technologies to enhance privacy in data processing.
5. Address privacy challenges in emerging technologies.

Course Outcome:

CO1: Evaluate and apply privacy laws and ethical data processing.
CO2: Implement GDPR and DPDP Act requirements effectively.
CO3: Integrate data protection measures and mitigate privacy risks.
CO4: Implement PETs like anonymization, differential privacy, and cryptographic techniques.
CO5: Analyze and propose solutions for privacy in big data, AI, IoT, and cloud computing.

Unit 1: Fundamentals of Privacy and Data Protection 9

Evaluation of Privacy Laws: Principles Such as Data Minimization, Purpose Limitation, Data Subject Rights. Responsibilities and Roles of different Stakeholders in Data Processing: Analysis of Major Privacy Breaches, Ethical Implications of Data Processing.

Unit 2: Regulatory frameworks 9

Overview of GDPR: Provisions, Principles, GDPR Compliance Requirements, India's Data Protection Bill (DPDP Act) and its Implications, Data Subject Rights under GDPR and DPDP Act, Right to Access, Rectification, Erasure, Data Portability, Cross-Border Data Transfers, Rules and Mechanisms for Transferring Personal, Enforcement Mechanisms, Penalties and Compliance Strategies.

Unit 3: Data Protection Practices and Techniques 9

Data Protection by Design and by Default: Privacy Principles into the Design and Operation of Data Processing Systems, Risk Management and Data Protection Impact Assessments (DPIAs), Identify and Mitigate Privacy Risks, Data Security Measures: Encryption, Access Controls, Incident Response, Privacy Policies and Notices, Vendor Management and Third-Party Risk, Managing Privacy Risks

Unit 4: Privacy-Enhancing Technologies (PETs) 9

Introduction to PETs: Technologies designed to protect and enhance privacy in data processing, Anonymization and Pseudonymization, Differential Privacy, Cryptographic Techniques, Homomorphic Encryption and Secure Multi-Party Computation, Emerging PETs, Potential Applications in Various Domains.

Unit 5: Advanced Topics in Data Privacy 9

Privacy in the Age of Big Data and AI, Examining the Challenges and Solutions, Internet of Things (IoT) and Privacy, Privacy implications of IoT devices, Privacy in Cloud Computing, Intersection of Data Privacy and Cybersecurity, Future Trends and Challenges in Data Privacy.

Reading Materials:

1. General Data Protection Regulation (GDPR) - Official GDPR Text - https://eurlex.europa.eu/eli/reg/2016/679/oj
   EU GDPR Information Portal - https://www.eugdpr.org
   GDPR Key Changes - https://gdpr.eu/what-is-gdpr/
2. India's Data Protection Bill (DPDP Act) Draft Data Protection Bill (2019) - https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill -2019.pdf
3. Privacy Principles and Data Protection OECD Privacy Guidelines - http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
4. Data Privacy Resources International Association of Privacy Professionals (IAPP) Resource Center - https://iapp.org/resources/
   NIST Privacy Framework - https://www.nist.gov/privacy-framework
5. Certified Data Protection Officer (CDPO)
   CDPO Exam Preparation Resources - https://ec-council.org/programs/certified-data-protection-officer-cdpo/#become-a-cdpo

Reference Links:

1. Coursera and Udemy Courses on Data Privacy
   Coursera Data Privacy Courses - https://www.coursera.org/courses?query=data%20privacy
   Udemy Data Privacy Courses - https://www.udemy.com/topic/data-privacy/
2. Certified Data Protection Officer (CDPO)
   CDPO Certification - https://ec-council.org/programs/certified-data-protection-officer-cdpo/

Title	Digital Forensics	**Code**	
Prerequisite	Basic understanding of networks, IT, security operations, Computer Hardware, Data Storage concepts	**Credits |Total Hours**	3-0-0 [3] | 45

Course Objective:

1. Understand fundamentals of digital forensics and evidence handling.
2. Explore specialized forensics and new trends in the field.
3. Learn methodologies for creating forensic images.
4. Master key forensic software and data acquisition techniques.
5. Develop skills in forensic reporting and legal considerations.

Course Outcome:

CO1: Conduct digital forensic investigations ethically and effectively.
CO2: Explore specialized forensics and new trends in the field.
CO3: Create and verify forensic images ensuring data integrity.
CO4: Utilize forensic tools for comprehensive data analysis and acquisition.
CO5: Present digital evidence and maintain legal compliance in forensic processes.

Unit 1: Introduction to Digital Forensics 9

Introduction to Digital Forensics: History, Types of Digital Evidence, Various Digital Evidence Types such as Computer Files, Emails, mobile data. The Digital Forensics Process: Steps from Evidence Identification and Collection to Analysis and Reporting. Legal and Ethical Considerations: Legal Frameworks, Chain of Custody, eDiscovery & Ethical

Responsibilities. Digital Forensics Techniques: Extracting and Analyzing Data from Regular Digital Media. Network Forensics: Techniques for Analyzing Network Traffic and Identifying Security Incidents.

Unit 2: Specialized Digital Forensics and Emerging Trends 9

Mobile Device Forensics: Methods for Extracting and Analyzing Data from Mobile Devices. Cloud Forensics: Challenges of Acquiring Evidence from Cloud Environments, Techniques for Cloud Forensics. Incident Response and Forensics: Relation between Forensic Investigations and Incident Response, Integrating Forensics into Incident Response Plans. Data Recovery Techniques: Recovering Lost or Corrupted Data from Digital Storage Media, Tools for Data Recovery. Case Studies in Digital Forensics: Analysis of Real-World Forensic Cases, Techniques. Future Trends in Digital Forensics: Emerging Technologies and their Impact on Forensics.

Unit 3: Introduction to Forensic Imaging 10

Forensic Imaging: Importance and Methodologies using Opensource Tools, Imaging Storage Media with Opensource Tools. Types of Forensic Images: RAW, AFF Formats, Techniques for Verifying Forensic Images with Opensource Tools, Detailed usage of Popular Opensource Imaging Tools, Ensuring Data Integrity using Hash Values with Opensource Tools, Compressed and Encrypted Imaging, Imaging Live Systems, Imaging Network Drives, Handling Large Data Sets.

Unit 4: Forensics Software Tools & Techniques 11

Overview of Forensic Software: Introduction to Key Open Source and Commercial Forensic Software Tools. Forensic hardware tools: High Level Understanding, Features, and Benefits. Data Acquisition Techniques: Logical Acquisition, Physical Acquisition, Remote Acquisition, Memory Acquisition, Network Data Acquisition, Mobile Device Acquisition Theory, FTK and Encase: Tool Theory Lessons. Kali Linux: Overview of the other Forensics Tools Present in the Distribution and Practical, Autopsy & Sleuth Kit: Tool theory and Practical, Volatility Framework: Memory Forensics and Analysis, Wireshark: Network Protocol Analysis and Its Role in Forensics, Other tools in the Kali Distribution.

Unit 5: Reporting, eDiscovery, and Legal Aspects 6

Introduction to Forensic Reporting, Report Writing Techniques, Chain of Custody: Ensuring Data Integrity and Legal Admissibility. Handling Evidence: Legal Considerations for Handling and Presenting Digital Evidence. Techniques for Effectively Presenting Digital Evidence, Introduction to eDiscovery.

Reading Materials:

1. Eoghan Casey BS MA, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet 3rd edition – By Academic Press (2011)
2. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations 6th edition – By Cengage India Private Limited (2019)
3. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics 2nd edition – By Syngress (2014)
4. Easttom C, Computer Forensics: Investigating Data and Image Files 1st edition – By Cengage Learning (2009)
5. Jason T. Luttgens, Matthew Pepe and Kevin Mandia, Incident Response & Computer Forensics 3rd edition – By McGraw Hill (2014).
6. Chuck Easttom, Digital Forensics, Investigation and Response – By Jones & Bartlett Learning (2021)

7. Keith Jones, Richard Bejtlich and Curtis Rose, Real Digital Forensics: Computer Security and Incident Response 1st edition – By Addison-Wesley Professional (2005)
8. Oleg Skulkin, Donnie Tindall and Rohit Tamma, Learning Android Forensics: Analyze Android Devices with the Latest Forensic Tools and Techniques – By (2018)

Reference Links:

1. Incident Response: Detection and Analysis : https://app.pluralsight.com/library/courses/incident-response-detection-analysis/table-of-contents
2. Incident Response: Network Analysis : https://app.pluralsight.com/library/courses/incident-response-network-analysis/table-of-contents
3. Incident Response: Host Analysis : https://app.pluralsight.com/library/courses/incident-response-host-analysis/table-of-contents
4. Incident Response: Containment, Eradication and Recovery : https://app.pluralsight.com/library/courses/incident-response-containment-eradication-recovery/table-of-contents
5. Enumerating the Network Infrastructure as a Forensics Analyst : https://app.pluralsight.com/library/courses/enumerating-network-infrastructure-forensics-analyst/table-of-contents
6. Advanced Cyber Defense Analysis with Wireshark : https://app.pluralsight.com/library/courses/wireshark-advanced-cyber-defense-analysis/table-of-contents
7. Specialized DFIR: Windows Registry Forensics : https://app.pluralsight.com/library/courses/specialized-difr-windows-registry-forensics/table-of-contents
8. Specialized DFIR: Windows File System and Browser Forensics : https://app.pluralsight.com/library/courses/windows-file-sys-brows-forensic-special-dfir/table-of-contents
9. Specialized DFIR: Windows Event Log Forensics : https://app.pluralsight.com/library/courses/dfir-win-event-log-forensics/table-of-contents

Title	Data Security	**Code**	
Prerequisite	Computer and Network Security	**Credits |Total Hours**	2-0-0 [2] | 30

Course Objective:

1. Understand core principles and frameworks of data security.
2. Learn data discovery and classification techniques.
3. Master techniques for data masking and tokenization.
4. Understand cryptographic principles and algorithms.
5. Learn strategies to prevent data loss.

Course Outcome:

CO1: Apply security models and manage data risks effectively.
CO2: Implement data classification to enhance data protection.
CO3: Apply data masking and tokenization to secure sensitive information.
CO4: Utilize cryptographic techniques to protect data integrity and confidentiality.
CO5: Implement DLP policies and safeguard data across various platforms.

Unit 1: Fundamentals of Data Security 5

Principles of Information Security: Overview, Importance of Data for Clients and Customers, Key Concepts: Confidentiality, Integrity, Availability, Real-World Examples of Data Breaches and Their Impact, Security Models and Architectures: NIST Framework, ISO 27001 framework. Threats, Vulnerabilities, and Risk Management: Overview, Understanding and Examples of Recent Occurrences.

Unit 2: Data Discovery and Data Classification 5

Definition of Data Discovery: Data insight, trends, patterns etc. Understanding of Sensitive Information Types: PII, HIPPA, PCI. Definition of Data Classification: analyzing structured and unstructured data, Importance of Data Discovery and Classification. Categories of Data Classification: Internal, Confidential, Restricted, Public. Common Data Classification Standards and Requirements, Data Classification integrate with Data Protection.

Unit 3: Data Masking and Tokenization 7

Definition of Data Masking, Types of Data Masking: Static and Dynamic. Data Masking Techniques: Randomization, Shuffling, Hashing etc. Definition of Tokenization, Tokenization techniques: Word Tokenization, Character Tokenization etc. Vault and Vaultless Tokenization: Data Masking and Tokenization Best Practices.

Unit 4: Cryptography 7

Definition of Cryptography and its history, Types of Cryptography: Symmetric and Asymmetric Algorithms. Different Cryptography Algorithms and Their Uses: Common Cryptographic Algorithms, Applications of Cryptographic Algorithms, Hashing: Common Hashing Algorithms, Uses of Hashing in Security. Digital Signatures, Email Encryption.

Unit 5: Data Loss Prevention (DLP) 6

Definition of DLP, Types of DLP: Network DLP, Endpoint DLP, Cloud DLP, Comparison, Reasons for Data Loss: Common Causes, Case Studies Understanding the Impact of Data Loss. Prevention of Data Loss: Best Practices, DLP Policies and Procedures. Protecting from Endpoint Device Data Loss, Protecting from Email Based Data Loss, Safeguarding from Cloud and Web-Based Data Loss.

Reading Materials:

1. Kris Hermans, Mastering DLP: A Comprehensive Guide to Data Loss Prevention - Independently published (2023)
2. Gerardus Blokdyk, Data Loss Prevention A Complete Guide – By 5STARCooks (2020)
3. Colin Tankard, Data classification, The foundation of information security – Research Report
4. Carlisle Adams and Steve Lloyd, Understanding Public Key Infrastructure: Concepts, Standards and Deployment Considerations 2nd edition - By Addison-Wesley (2011)
5. Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C standard edition- By John Wiley (2015)

Reference Links:

1. Microsoft DLP-
   http://docs.microsoft.com/en-us/learn/paths/implement-information-protection
   http://docs.microsoft.com/en-us/learn/paths/implement-data-loss-prevention
   http://docs.microsoft.com/en-us/learn/paths/implement-information-governance
2. Microsoft Certified Information Protection Administrator Associate - SC-400 : Shoshin School (ltimindtree.com)
3. Hashicorp Vault: https://developer.hashicorp.com/vault/tutorials
4. Venafi: 22.1 Self-study VSA (venafi.com)

Title	Network Security Lab	Code	
Prerequisite	Basic understanding of networks and IT concepts.	Credits |Total Hours	0-0-4 [2] | 60

Network Security		
Experiment 1	Setup VMware Workstation. Create virtual network.	Group
Experiment 2	Install and Configure Windows and Linux virtual machines.	Group
Experiment 3	Setup and configure pfSense as a network firewall.	Group
Experiment 4	Implement VLANs and Inter-VLAN routing with pfSense.	Group
Experiment 5	Deploy OpenVPN for secure remote access.	Group
Experiment 6	Install and configure Snort for intrusion detection.	Group
Experiment 7	Implement Network Segmentation with iptables and Windows firewall.	Group
Experiment 8	Set Up and Use Wireshark for Network Traffic Analysis at various locations of the simulated network	Group
Experiment 9	Try performing different type of network connectivity tests across the network using different protocols like SSH, Telnet, RDP, PING, TRACEROUTE etc.	Group
Cyber Threat Management		
Experiment 10	Install and Configure Splunk Free Version: - Download and install Splunk Free version on a Linux or Windows VM. - Complete the initial setup and configure Splunk to start at boot. - Verify the installation by accessing the Splunk web interface.	Individual
Experiment 11	Ingest Data Sources into Splunk: Configure data inputs in Splunk to ingest various log sources (e.g., syslog, application logs, network device logs). Use sample log files to simulate different data sources. Verify data ingestion by checking the Splunk web interface for incoming data.	Individual
Experiment 12	Create and Use Splunk Dashboards for Monitoring: Create dashboards in Splunk to visualize log data. Design dashboards to display key metrics such as login attempts, network traffic, and error logs (Whatever matrices possible using the log files data).	Individual
Experiment 13	Set Up and Configure Splunk Alerts: Define alert conditions in Splunk based on specific log events (e.g., failed login attempts, network anomalies). Configure alert actions such as email notifications or scripts.	Individual
Experiment 14	Implement Splunk Searches for Threat Detection: Create custom search queries in Splunk to detect potential security threats. Save these searches as reports for regular review. Analyse search results to identify and investigate suspicious activities.	Individual
Experiment 15	Use Splunk to Correlate Security Events: Configure Splunk to correlate events from different data sources. Create correlation searches to identify complex attack patterns. Document findings and correlations to understand the context of security incidents	Individual
Experiment 16	Configure a vulnerable virtual machine in the virtual network: Download a vulnerable virtual machine .iso from the internet. Example - Dam Vulnerable Web Application or one from www.vulnhub.com. Select anything of your choice. There are ample options available to download on the internet. Run this vulnerable VM as an additional guest OS.	Individual
Experiment 17	Install Splunk Universal forwarder on this machine and configure it to send the log data to the Splunk VM.	Individual
Experiment 18	Configure a vulnerability scanner on a VM: - On another virtual machine, install trial version of Nessus or any other vulnerability scanner of your choice.	Individual

	- Install Splunk Universal forwarder on this machine and configure it to send the log data to the Splunk VM.	
Experiment 19	Check Splunk threat identification capabilities: Launch vulnerability scans from the scanner towards the the vulnerable virtual machine. Check Splunk alerts and dashboards.	Individual

Title	Data Security Lab	**Code**	
Prerequisite	Basic understanding of networks, IT, security operations, Computer Hardware, Data Storage concepts	**Credits |Total Hours**	0-0-4 [2] | 60
Digital Forensics			
Experiment 1	Setup and Preparation of the Environment: Install a forensic analysis platform (eg: Kali Linux) on a VM. Get yourself accustomed to the tools like: Autopsy, Sleuth Kit, Volatility, Wireshark, etc. These tools come as part of the Kali Linux distribution. (You can use any other Forensics Distribution of your choice)		Group
Experiment 2	Acquiring Disk Images: Use dd or dcfldd to create a bit-by-bit copy of the drive that you want to image. Verify the integrity of the image using hash functions (MD5, SHA1). You can use a tool like HashMyFiles Document the entire process, steps taken, tools used, commands executed etc. (You can try widely used - FTK Imager as well)		Group
Experiment 3	File System Analysis with Autopsy and Sleuth Kit: Load the disk image into Autopsy. Perform file system analysis to recover deleted files, extract metadata, and identify hidden files. Use Sleuth Kit command-line tools for deeper analysis. (Optional Step)		Group
Experiment 4	Memory Forensics with Volatility: Acquire a memory dump from a suspect machine (use tools like dumpit). Analyze the memory dump using Volatility to extract processes, network connections, and registry hives.		Group
Experiment 5	Performing Real Forensics using sample images: - Download an image from the internet that has artifacts available on it. You can try websites like https://digitalcorpora.org or https://cfreds.nist.gov/		Group
Data Security			
Experiment 1	Install the Active Directory Forest There is one domain controller that is also running Active Directory-integrated Domain Name Service (DNS). This computer will also provide the Lightweight Directory Access Protocol (LDAP) location for the CDP and the AIA point for the PKI configuration.		Individual
Experiment 2	Prepare the webserver for CDP and AIA publication		Individual
Experiment 3	Install the standalone offline root CA Perform post-installation configuration steps on the standalone offline root CA		Individual
Experiment 4	Install Subordinate Issuing CA Perform the post-installation configuration on the subordinate issuing CA		Individual
Experiment 5	Install and configure the online responder Verify the PKI hierarchy health		Individual

Experiment 6	Issuing Certificates * Submit CSR: Create and submit a Certificate Signing Request (CSR) to the CA. * Issue Certificates: The CA signs the CSR and issues a digital certificate. * Distribute Certificates: Distribute the issued certificate to the requesting entity	Individual
Experiment 7	Managing Certificates * Certificate Renewal: Renew certificates before they expire. * Revocation: Revoke compromised or no longer needed certificates and update the CRL. * CRL Distribution: Ensure the CRL is accessible to entities to verify the revocation status of certificates.	Individual

Semester - II

Title	Risk, Controls and Compliance	Code	
Prerequisite	Basic Network Security Concepts	Credits |Total Hours	3-0-0 [4] | 45

Course Objective:

1. Understand the foundational principles and importance of GRC in cybersecurity.
2. Learn methodologies for identifying and assessing cybersecurity risks.
3. Understand approaches to risk decision-making and treatment strategies.
4. Master the process of monitoring and reporting cybersecurity risks.
5. Understand and apply cybersecurity standards and regulations.
6. Learn the scope and methodologies of cybersecurity control assessment.

Course Outcome:

CO1: Define the key components and importance of Governance, Risk, and Compliance (GRC) in the context of cybersecurity.
CO2: Analyse the scope of risk management and develop a comprehensive risk register considering legacy systems and industry standards.
CO3: Evaluate cybersecurity risks and formulate appropriate risk treatment strategies, including acceptance, transfer, remediation, and insurance.
CO4: Apply metrics to monitor and report cybersecurity risks, ensuring alignment with organizational objectives and compliance requirements.
CO5: Understand and implement cybersecurity control standards from various regulations, managing changes and ensuring compliance across the organization.
CO6: Create and execute a cybersecurity control assessment plan, including control attestation, testing, and compliance management.

Unit 1: GRC Overview 6

Introduction to GRC: Definition and importance of Governance, Risk, and Compliance (GRC), Overview of GRC in the context of cybersecurity; GRC Framework: Sources to Define Cybersecurity Objectives, Regulatory requirements, Organizational goals; Process to Define Cybersecurity Objectives: Long-term strategy development, Short-term strategy development; Cybersecurity Architecture from GRC Perspective: Identifying Sources to Define Policies & Procedures, Lifecycle Process for Policies & Procedures; Measuring Criteria Based on Cybersecurity Objectives: Key Performance Indicators (KPIs), Metrics and measurements; Risk Calculation Framework, Cybersecurity Governance, Developing KPIs and Monitoring Process, Meeting Cadences and Coverage, Developing Resource Management Plan for Cybersecurity.

Unit 2: Risk Identification & Assessment 7

Determining the Scope of Risk Management: Cybersecurity Risk Management Framework, Developing objectives for cybersecurity risks, Business Context Development; Establishing the Risk Register: Building Risk Registers, Approach considering legacy systems and industry standards, Risk Taxonomy, Risk Ownership, Current State Assessment;
Risk Assessment: Calculating Cybersecurity Risks (Qualitative and quantitative modeling approaches), Risk Factors, Rating Classification, Control Attestation, Residual Risk Calculation, Types of Risks - Calculating inherent risk, calculated risk, and residual risk

Unit 3: Risk Decision & Treatment 7

Risk Decision: Formulating approach based on cybersecurity risk ratings, categorizing decisions: risk acceptance, transfer, remediation, Defining risk appetite/tolerance level for an organization, Cybersecurity risk acceptance approval/exception process, Provisioning Cybersecurity Risk Capital; Risk Treatment: Risk Remediations - Identifying and implementing cybersecurity risk remediations, Remediation Tracking, Duplication of Risks and Remediations,

Stakeholders in Risk Remediation - Roles of control owner, risk owner, Information Security Officer, etc. Risk Treatment Approaches - Cybersecurity risk insurance, risk sharing, risk transfer. Re-Validating Risks - Process to re-validate risks post-remediation.

Unit 4: Risk Monitoring & Reporting 7

Risk Monitoring: Monitoring Requirements - Aligning with organizational cybersecurity objectives and related risks, Logic of risk roll-up and segregation at different organizational levels, Real-Time Risk Status Update, Risk Validation, Cybersecurity Metrics - Defining and measuring Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), Utilizing metrics for risk monitoring; Risk Reporting: Maintaining Cybersecurity Risk Posture, defining cybersecurity requirements for stakeholders through dashboards and reports, Requirements based on compliance and management initiatives, Risk Remediation Process, Aging and Performance Report, Managing changes in cybersecurity risk management, Process of reporting, escalation, and approvals.

Unit 5: Cybersecurity Standards & Regulations 9

Understanding the Landscape: Identifying Applicable Regulations - Approach and process for identification, Unique Cybersecurity Control Standards, Managing Regulatory/Standard Changes; Control Identification & Implementation: Identifying Cybersecurity Controls - From various regulations and standards, Controls Library Management, Control Owners and Compliance - Importance of control owners and their attestation; Identifying Reporting Requirements: Defining Compliance Reporting Requirements, Compliance Reporting Format, Compliance Collection Frequency - Role of various functional departments (legal, procurement, HR, admin); Educate and Train: Importance of Cybersecurity Training, Training and Awareness Programs.

Unit 6: Cybersecurity Control Assessment & Compliance 9

Identifying the Scope of Assessment: Defining the Control Universe - Approach based on compliance requirements, risks, criticality, Applicability of controls to auditable entities, Unified Compliance Framework (UCF) - Reducing duplicate efforts, defining assessment frequency based on business criticality; Control Attestation: Cybersecurity Control Lifecycle - Role of control owners through implementation, self-assessments, KPIs, Building Evidence Library for auditors; Control Assessment: Control Testing Approaches- Test of Design - TOD and Test of Operational Effectiveness - TOE, Audit/Assessment Process - Using annual plan, audit engagement, working papers, reports, Issue Management - Identification of findings, implementation of remediations; Compliance: Role of Stakeholders- Internal and external stakeholders in compliance reporting, Compliance Reporting Requirements, Compliance Management.

Reading Materials:

1. C Brumfield, Cybersecurity Risk Management - Mastering the Fundamentals Using the NIST Cybersecurity Framework 1st edition - By Wiley-Blackwell (2022)
2. Stephen D. Gantz, The Basics of IT Audit: Purposes - Processes - and Practical Information - By Syngress (2013)
3. Peter Trim & Yang-Im Lee, Cyber Security Management: A Governance - Risk and Compliance Framework 1st edition – By Routledge (2020)
4. Industry Standards: NIST CSF - PCI DSS & ISO 27001

Reference Links:

1. Information and Cyber Security GRC: Compliance Assessment and Reporting https://app.pluralsight.com/library/courses/compliance-assessment-reporting-information-cyber-security-grc/table-of-contents

2. Information and Cyber Security GRC: Governance: https://app.pluralsight.com/library/courses/governance-security-grc/table-of-contents
3. Information and Cyber Security GRC: Risk Management Frameworks and Structures https://app.pluralsight.com/library/courses/risk-management-frameworks-structures-information-cyber-security-grc/table-of-contents
4. Information and Cyber Security GRC: Risk Management: https://app.pluralsight.com/library/courses/info-cyber-security-grc-risk-mgmt/table-of-contents
5. Information and Cyber Security GRC: Supply Chain and Third-party Risk https://app.pluralsight.com/library/courses/supply-chain-third-party-risk-info-cyber-sec-grc/table-of-contents

Title	Identity and Access Management	**Code**	
Prerequisite	Computer and Network Security - Basics of Cybersecurity - Cryptography and PKI	**Credits |Total Hours**	2-0-2 [3] | 60

Course Objective:

1. Understand the fundamental concepts and principles of Identity and Access Management (IAM).
2. Explore and implement identity governance and administration principles.
3. Learn methodologies and technologies for regulating access to resources.
4. Understand and secure privileged access to organizational systems.
5. Examine and implement the latest trends and innovations in IAM.

Course Outcome:

CO1: Understand the IAM framework, standards, and architecture components and their lifecycle.
CO2: Analyse governance frameworks, standards, and technologies supporting robust Identity and Access governance implementation.
CO3: Evaluate the effectiveness of access management policies and procedures in ensuring security.
CO4: Implement PAM policies and procedures for managing privileged credentials.
CO5: Design an IAM solution incorporating the latest trends like Zero Trust and decentralized identity, and assess the impact of emerging technologies on IAM.

Unit 1: Fundamental Concepts and Principles of IAM 10

Introduction to IAM: Basics and Evolution of IAM, Understanding IAG, AM, PAM, UAM, PKI, and Directory Services, IAM Framework and Standards (NIST SP 800-63-3, SP 800-63A, SP 800-63B, SP 800-63C); IAM Architecture: Components and Lifecycle (PDP, PEP, PIP, Policy Engine, Policy Administrator), Deployment Models (IdaaS, On-Prem, Hybrid); IAM Processes: Identification, Authentication, Authorization, Accounting (IA); Access Control Models: RBAC, MAC, DAC, ABAC and Importance of IAM.

Unit 2: Identity Governance and Administration 10

Foundation and Concepts: Identity, Roles, Access, Entitlement, Provisioning, Deprovisioning; Governance Frameworks and Standards: Analysis of Aspects, Challenges, Compliance Requirements, and Importance; Unified Identity Governance: Definition, Need, Implementation Challenges; Policies and Procedures: Managing Entitlement, Access Policies, Roles, Identities (Employee, Non-Employee, Machine), End-to-End Management, Application Onboarding/Offboarding, Connectors; Identity Governance Administration: Managing Access, Provisioning, Deprovisioning, Separation of Duties, Workflow Automation, Triggers; Access Certification and Attestation: Aggregation, Correlation, Elevated Access, Certification, Access Review, Types of Reviews; Tools and Technologies: SailPoint, Saviynt, Entra ID, Okta.

Unit 3: Access Management 10

Access management Concepts: AAA - CIA Triad - modern authentication; User Access Management: Identity – Access - Permissions and Privilege; Authentication Mechanism: Legacy vs Modern Authentication – SAML – OAuth – OIDC; Authorization and access control Models: MAC – DAC – RBAC – ABAC - Rule-based; Advance Authentication and MFA: Application onboarding - Authentication Policies - MFA Policies - Adaptive Authentication - Different Factors - Need - pros and cons; Access Management Tools and Technologies: On-Premises and Cloud Tools, Market Leaders, Customer Requirements; Identities and Directory Services: AD – LDAP - Virtual Directory - Cloud Directory - DB vs Directories – schema - Replication and Implementation

Unit 4: Privilege Access Management 10

Introduction to PAM: Basic concepts, roles, importance in organizations; Identifying and Classifying Privileged Accounts: Understanding privileged accounts, inventorying existing ones, identifying elevated access, categorizing by privilege level; PAM Policies and Procedures: Authentication and Authorization for PAM - Password management, strong password policies, SSO, MFA, biometrics, Session management, recording for audit and termination; PAM Tools and Technologies: CyberArk, BeyondTrust, Thycotic, Delinea; Secure management of privileged credentials, Monitoring and Auditing Requirements, Incident Response and Risk Management; Emerging Trends and Technologies in PAM: Privileged behavior analytics, Zero Trust Architecture, JIT, convergence of PAM and IGA, support for cloud and hybrid environments, UEBA; Public Key Infrastructure (PKI) and Its Components.

Unit 5: IAM implementation - Automation - IDaaS - IAM for Cloud - and latest Trends 5

IAM components: Authentication, Authorization, User Management; Implementation Architecture: Designing IAM Architecture, Deployment and IAM end-to-end integration, Automation scope, Monitoring and Maintenance; IAM in Cloud Service: AWS IAM - Azure IAM - Google Cloud IAM; Challenges of identity and access in the cloud, IDaaS offering and advantages; Zero trust - Decentralized Identity - Quantum Security.

Practical: 30

1 Configure AD & LDAP with one of the IDaaS solutions.
1. AD Agent to Sync User details between on-prem and Cloud
2. Test user authentication using AD credentials, enable one way and both-way sync, and test users
3. Create Attribute mapping and 10 Custom attributes using the profile editor.
4. Import users manually to the cloud directory.
5. LDAP Agent to sync user details and map users to the cloud directory

2 Configure User Lifecycle management.
1. User Registration, Password reset, Forgot password.
2. Customize and Branding using your custom logs and brand names
3. Customize email & SMS using your custom brand names/logos

3 Integrate 2 SaaS applications.
1. Configure 1 Application using SAML and create an authentication policy.
2. Configure 1 application using OIDC and configure MFA
3. Configure Conditional/Adaptive authentication

4 Create Workflows and automate user onboarding to the above 2 applications

5	Create automation using inline or event hooks in Okta /using Microsoft graph in Entra ID 1. 2 use case demos of inline or event hooks with your existing Okta tenant
6	API Automation 1. Use API to manage user(create/edit/delete/add/remove group/bulk import/update/delete) using Python/PowerShell or any other languages 2. Use API to read logs and manage alerts in a better way, alerts for issues/threshold limits/errors/exceptions, etc 3. Use API to Create/Modify/delete application details, policies and other information's

Reading Materials:

1. Mike Chapple, Access Control and Identity Management 3rd edition - By Jones and Bartlett Publishers, Inc (2020)
2. Elisa Bertino & Kenji Takahashi, Identity Management: Concepts - Technologies and Systems - By Artech House Publishers (2010)
3. Michael Schwartz & Maciej Machulak, Securing the Perimeter: Deploying Identity and Access - Management with Free Open Source Software 1st edition – By Apress (2018)
4. Morey J. Haber & Darran Rolls, Identity Attack Vectors: Implementing an Effective Identity And Access Management Solution 1st edition – By Apress (2019)
5. Abhishek Hingnikar & Yvonne Wilson, Solving Identity Management in Modern Applications: Demystifying OAuth 2.0 - OpenID Connect - and SAML 2.0 1st edition – By Apress (2019)
6. Gerardus Blokdyk, Privileged Access Management Pam A Complete Guide - 2020 Edition – By 5starcooks
7. Charles J. Brooks, Christopher Grow, Philip Craig & Donald Short, Cybersecurity Essentials 1st edition - By Sybex (2018)
8. Morey J. Haber & Brad Hibbert, Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations 1st edition – By Apress (2018)
9. Suranjan Choudhury, Public Key Infrastructure Implementation & Design Implementation & Design - By M & T Books (2002)
10. Carlisle Adams & Steve Lloyd, Understanding PKI: Concepts, Standards and Deployment Considerations 2nd edition - By Addison-Wesley (2011)
11. Nancy Cox, Directory Services: Design, Implementation and Management (Enterprise Computing) - By Digital Press (2001)
12. Beth Sheresh & Doug Sheresh, Understanding Directory Services 2nd edition - By Sams (2001)
13. Samuel O Omoniyi, Identity and Access Management (IAM) Architect: A Practice Guide – By Independently Published (2023)

Reference Links:

1. Identity and Access Management: The Big Picture : https://app.pluralsight.com/library/courses/identity-access-management-big-picture/table-of-contents
2. CyberArk Fundamentals https://app.pluralsight.com/library/courses/cyberark-fundamentals/table-of-contents
3. Microsoft Entra Fundamentals: https://app.pluralsight.com/library/courses/microsoft-entra-fundamentals/table-of-contents

Title	Cloud Security	**Code**	
Prerequisite	Basic Network Security and Cloud Computing Concepts	**Credits |Total Hours**	3-0-0 [3] | 45

Course Objective:

1. Understand fundamental cloud computing concepts and secure cloud design principles.
2. Apply strategies for securing data in the cloud.
3. Analyze and secure cloud platform, applications, and infrastructure.

4. Evaluate cloud security operations and monitoring.
5. Create strategies to manage legal and compliance requirements in the cloud.

Course Outcome:
CO1: Define and describe key cloud computing concepts, including on-demand self-service, broad network access, and rapid elasticity.
CO2: Explain the application of data security technologies, such as encryption, hash functions, and Data Loss Prevention (DLP), in securing cloud data.
CO3: Analyse cloud application architecture, including the use of cryptography and sandboxing, for secure application development and deployment in the cloud.
CO4: Evaluate incident management procedures and vulnerability assessments for their effectiveness in maintaining security in cloud operations.
CO5: Apply audit processes and methodologies, such as SSAE and ISAE, adapted for the cloud environment, to ensure compliance and security.

Unit 1: Cloud Concepts - Architecture and Design 8

Understand cloud computing concepts :Definition, Key Characteristics: On-demand self-service - broad network access - multi-tenancy - rapid elasticity and scalability - resource pooling - measured service; Cloud reference architecture: Software as a Service (SaaS) - Infrastructure as a Service (IaaS) - Platform as a Service (PaaS)); Understand security concepts relevant to cloud computing: Access – Cryptography - Network Security; Understand design principles of secure cloud computing: BIA - DC/DR.

Unit 2: Cloud Data Security 8

Cloud data concepts: Data dispersion - Data flows; Design and apply data security technologies and strategies: Encryption - Hash - DLP; Implement data discovery & data classification: Data labelling - data mapping; Design and implement Information Rights Management (IRM): Data rights - Provision; Plan and implement data retention - deletion - and archiving policies: logging - custody - non-repudiation

Unit 3: Cloud Platform - Application & Infrastructure Security 12

Cloud infrastructure components: Network – Server – Virtualization - Storage etc.; Risks associated with cloud infrastructure: Cloud Vulnerabilities - Risk Assessment - Risk Mitigation; Cloud security controls: WAF - Firewalls - ALB – DDOS - API Gateways etc; Common cloud vulnerabilities (e.g. - Open Web Application Security Project (OWASP) Top-10 - SANS Top-25); Cloud application architecture: Cryptography - Sandboxing etc; Identity and Access Management (IAM) solutions: MFA – SSO – PIM - RBAC; Cloud Native Application Protection (CSPM - CWPP - CTDR).

Unit 4: Cloud Security Operations 10

Hardware specific security configuration requirements (e.g. - hardware security module (HSM) and Trusted Platform Module (TPM)); Network security controls (e.g. - firewalls - intrusion detection systems (IDS) - intrusion prevention systems (IPS) - honeypots - vulnerability assessments - network security groups - bastion host); Intelligent monitoring of security controls (e.g. - firewalls - intrusion detection systems (IDS) - intrusion prevention systems (IPS) – honeypots - network security groups - artificial intelligence (AI)); Log capture and analysis (e.g. - security information and event management (SIEM) - log management) - Incident management - Vulnerability assessments.

Unit 5: Legal - Risk and Compliance 07

Legal requirements and unique risks within the cloud environment; Understand privacy issues - e.g., protected health information (PHI) - personally identifiable information (PII)); Understand audit process - methodologies - and required adaptations for a cloud environment. ((e.g. - Statement on Standards for Attestation Engagements (SSAE) - Service Organization Control (SOC)International Standard on Assurance Engagements (ISAE)); Understand implications of cloud to enterprise risk management (e.g. - breach notification - Sarbanes-Oxley (SOX) - General Data Protection Regulation (GDPR)); Quick look at CSA - NIST and ENISA guidelines for Cloud Security.

Reading Materials:

1. Tim Mather, Subra Kumaraswamy & Shahed Latif, Cloud Security and Privacy 1st edition – By O'Reilly Media (2009)
2. Ronald L. Krutz & Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing 1st edition - By Wiley (2010)
3. Brian T. O'Hara & Ben Malisow, CCSP Certified *Cloud Security Professional* Study Guide edition – By Sybex (2017)
4. Vic (J.R.) Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics Illustrated edition – By Syngress (2011)
5. Ryan Ko and Kim-Kwang Raymond Choo, The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues Illustrated edition – By Syngress (2015)

Reference Links:

1. Azure Security Engineer Associate - AZ-500: Shoshin School (ltimindtree.com)
2. Security, Compliance, and Identity Fundamentals (SC-900): Shoshin School (ltimindtree.com)
3. AWS Cloud Practitioner: LTI - AWS Cloud Practitioner | Pathway | Degreed
4. AWS Certified Security – Specialty: LTI - AWS Certified Security – Specialty (SCS-C01) | Pathway | Degreed
5. Google Cloud Basics: Shoshin School (ltimindtree.com)
6. Google Cloud Practitioner: Shoshin School (ltimindtree.com)
7. Microsoft Defender: Implementing and Managing Microsoft Defender XDR Path | Pluralsight

Title	Business Continuity Planning	**Code**	
Prerequisite	Governance Risk and Control basics	**Credits |Total Hours**	2-0-0 [2] | 30

Course Objective:

1. Understand the foundational principles and framework of Business Continuity Management.
2. Apply techniques for business impact analysis and risk assessment.
3. Examine and develop recovery strategies and plans.
4. Prepare and enhance the effectiveness of business continuity plans.
5. Create and manage effective crisis response and recovery plans.

Course Outcome:

CO1: Understand the principles and framework of business continuity management (BCM) and its importance for cybersecurity professionals.
CO2: Explain the concept of Business Impact Analysis (BIA) and its importance in quantifying the impact of business outages.
CO3: Describe the components of a recovery plan, including initial incident response, resume critical/non-critical operations, and restoration steps.
CO4: Analyse audit program results to identify non-conformities and improvement recommendations per industry standards.
CO5: Apply crisis management principles to identify threats, notify leadership, and handle incidents effectively.

Unit 1: Fundamental Concepts and Principles of BCMS 4

Introduction to Business Continuity Management: Definition - ISO standard; Establishing business continuity context: BCMS business case - management buy-in - identification of stakeholders - regulatory & compliance requirements for BCMS; Defining BCMS framework: Business Continuity objectives – strategy - policies & procedures - roles & responsibilities - measuring criteria or KPIs - maturity state and goal state; Awareness & Training: BCP/DR team regular trainings & drills - awareness program.

Unit 2: Business Impact Analysis & Risk Assessment 8

Business Impact Analysis: Identification of business - critical processes – applications - servers- interdependencies- analyze impact of failure of these processes- Recovery objectives (RTO & RPO)- quantify the loss due to business outage; Risk Assessment: Identify risk scenarios (internal & external) - quantify the potential severity with potential damage and recovery/restoration time - frequency & likelihood - measures/controls - risk ranking.

Unit 3: Recovery Strategy & Plan Development 12

Recovery Strategies: Identify the recovery options - compare RTO/RPO - cost-benefit analysis - recovery chain - third-party (outsourcing) - prioritizing and deciding based risk - long-term solution & interim solution; Recovery Plan: Business & Service recovery plans (initial incident response- call tree- resume critical business operations- resume non-critical business operations- restoration steps/guide/playbook- maintenance- awareness & training- testing- integrating with external groups (customer- media- emergency responders); Business Continuity Plan: Work-around- temporary arrangements- agreements/contracts- back-up- communication- training- and testing.

Unit 4: BCP Maintenance Exercise and Evaluation 4

Testing: Unit testing & integrated testing - table-top - structured walk-through - checklist - simulation - parallel run - full interruption; Governance and Management Reviews – Senior Leadership reviews - KPI reporting - Plan Vs Actual assessments; Maintenance: Issue remediations - re-validation & documentation - training - contract renewals; Audit Program: Cross functional review - Control validation and remediation - internal/ external audit - improvement recommendations per industry good practices - non-conformity identification and remediation; Adoption to changes in industry standards or recommendations.

Unit 5: Crisis Management 2

Crisis Monitoring: Threat identification and evaluation- Crisis notification to leadership and stakeholders; Incident handling: Crisis declaration- Emergency response plan- Crisis communication- Response and recovery; Post incident actions: Damage assessment- Gap analysis- Incident reports- Action planning and reporting

Reading Materials:

1. Susan Snedaker, Business Continuity and Disaster Recovery Planning for IT Professionals 2nd edition – By Syngress (2013)
2. Kurt J Engemann and Douglas M Henderson, Business Continuity and Risk Management: Essentials of Organizational Resilience - By Rothstein Associates Inc. (2011)
3. Andrew Hiles and Kristen Noakes-Fry, Business Continuity Management: Global Best Practices 4th edition – By Rothstein Publishing (2014)
4. Industry Standards: ISO 22301 - ISO27031 - Certified Business Continuity Professional (CBCP) - Business Continuity Certified Planner (BCCP)
5. Michael Wallace & Lawrence Webber, The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities and Assets – By Amacom (2004)

Reference Links:

1. https://www.cio.com/article/288554/best-practices-how-to-create-an-effective-business-continuity-plan.html
2. https://www.iarminfo.com/bcp-simplified-easy-to-understand-bcp/
3. https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity-action-plan

Title	API Security Testing	**Code**	
Prerequisite	Understanding concepts of security testing and API concepts	**Credits |Total Hours**	2-0-0 [2] | 30

Course Objective:

1. Understand the fundamentals of API security and its importance.
2. Apply various tools and techniques for API security testing.
3. Analyze and evaluate API security testing techniques.
4. Create and implement API security best practices and governance frameworks.

Course Outcome:

CO1: Explain the types of APIs, common vulnerabilities, and security best practices.
CO2: Analyse API security testing results to identify vulnerabilities and propose remediation strategies.
CO3: Evaluate an API security testing approach incorporating best practices from OWASP, SANS, and NIST, and implement automation for continuous assessments.
CO4: Develop automated solutions for API security testing and program governance.

Unit 1: Introduction to API Security 6

Introduction to API security testing: Why API Security Testing and its importance - Common Risks - Type of Vulnerabilities - Tools and Techniques - Types of API's (SOAP, REST, etc.); Best Practices – OWASP, SANS, etc.

Unit 2: API Security Testing 10

Tools & Technologies: Understand various tools and testing methodology; Implementation: Tool Implementation & Configuration - API Security Testing techniques - Manual Analysis Techniques - DevSecOps implementation (azure DevOps, etc.) – Introduction – Integrations - Continuous Assessments, etc.

Unit 3: API Security Testing Approach 8

Testing Techniques - Understanding API Endpoints, Authentication and Authorization Testing, Input Validation and Data Integrity, Error Handling and Exception Management, Rate-limiting and Throttling, API Abuse and Security Testing Automation.

Unit 4: Best Practices and Governance 6

Best Practices Implementation - OWASP, SANS, NIST, etc. Using tools and techniques; Automation & Program Governance – Ticketing and Tracking automation, Report Presentation, Stakeholder communication.

Reference Books:

1. Corey J. Ball, Hacking APIs: Breaking Web Application Programming Interfaces - By No Starch Press (2022)
2. Neil Madden, API Security in Action 1st edition – By Manning (2020)
3. Prabath Siriwardena, Advanced API Security: OAuth 2.0 and Beyond 2nd edition - By Apress (2019)

Reference Links:

1. API Security Fundamentals Course:
   https://www.youtube.com/watch?v=o6d6BjX-Iys &
   https://www.akamai.com/resources/white-paper/api-security-fundamentals
2. Best Practices
   https://www.techtarget.com/searchapparchitecture/tip/10-API-security-guidelines-and-best-practices
3. API Basics:
   https://www.esecurityplanet.com/applications/api-security/
4. API guide:
   https://brightsec.com/blog/api-security/

Title	Operational Technology and IoT	**Code**	
Prerequisite	Basic Understanding of Network Security Concepts	**Credits |Total Hours**	3-0-0 [3] | 45

Course Objective

1. Understand the foundational concepts and architectures of OT and IoT.
2. Understand OT architecture components and industry standards.
3. Apply cybersecurity principles to OT and IoT environments.
4. Analyze network and access management techniques in OT and IoT environments.
5. Create ethical hacking strategies for securing OT and IoT systems.

Course Outcome:

CO1: Understand the fundamental concepts of Operational Technology and Internet of Things.
CO2: Identify and explain the components of OT architecture, including sensors, actuators, control systems, and communication networks.
CO3: Analyze various threats and attack vectors in OT environments and their impact.
CO4: Evaluate the use of role-based access control (RBAC) and least privilege principles for managing access to critical systems.
CO5: Apply countermeasures to protect IoT and OT systems from potential attacks.

Unit 1: Introduction to OT and IoT 8

Overview of OT and IoT control systems: Architecture and process models; Operational Technology (OT) in industrial sectors: Role in Manufacturing, Energy, Transportation, Utilities, etc.; Components of OT/ICS environment: Hardware, Software, Sensors, Actuators, Controllers, Valves, RTU, HMI, ICS, DCS, PLC, etc.; IoT and its industrial applications: Sensors, Devices, Connectivity, Data processing, Networking, Cloud Infrastructure, Data storage, Analytics, User interface, Security; Difference between IT and OT: Objectives, Technology stack, Requirements; Emerging trend: Convergence of IT with OT and IoT, Implications for cybersecurity; Industrial Control Systems (ICS) and Manufacturing: Usage in manufacturing, Process control, SCADA, PLCs, DCS, MES; Interdependencies of ICS with critical infrastructure sectors: Energy, Water and wastewater management, Transportation system, Telecommunications, Healthcare, Financial services, Defense; ICS Process Models: Functional models, Data flow models, State models, Control system models, Physical models, Simulation models, etc.

Unit 2: Introduction to OT Components and Industry Standards 8

OT Architecture Components: Sensors, Actuators, Control Systems (PLCs, DCS, SCADA), Communication Networks, HMI, Historian and Data Storage, Edge Computing, Security Measures; DCS & PLC Components: Controllers, I/O Modules, Communication Networks, Operator Stations, Engineering Workstations, Redundancy and Fault Tolerance,

CPU, Memory, Communication Ports, Power Supply, Programming Software; Basic ICS Control Logic: Sequential Control, PID Control, On/Off Control, Fuzzy Logic Control, State-based Control, Advanced Control Strategies; DCS vs. PLC; OT Operating Systems: RTOS, Windows Embedded, Linux, Proprietary OS (e.g., ABB's System 800xA, Siemens' SIMATIC WinCC, Schneider Electric's EcoStruxure); Industrial Communication Protocols: Modbus, Profibus, Foundation Fieldbus, EtherNet/IP, Profinet, DNP3, OPC; IoT Devices and Protocols: IoT Devices, Sensors, Actuators, MQTT, CoAP, OPC UA, Sigfox, LoRaWAN, DDS, AMQP; IoT Connectivity Options: Wi-Fi, Bluetooth, Zigbee, LoRaWAN; OT Security Controls and Compliance: IEC 62443, NIST 800-82.

Unit 3: Cyber Security in OT/ IoT Environment 10

Cybersecurity challenges faced by OT and IoT environments - including legacy systems - lack of encryption - and device diversity - Understanding the potential impact of cyber-attacks on critical infrastructure and industrial operations. - Threats in OT Environment - Attacks on Control Systems - Impacts of Threats in OT Environment - Unique Security Concerns for ICS/OT - Attack Vector Analysis - Common Vulnerability Identifiers - Examples of cyberattacks on OT Systems - ICS MITRE ATT&CK Framework

Unit 4: OT Network and Access Management 12

Understanding network segmentation - firewalls - and intrusion detection/prevention systems (IDS/IPS) to protect OT and IoT networks - Basics of IT networking (IP protocols - IP configurations - Netting and Subnetting - VLANs - NAT - DNS etc.); Open Systems Interconnect (OSI) Model: Physical layer- Data Link layer- Network layer- Transport layer- Session layer- Presentation layer- Application layer; OT Networking - Network Segmentation and Conduits - Enforcement Zone Devices - Firewalls - IDS/ IPS - Firewall management between Corporate Network and Control Network - SANS IEC 62443 Reference Model - Secure Remote Access - ICS/ OT DMZ – OT Purdue Model - Securing wireless communication in IoT deployments - Implementing authentication mechanisms for OT and IoT devices - including certificate-based authentication and OAuth - Role-based access control (RBAC) and least privilege principles for managing access to critical systems.

Unit 5: Ethical Hacking in IoT and OT 7

Investigating IoT and OT Concepts - Reviewing IoT and OT Attacks - Understanding IoT and OT Hacking Methodologies - Exploring IoT and OT Hacking Tools - Implementing Countermeasures - Exploring ICS and OT Attacks - Exploiting the Modbus Protocol.

Reading Materials:

1. ICS/SCADA Security Fundamentals – Infosec

Reference Links:

1. Internet Of Things (IOT): The Big Picture – PluralSight
2. Fundamentals of OT Protocols – PluralSight
3. Fundamentals of OT Security - PluralSight

Title	Security Compliance Lab	Code	
Prerequisite	Basic Network Security and Cloud Computing Concepts	Credits |Total Hours	0-0-4 [2] | 60
Cloud Security			
Experiment 1	Enable Sentinel service (pre-requisites -> Log analytics workspace to be created) Integrate some security events from the available data connector outside of the cloud and test the same. Create an analytic rule that based on specific event some incident to be created and notified.		Individual
Experiment 2	Enable standard security services in the azure so that you will get the security events /logs in the workspace. Create some analytic rule in the sentinel to trigger the event- create alert logic to alert an event to email.		Individual
Experiment 3	Create automation by using the logic apps like if anyone create NSG with source as “All” the NSG to be deleted automatically and to be intimated to the admin group. Like similar way create some automation rule and execute Connect with the third-party Threat Intel feed.		Individual
Experiment 4	Create workbooks for the better visibility use the sample template and create your own workbook. Create Hunting query and check for the security threat.		Individual
Experiment 5	Enable defender for cloud in azure which is a CSPM native service by Azure. If possible and if you have AWS or GCP , try integrating those cloud providers with the Azure Defender for cloud. Check the security posture, review the secure score, and analyze the reason for the low security score and improve the security score by validating the recommendation. Check the inventory and analyze the resource and resource type and also check for any recommendations and can be implemented.		Individual
Experiment 6	Check for the regulatory compliance by visiting the different compliance standards like CIS Azure Foundations v2.0.0. Enable workload protection for the workload like servers, storage , containers key vault. Sql servers. Analyse the attach path data and create a RCA document for the available threat. Provide recommendation for the same.		Individual
Compliance Lab			
Experiment 1	Case Study Intro Consider the risk and compliance opportunities for a dummy company and document possible risks & policies		Individual
Experiment 2	User Roles Define various users with what that user has access to and the operations that he or she can perform.		Individual
Experiment 3	Create Policy Create a password policy and connect password control objectives to the new policy.		Individual
Experiment 4	Publish Policy Run the policy lifecycle and publish the policy.		Individual
Experiment 5	Create Entity Types and Entities Create entity framework necessary to scope the dummy company		Individual

Experiment 6	Create Risk Framework and Risk Statements Create a password policy and connect password control objectives to the new policy	Individual
Experiment 7	Define and Order Risk Criteria Create a Risk Framework and associate with Entity Types and review the risks created and Change risk scoring to qualitative and new risk criteria and realign values	Individual
Experiment 8	Risk Statement Scope Review a risk statement that addresses that involves disclosure of confidential information and select a risk response to generate a task and relate controls to registered risk	Individual
Experiment 9	Define and Execute an Indicator Create an indicator and manually execute testing for when a device is lost or stolen	Individual
Experiment 10	Controls and Continuous Monitoring Review both compliant and non-compliant controls and assign a configuration test to a control objective and evaluate the outcomes	Individual
Experiment 11	Issues Management Create two groups of related issues: Offline Servers and Business Critical Servers and Disposition the Business-Critical Servers grouped Issues	Individual
Experiment 12	Policy Exception Management Request Policy exception to control objective, configure minimum password age for offline servers and approve the policy exception	Individual
Experiment 13	Create Audit Test Template Create a Test Template and Generate Test Plans for each of the scoped Controls	Individual
Experiment 14	Create and Scope Audit Engagement Create an Engagement and scope it with Entities for auditing, Review the engagement workbench and create and complete a control test.	Individual
Experiment 15	GRC Homepages and Reporting Review the Risk and Compliance Overview Homepages and Create a new ad hoc report for Calculated ALE by Entity and Risk Framework	Individual

Title	[BCP/API Security Testing] & OT and IoT Lab	**Code**	
Prerequisite	Understanding concepts of network security, security testing and API concepts	**Credits |Total Hours**	0-0-4 [2] | 60
BCP			
Experiment 1	BCM framework design 1. Create a proposal to senior leadership on BCM framework 2. Prepare the objectives of the BCM program 3. Define measurement criteria or KPIs		Individual
Experiment 2	Define Recovery objectives through examples 1. RTO 2. RPO 3. MBCO 4. MTPD		Individual

Experiment 3	Classify business/ process to Create Recovery Tiers 1. Mission Critical 2. Critical 3. Essential 4. Desirable	Individual
Experiment 4	Create a Business Impact Analysis Template	Individual
Experiment 5	Conduct a Business Impact Assessment	Individual
Experiment 6	Create a risk register for a company 1. Cyber risk register for IT company 2. Climate risk register for manufacturing company 3. Financial risk register for Insurance company	Individual
Experiment 7	Create a new Plan Template 1. Business Recovery plan 2. Crisis response plan 3. Site recovery plan 4. Technology recovery plan	Individual
Experiment 8	Create an Incident Simulation Exercise	Individual
Experiment 9	Create a post incident report	Individual
Experiment 10	Create the BCMS Audit Checklist	Individual
API Security Testing		
Experiment 1	Install and Implement API security tools and verify if the tool has been configured successfully for testing	Individual
Experiment 2	Using open-source or commercial tools identify API (leverage bug bounty program) that can be tested. Test them using the tools identified	Individual
Experiment 3	Try identifying potential vulnerabilities based on OWASP API Top 10 2023	Individual
Experiment 4	Create a detailed report capturing potential vulnerabilities. Also, provide POC on the approach taken for vulnerability identification	Individual
OT & IoT		
Experiment 1	Claroty CTD and/ or Claroty Edge tool installation (Could be any asset and threat discovery tool such as Claroty, Armis, Nozomi) – Installation – Install and configure VMware. Install CTD successfully on Host machine OS Windows, guest OS Linux/ Unix.	Individual
Experiment 2	Configure Claroty CTD and/ or Claroty Edge tool – CTD management console set-up and configuration, Enable Process data to receive the OT traffic from Switch SPAN port. Update Threat bundle with latest version.	Individual
Experiment 3	Enable Port Mirroring in Core Switch – For CTD to receive the OT traffic. Test with sample data and validate whether the switch has sent the data to CTD server.	Group
Experiment 4	Network Segmentation – Deploy an OT Firewall at Purdue level 3.5. Create Network Segmentation - OT VLANs with zones and conduits. Create a presentation with proposed OT Security Network Architecture and Segmentation.	Group

LTIMindtree

Let’s get to the future, faster. Together.