CSE 807 Information Security Management

Cyber Security Framework: Critical Success Factors of Information &amp; Cyber Security, Information vs Cyber Security, Cyber Security Layers/Model, Cyber Security Framework (cont.): Common Cyber Threats and Attack Vectors, Cybersecurity Frameworks and Best Practices, Anomaly detection and attack graphs, Information Protection: Asset Classification, Inventory of information and other associated assets, Asset and Data Ownership, Data life cycle, Classification of information with the process, Labelling of information, Information transfer, Access control of information, Acceptable use of information and other associated assets, Data Classification and Sensitivity, Data Encryption Techniques and Algorithms, Secure Data Storage and Backup Strategies. Infrastructure Protection: Secure Network Design and Architecture, Network Access Control and Segmentation, Firewalls, Intrusion Detection, and Prevention Systems, Vulnerability and Configuration Analysis: logic-based and model-based approaches. Access Control and Identity Management: Principles of Access Control and Identity Verification, Role-Based Access Control (RBAC), Privileged Access Management (PAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO), Managing Identity and Authentication, Controlling and Monitoring Access. Risk Management Life Cycle: Risk Assessment, Risk, Threats, vulnerabilities, and misconfiguration analysis, Qualitative and Quantitative Risk Assessment, Risk Management, standard, and best practices, standards (e.g., OCTAVE) and best practices. Risk assessment and Management case study, Risk assessment based on the scenario; Governance &amp; Compliance: Security Policies, Standards, and Procedures (SOP), Working Instructions, User Manual, Work-flow diagram, Security Awareness and Training, ISO, PCI DSS, HIPAA, GDPR and other international standards, InfoSec Risk Based Audit Management Lifecycle, Business Continuity &amp; Disaster Recovery Management: Business continuity program, Disaster Recovery Planning, Incident Response Planning and Preparation, Incident

Detection, Analysis, and Containment, Incident Recovery and Post-Incident Reporting, Proactive and Post-Incident Cyber Services, computer emergency response teams, Cyber Drill, DR Drill.

Textbook and Reference:

– *Thomas R. Peltier*, **Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management**.
– *Mark S. Merkow and Jim Breithaupt*, **Information Security: Principles and Practices**.
– *Michael D Workman*, **Information Security Management.**
– *Mark Rhodes*, **Information Security-The Complete Reference**.