Information Security And Risk Management

Course Objectives

The program is designed to increase security knowledge and for understanding the influence of appropriate employee behavior at all levels of the workforce. This course provides knowledge in principles of Information Security, not knowledge of specific technologies or products.

Syllabus

Information Security Principles, Information Risk, Threats and Vulnerabilities, Risk Management, Information Security Framework, Organization and Responsibilities, Policy Standards & Procedures, Information Security Governance, Incident Management, Legal Framework

Expected Outcomes

Upon completion of this course, the students will be able to:

1. Acquire knowledge of Information Security and Risk Management concepts 2. Candidate will be able to anticipate threats on information in various levels of an organization. 3. The candidate can find, assess and refer to information and material necessary to carry out a risk assessment. 4. The candidate can use guidelines and standards to structure the implementation of information security in an organization.

References

1. Manish Agrawal, Alex Campoe, Eric Pierce (2014), Information Security and IT Risk Management, 2nd edition Wiley India

2. Evan Wheeler , Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, 1st edition Syngress

3. Mark Stamp (2011), Information Security: Principles and Practice, 2nd edition Wiley India

4. David Alexander, Amanda Finch, David Sutton, Andy Taylor (2013), Information Security Management Principles, 2nd edition BCS

5. Sari Greene (2014), Security Program and Policies: Governance and Risk Management, 2nd edition Pearson

Course Plan

1 Information Security Principles Introduction- Principles of Information Security-Concepts and Definitions of Information Security Principles-CIA Triad-Information Security Ethics-Information Security & your Business needs-Hi-tech crime.

2 Information Risk, Threats and Vulnerabilities Information Risk- Threats- Vulnerability-Business Impact of Realized Threats Vulnerabilities. Threat models- Threat Agent- Threat Action. Addition of threat intelligence, big data, the Internet of things and the vulnerabilities in social media and networks.

First Internal Examination

3 Risk Management Introduction-Risk Management Life Cycle- Risk Analysis - Risk Assessment-Risk Mitigation-Risk Dealing Options-Value of Information Assets-Risk Registers Contribution-Information Classification Strategies. Information Security Framework-Introduction to Information Security Framework- Introduction to Information Security Management.

4 Risk Assessment Techniques Identification of Risks- Risk Assessment in Business. -Operational Assessment- Project Based Assessment- Third Party Assessment. Reports and Consulting – Structure of Risk Assessment Report- Writing Audit Reports.

Second Internal Examination

5a Information Security Governance Introduction to Information Security Governance-Organization and Responsibilities-Introduction to Organization and Responsibilities- Roles and Responsibilities-Good Principles Policy Standards & Procedures-Policy Standards and Procedures.

5b Incident Management Introduction to Incident Management-Concepts of Incident Management -Techniques for Investigation-Evidence Preservation.

Legal Framework-Protection of Personal Data -Employment Issues- Computer Misuse-Credit Card Fraud-IT Act-Record Retention.

Final Examination