Cybersecurity Analysis Course Structure

Module 1 - Introduction to Cybersecurity Analysis

1.1 Course Overview

1.2 Importance of Security

1.3 IT Functions & Roles

1.4 IT 101 - 1: The Pieces

1.5 IT 101 - 2: Using & Managing the Pieces

1.6 IT 101 - 3: Advancement

1.7 The Role of Business Analysis in Cybersecurity

1.8 Governance Perspectives of Cybersecurity

Module 2 - Enterprise Cybersecurity Concepts

2.1 Security Accountability

2.2 Cost of Securing an Organization

2.3 Outsourcing for Cybersecurity Expertise & Services

2.4 Risk Tolerance

2.5 Compliance

2.6 Best Practices & Benchmarking

2.7 Data Privacy - 1: Basics

2.8 Data Privacy - 2: Nuances

2.9 Digital Rights Management

2.10 Audit: Internal & External

Module 3 - Enterprise Risk

3.1 Risk Management & Control Assurance Framework

3.2 Organizational Risk Assessment

3.3 Risk Analysis: Threat Risk Assessments

3.4 Risk Analysis: Vulnerability Assessments

3.5 Business Case Development

3.6 Disaster Recovery & Business Continuity

Module 4 - Cybersecurity Risks and Controls

4.1 Understanding Security Controls & IT RIsk -1

4.2 Understanding Security Controls -2

4.3 CIA Triad

4.4 Applying Controls

4.5 Cybersecurity Threats - 1

4.6 Cybersecurity Threats - 2

4.7 Cybersecurity Vulnerabilities - 1

4.8 Cybersecurity Vulnerabilities - 2

4.9 Adverse Impacts

4.10 Risks & Controls: Putting it all Together

Module 5 - Securing the Layers

5.1 Physical Security

5.2 Endpoint Security

5.3 Network Security: Security Architecture

5.4 Network Security: Firewalls

5.5 Network Security: Anti-Virus/Anti-Malware

5.6 Network Security: Segregation

5.7 System Security: Servers

5.8 Platform Security

5.9 Product Security: Threat Models

5.10 Product Security: Embedded Systems

5.11 Product Security: Internet of Things

Module 6 - Data Security

6.1 Data Security – At Rest: Information Classification & Categorization

6.2 Data Security - In Transit: Encryption & Keys

6.3 Data Security - In Transit: SSL/TLS

6.4 Data Security - In Transit: Digital Signature & Identification

Module 7 - User Access Control

7.1 Directory Management

7.2 Authorization

7.3 Authentication and Access Control

7.4 Privileged Account Management

7.5 Users and Security Awareness

Module 8 - Solution Delivery

8.1 SDLC & Solution Security Planning

8.2 Requirements & Security Engineering

8.3 Requirements & Solution Development

8.4 Solution Security: Applications

8.5 Solution Security: Databases

8.6 Solution Security: Web

8.7 Change Impact Analysis

Module 9 - Operations

9.1 Incident Response, Recovery & Remediation

9.2 Metrics & Reporting

9.3 Risk Logging & Mitigation Tracking

9.4 Operational Risk Ownership

9.5 Computer Forensics: SOC, SIEM

9.6 Future Proofing your Security Posture

To learn more or to purchase these materials please visit iiba.org/cybersecurity