



Detailed Table of Contents for **Certificate in Cybersecurity Management**

Developed and Prepared by
First Atlantic Cybersecurity Institute
7429 Lighthouse Pt, Pittsburgh, USA
www.facyber.com

Email: info@facyber.com

Enroll Here: <http://facyber.com/product/certificate-in-cybersecurity-management/>

week-1

week-2

week-3

week-4

week-5

week-6

week-7

week-8

week-9

week-10

week-11

week-12

Chapter -1 Structure of Information Systems

COMPUTER FUNDAMENTALS

1.1 WORKING PROCESS OF COMPUTER [VIDEO]

1.2 ORGANIZATION OF COMPUTER

1.3 COMPUTER PERIPHERALS & SOFTWARE

Chapter -1 Structure of Information Systems

COMPUTER FUNDAMENTALS

1.1 WORKING PROCESS OF COMPUTER [VIDEO]

1.2 ORGANIZATION OF COMPUTER

1.3 COMPUTER PERIPHERALS & SOFTWARE

1.4 OPERATING SYSTEM & ARCHITECTURE

1.5 COMPUTER LANGUAGE

FUNDAMENTAL OF INTERNET

1.6 HISTORY OF INTERNET

1.7 SERVICE OF INTERNET

1.8 WEB ADDRESS AND WEB BROWSER

NUMBER SYSTEM

1.9 BINARY NUMBER SYSTEM

1.10 DECIMAL NUMBER SYSTEM

1.11 OCTAL NUMBER SYSTEM

1.12 HEXADECIMAL NUMBER SYSTEM

1.13 CONVERSION BETWEEN NUMBER SYSTEM

1.14 WHAT IS INFORMATION SYSTEM?

1.15 IMPORTANCE OF IS - BUSINESS PERSPECTIVE/PROCESS

1.16 INFORMATION SYSTEM TO SOLVE MANAGEMENT ISSUES

MISCELLANEOUS

1.17 ANALYZING & IMPROVING EXISTING BUSINESS STRATEGY

1.18 IMPROVING DECISION MAKING USING GATHERED INFORMATION

1.19 INFORMATION SYSTEM STRUCTURE MODEL

1.20 RISK MANAGEMENT

1.21 BUSINESS CONTINUITY & PLANNING

1.22 DISASTER RECOVERY

Chapter -2 Information Security & Network Vulnerabilities

ACCESS CONTROL TECHNIQUES

2.1 WHAT IS ACCESS CONTROL ? [VIDEO]

2.2 REQUIREMENT OF ACCESS CONTROL

2.3 ACCESS CONTROL TECHNIQUE

ACCOUNT ADMINISTRATION

2.4 CREATING NEW ACCOUNTS

2.5 ACCOUNT MAINTENANCE

2.6 ACCOUNT, LOG, AND JOURNAL MONITORING

2.7 ACCESS RIGHTS AND PERMISSIONS

ACCOUNT ACCESSIBILITY

2.8 IDENTIFICATION

2.9 AUTHENTICATION

2.10 AUTHORIZATION

AUTHENTICATION TECHNIQUES

2.11 PASSWORD

2.12 BIOMETRICS

2.13 RFID CARD

2.14 TOKEN

NETWORKING & TYPES

2.15 WHAT IS NETWORKING AND ITS BENEFITS?

2.16 TYPES OF NETWORK

ISO MODEL

2.17 LAYERS OF OSI MODEL

2.18 THE OSI MODEL FOR NETWORKING

NETWORKING DEVICES & TOPOLOGIES

2.19 NETWORK DEVICES

2.20 NETWORK TOPOLOGY

IP ADDRESS

2.21 WHAT IS IP ADDRESS?

2.22 PUBLIC AND PRIVATE IP ADDRESSES

MAC ADDRESS & PORTS

2.23 PORTS & SERVICES

2.24 HOW TO FIND OPEN PORTS ON YOUR OWN SYSTEM

2.25 WHAT IS MAC ADDRESS?

2.26 HOW TO FIND MAC ADDRESS IN WINDOWS AND LINUX?

DNS & DHCP SERVER

2.27 DNS & DHCP SERVER

NETWORK VULNERABILITIES & TYPES OF ATTACKS

2.28 WHAT IS VULNERABILITY?

2.29 TYPES OF NETWORK VULNERABILITIES AND THEIR EFFECTS

2.30 LIST OF TOOLS

2.31 TYPES OF ATTACKS

2.32 COUNTERMEASURE FOR NETWORK VULNERABILITIES AND NETWORK ATTACKS

Chapter -3 Foundation of Cybersecurity

HACKING

3.1 DEFINE HACKING [VIDEO]

3.2 HACKING VS ETHICAL HACKING

3.3 UNDERSTANDING THE PURPOSE OF ETHICAL HACKING

3.4 TYPES OF HACKERS

3.5 WHAT DO ETHICAL HACKERS DO?

3.6 GOALS ATTACKERS TRY TO ACHIEVE

THE PHASE OF ETHICAL HACKING

3.7 INFORMATION GATHERING

3.8 SCANNING

3.9 GAINING ACCESS

3.10 MAINTAINING ACCESS

3.11 COVERING TRACKS

TESTING, CYBER WARFARE & CYBER TERRORISM

3.12 WHITE BOX TESTING

3.13 GRAY BOX TESTING

3.14 BLACK BOX TESTING

3.15 CYBERWARFARE AND CYBERTERRORISM

3.16 EFFECTS OF CYBERWARFARE & CYBERTERRORISM

3.17 PREVENTION OF CYBERWARFARE & CYBERTERRORISM

3.18 DISSECTING CYBER RISK

3.19 CYBERSECURITY THREATS

SECURITY IMPLEMENTATION

3.20 SECURITY IMPLEMENTATION

IT GOVERNANCE & MANAGEMENT FRAMEWORKS (COBIT 5 & DSS05)

3.21 IT GOVERNANCE & MANAGEMENT FRAMEWORKS (COBIT 5 & DSS05)

INCIDENT HANDLING & MANAGEMENT

3.22 INCIDENT HANDLING & MANAGEMENT

GOVERNMENT ROLE IN CYBERSECURITY

3.23 GOVERNMENT ROLE IN CYBERSECURITY

ENTERPRISE CYBERSECURITY STRATEGY

3.24 ENTERPRISE CYBERSECURITY STRATEGY

Chapter -4 BYOD & SMAC Security

SMAC

4.1 INTRODUCTION TO SMAC [VIDEO]

4.2 OBJECTIVES

4.3 SOCIAL

4.4 SMAC- MOBILE

4.5 SMAC- ANALYTICS

4.6 SMAC- CLOUD

4.7 SMAC BENEFITS AND IMPORTANCE

4.8 CHALLENGE AND SOLUTIONS

4.9 SMAC IMPLEMENTATION

4.10 SMARTPHONE FORENSIC AND BACKUPS

BYOD

4.11 WHAT IS BYOD?

4.12 NEW TRENDS

4.13 BYOD IN ENTERPRISE

4.14 ADVANTAGE

4.15 DISADVANTAGE

4.16 POLICY AND STANDARD FOR BYOD

4.17 BYOD SECURITY CHALLENGES AND MITIGATION STRATEGY

4.18 COMMON PRACTICE FOR BYOD

4.19 BYOD SECURITY & POLICIES

Chapter -5 Preventing Cyber Intrusion

PREVENTING CYBER INTRUSION

5.1 WHAT IS CYBER ATTACK ? [VIDEO]

5.2 CYBER ATTACK RESPONSE PLAN

5.3 COMPLIANCE PLAN AGAINST CYBER ATTACK

5.4 TECHNOLOGY FOR PREVENTING CYBER INTRUSION

Chapter -6 Evaluating Emerging Cybersecurity Technology

EVALUATING EMERGING CYBERSECURITY TECHNOLOGY

6.1 EVALUATING EMERGING CYBERSECURITY TECHNOLOGY INTRODUCTION [VIDEO]

6.2 CHANGING TRENDS IN CYBERSECURITY

6.3 SOCIAL MEDIA ROLE IN CYBERSECURITY

6.4 CYBERSECURITY TECHNIQUES

6.5 CYBER ETHICS

Chapter -7 Physical & Human Security Management

PHYSICAL SECURITY

7.1 INTRODUCTION OF "PHYSICAL SECURITY" [VIDEO]

7.2 NEEDS OF PHYSICAL SECURITY

7.3 COMMON PHYSICAL SECURITY THREATS

7.4 PLANNING & EXECUTING PHYSICAL SECURITY TEST

7.5 PHYSICAL SECURITY CHECKLIST

7.6 WIRELESS NETWORK SECURITY

7.7 HARDWARE THEFT (LAPTOP/HARD DISK/CD/DVD/USB DRIVES)

7.8 LOCKS PICKING

HUMAN SECURITY MANAGEMENT

7.9 INTRODUCTION TO "HUMAN SECURITY"

7.10 COMMON HUMAN SECURITY THREATS

7.11 SOCIAL ENGINEERING TECHNIQUES

7.12 DUMPSTER DIVING & SHOULDER SURFING TECHNIQUES

7.13 PHISHING ATTACK & COUNTERMEASURE

7.14 COUNTERMEASURE-EMPLOYEE & STAFF TRAINING

Chapter -8 Cybersecurity Essentials for Leaders

PLANNING & MANAGING ENTERPRISE INFORMATION SYSTEM

8.1 PLANNING INFORMATION SYSTEM & PROJECTS [VIDEO]

8.2 BUDGET MANAGEMENT

8.3 MANAGING NETWORK INFRASTRUCTURE & COMPUTER SYSTEM

PLANNING & MANAGING ENTERPRISES NETWORK STRUCTURE

8.4 MANAGING NETWORK ADDRESSING & IP ADDRESSES

8.5 VULNERABILITY MANAGEMENT

PLANNING & MANAGING ENTERPRISES NETWORK STRUCTURE

8.6 COMMON ATTACKS AGAINST ENTERPRISE

8.7 PLANNING DEFENSE AGAINST ATTACKS

8.8 PLANNING & MANAGING ACCESS CONTROL AND PASSWORD POLICY

PLANNING & MANAGING ENTERPRISE INFORMATION SECURITY

8.9 SECURE COMMUNICATION & INFORMATION TRADE

8.10 CRYPTOGRAPHY & STEGANOGRAPHY

8.11 PRIVACY MANAGEMENT

8.12 IDENTITY AND ACCESS MANAGEMENT

PLANNING & MANAGING SECURITY ASSESSMENT AND TESTING

8.13 PLANNING PENETRATION TESTING & SECURITY AUDITS

8.14 MANAGING SECURITY POLICY

8.15 PLANNING INCIDENT HANDLING

8.16 IT RISK MANAGEMENT

8.17 DISASTER RECOVERY/CONTINGENCY PLANNING

Chapter -9 Cyber Incident Analysis and Response

CYBER INCIDENT ANALYSIS AND RESPONSE

9.1 UNDERSTANDING CYBERSECURITY INCIDENT AND RISK [VIDEO]

9.2 EFFECTS OF CYBERSECURITY INCIDENT ON ORGANIZATION

9.3 CHALLENGES IN FACING CYBERSECURITY INCIDENT

9.4 PLANNING & PREPARING FOR CYBER INCIDENT

9.5 PLANNING CYBERSECURITY INCIDENT RESPONSE

9.6 PLANNING RISK MANAGEMENT

9.7 DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

9.8 CYBER INCIDENT FOLLOW-UP

Chapter -10 Building Secure Enterprises & Organizations

BUILDING SECURE ENTERPRISES & ORGANIZATIONS

10.1 INTRODUCTION OF BUILDING SECURE ENTERPRISES & ORGANIZATIONS [VIDEO]

10.2 WHAT IS AN ENTERPRISE & ORGANIZATIONS SECURITY

10.3 IMPORTANCE OF ENTERPRISE & ORGANIZATIONS SECURITY

10.4 SCOPE AND APPROACH

10.5 IDENTIFY THE BUSINESS GOALS ASSOCIATED WITH THE SECURITY FOCUS

10.6 PERFORM AND DOCUMENT A BASELINE ANALYSIS AND EVALUATE THE DESIRED STATE

10.7 PRIORITIZE AND GENERATE PLANS TO ADDRESS GAPS AND FUTURE DEVELOPMENTS

10.8 POLICY AND PROCEDURES

Chapter -11 Cybersecurity Project Management

CYBERSECURITY PROJECT MANAGEMENT

11.1 INTRODUCTION OF CYBERSECURITY PROJECT MANAGEMENT [VIDEO]

11.2 IMPORTANT FACTORS FOR SUCCESSFUL CYBERSECURITY PROGRAMS

11.3 FRAMEWORK FOR CYBERSECURITY PROGRAMS

11.4 USAGE OF FRAMEWORK

11.5 IMPLEMENTATION OF FRAMEWORK

11.6 IMPORTANCE OF CYBERSECURITY PROJECT MANAGEMENT

11.7 CONCLUSIONS OF CYBERSECURITY PROJECT MANAGEMENT

Chapter -12 EXAM



EXAM



Exam - CCYT



Certificate-CCYT



Not available unless: You achieve a required score in Exam - CCYT