# Cyber Security Foundation Professional Certificate CSFPC™

## Syllabus V062022

## Content

Recover
Sample Recover Activities
Framework
Everyday Tips
Resources

**Module 1: CyBOK – Cyber Security Fundamentals**

Cyber Security Definition
CyBOK Knowledge Areas
Deploying CyBOK Knowledge To Address Security Issues
Functions Within A Security Management System
Principles
Crosscutting Themes
Cyberspace

**Module 2: Risk Management & Governance**

Topics Covered in this Lesson
What is Risk?
Why is risk assessment and management important?
What is cyber risk assessment and management?
Risk Governance
The Human Factor and Risk Communication
Security Culture and Awareness
Enacting Security Policy
Risk Assessment and Management Principles
Element of Risk
Risk Assessment and Management Methods
Component-driven Cyber Risk Management Frameworks
System-driven Cyber Risk Management Methods
Risk Assessment and Management In Cyber-physical Systems and Operational Technology
Security Metrics
What constitutes Good and Bad metrics?
Business Continuity
ISO/IEC 27035-1:2016
NCSC- ISO/IEC 27035
Conclusion

**Module 3: Law and Regulation**

Introduction
Challenges
Response
Out of Scope

Introductory Principles of Law and Legal Research
"To Prove" Something
"Standards" of Proofs
Applying Law to Cyberspace and Information Technologies
Distinguishing Criminal and Civil Law
Jurisdiction
A Taxonomy of Jurisdiction
Prescriptive Jurisdiction
Enforcement Jurisdiction
The Data Sovereignty Problem
Privacy Laws in General and Electronic Interception
State Interception (Lawful Access)
Non-state Interception
Data Protection
The "Players"
What is regulated?
"Personal Data" vs "PII"
Data Protection Highlights
Computer Crime
Crimes Against Information Systems
Recurring Challenges
Contract
Contract as Means to Encourage Security Behaviours
Limits of Influence
Relative Influence of Contract Over Security Behaviours
Breach of Contract & Remedies
Tort
Tort Examples
Negligence (Fault Based Liability)
Product Liability (Strict Liability)
Quantum of Loss (QQ)
Attributing and Apportioning Liability
Intellectual Property
Reverse Engineering
Internet Intermediaries Shields from Liability and Take-down Procedures
Dematerialization of Documents and Electronic Trust Services
Legal Challenges Emerge
Other Regulatory Matters
Public International Law

State Attribution
Limiting Operations
Ethics
Codes of Conduct
Vulnerability Testing and Disclosure
Legal Risk Management

**Module 4: Human Factors**

Introduction
Human Factors
Security Has to be Usable
Fitting the Task to the Human
Human Capabilities and Limitations
STM and One-time password (OTPs)
General Human Capabilities and Limitations
CAPTCHA
Goals and Tasks
Capabilities and Limitations of the Device
Human Error
Latent Design Conditions
Awareness and Education
What usability issues do developers face?
Developers are not the Enemy! The Need for Usable Security APIs
Usability Smells: An Analysis of Developers' Struggle With Crypto Libraries

**Module 5: Privacy & Online Rights**

Introduction
Overview
Privacy as Confidentiality
What is the problem?
What is privacy?
Defining Privacy
Privacy as…
Privacy as Transparency
Privacy as Control
Limits of Control and Transparency
Privacy as Confidentiality
Privacy Threat Landscape
Formal Approach to Inference Control
Privacy as Confidentiality
Data Confidentiality

Metadata Confidentiality
Privacy as Control
Privacy as Transparency
Privacy Technologies
Privacy Engineering
Privacy Evaluation
Conclusions

**Module 6: Malware & Attack Technologiesv**

Introduction
Malware
A Taxonomy of Malware
Malware Taxonomy: Dimensions
Taxonomy: Examples
Potentially Unwanted Programs (PUPs)
Malicious Activities by Malware
The Cyber Kill Chain
The Cyber Kill Chain Model
Underground Eco-system
Action Objectives
Malware Analysis
Acquiring Malware Data
Static Analysis
Other Analysis Techniques
Analysis Environments
Common Environments
Safety and Live-Environments
Anti-Analysis and Evasion Techniques
Malware Detection
Evasion and Countermeasures
Detection of Malware Attacks
ML-based Security Analytics
ML-based Malware Detection
Evasion of ML-based Malware Detection
Concept Drift
Malware Response
Disrupt Malware Operations
Attribution
Evasion and Countermeasures
Conclusion

**Module 7: Adversarial Behaviour**

- Introduction
- A Characterization of Adversaries
- Interpersonal Offenders
- Cyber-enabled Organized Criminals
- Cyber-dependent Organized Criminals
- Hacktivists
- State Actors
- The Elements of a Malicious Operation
- Specialized Services
- Human Services
- Payment Methods
- Models to Understand Malicious Operations
- Attack Trees : Example of an Attack
- Cyber Kill Chain
- Environmental Criminology
- Attack Attribution

**Module 8: Security Operations & Incident Management**

- Introduction
- What is it about?
- Timeline and Scope
- Overall MAPE-K loop
- Components of MAPE-K Monitor-Analyse-Plan-Execute
- Deployment of SOIM Technologies
- Architectural Principles Typical Architecture
- Intrusion Detection and Prevention Systems
- MONITOR: Data sources
- Network Data Sources: Possible Detections
- Application Data Sources
- System Data Sources
- Syslog
- Frequent Data Sources Issues
- Analysis of Traces
- From Event to Incident
- Misuse Detection
- Anomaly Detection
- General Intrusion Detection Issues
- Typical Architecture Security Information and Event Managementures
- Data Collection in SIEMs

Alert Correlation
Mitigations and Countermeasures Tools and Techniques
Intelligence and Analytics
Incident Management Lifecycle
Conclusion

**Module 9: Certification Exam**

Badge
Exam Conditions