Programme/Module Outline

Programme/Module Title:	Advanced Certificate for ECF on Cybersecurity
QF Level:	4
QF Credit:	20 (9 or 15 contact hours, 188.5 or 182.5 self-study hours and 2.5 examination hours)
Teaching/Training Activities:	Training Class
Pre-requisite:	Nil

Programme/Module Objective:

This programme/module has been developed with the aim to nurture a sustainable talent pool of cybersecurity practitioners for the banking industry. Candidates will learn the technical foundation of cybersecurity and the cybersecurity controls used in the banking environment. Also, candidates will be equipped with the essential knowledge and tools to gain a better understanding of computer security vulnerabilities and typical security pitfalls, enabling them to identify potential security threats and apply early intervention to common cybersecurity problems.

Programme/Module Intended Learning Outcome (PILO/MILO) & Unit of Competency (UoC)

Upon completion of the Programme/Module, learners should be able to:

PILO/MILO1:	Describe the foundation of various network protocols and their hierarchical relationship in hardware and software.	• 107405L5 • 107408L4 • 107409L4 • 107426L4 • 107427L4 • 106721L4
PILO/MILO 2:	Apply the principles and knowledge of international standards to enhance network and system security.	
PILO/MILO 3:	Apply cybersecurity related monitoring measures for managing different types of cybersecurity threats.	
PILO/MILO 4:	Conduct a security incident response process and present an analysis of the results for management's review.	
PILO/MILO 5:	Assess security risks in the cyber environment and IT systems by applying the IT Risk Management and Control principles.	
PILO/MILO 6:	Conduct IT audits and security testing to assess cybersecurity risk protection.	

Assessment Activity

Type of Assessment Activity	PILO/MILO	Weighting (%)
Examination	PILO/MILO 1-6	100

Examination Format and Duration

Time allowed: 2.5 hours

The examination consists of 80 multiple choice questions

Passing mark for this subject is 70%

Syllabus

Chapter 1: Technical Foundation of Cybersecurity	
1	**Foundation of a Network**
1.1	- OSI and TCP/IP Model
1.2	- LAN and WAN Technologies and Devices
1.3	- An Overview of Internet Architecture
1.4	- Firewalls and Proxy
1.5	- Intrusion Detection System and Intrusion Prevention System
1.6	- Common Network Protocols
1.7	- Common Network Attacks
1.8	- DMZ and Network Segmentation
1.9	- Wireless Network Infrastructure
2	**IT Security Principles**
2.1	- Confidentiality, Integrity, Availability
2.2	- Accountability, Non-repudiation
2.3	- Types of Security Controls
2.4	- Least Privilege
2.5	- Segregation of Duties
2.6	- IT Asset Management
3	**Foundation of Access Control**
3.1	- Access Control Concepts
3.2	- Identification, Authentication, Authorisation
3.3	- Identity and Access Management
3.4	- Common Access Control Implementation

4	**Foundation of Cryptography**
4.1	- Hashing
4.2	- Salting
4.3	- Symmetric/Asymmetric Encryption
4.4	- Digital Signatures
4.5	- Cryptographic Key Management
4.6	- Blockchain
5	**Foundation of Cloud Computing**
5.1	- Virtualisation
5.2	- Infrastructure as a Service, Software as a Service and Platform as a Service
5.3	- Private Cloud and Hybrid Cloud
5.4	- Data Governance on Cloud Computing
5.5	- Concerns about Jurisdiction
6	**Open Banking with API Framework**
6.1	- The Readiness of Open API Adoption
6.2	- Threats to Open Banking APIs
Chapter 2: Bank IT Security Controls	
1	**International Standards and Regulatory Requirements**
1.1	- ISO 27001 Principles and Process
1.2	- ISO 27002 Control Objectives
1.3	- HKMA Technology Risk Management and Cybersecurity Fortification Initiatives
1.4	- Well-known International Security Organizations
2	**Network Security Administration**
2.1	- Firewalls and Proxy
2.2	- Intrusion Detection System and Intrusion Prevention System
2.3	- Understanding Wireless Security
2.4	- Protecting the Network Infrastructure
2.5	- Protecting the Network Management Platform
2.6	- Network Vulnerability Management and Patch Management
2.7	- Mobile Commerce Security

3	**System Security Administration**
3.1	- Database Security
3.2	- System Hardening
3.3	- Sandboxing
3.4	- Application Whitelisting
3.5	- Virtual Desktop
Chapter 3: Cybersecurity Monitoring	
1	**Malware and Malicious Activities**
1.1	- Malware
1.2	- Rootkits
1.3	- Botnets
1.4	- Advanced Persistent Threat (APT)
1.5	- Fileless Malware
1.6	- Distributed Denial of Service Attack (DDoS)
2	**Malware Infection Vectors**
2.1	- Social Engineering
2.2	- Spam, Phishing, Spear-phishing
2.3	- Social Networks
2.4	- Physical Media
2.5	- Software Vulnerability
2.6	- Zero-day Vulnerability
3	**Network Monitoring**
3.1	- Log Files and Log Management
3.2	- Security Event and Detection Mechanisms
3.3	- Monitoring Tools
3.4	- Monitoring of Wireless Attacks
4	**Analysis**
4.1	- SIEM Architecture and Components
4.2	- Correlation Rules
4.3	- Detection of Malicious Activities
4.4	- Cybersecurity Labs

Chapter 4: Security Incident Response	
1	**Security Incident Response Process**
1.1	- Containment
1.2	- Eradication
1.3	- Recovery
1.4	- Improvement
1.5	- ISO 27043 Incident Investigation Principles and Processes
2	**Digital Evidence**
2.1	- First Responder
2.2	- Evidence Handling
2.3	- Preservation of the Scene
2.4	- Evidence Related to Network Events
3	**Security Incident Communication**
3.1	- Internal Communication
3.2	- Preparing Management Reports
3.3	- Cyber Intelligence
3.4	- Communication between Banks and Other Parties
Chapter 5: Technology Risk Management and Control	
1	**Risk Management Process**
1.1	- Risk Management Concepts
1.2	- Risk Assessment
1.3	- Risk Treatment (Accept, Transfer, Mitigate, Avoid)
2	**Risk Monitoring and Compliance Checking**
2.1	- Risk Visibility
2.2	- Risk Register and Risk Dashboard
2.3	- Compliance Self-assessments
3	**Risk Acceptance**
3.1	- Risk Ownership
3.2	- Risk Acceptance Process
4	**Security and Risk Awareness Training**

Chapter 6: IT Audit	
1	**Principles of IT Audit**
1.1	- Audit Organization Functions
1.2	- Independence
1.3	- Audit Trail
1.4	- IT Audit
2	**Security and Compliance Control Testing**
2.1	- Major Steps in IT Audit
2.2	- Sampling
2.3	- Walkthrough and Control Verification
2.4	- Cybersecurity Audit
3	**Audit Reports and Follow Up**
3.1	- Audit Report
3.2	- Root Cause Analysis
Chapter 7: Security Test	
1	**Penetration Test Principles**
1.1	- Functions of Penetration Tests
1.2	- Types of Penetration Tests
2	**Penetration Test Process**
2.1	- Test Preparations
2.2	- Vulnerability Scanning and Assessment
2.3	- Network Penetration Test
2.4	- Application Penetration Test
2.5	- Common Vulnerabilities and Exposures (CVE)
3	**Red Team Approach**
3.1	- Red Team Testing Approach

Recommended Readings

Essential Readings:

HKIB Study Guide – Advanced Certificate for ECF on Cybersecurity (2020).

Supplementary Readings:

1. Josiah Dykstra (2015). Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems, "O'Reilly Media, Inc."
2. Vacca, J. (Ed.). (2013). Computer and Information Security Handbook, Second Edition. Morgan Kaufmann.
3. European Union Agency for Network and Information Security (ENISA). (2017). Cyber Security Culture in organisations ENISA. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
4. Cole, E. (2013). Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Syngress Publishing.
5. Michael S. Collins (2016) Network Security Through Data Analysis: Building Situational Awareness, 2nd Edition. "O'Reilly Media, Inc."
6. Federal Office for Information Security. (n.d.). A Penetration Testing Model. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf
7. Hong Kong Monetary Authority. (2016). Cyber Resilience Assessment Framework. Retrieved from http://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf
8. HKCERT
   https://www.hkcert.org/faq
9. CIS – Center of Internet security
   https://www.cisecurity.org/cybersecurity-best-practices
10. GovCERT
    https://www.govcert.gov.hk/en/index.html
11. Cybersechub
    https://www.cybersechub.hk/en/home/cert
12. HK Police CSTCB
    https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/index.html
13. HKIB e-learning course: Cybersecurity Essentials
    https://secure.kesdee.com/ksdlms/?Partner=HKIB

Further Readings:

For Chapter 1:

1. Schneier, B. (1993). Applied Cryptography. John Wiley & Sons Inc.
2. Jonathan Katz, Yehuda Lindell, CRC Press. (2007). Introduction to Modern Cryptography: Principles and Protocols
3. Kavis, M. J. (2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Wiley.

For Chapter 2:

1. BackTrack 5 Wireless Penetration Testing by V. Ramachandran, published in September 2011 by Packet Publishing
2. Australian Signals Directorate. (2018). Protect: Implementing Application Whitelisting. Retrieved from https://www.asd.gov.au/publications/protect/application_whitelisting.htm
3. Vacca , J. (Ed.). (2013). Computer and Information Security Handbook, Second Edition . Morgan Kaufmann.

For Chapter 3:

1. The Art of Deception: Controlling the Human Element of Security by Kevin D. Mitnick and William L. Simon, published in 2002 by John Wiley & Sons.
2. Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization by Eric Cole, published in 2013 by Syngress Publishing.
3. Applied Network Security Monitoring: Collection, Detection, and Analysis, by Chris Sanders and Jason Smith, published in 2014 by Syngress Publishing.

For Chapter 4:

1. Schultz, E. E. J., & Shumway, R. (2001). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Sams Publishing.
2. Johansen, G. T. (2017). Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing.
3. Anatomy of a Breach, Microsoft. (2016)

For Chapter 5:

1. Hoo, K. J. (2000). How Much Is Enough? A Risk-Management Approach to Computer Security. US: Consortium for Research on Information Security and Policy.
2. General Principles for Technology Risk Management. (2003). HK: HKMA.
3. Joint Task Force Transformation Initiative (Ed.). (2012). Guide for Conducting Risk Assessments. HK: National Institute of Standards and Technology (NIST).
4. COBIT 5, ISACA

5. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
6. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems requirements
7. Trull, J. C. C. (2016, October 16). Use Security Education and Awareness Programs to Your Advantage. Available from: https://cloudblogs.microsoft.com/microsoftsecure/2016/10/26/use-security-education-and-awareness-programs-to-your-advantage/

For Chapter 6:

1. Leveraging COSO across the Three Lines of Defense. The Institute of Internal Auditors (2015).
2. Moeller, R. (Ed.). (2010). IT Audit, Control, and Security. Wiley.
3. National Institute of Standards and Technology. (2018). Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework

For Chapter 7:

1. Scarfone, K., Souppaya, M., Orebaugh, Angela, & Cody, A. (2008). Technical Guide to Information Security Testing and Assessment. NIST.
2. Shrestha, N. (2012). Security Assessment via Penetration Testing: A Network and System Administrator’s Approach. UNIVERSITY OF OSLO.