

# Module Outline

# ECF on Cybersecurity (Cybersecurity)

Benchmarked HKQF Level:	4
No. of Credits:	20
Total Notional Learning Hours:	200
a) Class contact hours:	15 hours (3-hour per session x 5)
b) Self-study hours:	182.5 hours
c) Assessment hours:	2.5 hours
Pre-requisite:	NA

## Module Objective

The 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.

## Module Intended Outcomes (MIOs) and Units of Competencies (UoCs)

l	Upon	comp	letion	of the	Modul	e, canc	lidates	should	d be	able	e to:	
-												

MIOs	Intended Outcomes / Competence	*Unit of Competencies (UoCs)
MIO-1	Describe the foundation of various network protocols	107408L4
	and their hierarchical relationship in hardware and	107409L4
	software.	107426L4
MIO-2	Apply the principles and knowledge of international	107427L4 / 109375L4
	standards to enhance network and system security.	109303L4
MIO-3	Apply cybersecurity related monitoring measures for	109391L5
	managing different types of cybersecurity threats.	
MIO-4	Conduct a security incident response process and	
	present an analysis of the results for management's	
	review.	
MIO-5	Assess security risks in the cyber environment and	
	IT systems by applying the IT Risk Management and	
	Control principles.	
MIO-6	Conduct IT audits and security testing to assess	
	cybersecurity risk protection.	



CERTIFIED BANKER

\*Note: For the details of the UoCs, please refer to the Specification of Competency Standards (SCS) of <u>Retail Banking</u> and <u>Corporate & Commercial Banking</u> which were developed by HKCAAVQ.

### Assessment

Examination duration:	2.5 hours
Examination format:	Multiple Choice Questions (MCQ) with 80 questions
Pass mark:	70%

## Syllabus

Chapter	Chapter 1: Technical Foundation of Cybersecurity		
1.1	Importance of Cybersecurity in the Banking Industry		
1.1.1	- Cybersecurity applied in the banking industry		
1.1.2	- Importance of Cybersecurity on the operation of a bank		
1.2	Foundation of a Network		
1.2.1	- OSI and TCP/IP Model		
1.2.2	- An Overview of Internet Architecture		
1.3	IT Security Principles		
1.3.1	- Confidentiality, Integrity, Availability		
1.3.2	- Accountability, Non-repudiation		
1.3.3	- Types of Security Controls		
1.3.4	- Least Privilege		
1.3.5	- Segregation of Duties		
1.3.6	- IT Asset Management		
1.4	Foundation of Access Control		
1.4.1	- Access Control Concepts		
1.4.2	- Identification, Authentication, Authorisation		
1.4.3	- Identity and Access Management		
1.4.4	- Common Access Control Implementation		
1.5	Foundation of Cryptography		
1.5.1	- Hashing		
1.5.2	- Salting		



1.5.3	- Symmetric/Asymmetric Encryption
1.5.4	- Digital Signatures
1.5.5	- Cryptographic Key Management
1.6	Foundation of Cloud Computing
1.6.1	- Virtualisation
1.6.2	- Infrastructure as a Service, Software as a Service and Platform as a Service
1.6.3	- Cloud Computing Strategy
1.6.4	- Data Governance on Cloud Computing
1.6.5	- Concerns about Jurisdiction
1.6.6	- Major Cloud Security Considerations
1.6.7	- Guidance on Cloud Computing
Chapter	2: Bank IT Security Controls
2.1	International Standards and Regulatory Requirements
2.1.1	- ISO 27001 Principles and Process
2.1.2	- ISO 27002 Control Objectives
2.1.3	- HKMA Technology Risk Management and Cybersecurity Fortification Initiatives
2.1.4	- Well-known International Security Organizations
2.2	Network Security Administration
2.2.1	- Common Network Protocols
2.2.2	- Common Network Attacks
2.2.3	- DMZ and Network Segmentation
2.2.4	- Wireless Network Infrastructure
2.2.5	- Firewalls and Proxy
2.2.6	- Intrusion Detection System and Intrusion Prevention System
2.2.7	- Understanding Wireless Security
2.2.8	- Protecting the Network Infrastructure
2.2.9	- Protecting the Network Management Platform
2.2.10	- Network Vulnerability Management and Patch Management
2.2.11	- Mobile Commerce Security
2.3	System Security Administration
231	
2.5.1	- Database Security

Certified Banker





2.3.3   - Sandboxing     2.3.4   - Application Whitelisting     2.3.5   - Virtual Desktop     Chapter 3: Cybersecurity Monitoring     3.1   Malware and Malicious Activities     3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Security Event and Detection Mechanisms     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   -	2.3.2	- System Hardening
2.3.4   - Application Whitelisting     2.3.5   - Virtual Desktop     Chapter 3: Cybersecurity Monitoring     3.1   Malware and Malicious Activities     3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Security Event and Detection Mechanisms     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring ools     3.3.4   - Endpoint Detection and Response     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1	2.3.3	- Sandboxing
2.3.5   - Virtual Desktop     Chapter 3: Cybersecurity Monitoring     3.1   Malware and Malicious Activities     3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Social Networks     3.2.8   - Zero-day Vulnerability     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring Of Wireless Attacks     3.4   Endpoint Detection and Response     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis <td>2.3.4</td> <td>- Application Whitelisting</td>	2.3.4	- Application Whitelisting
Chapter 3: Cybersecurity Monitoring     3.1   Malware and Malicious Activities     3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Security Event and Detection Mechanisms     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring Of Wireless Attacks     3.4   - Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2	2.3.5	- Virtual Desktop
3.1   Malware and Malicious Activities     3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Security Event and Detection Mechanisms     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3	Chapter	3: Cybersecurity Monitoring
3.1.1   - Malware     3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS) <b>3.2</b> Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Security Event and Detection Mechanisms     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1	Malware and Malicious Activities
3.1.2   - Rootkits     3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS) <b>3.2</b> Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   - Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.1	- Malware
3.1.3   - Botnets     3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring     3.4.1   - Endpoint Monitoring     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.2	- Rootkits
3.1.4   - Advanced Persistent Threat (APT)     3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Social Log Management     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.3	- Botnets
3.1.5   - Fileless Malware     3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.4	- Advanced Persistent Threat (APT)
3.1.6   - Distributed Denial of Service Attack (DDoS)     3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Detection and Response     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.5	- Fileless Malware
3.2   Malware Infection Vectors     3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.2.7   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.1.6	- Distributed Denial of Service Attack (DDoS)
3.2.1   - Social Engineering     3.2.2   - Spam, Phishing, Spear-phishing     3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.2	Malware Infection Vectors
3.2.2Spam, Phishing, Spear-phishing3.2.3Social Networks3.2.4Physical Media3.2.5Software Vulnerability3.2.6Zero-day Vulnerability3.3Network Monitoring3.3.1Log Files and Log Management3.3.2Security Event and Detection Mechanisms3.3.3Monitoring Tools3.3.4Monitoring of Wireless Attacks3.4Endpoint Monitoring3.4.1Endpoint Detection and Response3.4.2EDR Key Functions3.5.1SIEM Architecture and Components3.5.2Correlation Rules3.5.3Detection of Malicious Activities	3.2.1	- Social Engineering
3.2.3   - Social Networks     3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.2.2	- Spam, Phishing, Spear-phishing
3.2.4   - Physical Media     3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.2.3	- Social Networks
3.2.5   - Software Vulnerability     3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.2.4	- Physical Media
3.2.6   - Zero-day Vulnerability     3.3   Network Monitoring     3.3.1   - Log Files and Log Management     3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.2.5	- Software Vulnerability
3.3Network Monitoring3.3.1- Log Files and Log Management3.3.2- Security Event and Detection Mechanisms3.3.3- Monitoring Tools3.3.4- Monitoring of Wireless Attacks3.4Endpoint Monitoring3.4.1- Endpoint Detection and Response3.4.2- EDR Key Functions3.5Analysis3.5.1- SIEM Architecture and Components3.5.2- Correlation Rules3.5.3- Detection of Malicious Activities	3.2.6	- Zero-day Vulnerability
3.3.1- Log Files and Log Management3.3.2- Security Event and Detection Mechanisms3.3.3- Monitoring Tools3.3.4- Monitoring of Wireless Attacks3.4Endpoint Monitoring3.4.1- Endpoint Detection and Response3.4.2- EDR Key Functions3.5Analysis3.5.1- SIEM Architecture and Components3.5.2- Correlation Rules3.5.3- Detection of Malicious Activities	3.3	Network Monitoring
3.3.2   - Security Event and Detection Mechanisms     3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.3.1	- Log Files and Log Management
3.3.3   - Monitoring Tools     3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.3.2	- Security Event and Detection Mechanisms
3.3.4   - Monitoring of Wireless Attacks     3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.3.3	- Monitoring Tools
3.4   Endpoint Monitoring     3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.3.4	- Monitoring of Wireless Attacks
3.4.1   - Endpoint Detection and Response     3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.4	Endpoint Monitoring
3.4.2   - EDR Key Functions     3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.4.1	- Endpoint Detection and Response
3.5   Analysis     3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.4.2	- EDR Key Functions
3.5.1   - SIEM Architecture and Components     3.5.2   - Correlation Rules     3.5.3   - Detection of Malicious Activities	3.5	Analysis
3.5.2 - Correlation Rules   3.5.3 - Detection of Malicious Activities	3.5.1	- SIEM Architecture and Components
3.5.3 - Detection of Malicious Activities	3.5.2	- Correlation Rules
	3.5.3	- Detection of Malicious Activities





3.5.4	- Cybersecurity Labs
Chapter	4: Security Incident Response
4.1	Security Incident Response Process
4.1.1	- Containment
4.1.2	- Eradication
4.1.3	- Recovery
4.1.4	- Improvement
4.1.5	- ISO 27043 Incident Investigation Principles and Processes
4.2	Digital Evidence
4.2.1	- First Responder
4.2.2	- Evidence Handling
4.2.3	- Preservation of the Scene
4.2.4	- Evidence Related to Network Events
4.3	Security Incident Communication
4.3.1	- Internal Communication
4.3.2	- Preparing Management Reports
4.3.3	- Cyber Intelligence
4.3.4	- Communication between Banks and Other Parties
Chapter	5: Technology Risk Management and Control
5.1	Risk Management Process
5.1.1	- Risk Management Concepts
5.1.2	- Risk Assessment
5.1.3	- Risk Treatment (Accept, Transfer, Mitigate, Avoid)
5.2	Risk Monitoring and Compliance Checking
5.2.1	- Risk Register and Risk Dashboard
5.2.2	- Compliance Self-assessments
5.3	Risk Acceptance
5.3.1	- Risk Ownership
5.3.2	- Risk Acceptance Process
5.4	Third Party Risk Management
5.5	Security and Risk Awareness Training





Chapter 6: IT Audit		
6.1	Principles of IT Audit	
6.1.1	- Audit Organization Functions	
6.1.2	- IT Audit	
6.2	Security and Compliance Control Testing	
6.2.1	- Major Steps in IT Audit	
6.2.2	- Walkthrough and Control Verification	
6.2.3	- Cybersecurity Audit	
6.3	Audit Reports and Follow-Up	
6.3.1	- Audit Report	
Chapter	7: Security Test	
7.1	Penetration Test Principles	
7.1.1	- Functions of Penetration Tests	
7.1.2	- Types of Penetration Tests	
7.1.3	- Cyber Attack Simulation Testing	
7.2	Penetration Test Process	
7.2.1	- Test Preparations	
7.2.2	- Vulnerability Scanning and Assessment	
7.2.3	- Network Penetration Test	
7.2.4	- Application Penetration Test	
7.2.5	- Common Vulnerabilities and Exposures (CVE)	
7.2.6	- Lateral Movement	
7.2.7	- Adversarial Tactics, Techniques, and Common Knowledge	
7.3	Red Team Approach	
Chapter	8: Impact of Emerging Technologies on Cybersecurity	
8.1	Generative AI	
8.1.1	- Risks of Generative AI ("Gen AI")	
8.1.2	- Risk Governance on Gen Al	
8.2	DLT / Digital Asset	
8.2.1	- Introduction of Digital Asset	
8.2.2	- Risk & Control of Digital Asset	



8.3	Emerging Threat on Ebanking
8.3.1	- Emerging Threat on Ebanking
8.3.2	- Proposed Mitigation Controls

## **Recommended Readings**

#### **Essential Readings:**

1. HKIB Study Guide of ECF-Cybersecurity. (2025).

#### Supplementary Readings

- 1. Center for Internet security (CIS), <u>https://www.cisecurity.org/cybersecurity-best-practices</u>
- 2. Collins, M. S. (2016). *Network Security Through Data Analysis: Building Situational Awareness* (2<sup>nd</sup> ed.). "O'Reilly Media, Inc.".
- 3. Cybersechub, <u>https://www.cybersechub.hk/en/home/cert</u>
- 4. Dykstra, J. (2015). *Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.* "O'Reilly Media, Inc."
- 5. E-learning on HKIB Website: Cybersecurity Essentials, <u>https://secure.kesdee.com/ksdlms/?Partner=HKIB</u>
- 6. European Union Agency for Network and Information Security (ENISA). (2017). *Cyber Security Culture in organisations ENISA*.
  - <u>https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations</u> Federal Office for Information Security. (n.d.). *A Penetration Testing Model*.
- 7. Federal Office for Information Security. (n.d.). *A Penetration Testing Model*. <u>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration\_pdf</u>
- 8. GovCERT, https://www.govcert.gov.hk/en/index.html
- 9. HKCERT, https://www.hkcert.org/faq
- 10. HK Police CSTCB, <u>https://www.police.gov.hk/ppp\_en/04\_crime\_matters/tcd/index.html</u>
- 11. Hong Kong Monetary Authority. (2016, May 18). *Cyber Resilience Assessment Framework*. <u>http://www.hkma.gov.hk/media/eng/doc/key-</u> information/speeches/s20160518e2.pdf
- 12. Hong Kong Monetary Authority. (2020, November 3). *Cybersecurity Fortification Initiative* 2.0. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1a1.pdf</u>
- 13. Hong Kong Monetary Authority. (2021, June 8).
  - Opening remarks at HKAB Fintech Seminar: Next Phase of Hong Kong's Fintech Journey – "Fintech 2025". <u>https://www.hkma.gov.hk/eng/news-and-media/speeches/2021/06/20210608-3/</u>



- II. Media Briefing on "Fintech 2025" Strategy. https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20210608e1.pdf
- 14. Hong Kong Monetary Authority. (2024, September 27).
  - I. Research Paper on Generative Artificial Intelligence in the Financial Services Sector. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-</u> <u>circular/2024/20240927e1.pdf</u>
  - II. Encl. Generative Artificial Intelligence in the Financial Services Space. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2024/GenAl\_research\_paper.pdf
- 15. Hong Kong Monetary Authority. (2024, September 27).
  - I. Use of Artificial Intelligence for Monitoring of Suspicious Activities. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240909e1.pdf</u>
  - II. Annex Use of Technologies to improve the Effectiveness and Operational Efficiency of Monitoring for MLTF. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/2024/0909e1a1.pdf</u>
  - 16. Hong Kong Monetary Authority. (2024, April 16). Risk management considerations related to the use of distributed ledger technology. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240416e1.pdf</u>
  - 17. Hong Kong Monetary Authority. (2023, December 21).
    - I. Managing cyber risk associated with third-party service providers.<u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-</u> <u>circular/2023/20231221e1.pdf</u>
    - II. Annex Managing cyber risk associated with third-party service providers. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-</u>circular/2023/20231221e1a1.pdf
  - 18. Hong Kong Monetary Authority. (2023, October 31). Enhancement to security of electronic banking services. <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231031e1.pdf</u>

## Further Readings

- 1. Australian Signals Directorate. (2018). *Protect: Implementing Application Whitelisting*. https://www.asd.gov.au/publications/protect/application\_whitelisting.htm
- 2. COBIT 5, ISACA
- 3. Hong Kong Monetary Authority. (2024, June 3). *General Principles for Technology Risk Management*. <u>https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-</u> <u>stability/supervisory-policy-manual/TM-G-1.pdf</u>
- 4. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems requirements





- 5. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
- 6. 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.
- 7. Kavis, M. J. (2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Wiley.
- 8. Microsoft. (2016). Anatomy of a Breach. https://download.microsoft.com/download/E/9/2/E92BB61B-ED07-431C-A33B-971FD91B31D4/Anatomy of a Breach ebook en-CA.pdf
- 9. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework*. <u>https://www.nist.gov/cyberframework</u>
- 10. Sanders, C., & Smith, J. (2014). *Applied Network Security Monitoring: Collection, Detection, and Analysis.* Syngress Publishing.
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). *MITRE ATT&CK: Design and Philosophy*. MITRE. <u>https://attack.mitre.org/docs/ATTACK Design and Philosophy March 2020.pdf</u>
- 12. The Institute of Internal Auditors. (2015). *Leveraging COSO across the Three Lines of Defense*. COSO.
- 13. Trull, J. C. (2016, October 16). Use Security Education and Awareness Programs to Your Advantage. Microsoft. <u>https://cloudblogs.microsoft.com/microsoftsecure/2016/10/26/use-security-education-and-awareness-programs-to-your-advantage/</u>
- 14. Data Security. Office of the Privacy Commissioner for Personal Data (PCPD). https://www.pcpd.org.hk/english/data\_security/index.html