ISCA Financial Forensic Accounting Qualification

Request for Proposal (RFP)

Introduction

The **ISCA Financial Forensic Accounting Qualification (FFAQ)** is a comprehensive programme designed to equip professionals with critical skills in forensic accounting, enabling them to identify, investigate, and prevent financial crimes, fraud, and misconduct across various industries. The qualification offers a practical curriculum that combines theoretical knowledge with real-world application.

The Qualification is designed to:

i. Upskill accountants who aspire to specialise in financial forensics and deepen the skills of professionals currently practicing in the field.

ii. Broaden the competencies of accounting and finance professionals by equipping them with complementary financial forensics knowledge.

iii. Confer professional recognition through the ISCA Financial Forensic Professional (FFP) Credential and ISCA membership, acknowledging expertise and experience in the domain.

Profile of participants:

- Accounting and finance professionals
- Audit practitioners (internal and external)
- Banking and financial services professionals
- Forensic accountants and analysts
- Compliance and risk management professionals
- Law enforcement officers

Scope of Work

ISCA invites proposals from qualified vendors to **review the current syllabus and develop training materials** for the following 3 modules of the FFA Qualification:

Delivery Format:

Blended learning – consisting of interactive e-learning with a live workshop. The workshop(s) will focus on hands-on application of knowledge.

Module	Learning Objective	Proposed Format
Forensic Accounting and Investigation	Equip participants with the roles and responsibilities of forensic accountants, knowledge of white-collar crime typologies, and skills to conduct investigations and prepare reports for various stakeholders. (Refer **Annex 1** for full syllabus.)	E-learning: 10 hours Workshop: 1 day (7 hours)
Digital Forensics	Equip participants with digital forensics methodologies and essential techniques to recover, authenticate and preserve electronic data as a form of legal evidence. (Refer **Annex 2** for full syllabus.)	E-learning: 10 hours Workshop: 1 day (7 hours)
Financial Crime	Provide practical insights into the financial industry structures, the types of financial crimes (e.g. money laundering, terrorism financing), relevant laws and regulations, and investigative approaches of financial institutions. (Refer **Annex 3** for full syllabus.)	E-learning: 5 hours Workshop: 1 day (7 hours)

The scope of work includes:

1. **Syllabus Review and Refresh**

   The vendor will be responsible for:

   - **Reviewing and refining the existing module syllabus** to ensure it remains relevant, up-to-date, and aligned with current industry practices and emerging trends.
   - **Revising the study guide** to reflect updated content, recommended learning hours, assessment approach, and recommended reading references.

2. **Content Development**:

   The vendor will be responsible for designing and developing content to support both **e-learning** and **workshop delivery**. This includes the creation of high-quality, engaging, and pedagogically sound materials tailored to each module.

   Key deliverables include:

   - **Design and curation of content** for both self-paced e-learning and instructor-led workshops.
   - **Develop comprehensive training materials**, including:
     - Course presentation slides for trainers and participants.
     - Detailed written notes to elaborate on the presentation slides (these may serve as the trainer's notes for workshop delivery and narrative scripts for recording).
     - Learning activities, illustrative examples, and case-based scenarios to enhance participant engagement and practical understanding.
   - **E-learning content recording**
     - Prepare and script the content to be recorded. ISCA will facilitate the recording process (e.g., studio access, equipment, technical support).
   - **End-of-module assessment**, comprising a question bank of 300 multiple-choice questions (MCQs) per module:
     - Review and refine existing MCQs to ensure their relevance and alignment with the refreshed syllabus.
     - Develop new MCQs as necessary to address updated or expanded content areas.

   Please note: All training materials and deliverables developed under this engagement will be the intellectual property of ISCA.

3. **Project Timeline**

   All deliverables are to be completed **by 15 July 2025.**

Quotations Submission

Vendors may submit proposals for one or more modules.

Please include the following in your proposal:

(1) Indicate the module(s) you wish to undertake.
(2) Proposed development fees
(3) Any suggested enhancements to the existing syllabus

Please submit your proposal and quotation by 15 May 2025, to qualifications@isca.org.sg with the email subject "CAA-15-2025

For any enquires, please email Ms Chiew Yeng at chiewyeng.kaw@isca.org.sg.

Annex 1

Forensic Accounting and Investigation

Scope of Content

Scope of content

Detailed Topics	Learning Outcomes	Proficiency Level
1. White-collar crime overview 1.1. What is fraud 1.2. What is forensic accounting 1.3. Evolution of White-Collar Crime	Candidates will be able to define: (1) Define fraud and forensic accounting (2) Recognise advancements in forensic accounting practices	Foundation[1]
2. Roles and duties 2.1. The roles of the: 2.1.1. Audit committee 2.1.2. External auditor 2.1.3. Forensic accountant 2.1.4. Internal auditor 2.1.5. Management 2.2. The duties of the forensic accountant 2.2.1. Asset tracing 2.2.2. Damage calculations 2.2.3. Dispute resolution 2.2.4. Expert witness 2.2.5. Forensic accounting investigations 2.2.6. Testimony 2.3. Stakeholder management 2.4. Expanded Roles and Responsibilities	Candidates will be able to: (1) Describe the roles and duties of a forensic accountant as an investigator. (2) Explain how the forensic accountant could work alongside other experts including lawyers when conducting forensic accounting investigations for litigation purposes. (3) Explain the importance and use of financial statements for conducting forensic accounting investigations. (4) Improve stakeholder communication strategies	Foundation

[1] Learning outcomes at the foundation level relate to work environments that are characterized by low levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board.*

3. Types of white-collar crime 3.1. Asset misappropriation 3.2. Bribery and corruption 3.3. Cash fraud 3.4. Complex financial fraud 3.5. Consumer fraud 3.6. Corporate fraud 3.7. Expense fraud 3.8. Financial statement fraud 3.9. Inventory fraud 3.10. Money laundering and terrorism financing 3.11. Payroll fraud 3.12. Procurement fraud **Emerging Fraud Typologies** 3.13. Cyber fraud and ransomware 3.14. Cryptocurrency-related fraud 3.15. Environmental, Social, and Governance (ESG) fraud 3.16. Deepfake and synthetic identity fraud 3.17. Advanced money laundering techniques	Candidates will be able to: (1) Identify and explain the types of frauds and misconduct that are typically investigated by forensic accountants. (2) Identify the means through which fraud and misconduct may occur within accounting and business cycles. (3) Address new and sophisticated fraud schemes that have emerged with technological advancements.	Foundation

4. Law 4.1. Singapore legal system 4.2. Criminal justice system in Singapore 4.3. Criminal Procedure Code 4.4. Evidence Act 4.5. Penal Code 4.6. Prevention of Corruption Act 4.7. Companies Act 4.8. Tax fraud and law 4.9. Legal privilege	Candidates will be able to: (1) Explain and apply Singapore legislation which may be relevant when conducting forensic accounting investigations.	Foundation
5. Financial accounting 5.1. Accounting cycle 5.2. Assets and liabilities 5.3. Income and expenditure 5.4. Debits and credits 5.5. Revenue recognition	Candidates will be able to: (1) Explain the accounting cycle. (2) Explain how financial statements are prepared. (3) Interpret accounting concepts, fundamentals, principles and definitions which are useful in forensic accounting.	Foundation

6. Forensic accounting investigative approaches 6.1. Investigation planning and tools 6.2. Obtaining evidence from accounting records and computerized accounting systems 6.3. Financial document analysis and investigation leads 6.4. Ratio and financial statement analysis 6.5. Forensic data analytics 6.6. Brief overview of Innovative Investigative Techniques	Candidates will be able to: (1) Apply the methodologies and identify the appropriate investigative techniques or tools that can be deployed in forensic accounting investigations to detect financial fraud and gather evidence. (2) Identify the sources of evidence for forensic accounting investigations. (3) Explain the considerations for gathering evidence for forensic accounting investigations and apply the principles and methods of gathering evidence for the purposes of conducting investigations. (4) Apply ratio and financial statement analyses to identify financial statement fraud and red flags/investigation leads. (5) Explain the benefits and use of data analytics in forensic accounting investigations.	Intermediate[2]

[2] Learning outcomes at the intermediate level relate to work environments that are characterized by moderate levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board.*

7. Investigative interviews 7.1. The importance and relevance of interviews in forensic accounting investigations 7.2. Planning and preparing for an interview 7.3. Interview styles and techniques 7.4. Types of questions to ask during an interview 7.5. Interviewees' rights during an interview 7.6. Interview records 7.7. Conducting virtual interviews 7.8. Cultural considerations in global investigations	Candidates will be able to: (1) Explain the objectives of conducting interviews. (2) Plan for interviews. (3) Execute investigative interview techniques during a forensic accounting investigation. (4) Explain the considerations for conducting an interview with a witness. (5) Explain the considerations for conducting an interview with a subject. (6) Prepare a list of technical questions for the interviewees (7) Use the appropriate types of records to document the interviews.	Intermediate

8. Evidence management and document examination 8.1. Types of evidence that may be relevant in forensic accounting investigations 8.2. Documenting the process of gathering evidence 8.3. Obtaining, handling and examining evidence 8.4. Engagement of an expert to examine evidence 8.5. Rights and duties of the various parties involved in a forensic accounting investigation 8.6. Documenting the results of the analysis 8.7. Integrity and admissibility of evidence	Candidates will be able to: (1) Apply the principles of gathering evidence (including chain-of-custody and legal considerations). (2) Identify the types of evidence that may be relevant for a forensic accounting investigation. (3) Explain the methods of gathering evidence in order to preserve the evidence collected during an investigation. (4) Explain the types of analyses that can be performed on evidence gathered for forensic accounting investigations. (5) Prepare reports to document the results of evidence analyses.	Intermediate
9. Reporting 9.1. Planning and preparing a report 9.2. Types of reporting 9.3. Report structure 9.4. Inclusion of references to sources/evidence in a report 9.5. Use of visual aids in a report 9.6. Expert witness report 9.7. Preview of interactive and dynamic reporting tools	Candidates will be able to: (1) Explain the importance of writing an effective report. (2) Prepare various reports, containing the standard sections that are fit for purpose, for various stakeholders.	Foundation

10. Fraud risk management	Candidates will be able to: (1) Explain and apply the concepts of fraud risk management. (2) Identify the key success factors of an effective fraud risk management framework. (3) Identify and explain the attributes that are important to preventing, detecting and investigating fraud. (4) Identify and assess the fraud risks within an organization. (5) Prepare a fraud risk management framework.	Foundation
11. Mock investigation	Candidates will be able to: (1) Explain the forensic accounting investigation process from commencement to completion. (2) Identify and apply the investigation techniques in an investigation. (3) Perform a forensic accounting investigation.	Foundation

Annex 2

Digital Forensics

Scope of Content

Scope of content

Detailed Topics	Learning Outcomes	Proficiency Level
1. Digital forensics overview 1.1. History of digital forensics 1.2. Sources of electronic evidence 1.3. Chain of custody 1.4. Evolution and milestones in digital forensics 1.5. Importance of digital evidence 1.6. Overview of common types of Digital Evidence	Candidates will be able to: (1) Define digital forensics and explain its importance to a financial forensic accountant. (2) Explain the benefits and limitation of digital forensics. (3) Recognize the tools and able to summarize their function in digital forensic investigation. (4) Identify sources of electronic evidence. (5) Explain the importance of maintaining a proper chain of custody for digital evidence.	Foundation[3]
Comments: • Useful to make a mention of this data point to emphasise the importance of digital evidence: "According to the 2022 Industry Trends Survey commissioned by Cellebrite, it was revealed that most law enforcement agencies and prosecutors now believe that digital evidence is more important than physical evidence and DNA in successfully prosecuting cases." https://cellebrite.com/en/2022-industry-trends-form/ • To consider listing the common types as an overview: Computer Forensics, Memory forensics, Email forensics, Cloud forensics, Malware forensics, Mobile device forensics, Network forensics, IOT/OT forensics, Multimedia (video/audio/image) forensics, eDocument forensics.		

[3] Learning outcomes at the foundation level relate to work environments that are characterized by low levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board.*

2. Digital forensics methodology 2.1. Investigation logs and documentation 2.2. Forensic methodology	Candidates will be able to: (1) Explain the processes and techniques to perform at each phase to ensure completeness and accuracy of work. (2) Able to apply forensic methodology to resolve contingencies during field work.	Foundation
3. Forensic data collection 3.1. Electronic evidence preservation 3.2. Electronic evidence identification 3.3. Challenges of forensic acquisition 3.4. Order of acquisition 3.5. Recovery of deleted data, especially in mobile devices 3.6. Acquisition and preservation of internet artefacts	Candidates will be able to: (1) Apply appropriate methods to pack, transport, and store electronic evidence. (2) Identify and classify different sources of electronic evidence. (3) Explain the challenges during forensic acquisition. (4) Explain the ephemeral nature of digital evidence and accurately determine their collection priority. (5) Perform the orderly acquisition of data using industry-standard methods, ensuring minimal alteration to original evidence. (6) Identify and recover deleted data from various devices, including advanced techniques for mobile devices. (7) Acquire and preserve internet artefacts (e.g., browser history, cookies, cached data) while ensuring forensic soundness. (8) Evaluate tools and techniques for handling encrypted or volatile data and their impact on forensic integrity.	Intermediate[4]

[4] Learning outcomes at the intermediate level relate to work environments that are characterized by moderate levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board.*

4. Forensic examination and analysis		
4.1 MS Window investigation 4.1.1 File analysis 4.1.2 Registry analysis 4.1.3 Timeline analysis 4.1.4 Log analysis 4.1.5 Correlation of artefacts	Candidates will be able to: (1) Analyse core Windows forensic file artefacts and explain their implication(s). (2) Explain what is contained within Windows registry hives and identify the tools to assist in their investigation. (3) Explain what forensic timestamps are and the role they play in timeline analysis. (4) Analyse and interpret Windows and Linux event logs, and evaluate how commercial tools can aid in log analysis. (5) Explain the correlation between artefacts and interpret user activity based on the findings.	Intermediate
4.2 Email investigation 4.2.1 Parts of an email 4.2.2 Email infrastructure, protocols and technology 4.2.3 Email header analysis	Candidates will be able to: (1) Explain the limitation and challenges associated with email investigations. (2) Analyse email headers and use them to gain insight about the infrastructure an email has traversed.	Intermediate
4.3 Cyber investigation 4.3.1 Website defacement 4.3.2 Malware analysis	Candidates will be able to: (1) Explain the forensic implications of website defacement, including detection and evidence preservation. (2) Explain what is malware and how to identify them based on forensic artefacts.	Intermediate
4.4 Social media investigation	Candidates will be able to:	Intermediate

	(1) Explain the challenges of performing internet-based investigation. (2) Explain anonymization technologies and how they can hamper investigation. (3) Explain how popular online tools can be used to perform social media investigations.	
5 Forensic data analytics (FDA)	Candidates will be able to: (1) Define general forensic analytics strategy. (2) Identify relevant data analytics techniques and explain the advantages and disadvantages of each of these techniques. (3) Prepare and use visualisations to communicate findings of analyses effectively.	Foundation
6 Electronic discovery (eDiscovery) 6.1 Background 6.2 Approach 6.3 Direction 6.4 Tools	Candidates will be able to: (1) Explain the impetus behind eDiscovery and the practice direction. (2) Explain basic e-Discovery approaches. (3) Explain the methodology to process evidence for eDiscovery. (4) Explain the challenges of eDiscovery.	Foundation

7 Law	Candidates will be able to explain and apply the: (1) Computer Misuse Act (2) Cybersecurity Act 2018 (3) Personal Data Protection Act 2012 (Singapore)	Foundation
8 Emerging technologies and trends on financial crime	Candidates will be able to: (1) Appreciate the impact of emerging technologies on forensic investigations including: • Artificial intelligence • Cryptocurrency and blockchain • Machine learning • Deepfake scams (2) Understand the opportunities and challenges these technologies present for financial forensic professionals.	Foundation

Additional notes:

1. Focus and in-depth coverage of the following topics with time allocated for hands-on workshop:
   - Topic 3: Forensic data collection
   - Topic 4: Forensic examination and analysis (reduce the technicality coverage)
   - Topic 5: Forensic data analytics

2. Structure the hands-on workshops around different types of investigation case studies, for example,
   - Insider threat or data theft/exfiltration – Windows artifacts, USB, timeline analysis etc.
   - Business email compromise – email spoofing, phishing, etc.
   - Procurement fraud – social media, document meta-data analysis

Annex 3

Financial Crime

Scope of Content

Scope of content

Detailed Topics	Learning Outcomes	Proficiency Level
1. Singapore and international financial industry	Candidates will be able to:	Foundation[5]
1.1. Singapore and global financial industry	(1) Understand and appreciate the role and importance of the Singapore and global financial industry. (2) Summarise key aspects of the banking and financial industry, including: a. Types of financial institutions (e.g. banks, insurers, trusts); b. Central bank equivalent and financial regulatory authority, e.g. Monetary Authority of Singapore (MAS); c. Other relevant professional bodies, e.g. Financial Action Task Force (FATF), Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)); d. Products; and e. Delivery channels.	
1.2. Information in financial institutions	(1) Understand and appreciate a typical set up within a financial institution (e.g. front office, middle office and back office). (2) Understand and appreciate the various information sources within a financial institution.	

[5] Learning outcomes at the foundation level relate to work environments that are characterized by low levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board*.

Detailed Topics	Learning Outcomes	Proficiency Level
1.3. Financial crime	(1) Define financial crime. (2) Identify main types of financial crime, including fraud, money laundering and terrorist financing. (3) Discuss how the different types of financial institutions are susceptible to the different types of financial crime. (4) Identify risks arising from financial crime (e.g. reputational risk, compliance risk and legal risk).	
1.4. Financial institution investigation	(1) Discuss parties that may be involved in a financial institution investigation (i.e. internal and external investigation teams).	
2. Law 2.1. Regulatory legislation and instruments issued by MAS	Candidates will be able to: (1) List key legislation and regulatory instruments issued by MAS such as Notices and Guidelines and identify key legislation and instruments relevant to financial crime including Banking Act and Securities and Futures Act.	Foundation
2.2. Money laundering and terrorist financing laws in Singapore	(1) Discuss money laundering and terrorist financing laws in Singapore, including: a. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA); and b. Terrorism (Suppression of Financing) Act (TSOFA). (2) Explain key offences within the CDSA and TSOFA.	

Detailed Topics	Learning Outcomes	Proficiency Level
2.3. MAS Anti-Money Laundering (AML) regulations, guidelines and guidance	(1) Discuss key AML regulations, guidelines and guidance issued by MAS for financial institutions in Singapore. These will include: a. MAS Notice 626[6] – Prevention of Money Laundering and Countering the Financing of Terrorism – Banks; b. Guidelines to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism; c. Guidance on Anti-Money Laundering and Countering the Financing of Terrorism controls in Trade Finance and Correspondent Banking; d. Guidance on Private Banking Controls; e. Singapore National Risk Assessment; and f. ABS Guidelines on AML/CFT.	
2.4. Securities and Futures Act (SFA)	(1) Explain the legislative framework of SFA. (2) Explain key offences within SFA.	

[6] MAS has issued specific notices, guidelines and guidance for the different types of financial institutions under their purview. We will be covering the notice, guidelines and guidance for banks as the key AML requirements do not differ much among the various financial institutions.

Detailed Topics	Learning Outcomes	Proficiency Level
2.5. International standards and guidelines relevant to AML and Sanctions	(1) Identify international AML standards and guidelines such as: a. FATF 40+9 Recommendations; b. Wolfsberg Standards; c. Publications from Basel; and d. United Nations Security Council Resolutions relating to prevention and suppression of terrorist financing (e.g. United Nations Security Council Resolution 1373 (2001)).	
3. Money laundering, terrorist financing and sanctions	Candidates will be able to:	Intermediate[7]
3.1. Money laundering and terrorist financing	(1) Differentiate between money laundering and terrorist financing. (2) Outline the three stages of money laundering (i.e. placement, layering and integration). (3) Analyse that different geographical locations pose different ML/TF risks.	
3.2. Sanctions	(1) Explain what sanctions are, including the different types of sanctions (i.e. country versus individual/entity sanctions). (2) Identify the key enforcing parties of sanctions. (3) Explain when a specific country's sanction will apply. (4) Explain the impact of violating sanctions.	

[7] Learning outcomes at the intermediate level relate to work environments that are characterized by moderate levels of ambiguity, complexity, and uncertainty. *Source: International Accounting Education Standards Board.*

Detailed Topics	Learning Outcomes	Proficiency Level
3.3. Regulatory landscape and enforcements	(1) Outline how financial institutions are supervised by MAS in Singapore, which will include key elements within MAS framework; progressive regulations, intensive supervision, rigorous enforcement and international co-operation and industry partnerships. (2) Discuss recent real life financial crime investigations undertaken by Singapore and international regulators and the impact of the investigations (i.e. action being taken against the financial institution and individuals).	
3.4. AML program framework and the control components	(1) Identify key components in an AML program framework and relevant control components. Candidates should also be able to explain control components within higher risk areas such as Correspondent Banking, Private Banking and Trade Finance.	
3.5. Leadership and governance	(1) Outline the lines of defence within a typical financial institution and explain their respective roles in leadership and governance. (2) Explain the importance of risk culture within a financial institution.	
3.6. Enterprise risk assessment	(1) Summarise the main components of an enterprise risk assessment framework and explain how an enterprise risk framework can be performed.	
3.7. AML policies and procedures	(1) Distinguish the difference between AML Policy Standard and AML Procedures Manual.	

Detailed Topics	Learning Outcomes	Proficiency Level
	(2) Explain how one performs gap analysis on policies and procedures to ensure compliance to regulatory requirements.	
3.8. Customer due diligence (CDD)	(1) Distinguish the different types of legal persons and legal arrangements, for example, Personal Investment Companies, Sole Proprietors, Trusts and Foundations. (2) Discuss the following topics: a. Who must CDD be performed on? b. When should CDD measures be performed? c. What does one perform as part of CDD measures (i.e. identification and verification measures)? d. What are the typical CDD documentary requirements for individuals and entities (e.g. corporates, partnerships)? e. What is a customer risk assessment and what are the common risk factors used to calculate customer risk rating in a financial institution? f. How does one inquire into corporate structures to identify shareholders and ultimate beneficial owners? g. Who are Politically Exposed Persons (PEPs) and how does one identify them? h. What does simplified due diligence measures and enhanced due diligence	

Detailed Topics	Learning Outcomes	Proficiency Level
	measures entail and when does one apply them? i. What is Source of Wealth and Source of funds? j. How does one corroborate Source of Wealth? k. What is involved in ongoing monitoring of customers? l. When does one perform ongoing monitoring of customers? (3) Understand what are bearer shares and risk associated with bearer shares.	
3.9. Client screening	(1) Explain what is involved in the client screening process within a financial institution, which will include periodic reviews of the effectiveness of the client screening system. (2) Recognise a "good" disposition of client screening alert sample.	
3.10. Transaction filtering including payments, loans, and trade finance	(1) Explain what is involved in the transaction filtering screening process within a financial institution, which will include periodic reviews of the effectiveness of the transaction filtering system across different financial activities (e.g., payments, loans, trade finance). (2) Recognise a "good" disposition of transaction filtering alert samples, including those related to payments, loans, and trade finance.	

Detailed Topics	Learning Outcomes	Proficiency Level
3.11. Transaction monitoring	(1) Explain what is involved in the transaction monitoring process within a financial institution, which will include setting thresholds and parameters and performing periodic calibration of thresholds and parameters of a transaction monitoring system. (2) Recognise a "good" disposition of transaction monitoring sample. (3) State the examples of suspicious transaction red flags.	
3.12. Suspicious transaction reporting (STR)	(1) Explain what is involved in the suspicious transaction reporting process within a financial institution. (2) List the parties who may be involved in the STR process (e.g. Suspicious Transaction Reporting Office, the financial intelligence unit within the financial institution and Egmont Group) and their roles and responsibilities. (3) Outline the characteristics of an effective STR narrative. (4) Explain the consequences of tipping off.	

Detailed Topics	Learning Outcomes	Proficiency Level
3.13. Record keeping and information sharing	(1) Explain the recordkeeping requirements. (2) Summarise on a high level the different ways information sharing is done within and outside a financial institution, including frameworks in place such as the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) and Singapore's membership in international AML/CFT organisations.	
3.14. Employee due diligence	(1) Understand and appreciate what does employee due diligence entail.	
3.15. Training	(1) Explain the importance of training and when training should be conducted.	
3.16. Compliance monitoring and testing	(1) Understand and appreciate how compliance monitoring and testing can be organised to ensure regulatory requirements have been met and that there are adequate controls in place to mitigate key risks.	
3.17. Typologies used in ML/TF	(1) Differentiate known typologies for ML/TF.	

4. Other financial crime 4.1. Other financial crime risk areas	Candidates will be able to: (1) Identify other financial crime risk areas.	Foundation
4.2. Key control components for fraud, bribery and corruption	(1) State the key control components for other financial crime risk areas including 3rd party and employee due diligence, whistleblowing hotline, gift and entertainment register and forensic data analytics.	
4.3. Key control components for market conduct control areas	(1) State the key control components for market conduct control areas including trade and communication surveillance.	
5. Investigations in financial institutions 5.1. Financial institutions investigative approaches	Candidates will be able to: (1) Identify the types of financial frauds. (2) Prepare an investigation plan. (3) Identify the sources of evidence within a financial institution including, hardcopy and computerised accounting books and records, outputs from various financial institution systems such as call reports, trade finance systems.	Intermediate

		(4) Apply the methodologies and identify the appropriate investigative techniques or tools that can be deployed to detect financial fraud and gather evidence.
5.2.	Evidence gathering and management	(1) Apply the principles of gathering evidence including chain-of-custody and legal considerations. (2) Apply the methods of gathering evidence in order to preserve the evidence collected (including labelling, recording, tracking, use, retention, storage and security of evidence) during investigation. (3) Identify the types of analysis that can be performed on evidence gathered (4) Analyse the evidence and prepare report to document the results.
5.3.	Regulatory inspections and investigations (specific to financial crime / AML)	(1) Identify the stages and processes involved in regulatory inspections related to AML. (2) Prepare documentation and evidence to respond effectively to regulatory inquiries. (3) Apply best practices for addressing regulatory findings

	and implementing remediation plans.	
5.4. Use of Artificial Intelligence (AI) and Machine Learning (ML) by the Financial Industry	(1) Describe how AI and ML are applied in financial crime detection and prevention. (2) Evaluate the potential benefits and challenges of using AI/ML in AML/CFT programs. (3) Recognise regulatory expectations and ethical concerns when adopting AI/ML solutions.	