INSTITUTE OF
SINGAPORE
CHARTERED
ACCOUNTANTS

ISCA Financial Forensic Accounting Qualification

Digital Forensics

Scope of Content

Version: as at 28 February 2019

1. 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	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[1]
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

[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.*

Detailed Topics	Learning Outcomes	Proficiency Level
3. Forensic acquisition and investigation 3.1. Electronic evidence preservation 3.2. Challenges of forensic acquisition 3.3. Order of acquisition 3.4. Windows file analysis 3.5. Windows registry analysis 3.6. Timeline analysis 3.7. Malware analysis 3.8. Correlation of artefacts	Candidates will be able to: (1) Apply the proper method to pack and transport electronic evidence. (2) Explain the likely challenges during forensic acquisition (3) Explain the ephemeral nature of digital evidence and accurately determine their collection priority. (4) Analyse basics Windows forensic file artefacts and explain their implication(s). (5) Explain what is contained within Windows registry hives and identify the tools to assist in their investigation. (6) Explain what are forensic timestamps and the role they play in timeline analysis. (7) Explain what is malware and how to identify them based on forensic artefacts. (8) Explain the correlation between artefacts and interpret user activity based on the findings.	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.*

4. Email investigation 4.1. Parts of an email 4.2. Email infrastructure, protocols and technology 4.3. Email header analysis	Candidates will be able to: (1) Explain the limitation of email investigation. (2) Analyse email headers and use them to gain insight about the infrastructure an email has traversed.	Intermediate
5. Cyber investigation 5.1. Social media crime and investigations 5.2. Acquisition and preservation of Internet artefacts. 5.3. Internet based Social media investigation	Candidates will be able to: (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.	Intermediate
6. Log analysis 6.1. Windows event logs 6.2. Linux event log location and interpretation 6.3. Log based case studies 6.4. Tools	Candidates will be able to: (1) Analyse basics Windows logs. (2) Analyse basics Linux logs. (3) Explain how commercial tools can aid in log analysis.	Intermediate
7. Forensic data analytics	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.	Foundation

	(3) Prepare and use visualisations to communicate findings of analyses effectively.	
8. Electronic discovery (eDiscovery) 8.1. Background 8.2. Approach 8.3. Direction 8.4. 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
9. Law	Candidates will be able to explain and apply the: (1) Computer Misuse Act (2) Cybersecurity Act 2018 (2) Personal Data Protection Act 2012 (Singapore)	Foundation