BCS Foundation Certificate in Information Security Management Principles

Sample Paper

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 40 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

Pass mark is [65/100]

This professional certification is not regulated by the following United Kingdom Regulators - Ofqual, Qualifications in Wales, CCEA or SQA

1 Which of the following techniques is used to ensure confidentiality?

A Encryption.
B Hashing.
C Encapsulation.
D Authentication.

2 Which of the following can be defined as a threat?

A The likelihood of a cybercriminal getting caught.
B Use of malicious software to generate an attack.
C The probability that a cyber-attack will be successful.
D A cyber-attack that can cause damage to information assets.

3 Which of the following is the function of specifying user access rights/privileges to computing resources?

A Authentication.
B Enabling.
C Accounting.
D Duplication.

4 Which concept describes the amount of confidence that an organisation has that its controls satisfy the necessary security requirements?

A Assurance.
B Governance.
C Non-repudiation.
D Trust.

5 Which information security principle requires that an organisation **SHOULD** implement overlapping security controls wherever feasibly possible?

A Separation of Duties.
B Fail Safe Configuration.
C Defence in Depth.
D Web of Trust.

6 With the increasing global operation of many corporate organisations, which of the following is **LIKELY** to be the more important consideration with respect to information security?

A Understanding that different countries have differing legislation with respect to how information can be handled.
B Ensuring that for all countries that an organisation has an office in, will all operate in the same time zone.
C Ensuring that regional preferences for security related hardware and software are adhered to.
D Storing all corporate data only in one country where an organisations central office is located.

7 Whilst drafting a company's information security policy, what would be an important consideration?

A The policy should be a standalone document.
B The policy must be integral to all areas of an organisation.
C The policy should only be visible to senior management.
D The policy only applies to staff handling confidential information.

8 Why could an organisation's "clear desk" policy be seen as a good example of "security as an enabler"?

A Clear desks allow staff to "hot desk" making them less likely static "sitting" targets for cyber-attacks.
B Conformance to data protection laws will be enhanced by not using paper files.
C Staff no longer need physical desk as they can work remotely and data theft is no longer a problem.
D The removal of confidential information from desks reduces the chances of opportunistic theft, and keeps it available to the business.

9 Legislation in individual countries such as the Sarbanes-Oxley in the USA and the Companies Act (UK) have had the effect of strengthening corporate responsibility for risk management.

Who now has this ultimate responsibility?

A IT Manager.
B IT Security Team.
C All Supervisory Roles.
D Corporate Board.

10 Within any organisation, from both an information assurance and "security culture" perspective, whose responsibility is information security?

A All staff.
B IT Department.
C Chief Executive Officer.
D Data Protection Officer.

11 Which of the following is **NOT** considered an "accidental threat" to information systems?

A An unexpected flood due to abnormal rainfall.
B A building fire in Corporate Data Centre.
C A person clicking the wrong button.
D A disgruntled employee destroying backup files.

12 Which of the following relationships **BEST** describes how a risk is determined?

A Risk = Threat * Vulnerability
B Risk = Asset * Vulnerability.
C Risk = Impact * Likelihood.
D Risk = Exploit * Likelihood.

13 Which of the following can be considered an "internal threat"?

A Cybercriminal blackmailing a service provider with a denial of service attack.
B Compromised supplier connected to an organisation's order system.
C Employee's laptop compromised by a malicious drive by infection from a website.
D Theft of login credentials from a restaurant's free Wi-Fi hotspot.

14 When customer PII (Personal Identifiable Information) has been stolen from an organisation's online store using SQL Injection, where can the vulnerability that led to this exploit usually be found?

A In the organisation's firewall rules.
B In an employee's laptop connected to Wi-Fi.
C In the database connected to the organisation's ecommerce website.
D In the organisation's internal email server.

15 When a financial institution that has been the victim of a sophisticated cyber-attack, which of the following is the **MOST LIKELY** outcome of an impact assessment of typical realised threats?

A Loss of confidence by financial investors.
B Increased business opportunity for attracting more investment.
C New intrusion detection software purchased.
D Increased bonus for the financial institutions CEO.

16 What are the **four** main components of a risk management process used in the CORRECT life-cycle order?

A Identify, Analyse, Treat and Monitor.
B Assess, Verify, Treat and Maintain.
C Identify, Quantify, Validate and Monitor.
D Monitor, Analyse, Assess and Treat.

17 When undertaking a quantitative risk assessment of an ongoing denial of service threat to an information system, what type of evidence is **LIKELY** to form part of that assessment?

A Descriptive analysis of the system's capabilities.
B Closed questionnaire for the system administrator.
C Statistical chance of another attack re-occuring.
D Firewall rule documentation protecting the information system.

18 A financial institution is concerned that it may be at risk of cybercriminals stealing PII (personal Identifiable Information) stored on the organisation's web server. To address this issue they have adopted a risk mitigation strategy.

Which of the following would support this strategy?

A Deleting the data.
B Encrypting the data.
C Taking out Cyber Liability insurance.
D Do nothing.

19 Which risk assessment approach uses a risk matrix that maps risk likelihood against impact, and is usually represented as a 2x2, 3x3 or up to 5x5 sectors representing low, medium or high risk levels?

A Quantitative.
B Qualitative.
C Survey based.
D Cost based.

20 A qualitative risk assessment is being undertaken for an organisation.

The two most important risk elements which should form the MOST major part of the analysis of risk are likelihood and which other element?

A Threat.
B Vulnerability.
C Impact.
D Cost.

21 What is **one** of the **KEY** reasons for appointing a Chief Information Security Officer (CISO) at Boardroom level?

A Single Point of Responsibility for Information Assurance.
B A typical CIO cannot be trusted with security.
C To ensure a bottom up security culture.
D To ensure compliance with data protection regulations.

22 An e-commerce company has been the victim of a data breach on its credit card payment systems and will need to report on its regulatory compliance.

Which of the following standards or laws would the company be auditing against as a **first** priority?

A PCI-DSS.
B GDPR.
C Sarbanes Oxley.
D NIS Directive.

23 For an organisation looking to develop an information assurance strategy, which of the following is the **MAIN** difference between a security policy and standard?

A A standard only offers guidance whilst a policy is obligatory.
B A policy contains implementation specific detail and a standard offers only generic detail.
C A policy sets out what needs to be done - a standard sets out how the policy should be implemented.
D A policy details specific work instructions and a standard offers only high level objectives.

24 In order to prevent the reoccurrence of a previous incident, which phase of an incident response process would involve a security administrator designing new security controls?

A Reporting.
B Responding.
C Investigation.
D Corrective Action.

25 When developing an information security strategy, which of the following would **NOT** be a consideration?

A Expected developments in software and hardware.
B Legal, compliance and audit requirements.
C Trends in threats and vulnerabilities.
D Log of recent security incidents.

26 From a legal perspective, which of the following is considered to be misuse of a computer?

A Theft of a computer laptop from the boot of a car.
B Illegal interception of information.
C Use of one's own computer for cryptomining.
D Using a computer to access the Dark Web.

27 Under what circumstances might it be legal for an employer to monitor an employee's online communication?

A When a statement is included in the organisation's information assurance policy or employee's contract of employment.
B An employer can monitor communications whenever or however they want without ever informing the employee.
C The use of Data Protection (e.g. GDPR) laws allows the employer to monitor communications whenever they like.
D When an employee is using online communications outside of normal office hours.

28 When collecting digital evidence which may be required to be used in a court of law, which of the following principles is considered BEST practice?

A Digital evidence can only be handled by a member of law enforcement.
B Any digital forensics investigator handling digital evidence must be competent to do so.
C Digital evidence may be altered under supervision by another investigator.
D Acquiring digital evidence can only be carried on digital devices which have been turned off.

29 When transferring encrypted information or cryptography based tools between one legal jurisdiction to another, according to ISO/IEC 27000 series, which of the following is **NOT** a factor which should be considered?

A Restrictions on import and export of computer hardware and software for performing cryptographic functions.
B Restrictions on the transmission of symmetric and/or asymmetric keys over communication networks.
C Restrictions on import and export of computer hardware and software that is designed to have cryptographic functions added to it.
D Mandatory or discretionary methods of access by the countries authorities to information encrypted by computer hardware or software to provide confidentiality of content.

30 When trying to protect the source code for information security related software being "pirated", which of the following legal protection will be **MOST** effective?

A Data Protection law.
B Computer Misuse law.
C Copyright law.
D Patents.

31 Which of the following standards bodies produces international standards which cover information security management systems?

A BSI.
B ETSI.
C ISO.
D PCI.

32 Which body is responsible for publishing technical standards for interoperability of internet protocols and applications?

A IEEE.
B ENISA.
C ISO.
D IETF.

33 Which internationally recognised standard was created to evaluate if security functions of IT products are appropriately designed and implemented in order to sufficiently counter threats?

A ISO27001.
B ISO15408.
C PCIDSS.
D ENISA NIS.

34 Which international standard deals with the management of IT security, focusing on the technical security control measures?

A ISO/22301:2019.
B ISO/IEC13335.
C BS7799 Part 2.
D EIA232.

35 Which of the following frameworks focuses on IT Service Management (including areas such as configuration management, change control and service level agreements)?

A ITIL.
B PCIDSS.
C TOGAF.
D ISO27002.

36 What are the **TYPICAL** stages of an information lifecycle?

A Create, Clone, Copy, Print, File.
B Create, Store, Retrieve, Use, Remove.
C Create, Use, Store, Retrieve, Delete.
D Copy, Store, Use, Print, Delete.

37 Which of the following is **NOT** a legitimate form of generating or acquiring information as part of the information lifecycle?

A Typed Letter in the Post.
B Phone Call.
C Through an email.
D Printing a document.

38 The information lifecycle articulates a "publishing" or use of information stage.

Which of these actions occurs within this stage?

A Locking an "actioned" letter in a filing cabinet.
B Moving an email to a folder.
C Sending a tweet advertising an event.
D Deleting a voicemail.

39 Which of the following **BEST** represents the main components of the DevOps model?

A Software Development, Quality Assurance and Operations.
B Hardware Development, Product Management and Operations.
C Brand Development, Testing and Security Operations.
D Software Development, Change Management and Security Operations.

40 Which **four** architecture domains are commonly accepted as the subsets of an overall enterprise architecture supported by TOGAF?

A Business, information, technology and application.
B Application, data, infrastructure and business.
C Technology, application, integration and business.
D Technology, data, application and business.

41 The security team at a cloud service provider are continually updating the firewall 's rules on the Internet facing firewall to meet customer demands but each new set rules causes additional access problems for different customers.

What process **SHOULD** the organisation adopt to ensure that the firewall rules are thoroughly tested before deployment on a production system?

A Configuration Management.
B Change Control.
C Unit Testing.
D Release Control.

42 When a network administrator needs an insight into remote console connection events which have been occurring on switches and routers within an organisation's infrastructure, which of the following describes the **MOST** appropriate form of logging to use?

A Audit Logging.
B Flow Logging.
C Route Logging.
D Trace Logging.

43 What type of software program makes the entire source code available to any person who wishes to inspect, manipulate or otherwise redistribute for no cost?

A Open source.
B Proprietary source.
C Closed source.
D Free source.

44 Which of the following testing methodologies **TYPICALLY** involves conducting tests without any knowledge of the underlying source code or the vulnerabilities it may contain?

A Static Testing.
B User Testing.
C Dynamic Testing.
D Code Review.

45 Which of the following risks is **NOT** associated with using third party libraries when developing software applications?

A Risk that malware toolkits can be written into untrusted libraries.
B Risk that common cryptographic routines may reveal secure data.
C Risk that software libraries have not been tested by the user community.
D Risk that in house development routines have not been patched.

46 What process **SHOULD** be adopted when an employer wants a high degree of confidence in the trust for an individual who will be handling confidential data?

A Security clearance and vetting.
B Psychometric testing.
C DNA testing.
D Personal reference checking.

47 When considering an employee's personal responsibility for information security, which legal document **SHOULD** be the final arbitrator?

A Contract of Employment.
B Annual Tax Return.
C Service Level Agreement.
D Acceptable Use Policy.

48 What type of internal control is achieved by disseminating common IT administrative tasks/processes and associated privileges amongst multiple system administrators?

A Task Independence.
B Segregation of Duties.
C Role Redundancy.
D Fail Safe Operation.

49 When considering suitable content for an organisation's End User Code of Practice, which of the following is **NOT** a suitable topic for inclusion?

A When work computers can be used for browsing the web.
B The use of personal devices such as smartphones within the organisation.
C An employee's individual contractual hours.
D The need to report all security based incidents.

50 Which of the following **SHOULD** a business consider when managing the risks of third party suppliers' information security?

A Ability to audit a third party supplier complying with contractual security requirements.
B Ability to undertake a random vulnerability assessment of third party systems.
C Ability to undertake the security vetting of key employees.
D Ability to demand the declaration of third party suppliers private keys.

51 Which of the following multi-factor authentication techniques provides a combination of both flexibility and low management overhead?

A Synchronous Hardware Tokens.
B Biometrics.
C Asynchronous Hardware Tokens.
D Software Tokens.

52 For an organisation with a set of dispersed international offices and poor Internet connectivity between the offices, what choice of access control system would allow the **MOST** flexibility?

A Mandatory access control.
B Centralised access control.
C Decentralised access control.
D Role-based access control.

53 On a Linux file system, when a user performs a directory listing, every displayed file and directory has a set of attributes labelled with 3 combinations of the attributes rwx.

What do these different combinations of rwx represent?

A Identification Profiles.
B Authorisation Permissions.
C Authentication Identities.
D Accounting Settings.

54 When determining an organisation's password policy, which of the following **SHOULD NOT** be considered best practice for employee's passwords?

A Use Password Managers to manage complex passwords.
B Use additional forms of authentication alongside passwords.
C Use well remembered names or phrases from a social media profile.
D Use three random words to form a password.

55 When an organisation labels its media based on the classification of the data it contains, which of the following typical rules is applied to those labels?

A Data is labelled as to the integrity of the information it contains.
B Media is labelled at the highest level of classification of the information it contains.
C Media is labelled at the lowest level of classification of the information it contains.
D Data is labelled with all levels that apply to the information it contains.

56 Which type of penetration testing technique can be used to help inform an organisation about its security training and awareness response?

A Enumeration.
B Reconnaissance.
C Social Engineering.
D Vulnerability Scanning.

57 Whilst preparing an organisation for a potential disaster recovery situation, who **SHOULD** receive initial business continuity training?

A Everyone within the organisation.
B The Executive Board.
C First Responders.
D Those involved in disaster recovery.

58 For those involved in penetration testing, which of the following is an accepted way of being able to put formal "ethical hacking" training into practice whilst remaining within the law?

A Performing a port scan of service providers website.
B "Capture the Flag" competitions.
C Security based online multiple choice quiz.
D Use of streaming video "hacking" content.

59 Which of the following information sources would be the **MOST** authoritative for an information security professional to keep themselves up to date with the latest technical cyber threats affecting their industry?

A Reading posts on social media.
B Reading a post on a dark web malware forum.
C Attending an internal company security awareness course.
D Watching industry webinars held by a security professional body.

60 Which of the following statements is the **MOST** relevant for application developers who need to learn application security skills?

A Secure Software development only needs to be undertaken as part of an undergraduate course.
B Secure coding training never finishes and always needs refreshing.
C Secure coding only needs to be learnt once as a part of learning how to use a development environment.
D Application security only needs to be taught to security operations staff and security analysts.

61 Which type of malicious software is characterised by replicating itself from system to system over a communications network without the need for user intervention?

A Virus.
B Worm.
C Trojan Horse.
D Spyware.

62 An accounts clerk has received a suspicious email, allegedly from the organisation's suppliers, with a spreadsheet attachment, asking them to pay the attached invoice.

What is the **MOST LIKELY** scenario?

A This is a ransomware attack.
B This is a vishing attack.
C This is a phishing attack.
D This a man-in-middle attack.

63 How might open source intelligence be used to better protect against new virus malware attacks?

A Gather intelligence from dark web malware forums.
B Gather intelligence from social media on user download habits.
C Gather information on domain names via WHOIS.
D Gather information on an organisation's public security profile.

64 When looking to determine the controls necessary to protect web servers and web applications against web based attack vectors, which of the following organisation’s materials **SHOULD** a security analyst consult?

A PCIDSS.
B OWASP.
C IETF.
D CSA.

65 Which of the following conditions makes an application more vulnerable to a cross site scripting attack (XSS)?

A Input Validation.
B Reflected Input.
C Token Injection.
D Man in the Middle.

66 What technique is used by firewalls to partition and stagger networks in order to provide better information security?

A Use of a demilitarised zone.
B Use of network address translation.
C Use of packet buffering in the firewall.
D Use of virtual private networks.

67 Which of the following is the BEST form of control when trying to block an attack on a well-known vulnerability which has been detected on the network internally and may have breached the outer defences of an organisation's network infrastructure?

A IDS.
B IPS.
C Firewall.
D VPN.

68 When determining which controls are necessary to ensure secure network management for an organisation's network infrastructure, which of the following protocols **SHOULD** be used to allow secure network transmission of console traffic to/from the organisation's routers, switches and servers?

A Telnet.
B EIA232.
C Rsh.
D SSH.

69 When connecting a remote worker home office network to an organisation's headquarters network infrastructure, which is the **MOST** appropriate VPN technology to secure the network transmission?

A IPSec.
B TLS/SSL.
C GRE.
D RDP.

70 When determining security controls on the provision or campus based LAN's, which of the following is **NOT** a valid statement?

A Wireless LAN's cannot be accessed outside of the buildings they are installed in.
B Wired networks are freely accessible outside of a cabled building infrastructure.
C Wireless LAN's do not respect physical or logical boundaries.
D PAN's can provide an alternative means for accessing campus networks.

71 Which of the following would be an appropriate security control for an organisation operating a BYOD policy?

A Ability to remotely delete individual emails on the device.
B Ability to remotely monitor the device locations at all times regardless of use.
C Ability to remotely remove corporate applicators, provided by enterprise app store.
D Ability to remotely download the login credentials from the device.

72 When protecting web servers and web applications against web based attacks in the corporate or cloud service provider data centre, what control would be the MOST effective?

A WAF.
B IDS.
C NAT.
D VPN.

73 If an organisation wants to implement a control to inspect the payload of secure web based communication entering or leaving its business network, which of the following techniques would be the **MOST** appropriate?

A Use of a Web Proxy.
B Key Declaration Policy.
C Use of a VPN.
D Packet Sniffing.

74 When trying to protect an organisation's VOIP systems, which of the following threats is the MOST important to consider?

A VLAN hopping between PC Desktop and VOIP based VLAN's.
B Denial of Service attacks on the call manager.
C Eavesdropping on LAN based conversations.
D Port Scanning individual VOIP phones.

75 When protecting secure email exchange between an email client and server or between message transfer agents, the use of what protocol would be an effective control?

A IMAP.
B SNMP.
C POP3.
D SMTPS.

76 In an Infrastructure as a Service cloud computing environment, who is responsible for ensuring firewall security controls are in place?

A Customer's security team.
B System’s Integrator.
C Cloud Provider.
D Customer’s Data Protection Team.

77 What is **one** of the **MAJOR** considerations relating to the storage of data in a cloud environment compared to conventional on premises data storage?

A Data could be stored in any geographic destination.
B Data may be prevented from crossing international borders.
C Data may not be duplicated as needed.
D Data must not be encrypted in cloud locations.

78 How might the adoption of Software as a Service cloud environments act as a control that improves the security of an organisation's client desktop environments?

A Negates the need to have anti-virus installed on end clients.
B Reduces the complexity of desktops as only a browser is needed.
C Negates the need to have any encryption on the user device.
D Can adopt BYOD as the organisation no longer needs to provide own clients.

79 Which of the following is the **MOST** significant risk to organisations adopting a cloud service and requiring a technical control?

A Termination of service by cloud service provider.
B Over subscription of customers storage allocation.
C Exceeding Service Level Agreement levels.
D Ownership of data stored on cloud systems.

80 Which of the following is **NOT** a valid statement on the technical controls necessary for cloud computing?

A Organisations can use proxy and brokerage services to separate clients from direct access to shared cloud storage.
B Any distributed application has a much greater attack surface than an application that is closely held within a LAN environment.
C As Cloud computing is entirely on-premise, all vulnerabilities associated with Internet applications are associated with the local hardware.
D As virtualisation underpins cloud computing, the hypervisor is a key security risk.

81 An essential function for any security operations team is to have a centralised event logging capability with an overall view of all incidents that happen within an organisation's infrastructure.

Which of following computing systems will provide this capability?

A IDS.
B SIEM.
C ISMS.
D CMS.

82 In which part of a threat modelling process is the acronym STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service & Elevation of Privilege) particularly useful?

A Vulnerability assessment.
B Threat categorisation.
C Data misuse testing.
D Penetration Test planning.

83 Which of the following can be used to help the "authorisation" process?

A Access Control List.
B Username.
C Password.
D Token.

84 An organisation has collected data from a range of industries to create a list of security controls for areas such as operating systems, server software and network devices.

Creating benchmarks from these lists is an example of what practice?

A Undertaking a risk assessment.
B Threat modelling.
C Checking system availability.
D Using security baselines.

85 What security measure can be put in place to provide an additional security control in the event that backup tapes (or other storage) are lost or stolen?

A Keep multiple copies of the backup media.
B Transfer the backup from one media to another.
C Use appropriate media identification labels.
D Use strong AES256 encryption.

86 Many modern data centre locations may operate on a 24/7 basis but may have few or even no security staff on site during the operational periods.

In order to manage physical security remotely, which of the following provide the **BEST** monitoring means of verifying results?

A IDS and IPS.
B CCTV and motion detectors.
C Faraday cage and turnstiles.
D Door keypad and asset tags.

87 Which of the following considerations does **NOT** describe the physical security requirements for a wiring closet?

A Locate only in areas regularly patrolled by security staff.
B Single use as a wiring closet and no sharing with other functions.
C Use door sensors to log entry attempts to the wiring closet.
D Perform regular physical inspections of the wiring closet.

88 When disposing of IT equipment with data retention capabilities (which may be built in flash memory or a magnetic hard drive) which of the following controls is the **MOST** reliable to ensure no data remains on the device?

A Multiple data wipes of the storage media.
B Removing the hard drive and selling the remaining device online.
C Ensuring device is crushed and reduced to small particles.
D Leave the device on a large magnet overnight.

89 When both confidential paper printouts and documents are no longer needed, which of the following is the recommended approach to ensure secure disposal?

A Use of a standard 1cm width shredder and selling as packaging.
B Burning documents in an incinerator in the employee car park.
C Use the local standard waste recycling service.
D Use of a diamond shredder before managed disposal takes place.

90 Which technology can be used to help track components and goods securely through a supply chain, during logistics operations, delivery and storage?

A RFID.
B IEEE 802.16.
C Barcodes.
D Tokens.

91 Which of these potential actions might take place as part of a business continuity plan?

A Relocating to a warm site.
B Restoring from backup media.
C Implementing a RAID system.
D Rebooting business operations.

92 In the event of a disaster, an organisation needs to have a contract with an alternative data processing facility which will provide HVAC, power and communications infrastructure but no computing hardware.

Which type of facility is this?

A Cold site.
B Warm site.
C Hot site.
D Spare site.

93 As part of disaster recovery planning, the storage of backup data multiple locations is considered best practice.

Which of the following are considered to be suitable locations?

1. Within a secure cloud storage service.
2. Offsite within a firesafe.
3. Onsite in an office cabinet.
4. Stored at workers home garage.

A 3 and 4.
B 1 and 2.
C 1, 2 and 3.
D 1, 2, 3 and 4.

94 When undertaking disaster recovery planning, which of the following would be considered a disaster?

1. Cyber Attack.
2. Flood.
3. Fire.
4. Riot.

A 1, 2 and 3.
B 2 and 3.
C 4 only.
D 1, 2, 3 and 4.

95 An organisation is planning to undertake a disaster recovery test. They want to perform a live test on the disaster recovery site without interrupting the operation of the live facility.

Which type of test **SHOULD** the organisation choose?

A Full disruption test.
B Checklist review.
C Parallel test.
D Simulation test.

96 When handling "digital evidence" especially with the involvement of third parties, what important concept **MUST** be adhered to?

A Separation of duties.
B Chain of custody.
C Shared keys.
D No copying of evidence.

97 As part of a law enforcement investigation which involves the recovery of digital evidence from a crime scene, which of the following are important concepts to adhere to when possible?

1. Investigators must be competent to undertake a review of evidence.
2. Data must not be altered unless absolutely necessary.
3. Only law enforcement officers can undertake forensic investigations.
4. Notes must be kept on all forensic investigations undertaken.

A 1, 2, 3 and 4.
B 1, 2 and 3.
C 1 and 2.
D 1, 2 and 4.

98 What technique is used by law enforcement and commercial organisations to determine what threat data may be available from sources on the Internet, Deep web and the Dark Web?

A Open Source Intelligence.
B Open Source Software.
C Open Cyber Analysis.
D Open Web Applications.

99 A message is sent from Bob to Alice.

In order for Alice to prove to a third party like Fred that the message received definitely came from Bob, which attribute of cryptography is being attempted?

A Non-repudiation.
B Authorisation.
C Confidentiality.
D Authentication.

100 Betty has received a message from Valerie, which Valerie has encrypted using symmetric cryptography.

Which key **SHOULD** Betty use to decrypt the message?

A Betty's public key.
B Valerie's public key.
C Shared secret key.
D Valerie's private key.

End of Paper