BCS Foundation Certificate in Information Security Management Principles

Specimen Paper

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

Specimen paper only 20 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 [33/50]

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

1 Which of the following statements describes the concept of non-repudiation?

A The ability to prove that an event occurred.
B The use of public key cryptography to prevent the republishing of keys.
C A technology-based non-disclosure agreement.
D Cyber security insurance to help reduce reputational harm.

2 Which term describes the concept used in information security in which multiple layers of security controls are placed within a system?

A Defence in depth.
B Honeypot.
C Fail safe.
D Anti-malware.

3 Which **two** terms are used in combination to define levels of risk?

A Threat and Impact.
B Threat and Vulnerability.
C Impact and Likelihood.
D Likelihood and Vulnerability.

4 What term defines the amount and type of risk that an organisation is prepared to pursue, retain or take?

A Risk Tolerance.
B Risk Appetite.
C Risk Aversion.
D Risk Acceptance.

5 What is the **PRIMARY** benefit of implementing appropriate information security within an organisation?

A Improved resilience against and recovery time from a harmful incident.
B Protection of shareholder value.
C Certification against ISO 27001.
D Protection of Board Members from post-event litigation.

6 How might threats such as human error, malfunctions, fire and flood be defined?

A Malevolent.
B Environmental.
C External.
D Accidental.

7 Which of the following is defined as a deliberate threat?

A Dark Web.
B Bring your own device (BYOD).
C Ransomware.
D Flood.

8 Within an information security context, which phrase describes the collection and analysis of information that is gathered from public sources?

A Pre-exploit vulnerability management (PE/VM).
B Open Source Intelligence (OSINT).
C Collecting applicable data and analysing behaviour to identify malevolent actors (AppAnAct).
D Analysis of information such as police crime recording systems and commercial sources (LawSys).

9 Which of the following is a strategic option for dealing with information risk?

A Avoidance.
B Detection.
C Impact assessment.
D Erasure.

10 When setting out an information classification strategy, what is the **first** step you should take?

A Agree the relevant information classification labels.
B Develop the information classification policy.
C Identify relevant information and process owners.
D Determine the classification programme objectives.

11 Which of the following describes the difference between a statutory requirement and an advisory requirement?

A Statutory requirements almost always only apply to specific industries and sector - advisory requirements need to be met by all organisations.
B Statutory requirements need government empowerment, advisory requirements are enacted through lower-level bodies.
C Both types of requirement are fundamentally the same in practice.
D A statutory requirement is prescribed by law, an advisory requirement is typically a recommendation.

12 What is the **MOST IMPORTANT** role of senior management in regard to information security?

A Ensuring all external and internal audits are completed on time.
B Providing visible and material support for information security within the organisation.
C Chairing the organisation's Security Working Group (SWG).
D Appointing a suitably qualified CISO.

13 What is a common term for an organisation's end user code of practice?

A Acceptable Use Policy.
B Joiners, Leavers and Movers (JLM) process.
C End User licence agreement.
D Security Aspects Letter.

14 What overarching term is used to describe the protection of personal data, restrictions on monitoring, surveillance, communications interception and so forth?

A Protective Monitoring.
B Authentication.
C Privacy.
D Non-repudiation.

15 In what circumstances might an information security legal obligation 'flow down'?

A Outsourcing to a third party via a contract.
B Within a process control mapping exercise.
C From Gold to Silver then Bronze levels during incident management.
D From Senior Security Working Groups to lower level bodies.

16 Which term is used to cover the legal rights which result from activity in the industrial, scientific, literary and artistic fields?

A Intellectual Property.
B The Right to be Forgotten.
C Moral principles.
D Exclusive authority to use a resource.

17 Which of the following **BEST** describes ISO/IEC 27001?

A A framework and a process for managing risk.
B Information Security Management System implementation guidance.
C A specification for an Information Security Management System.
D Guidelines for people aspects of business continuity.

18 Identify which of the following standards relate to the certification of security products?

A NIST 800-53.
B ISO/IEC 27002.
C ISACA.
D ISO/IEC 15408.

19 Which of the following is **NOT** recognised as one of the stages in the information lifecycle?

A The creation and/or acquisition of data.
B The securing of data.
C The publication of data.
D The retention and/or removal of data.

20 From a security viewpoint, why is the information management cycle **IMPORTANT**?

A It reduces risk.
B It reduces costs.
C It improves compliance.
D It improves service.

21 Which of the following is a security architecture framework?

A MS Azure.
B DevSecOps.
C SABSA.
D OWASP.

22 Which acronym describes the technique **NORMALLY** deployed by a Security Operations Centre (SOC) to prevent illicit intrusion?

A IPS.
B IDS.
C Whitelisting.
D Sandbox.

23 What term describes the mutually agreed storage of important source code to reduce risk of its loss or destruction?

A Escrow.
B Code verification.
C Reciprocity.
D Shrink-wrap.

24 Which of the following would you expect to find in an Acceptable Use Policy?

A Key management principles.
B Code of Conduct.
C SWG terms of reference.
D Risk acceptance criteria.

25 How might segregation of duties reduce risk?

A Preventing staff from attaining skills across an entire process and thereby rendering it vulnerable.
B Isolating key workers so they cannot socialise.
C Reducing the possibility of a unionised workforce.
D Preventing an individual from having sole responsibility for payments.

26 What term is used to describe the passing on of contractual obligations from a supplier to a third party organisation?

A Cascade.
B Pass-through.
C Flow down.
D Transmutation.

27 What term is used to describe the use of both passwords and a PIN-activated token device to access a system?

A Dual onion skin.
B Chip and PIN.
C Two Factor Authentication.
D Moat and Rampart.

28 How would you describe the management of system access by root users in UNIX and Database Administrators?

A Privileged User Management.
B Sysadmin and superuser containment.
C Sudo passthrough.
D OS segregation support.

29 Why might audio-visual based security training be more effective that standard PowerPoint slides?

A Not all systems use Windows so PowerPoint may not be appropriate in all circumstances.
B PowerPoint slides are becoming old fashioned and predictable.
C Audio-visual training provides input via two senses - improving and reinforcing learning.
D Voice delivery is always more effective than visual delivery.

30 Why might a system administrator require different training to a standard user?

A Administrators normally operate using skills, tools and access rights that exceed the normal user requirement.
B Administrators need to be made to feel they are a special case as they have special skills.
C Standard users rarely attain the education levels of administrators, so require training that contains simple terms and concepts.
D Standard users have no 'need to know' about technical risks and threats, so should not be made aware of them.

31 In information security terms, which of the following defines a Trojan?

A Malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
B Malware which misleads users of its true malicious intent whilst masquerading as something harmless.
C Malware that illicitly controls a number of internet-connected devices and makes them perform malicious actions such as denial of service attacks.
D Malware that replicates itself in order to spread to other computers.

32 What is meant by the term 'whaling'?

A Fraudulently telling rich bank account holders to dial a phone number regarding problems with their bank accounts.
B Cloning a legitimate, and previously delivered, email containing an attachment or link that is malicious.
C Redirecting web traffic using JavaScript commands to alter the address bar of a website.
D Creating spear-phishing attacks directed specifically at senior executives and similar high-profile targets.

33 How might network partitioning improve network security?

A Preventing users from having unrestricted universal access to all resources within a network.
B Reducing the logistical complexity of network administration.
C Increasing the range of access to resources across a large network.
D Merging the internal network with the Internet thereby reducing the visibility of public network end points.

34 What is the difference between a vulnerability assessment and a penetration test?

A Vulnerability assessments actively seek out and exploit vulnerabilities and assess the probable impact of their exploitation. Penetration tests are passive.
B There is no material difference between vulnerability assessment and penetration testing as they are both passive and stealthy.
C Vulnerability assessments search systems for known vulnerabilities, whilst penetration tests try to actively exploit vulnerabilities.
D Vulnerability assessments exploit the vulnerabilities they find. Penetration tests are stealthy and perform no actions that might betray their presence on a network.

35 Which of the following **BEST** describes a VPN?

A A VPN prevents SQL injection thereby preventing malicious scripts being inserted into trusted websites.
B A VPN secures data traffic by splitting a computer network into subnetworks.
C A VPN is a set of object-oriented programming technologies and tools that facilitate rich media playback.
D A VPN provides online privacy and anonymity by creating a private network through a public internet connection.

36 Which of the following seeks to stop illicit access into a network or system?

A IPS.
B IDS.
C PCI DSS.
D APT.

37 Which document sets out a code of practice for information security controls for cloud services?

A ISO/IEC 27017.
B ISO/IEC 27002.
C ISO 31000.
D ISO 9001.

38 Which of the following cloud based services is **LEAST LIKELY** to cause legal problems relating to Intellectual Property Rights (IPR)?

A Software-as-a-Service.
B Infrastructure-as-a-Service.
C Platform-as-a-Service.
D Analyst-as-a-Service.

39 What is the core change required when moving from a traditional IT management set up and a cloud-based approach?

A The redeployment or removal of current IT support staff.
B The dismantling of all physical security controls.
C Focus on management of contracts rather than technology.
D Immediate certification to ISO/IEC 27001.

40 Within which of the following would you expect to find a list of information assets within an organisation?

A CMDB.
B ISMS.
C BCDR.
D CISO.

41 Which of the following describes a SIEM capability?

A A repository that acts as a data warehouse that stores information on an IT estate.
B A software licensing and delivery model in which software is licensed on a subscription basis.
C A set of policies and standards that support the management of an organisation's sensitive data.
D Software that aggregates and analyses activity from many different resources across an IT estate.

42 Which term describes the process by which potential threats can be identified, enumerated, and mitigation actions planned?

A Threat modelling.
B Threat vectoring.
C Threat landscaping.
D Threat hunting.

43 What term is often used to describe an approach that uses multiple layers of physical security controls to protect information assets?

A Thermal layering.
B Onion skin.
C Security through obscurity.
D Asset dispersal.

44 What kind of countermeasure might be used to protect information in transit across a physically unprotected environment?

A Coaxial cable.
B Cat 5 Ethernet.
C Armoured cable.
D Twisted pair.

45 What control is **MOST LIKELY** to be used to monitor general user behaviour within a datacentre computer hall?

A Access control card.
B PIN Pad.
C CCTV.
D PIR.

46 Which of the following international standards is **MOST** closely associated with business continuity?

A COBIT.
B ISO/IEC 27001.
C NIST SP 800-53.
D ISO 22301.

47 What is the difference between business continuity and disaster recovery?

A Business continuity is about ensuring an organisation continues to operate during a disruptive event. Disaster recovery is the process of resolving the disruption itself.
B The two terms are so closely aligned they can be used interchangeably.
C Business continuity focuses entirely on planning. Disaster recovery focuses on tactical activities during a disaster.
D Business continuity sets out governance thereby providing policy and standards. Disaster recovery uses these to enact recovery.

48 What types of legislation **MUST** be taken into account when conducting investigations involving children and minors?

A Privacy / Data Protection.
B Computer Misuse.
C Intellectual Property protection.
D National security.

49 Which of the following terms describes forensic computer evidence such as cached data?

A Scientific.
B Fixed.
C Circumstantial.
D Volatile.

50 What is the core purpose of a PKI?

A To encrypt large databases containing personal and financial information.
B To facilitate the secure electronic transfer of information for a range of network activities.
C To protect national security when using the internet.
D To preserve the Intellectual Property Rights (IPR) organisations operating within the government and defence sectors.

End of Paper

BCS Foundation Certificate in Information Management Security Principles
Answer Key and Rationale

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	Non-repudiation is about proof.	LO1.1.
2	**A**	Defence in depth focuses on layering of controls.	LO1.1.
3	**C**	The components of risk are very specific.	LO1.1.
4	**B**	All the terms used are valid, but appetite is the specific term required.	LO1.2.
5	**A**	Resilience and recovery are PRIMARY benefits.	LO1.2.
6	**D**	Common denominator in this list is 'accidental'.	LO2.1.
7	**C**	Ransomware the only threat that involves deliberate action.	LO2.1.
8	**B**	OSINT is the only recognised term offered.	LO2.1.
9	**A**	All incorrect options are tactical.	LO2.2.
10	**D**	Correct option is the first in a well understood sequence.	LO2.2.
11	**D**	Statutes relate to law.	LO3.1.
12	**B**	Correct option is primary and strategic.	LO3.1.
13	**A**	All offered terms are common – AUP the only code of practice.	LO3.1.
14	**C**	Privacy is an over-arching term. The others are tactical or procedural.	LO3.2.
15	**A**	Flow down is the common contractual term.	LO3.2.
16	**A**	Intellectual property is the only response that meets the criteria listed. Others are more general.	LO3.2.
17	**C**	All responses are relevant to a degree, but the correct one is specific to 27001.	LO3.3.
18	**D**	ISO/IEC 15408 the only produce related response.	LO3.3.
19	**B**	Securing information isn't needed in all information lifecycles.	LO4.2.
20	**A**	Risk reduction is the most important result of information security.	LO4.1.
21	**C**	All terms are relevant to infosec – SABSA the only framework listed.	LO4.3.
22	**A**	All terms SOC related – IPS the only preventative measure.	LO4.4.
23	**A**	'Escrow' covers legal, mutual agreements.	LO4.5.
24	**B**	Acceptable use relates to conduct.	LO5.1.

Question	Answer	Explanation / Rationale	Syllabus Sections
25	**D**	Segregation of duties spreads responsibility.	LO5.1.
26	**C**	Flow down is the common term for the spread of obligations.	LO5.1.
27	**C**	TFA covers knowledge and possession of a secure device.	LO5.2.
28	**A**	All responses contain relevant terms - Privileged User Management.is the only recognised one.	LO5.2.
29	**C**	Two comms channels improve learning and knowledge retention.	LO5.3.
30	**A**	Admins requirements exceed the norm.	LO5.3.
31	**B**	Trojan horses are about deception.	LO6.1.
32	**D**	Whaling concerns itself with high level and high value targets.	LO6.1.
33	**A**	Partitioning reduces access to what is needed.	LO6.2.
34	**C**	Vulnerability assessments do not involve exploitation.	LO6.2.
35	**D**	VPNs create secure, private tunnels through insecure environments.	LO6.3.
36	**A**	IPS is about prevention of access.	LO6.3.
37	**A**	ISO/IEC 27017 is the only cloud specific publication listed.	LO6.4.
38	**B**	IaaS is only concerned with physical infrastructure, not the system content.	LO6.4.
39	**C**	Cloud and outsourcing require contract management before all else.	LO6.4.
40	**A**	All offered terms are genuine – only CMDB lists assets.	LO6.5.
41	**D**	SIEM services focus on activity.	LO6.5.
42	**A**	All offered terms relevant, but modelling is specific to the activities listed.	LO6.5.
43	**B**	Onion skin is a specific term of layering of controls.	LO7.1.
44	**C**	Armoured cables are the only network control listed.	LO7.1.
45	**C**	Only CCTV and PIR are monitoring tools. PIR rarely used in computer halls due to constant thermal changes and issues in such an environment.	LO7.1.
46	**D**	ISO 22301 is specific to BC/DR – others may reference the matter but are more general.	LO8.1.
47	**A**	Correct response covers the dual elements of preparation and mitigation.	LO8.1.
48	**A**	Almost all privacy legislation makes special reference to records relating to minors.	LO9.1.
49	**D**	Volatility relates to many temporary file stalls including caches.	LO9.1.

Question	Answer	Explanation / Rationale	Syllabus Sections
50	**B**	PKI is primarily about transference	LO9.2.