BCS Level 4 Award in Risk Assessment
QAN 603/0866/7

Specimen Paper

Version 3.0
July 2020

Change History

Any changes made to the specimen paper shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
Version 1.0 November 2016	Document created.
Version 2.0 September 2017	Updated following enhanced syllabus creation.
Version 2.1 July 2018	Updated – minor tweak.
Version 3.0 July 2020	Major changes to questions to match updated syllabus (V3.0). Title page, change history table and related syllabus section added.

Related Syllabus

This specimen paper and answer key are related to the following syllabus:

BCS Level 4 Award in Risk Assessment Syllabus V3.0 March 2020

BCS Level 4 Award in Risk Assessment
QAN 603/0866/7

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 for 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.

The pass mark is 13/20.

This is a specimen examination paper only.

This qualification is regulated by Ofqual (in England).

1 When assessing the impact of a risk, which of the following **COULD** be affected?

A Productivity.
B Wastage.
C Vulnerability.
D Finality.

2 When conducting a risk assessment, which of the following **SHOULD NOT** be considered?

A Vulnerability.
B Damage to reputation.
C Timing.
D Blame.

3 Which of the following is an industry recognised risk assessment methodology?

A OCTAVE.
B Risks Inside of Technology (RIOT).
C Risks Outside of Technology (ROOT).
D LAVA.

4 According to NIST SP 800-30, risk assessment can be integrated into which of the following?

A Risk and reward system.
B Risk management framework.
C Risk aversion therapy.
D OCTAVE.

5 What is the **KEY** element of a successful system-driven risk analysis?

A Specifying the most expensive system hardware available.
B Understanding the license model for that system.
C Understanding and defining the system's function(s).
D Having a valid support contract for the system.

6 Which of the following **BEST** describes how a company should address risk assessment?

A They must follow the guidance from their government (otherwise it is illegal).
B They should find out what their insurance company says and go with their recommendation.
C They should find what works for them (complying with any mandated requirements).
D They must follow an industry recognised standard (e.g. Octave).

7 A successful DDOS attack is **MOST LIKELY** a result of which vulnerability?

A Inadequate network defences.
B Training and awareness.
C Configuration and integration.
D Organisational change.

8 Which of the following statements **BEST** describes a company with poor patch management, lack of documentation, poor training and awareness and no monitoring?

A They have lots of little security problems to address.
B The management is only interested in profit.
C They have a weak security culture overall.
D The management need to test the staff.

9 Why are people usually considered to be the weakest link in the security chain?

A People always perform to the right standard.
B People are always easy to manipulate.
C People can never make mistakes at work.
D People can be poorly trained or get distracted and make a mistake.

10 Which of the following activities is **MOST LIKELY** to increase the culture of cyber security within a business?

A Training employees on their induction.
B Installing the latest anti-virus software every year.
C Installing the latest hardware every year.
D Regular employee training.

11 When thinking of cyber culture within an organisation, what is the **MOST LIKELY** outcome of employees being punished for a cyber incident?

A Incidents are more likely to be reported and the cyber culture is enhanced.
B Incidents will stop happening as the cyber culture is fully working.
C Incidents are less likely to be reported and the cyber culture is diminished.
D Incidents will happen all the time as the cyber culture has been diminished.

12 Which of the following combinations **BEST** describes the threat actor and threat in the following scenario?

A salesperson copies the company client database to use at his new job.

A An individual and information theft.
B An insider and information theft.
C An activist and information disclosure.
D An insider and information disclosure.

13 Which of the following is a 'threat actor'?

A Flood.
B SQL injection.
C Disgruntled insider.
D Failure to encrypt.

14 Which stage within the intelligence lifecycle includes understanding which information assets and business processes need to be protected?

A Direction.
B Processing.
C Analysis.
D Feedback.

15 Which of the following is the CORRECT order of the stages of the intelligence lifecycle?

A Direction, Collection, Processing, Analysis, Dissemination, Feedback.
B Direction, Analysis, Dissemination, Collection, Processing, Feedback.
C Analysis, Dissemination, Feedback, Direction, Collection, Processing.
D Direction, Feedback, Collection, Dissemination, Processing, Analysis.

16 Which of the following is **MOST LIKELY** to be a reason to use the transference of risk as an appropriate treatment?

A The technical solution is low cost and the skills are standard.
B The technical solution is complex and the skills required are in high demand.
C There are many technical solutions available with similar skills required.
D The technical solution is simple and the skills are standard.

17 Which of the following activities is **NOT** an example of using 'reduce' as a risk treatment?

A Purchasing anti-malware software.
B Purchasing cyber insurance for malware.
C Purchasing phishing training for staff.
D Purchasing an email filtering solution.

18 Which of the following **BEST** describes the role of a risk owner?

A The person who owns and maintains the company risk register.
B The person responsible for all the risk assessments in a company.
C The person who runs the company and owns all the risks.
D The person with knowledge and authority to manage the specific risk.

19 Which of the following **BEST** describes the purpose of the Single Loss Expectancy (SLE) calculation?

A It is the starting point to calculate the Annualised Rate of Occurrence (ARO).
B It is the starting point to calculate Annualised Loss Expectancy (ALE).
C It is the end of the Risk to Loss (RtL) calculations.
D It is the end of the Annual Loss Adjustment (ALA) calculations.

20 Why might a financial services organisation choose a quantitative risk assessment method rather than a qualitative approach?

A Qualitative methods are more objective.
B Qualitative methods take too long.
C Quantitative methods aim to measure exposure.
D Quantitative methods are mandatory in all sectors.

-End of Paper-