Annex C. Expert Knowledge Verification Questionnaire

This annexe presents the questionnaire used for expert knowledge verification. Questionnaire was prepared according ISACA CRISC (Certified in Risk and Information Systems Control) certification program. Questions were taken from ISACA CRISC Practise Quiz[1] and CRISC Certification Exam app by Zirotek[2] during the preparation of the questionnaire.

Table C.1. Seed questions for expert knowledge verification (Created by author)

No.	Question	Answer
1.	Which of the following is the BEST indicator that incident response training is effective? a) Decreased reporting of security incidents to the response team b) Increased reporting of security incidents to the response team c) Decreased number of password resets d) Increased number of identified system vulnerabilities	B
2.	Which of the following factors will have the GREATEST impact on the type of information security governance model that an enterprise adopts? a) The number of employees b) The enterprise's budget c) The organizational structure d) The type of technology that the enterprise uses	C
3.	An enterprise learns of a security breach at another entity using similar network technology. The MOST important action for a risk practitioner is to: a) Assess the likelihood of the incident occurring at the risk practitioner's enterprise b) Discontinue the use of the vulnerable technology c) Report to senior management that the enterprise is not affected d) Remind staff that no similar security breaches have taken place	A

[1] https://www.isaca.org/-/media/info/crisc-practice-quiz/index.html
[2] https://apps.apple.com/us/app/crisc-certification-exam/id1300743101

Continue of Table C.1

No.	Question	Answer
4.	Which of the following is MOST relevant to include in a cost-benefit analysis of a two-factor authentication system? a) The approved budget of the project b) The frequency of incidents c) The annual loss expectancy of incidents d) The total cost of ownership	D
5.	A global financial institution has decided not to take any further action on a denial-of-service vulnerability found by the risk assessment team. The MOST likely reason for making this decision is that: a) The needed countermeasure is too complicated to deploy b) There are sufficient safeguards in place to prevent this risk from happening c) The likelihood of the risk occurring is unknown d) The cost of countermeasure outweighs the value of the asset and potential loss	D
6.	Which of the following examples includes ALL required components of a risk calculation? a) Over the next quarter, it is estimated that there is a 30 percent chance of two projects failing to meet a contract deadline, resulting in a US $500,000 fine related to breach of service level agreements b) Security experts believe that if a system is compromised, it will result in the loss of US $15 million in lost contracts c) The likelihood of disk corruption resulting from a single event of uncontrolled system power failure is estimated by engineers to be 15 percent d) The impact to security of a business line of a malware-related workstation event is estimated to be low	A

Continue of Table C.1

No.	Question	Answer
7.	Which of the following is MOST useful in developing a series of recovery time objectives? a) Regression analysis b) Risk analysis c) Gap analysis d) Business impact analysis	D
8.	In an operational review of the processing environment, which indicator would be MOST beneficial? a) User satisfaction b) Audit findings c) Regulatory changes d) Management changes	A
9.	Which of the following is the BEST way to ensure that contract programmers comply with organizational security policies? a) Have the contractors acknowledge the security policies in writing b) Explicitly refer to contractors in the security standards c) Perform periodic security reviews of the contractors d) Create penalties for noncompliance in the contracting agreement	C
10.	An IT organization has put in place an anti-malware system to reduce risk. Assuming the control is working within specified parameters, which of the following statements BEST describes how this control reduces risk? a) The control reduces the probability of malware on company computers but does not reduce the impact of those attacks b) The control reduces the impact of malware on company computers but does not reduce the probability of those attacks c) The control reduces the probability and impact of malware on company computers d) The control reduces neither probability nor impact of malware on company computers	B

Continue of Table C.1

No.	Question	An-swer
11.	Which of the following risks is the risk that happen with an important business partner and affects a large group of enterprises within an area or industry? a) Contagious risk b) Reporting risk c) Operational risk d) Systematic risk	D
12.	What is the PRIMARY need for effectively assessing controls? a) Control's alignment with operating environment b) Control's design effectiveness c) Control's objective achievement d) Control's operating effectivenes	C
13.	Which of the following components of risk scenarios has the potential to generate internal or external threat on an enterprise? a) Timing dimension b) Events c) Assets d) Actors	D
14.	Which of the following is the priority of data owners when establishing risk mitigation method? a) User entitlement changes b) Platform security c) Intrusion detection d) Antivirus controls	A

Continue of Table C.1

No.	Question	Answer
15.	You are the project manager of your enterprise. You have introduced an intrusion detection system for the control. You have made identified a warning of violation of security policies of your enterprise. What type of control is an intrusion detection system (IDS)? a) Detective b) Corrective c) Preventative d) Recovery	A
16.	Which of the following should be PRIMARLY considered while designing information systems controls? a) The IT strategic plan b) The existing IT environment c) The organizational strategic plan d) The present IT budget	C
17.	Which of the following is the MOST important use of KRIs? a) Providing a backward-looking view on risk events that have occurred b) Providing an early warning signal c) Providing an indication of the enterprise's risk appetite and tolerance d) Enabling the documentation and analysis of trends	B
18.	Which of the following is an administrative control? a) Water detection b) Reasonableness check c) Data loss prevention program d) Session timeout	C
19.	Which of the following are the principles of access controls? Each correct answer represents a complete solution. Choos three. a) Confidentiality b) Availability c) Reliability d) Integrity	ABD

End of Table C.1

No.	Question	An-swer
20.	You are the project manager in your enterprise. You have identified risk that is noticeable failure threatening the success of certain goals of your enterprise. In which of the following levels do this identified risk exist? a) Moderate risk b) High risk c) Extremely high risk d) Low risk	A