Final control questions for the subject “Introduction to Information Security Risk Management” for fourth-year students of the educational program 5330300 - Information Security (by field)

1. Describe the concepts of risk, threat, and vulnerability?
2. What is an information asset and what objects does it include?
3. Explain the purpose of risk analysis?
4. What are the stages of risk analysis?
5. Describe the concept of "bow-tie" analysis.
6. Explain the factors indicated in the " bow-tie " analysis.
7. Describe the concept of negation tree analysis.
8. Explain the factors listed on the rejection tree.
9. Describe the concept of situational tree analysis.
10. What is the use of the situational tree?
11. What types of context exist?
12. What is the difference between external and internal context?
13. At which level of risk assessment is context initially established?
14. If the context provides sufficient information to effectively identify actions necessary to reduce risk to an acceptable level, what action is taken regarding the risk?
15. Explain the process of identifying information assets.
16. How is the value of a primary asset identified?
17. How is the value of a secondary asset identified?
18. What threats are associated with physical access to information systems?
19. What stages does the information security risk assessment process include?
20. What are the main methodological shortcomings of traditional approaches to assessing information security risks? What innovative approaches can be used to address these shortcomings?
21. What steps does the information security risk analysis process involve?
22. At which stages of the information security risk assessment might the participation of business process owners be required, and why?
23. Is it advisable to maintain a regularly updated list of the organization's assets, and how can this affect the process of assessing information security risks?
24. What is the process of assessing information security risks in Information and Communication Technologies?
25. What are the most important outcomes for the organization resulting from the information security risk assessment process?
26. What are the similarities and differences between high-level and detailed analysis approaches of information security risks?
27. What methods are available for assessing information security risks?
28. What is the essence of qualitative assessment of information security risks?
29. How is a quantitative assessment of information security risks conducted?
30. What do risk level and its relevance mean?

31. What actions can be taken regarding the identified risks?

32. What are the main methods of managing information security risks? What is the primary purpose of each method?

33. Who has sufficient authority to determine the acceptable level of risk in the organization, and why?

34. Based on what information should a decision be made about the acceptable level of information security risk?

35. What measures are available to reduce information security risk to an acceptable level?

36. How and by whom is the planning of measures for processing information security risks carried out?

37. What is the difference between the concepts of retaining and accepting information security risks?

38. What are the input and output data for the processes of retaining and accepting information security risks?

39. What is "information security risk attitude"?

40. What are the objectives of implementing activities related to information security risk attitude?

41.How are information security risks controlled and verified?

42. What is risk monitoring?

43. How is risk monitoring and revision carried out?

44. What is the essence of monitoring and revising AI risk indicators?

45. What are the input and output data for monitoring and reviewing the process of managing all AI risks?

46. What are the stages of automated procedures within the framework of the CRAMM method?

47.Describe the strengths of the CRAMM method.

48. What parameters does the CRAMM recommend using to assess potential damage?

49. How many common recommendations are there among CRAMM identified risks and countermeasures corresponding to their levels?

50. What value of the CRAMM vulnerability rating scale corresponds to an incident occurring on average every three years?

51. What do you mean by business continuity?

52. The basics of continuous work planning?

53. How to test the continuous control plan?

54. What is an asset that has the same value as other important assets of a business?

55. What does business continuity management include as a comprehensive management process?

56. What is the concept of information security risks?

57. How to define the term "information security risk management"?

58. What are the main tasks of managing information security risks?

59. List and label all the key components of the risk management process.

60. Identify a system for managing information security risks.

61.Which stage of the information security risk management process requires the most labor, and why?

62. How is the context of information security risk management defined?

63. What are the possible criteria for assessing information security risks?

64. How are the criteria for assessing the consequences (impact) of information security risks determined?

65. What are the possible criteria for accepting information security risks?

66.Explain the factors listed on the rejection tree.

67.What does the risk level and its urgency mean?

68.What is business continuity management as a comprehensive management process includes?

69.Describe the role of a Risk Assessment Matrix in evaluating risks?

70.What are the key components of a Business Impact Analysis (BIA)?

71.It is advisable to regularly maintain the organization's asset list and how might this impact the risk assessment process?

72.How are information security risks controlled and verified?

73.What are the most important results for the organization as a result of implementing the information security risk assessment process?

74.What are the steps in the risk management process?

75.Differentiate between qualitative and quantitative risk assessment methods. Provide an example of when each method is appropriate?

76.What are the similarities and differences between approaches to high-level and detailed analysis of information security risks?

77.What is an asset that has the same value as other important assets of a business?

78.What is business continuity management as a comprehensive management process includes?

79.What measures are available to reduce information security risks to an acceptable level?

80.How and by whom is the planning of measures for processing information security risks carried out implemented?

81.Explain the risk management lifecycle, including its key stages and the role of continuous monitoring.

82.What is the difference between the concepts of storing and accepting information security risks?

83.What are the input and output data for the processes of storing and accepting information security risks?

84.What are the objectives of implementing activities related to information security risk management?

85.Define the terms threat, vulnerability, and risk, and explain their interrelationship.
86.Why is it important to align information security risk management with organizational objectives?
87.Differentiate between qualitative and quantitative risk assessment methods. Provide an example of when each method is appropriate.
88.Has sufficient authority to address acceptable risk levels within the organization who and why?
89.Based on what data, make a decision about the acceptable level of risk need to do?
90.What is the essence of qualitative assessment of information security risks?
91.How is risk monitoring and revision carried out?
92. What are the input and output data for monitoring and reviewing the entire information security risk management process?
93.What are the threats associated with physical access to information systems?
94.What steps does the information security risk assessment process involve?
95.The main methodological foundations of traditional approaches to assessing information security risks what are the drawbacks? What innovations can be used to overcome these shortcomings can approaches be used?
96. Identify the value of the primary asset?
97.What steps does the information security risk analysis process involve?
98.At what stages of risk assessment are business process owners may be required and why?
99.Why is it important to align information security risk management with organizational objectives?
100. What is the difference between an external context and an internal context?