60610300 - Final exam questions for students of the information security education program “Access to information security risk management”

1. Define the concepts of risk, threat and vulnerability.
2. What is an information asset and which objects does it include?
3. Explain the purpose of risk analysis.
4. What stages does the risk analysis process include?
5. Define the concept of Bow-Tie analysis.
6. Explain the factors represented in Bow-Tie analysis.
7. Define the concept of Fault Tree Analysis (FTA).
8. Explain the factors represented in Fault Tree Analysis.
9. Define the concept of Event Tree Analysis (ETA).
10. For what purposes is an Event Tree used?
11. What types of context exist in risk management?
12. What is the difference between internal and external context?
13. At what level of risk assessment is the context initially established?
14. If the context provides sufficient information to effectively identify actions required to reduce risk to an acceptable level, what action is taken regarding the risk?
15. Explain the process of identifying information assets.
16. Identification of the value of primary assets.
17. Identification of the value of secondary assets.
18. What threats are associated with physical access to information systems?
19. What stages does the process of information security (IS) risk assessment include?
20. The main methodological shortcomings of traditional approaches to IS risk assessment and the use of innovative approaches to overcome them.
21. What stages does the IS risk analysis process include?
22. At which stages of IS risk assessment may the involvement of business process owners be required and why?
23. Is it advisable to maintain an up-to-date inventory of organizational assets, and how may this affect the IS risk assessment process?
24. What is the IS risk assessment process within an Information Security Management System (ISMS)?
25. What are the most important outcomes for an organization resulting from the IS risk assessment process?
26. Strategies for mitigating risks in telecommunications systems.
27. What methods exist for information security risk assessment?

28. What is the essence of qualitative IS risk assessment?
29. How is quantitative IS risk assessment performed?
30. What do risk level and risk relevance (criticality) indicate?
31. What actions may be taken regarding identified risks?
32. What are the primary methods of IS risk management, and what is the main objective of each?
33. Who within the organization possesses sufficient authority to determine acceptable risk levels, and why?
34. On which data should decisions regarding acceptable IS risk levels be based?
35. What measures exist to reduce IS risk to an acceptable level?
36. How is the planning of IS risk treatment measures carried out, and by whom?
37. What is the difference between retaining a risk and accepting a risk?
38. What are the input and output data of risk retention and risk acceptance processes?
39. What is meant by “risk response”?
40. Strategies for reducing risks associated with network attacks.
41. How is information security risk monitored and controlled?
42. What is risk monitoring?
43. How are IS risks monitored and reviewed?
44. What is the essence of monitoring and reviewing information security risk indicators?
45. What are the input and output data of monitoring and reviewing the entire IS risk management process?
46. Stages of executing automated procedures within the CRAMM methodology.
47. Describe the strengths of the CRAMM methodology.
48. Which parameters does CRAMM recommend for estimating potential damage?
49. How many general recommendations does CRAMM provide among countermeasures corresponding to identified threats and their levels?
50. Which value in the CRAMM vulnerability rating scale corresponds to an incident occurring approximately once every three years?
51. What is meant by business continuity?
52. Fundamentals of business continuity planning.
53. How is testing of a business continuity plan conducted?
54. Which asset possesses value equivalent to other critical business assets?

55. What does business continuity management include as an integrated management process?

56. Strategies for reducing risks at the application layer.

57. How can the term “information security risk management” be defined?

58. What are the main tasks of information security risk management?

59. All core components of the risk management process.

60. Define the Information Security Risk Management System.

61. Which stage of the information security risk management process is the most labor-intensive and why?

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

63. What are the possible criteria for IS risk assessment?

64. Criteria for evaluating the impact (consequences) of information security risks.

65. Possible criteria for accepting information security risks.

66. Scope and boundaries of information security risk management.

67. Why is it necessary to consider information security requirements in risk management, and how are they incorporated?

68. Risk management data and risk communication plans.

69. Planning for decision-making.

70. Establishing priorities in risk treatment and forming decisions on treatment and acceptance.

71. Which standards are included in the family of ISMS (Information Security Management System) standards?

72. Metrics for responding to security incident events.

73. What advantages result from adopting an ISMS standards family that enables sustainable success for an organization?

74. Key criteria of IS risk management, scope of risks, and their boundaries.

75. The importance of organizational structure in information security risk management.

76. Internal and external context, risk criteria, and risk evaluation/acceptance.

77. Which organizational information should be considered when defining scope and boundaries?

78. What are the criteria for assessing the value of assets?

79. Weaknesses of the CRAMM methodology.

80. Sequence of executing automated procedures in CRAMM.

81. What is the sequence for estimating potential losses from a threat?

82. Methods for ensuring and managing organizational business continuity.
83. How much productivity loss may a threat cause, and what is its cost?
84. Critical measures in asset identification.
85. International and national standards related to risk management.
86. What is the cost of losses if critical equipment fails?
87. What is the expected loss from a single event for each asset and each threat (SLE – Single Loss Expectancy)?
88. What types of risk monitoring exist?
89. Effective methods for monitoring and analyzing risk management strategies.
90. How is the initial security level determined in qualitative asset evaluation?
91. A generalized model for assessing organizational information security risk.
92. Determining the relevance of threats
93. Rules for evaluating threats based on relevance.
94. Methods for reducing risk after it has been identified.
95. Explain the advantages and disadvantages of the Bow-Tie method.
96. Explain the advantages and disadvantages of the Fault Tree method.
97. Explain the advantages and disadvantages of the Event Tree method.
98. Principles of ensuring organizational information security.
99. Information security considerations in managing business continuity.
100. Testing, maintenance, and reviewing of business continuity plans.