TOPICS TO PREPARE FOR THE EXAM

1. Risk terminology:
    a. risk (monetary units, level category)
    b. threats (event likelihood: probability, frequency, level category)
    c. vulnerability (level category, CVE, CAPEC, implicit)
    d. asset (monetary units)
    e. impact (monetary units, levels category, percentage of the asset value) – the amount of loss due to a threat
2. Security threat classification
3. Risk taxonomy and relations between components
4. Risk Treatment Options. Residual risk.
5. Which risks are usually accepted?
6. Risk tolerance curve
7. Types of security controls and their influence on the risk factors
8. Qualitative vs quantitative risk analysis
9. Risk Management Stages
10. Why it is important to communicate risks?
11. Probabilities of simple events
12. Event independence
13. Success probability of an attack strategy
14. Reliability and availability definitions
15. Reliability of individual components, of serial and parallel compositions.
16. Partial operational reliability (m out of n)
17. Availability calculations
18. Security modeling – motivation, for what reasons, when, how
19. Security definitions
20. Attack Trees, Bottom up cost propagation rules