CRM Reading guide 2017

Examination questions are based on understanding

I) the content of lectures provided and 

II) the topics discussed in the papers / videos.

The lists below indicate important concepts to focus on when reading / studying the literature. This does not mean that you can skip everything else. All of the papers is exam material unless explicitly stated otherwise.

Mandatory online video material

- ComputerWeekly: Managing IT Risk: Trends in Global Information Security
  - Disrupting the killchain
  - Risk tolerance
  - Capability extension

- George Cybenko: The Future of Cyber Security Risk (you can skip the first 3 minutes)
  - How to measure progress?
  - Worst-case vs. specific attacker
  - Where to get the data?
  - Challenges to cyber security risk

Mandatory literature

  - FAIR risk concepts and control types
  - You don’t need to remember the calculation tables
  - Several related definitions of cyberspace
  - Differences between information security and cyber security
  - 3-layer cyberspace model with key assets: cyber securities
  - Meaning of the bowtiemodel
  - Acceptable risk
  - You can skip section 4.0

  - Benefits of causal models; limitations of other risk assessment methods
  - Terminology in causal models for risk
  - Interpretation / semantics of causal models; correlation and causation

  - The difference between probabilistic and adversarial risk models
  - Assumptions in game theory
  - Difference between equilibrium analysis and minimax analysis, and relation to assumptions
  - You don’t need to calculate equilibriums, or distinguish types of equilibriums

  - The role of system models in risk analysis
  - Considerations in determining weakest links and the link to risk concepts

  - The role of attacker models in risk analysis
  - Relevant properties in attacker / threat agent models and how they can be used in risk analysis
  - Combining attacker models with system models
  - Assets, architecture graphs, and reachability
  - Possible paths and their likelihood
  - Link to attack trees

  - Types of metrics
  - Questions that can be answered with metrics
  - Relative and absolute metrics
  - Relation to qualitative approaches

  - Obviously the “key points”
  - Definition and calculation of ROSI
  - Quantifying exposure, mitigation and solution cost, and issues involved
  - Link to FAIR concepts

  - Approaches to justifying security investments and their limitations
  - Components of a typical security architecture
  - Metrics for the quality of components
  - The kinds of parameters that are used in investment models
  - The kinds of calculations that are used in investment models

  - Advantages and disadvantages of graphical and tabular risk models
  - Factors affecting comprehensibility of tabular and graphical risk models