University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 3: Risk Management and Business Continuity Planning

The following NIST special publication is available at:
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- **SP800-30 Risk Management Guide for Information Technology Systems**

.
The following standards are available to UIO students on the INF3510 Wiki.

- **AS/NZ 4360 Risk Management**,
- **ISO/IEC 27001 Information Security Management System**,
- **ISO/IEC 27002 Code of Practice for Information Security Management**.

QUESTION 1

A possible definition of risk is: risk = consequence × likelihood

a. Explain what is meant by consequence and likelihood in this definition.
b. Using an appropriate example, explain why this is a reasonable definition.

QUESTION 2

a. List the nine steps of the risk assessment methodology of NIST SP800-30, and mention the main input and output elements of each step.
b. List, and give a clear and concise explanation of the five steps that comprise the risk management phase in the PDCA cycle of ISO/IEC 27001.
c. Provide a mapping between risk management steps of NIST SP800-30 and those of the PDCA cycle in the ISMS framework.

QUESTION 3

In the context of risk analysis, what is the main difference between qualitative and quantitative analysis? Explain one important drawback of each type.

QUESTION 4

A qualitative risk analysis has identified three levels of likelihood (low, medium, high) and three levels of impact/consequence level (minor, moderate, major). Draw an appropriate table showing the qualitative level of risk taken from five levels (negligible risk, low risk, moderate risk, high risk, extreme risk).

QUESTION 5

Consider a quantatitive risk analysis for a business. A particular risk is expected to result in a security incident every two months at a cost of $3 000 per incident.

a. What are the single loss expectancy (SLE) and the annualised loss expectancy (ALE) for this risk?
b. How should the ALE be used in deciding how to treat this risk?
c. Once controls are put in place, how will they change a later risk analysis?
d. Suppose that the business decides not to put controls in place. Name two other ways that the business can treat this risk.

QUESTION 6

Apply the risk assessment methodology of SP800-30 to your personal laptop/computer. The analysis can be superficial, the important thing is to think about the necessary elements in the process. Rank the risks, and suggest ways to treat them.

QUESTION 7

a. As part of business continuity planning, a BIA (Business Impact Analysis) is often performed. Briefly explain the purpose of a BIA.
b. Specify the typical MTD (Maximum Tolerable Downtime) for a business functions that is defined as (i) critical; (ii) non-essential.
c. Assume that the information processing facilities of an organisation has suffered considerable damage, seriously impacting the business functions. How is the MTD taken into account when deciding whether business recovery at an alternative site should be invoked?
d. As part of the business continuity planning, a company is considering options for alternative sites for relocating the business in case of a disaster. Briefly explain the concepts of Hot Site, Warm Site, and Cold Site, and specify in each of the three cases how long it typically would take to be operable for running business functions.