**University of Oslo**
**INF3510 Information Security**
**Spring 2012**
**Workshop Questions**


# *Lecture 3: Risk Management and Business Continuity Planning*

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

- **ISO 27001 Information Security Management System**,
- **ISO 27002 Code of Practice for Information Security Management**.
- **ISO 27005 Information Security Risk Management**,

## QUESTION 1

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

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

## QUESTION 2

The Risk Management Process specified in ISO 27005 indicates two decision points.

a. Describe a situation where the answer to risk decision Ppoint 1 (after risk assessment) could be negative, thereby requiring a revision of the context establishment and risk assessment phases.
b. Describe a situation where the answer to risk decision point 2 (after risk treatment plan) could be negative, thereby requiring a possible revision of all the previous risk management phases.

## QUESTION 3

What is the main difference between qualitative and quantitative analysis? Explain one important drawback of each type.

## QUESTION 4

a) Assume that a risk assessment uses three levels of likelihood (low, medium, high) and three levels of impact/consequence level (minor, moderate, major). Draw an appropriate table of qualitative risk taken from 5 qualitative levels
b) Assume that a risk assessment uses four numerical levels of likelihood: 0 (extremely rare), 1 (rare), 5 (likely), 10 (very likely), and four levels of impact/consequence level: 0 (negligible), 1 (minor), 5 (moderate), 10 (major). Draw an appropriate table of semi-quantitative risk taken from 7 numerical levels

## 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

Assume that a semi-quantitative risk assessment has been done similarly to that of Question 4.b. Indicate how a semi-quantitative CBA (cost benefit analysis) can be done.

## 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.