University of Oslo
INF3510 Information Security
Spring 2017
Workshop Questions

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

## QUESTION 1

A possible definition of risk is: *risk = likelihood × impact*

a. Explain what is meant by *likelihood* and *impact* in this definition.
b. Discuss, e.g. with a relevant example, whether this is a reasonable definition.
c. Mention factors that contribute to *likelihood* of threat occurrence.
d. Discuss whether it is meaningful to dissect the concept of risk into more detailed factors during a practical risk analysis.

### Answer

a. The likelihood is the frequency (or probability) that a threat occurs. The impact is the consequence of a threat, i.e. the expected cost of a threat occurrence.
b. Many examples are possible. One could consider the threat of DDoS (Distributed Denial of Service) attack against a company web site. The likelihood is the expected probability of an actual DDoS attack taking place. The impact may be measured in terms of financial loss to the company due to customers not being able to make orders. When combined, the risk level increases as a conjunction of the likelihood and impact levels.
c. Factors are e.g. *threat agent strength*, and *vulnerability severity*. This is because the likelihood of a threat occurrence increases with the strength of the threat agent. Similarly, the likelihood increased with the severity of vulnerabilities. The factor *threat agent strength* can further be decomposed into *motivation* and *strength*. This is because the threat agent strength increases with motivation and capacity. An agent with the capacity (skills and technology) to execute an attack still needs the motivation to do it. Similarly, a motivated agent still needs the capacity to execute the attack.
d. It can be useful for analyzing specific threats in more detail, but it would take more time. For example, the likelihood/frequency of specific threats can be decomposed in terms of threat agent strength and vulnerability severity. Some frameworks explicitly take into account *threat agent strength* as well as *vulnerability severity* when estimating risk levels, e.g.:
    - NS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger –Risikohåndtering
    - NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

## QUESTION 2

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

a. Describe a situation where the answer to risk decision point 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.

### Answer

a. It is possible that the computed risks have a very skewed distribution, e.g. most risks have the same level (e.g. either very low or very high), which makes the risk ranking meaningless.
b. It is possible that the proposed risk treatment plan in unacceptable to management, e.g.
    i. Because the treatment plan is too expensive or too slow. If the plan is too expensive, then the level of acceptable risk could be increased.
    ii. Because the risk level of planned retained risk is too high to e accepted. If the level of retained risk is too high, more controls could be proposed.
    iii. Because the estimated cost of treatment plan or proposed retained risk is considered misleading due to wrong assessment of risk levels, so that the risk assessment and risk ranking needs to be revised.

## QUESTION 3

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

### Answer

Qualitative risk assessment uses words to describe the magnitude of potential consequences and likelihoods, whereas quantitative uses numerical values for likelihood and impact.

- qualitative scale could be: highly likely, likely, unlikely.
- quantitative scale could be probability values in the range [0, 1].

Major drawbacks of qualitative risk analysis are that the results are hard to justify objectively and that an exact value is not available for cost/benefit analysis. Major drawbacks of quantitative risk analysis are that the calculations are more ad hoc, it can be difficult to explain how the exact figures are obtained and the process can be very labour intensive (although tools are available).

## 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.

### Answer

a) Different assignments of risk levels are possible, but the most natural one is as follows. The important rule is that the level of risk cannot decrease when moving upwards or to the right in the table.

| | | | |
|---|---|---|---|
| **Major** | Moderate | High | Extreme |
| **Moderate** | Low | Moderate | High |
| **Minor** | Negligible | Low | Moderate |
| Impact/Likelihood | **Low** | **Medium** | **High** |

b) A semi-quantitative risk table computes risk as the product of impact and likelihood levels.

| | | | | |
|---|---|---|---|---|
| **10 (Very Likely)** | 0 | 10 | 50 | 100 |
| **5 (Likely)** | 0 | 5 | 25 | 50 |
| **1 (Rare)** | 0 | 1 | 5 | 10 |
| **0 (Extrmly-rare)** | 0 | 0 | 0 | 0 |
| Impact/Likelihood | **0 (Negligible)** | **1 (Minor)** | **5 (Moderate)** | **10 (Major)** |

## 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.

### Answer

a. SLE = $3 000. ALE = SLE x 6 = $18 000
b. Controls up to the value of $18 000 may be implemented. However, it also needs to be estimated to what extent the risk is reduced as a result of the controls. For example, if the frequency is reduced to once per 4 months as a result of controls costing $10 000 per year, then the controls are not justified.

c. The SLE and/or frequency normally decrease. These are computed after current controls are applied.
d. Any of: avoid the risk (cease the activity), share the risk (for example, by insurance), retain the risk (be prepared to accept the consequence).

## QUESTION 6

a. What is special about risks of disasters, in terms of likelihood and impact ?
b. Why is BIA often more useful than a traditional risk assessment in case of BCM and planning for disaster recovery.

### Answer

a. The likelihoods are very low, but the impcats are extreme.
b. The risk levels are difficult to assess because of the extreme values (very low likelihood and very high impact), so that qualitative and quantitative risk assessment methods become unreliable. BIA has a different focus, i.e. to identify essential business processes, and then to make plans for restoring 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 function 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.

### Answer

a. A BIA is performed at the beginning of business continuity planning to identify critical functions that in the event of a disruption would cause the greatest financial or otherwise negative impact.
b. Consider: • Critical: minutes to hours, • Non-essential: weeks to months
c. The estimated time to re-establish the business functions at the existing site is compared with the MTD. The business recovery plan must be invoked if the estimated time exceeds the MTD.
d. Consider • Hot site: fully configured and ready within hours • Warm site: partially configured, and ready within days • Cold site: only basic infrastructure, and ready within weeks