Universitetet i Stavanger

CANDIDATE

3840

TEST

RIS650 1 Enterprise Risk Management

Subject code	RIS650
Evaluation type	Skriftlig eksamen
Test opening time	06.12.2024 08:00
End time	06.12.2024 12:00
Grade deadline	31.12.2024 22:59
PDF created	09.12.2024 08:26

Seksjon 1

Question	Question title	Question type
1	Exam task RIS650 H2024	Essay

1 Exam task RIS650 H2024

Submit your answers here

Task 1.

1.

There are two sorts of probabilities we can use in risk assessments. The first one being a frequentist probability (Pf) and the second one being a subjective or knowledge based probability (Ps). The type of probability we use has an influence on how the risk assessment is carried out, and how results should be communicated.

If we use Pf, we will try to establish an estimate of the true Pf by looking at data sets and the probability of a sepcific risk event occurring. One specific method for this could for example be a monte-carlo simulation.

If we use Ps, we will use our expert judgement to establish a probability. By looking at the knowledge available, we can come up with an estimate of the likelihood of the event occurring.

The results of the risk assessment should be communicated differently depending on the type of probability that is used in the assessment.

For a frequentist probability, it is important that the data on which the Pf is based, is explained. This should include information on the completeness of the data and the suitability for the assessment. In addition, the probability distribution should be provided.

For a knowledge based probability, it is important that we explain the knowledge used in defining the probabilities used in the risk assessment. This should be done by defining the following knowledge aspects:

General Knowledge (GK): The general knowledge on which P and C are based. This could for example be knowledge about the industry the enterprise operates in. Or other broad but relevant information, such as conjuncture.

Specific Knowledge (SK): The specific knowledge on which P and C are based. This has to do with the knowledge directly related to the risk we are assessing. If we for instance are assessing the risk of operating certain machinery, we should provide information on how well we understand the machine, its common failure, safeguards ect.

Strength of Knowledge (Sok): The 'goodness' of the knowledge used to determine P and C. Is the phenomena well understood in the industry? Do scientist agree on the Phenomena? How much uncertainties are there related to the phenomena? These questions help determine the SoK. If the phenomena is well understood, we can say the the Sok is high. If there are significant uncertainties, we can argue that the SoK is low.

2.

Dear HRM team,

In our last meeting we discussed the companies risk management framework. Part of the discussion was about the risk concept we use in assessing the enterprise risks. Jean Paul suggested that we can continue using the risk concept of (C, Pf). Using the combination of

consequences and probabilities is a common way to define risk in the industry, but there are several reason why using this risk concept is problematic.

Using the combination of C and Pf would result in risks being presented as expected values. An expected value is the center of gravity of the probability distribution. Meaning that only the consequences that are most likely to happen are represented. There could however also be a potential for (severe) consequences that are not being represented by the expected value.

Second of all, Pf is insufficiently captures the uncertainties related to Pf and C. If the data on which Pf is determined is incomplete, the outcome of the risk assessment will provide a false sense of security. C and Pf should therefore be accompanied by a measurement of Uncertainty (Q).

I would propose that we use the risk concept of (A,C,U). We can discuss further details after the holidays.

Best regards,

B,W,

Senior Risk Assessor

3. Now that we have implemented A,C,U as the risk concept, we need a risk description that we can use to describe the enterprise risks. We will use the risk description: RS',A',C',Q,K. For now I would like to focus on the characterisation of knowledge K, Strenght of Knowledge SoK and its importance to 1) the application of the risk results, 2) risk understanding, 3) the identification and management of surprises, 4) the implementation of an appropriate risk management strategy.

First of all, K can be divided in Specific knowledge and General knowledge.

General Knowledge (GK): The general knowledge on which P and C are based. This could for example be knowledge about the industry the enterprise operates in. Or other broad but relevant information, such as conjuncture.

Specific Knowledge (SK): The specific knowledge on which P and C are based. This has to do with the knowledge directly related to the risk we are assessing. If we for instance are assessing the risk of operating certain machinery, we should provide information on how well we understand the machine, its common failure, safeguards ect.

Strength of Knowledge (Sok): The 'goodness' of the knowledge used to determine P and C. Is the phenomena well understood in the industry? Do scientist agree on the Phenomena? How much uncertainties are there related to the phenomena? These questions help determine the SoK. If the phenomena is well understood, we can say the the Sok is high. If there are significant uncertainties, we can argue that the SoK is low.

Explanation on why K and SoK aspects are important:

1. The application of the risk results. K and SoK has an influence on the application the risk results. K and SoK provide information on the uncertainties related to defined consequences. If for example the risk result shows that there is a small probability for extreme consequences and this risk is subject to high uncertainty. We might want to consider gathering more information to take away some of the uncertainties related to this risk. We might also consider a cautionary risk management strategy.

2. Risk understanding. K and SoK provide information on how well we understand the risk at hand. If there is little knowledge available to us, we can argue that our understanding of this risk is minimal.

3. Identification and management of surprises. K and Sok provide information on how we we identify surprises and how well we can manage them. If there is little Knowledge available in relation to a certain risk. We should be aware that we might not be able to identify and surprising events. Similarly, if the SoK in relation to a certain (group of) risk is low, we might not be to identify and manage surprises. Being cautious is recommend in this case.

4. The implementation of an appropriate risk management strategy. K and Sok had an influence on the implementation of an appropriate risk management strategy. If there is little Knowledge available in relation to a certain risk. We should be aware that we might not be able to identify and manage surprising events. Similarly, if the SoK in relation to a certain (group of) risk is low, we might not be to identify and manage surprises. We also have little understanding of the severity of the consequences. A cautionary risk management strategy would in that case be recommended. On the other hand, if there is much knowledge available and the SoK is strong, we could argue for a more efficient risk-based strategy. For managing risks that fall in between these two categories, we should opt for a risk assessment strategy.

4. Figure one shows a model for determining which risk management strategy to use bases on the available general and specific knowledge. The Dry feed vendor can use this model to determine how to manage the risk that the company identifies. For example, the company use processing machinery that come with safety risks to its employees. The company can use the figure to determine what type of strategy to use to manage this risk. First of all the general knowledge is assessed. How well does the company understand the general operation of processing dry feed? If the company has been around for some time, it probably has a good understanding and therefor good General knowledge. After this, the company should determine wether it has good specific knowledge on the phenomena. If the specific knowledge (knowledge specific about the safety risks) is weak, the company should try to increase this knowledge. If this is not possible, a cautionary or risk assessment strategy should be chosen. If the knowledge can be increased, a risk assessment or risk based strategy could be used.

Task 2.

1. Changes in Laws and regulations

Changes in laws and regulations can have a strong influence on risk exposure depending on the specifications of the regulatory change. Examples could be: reputational damage, legal fines, market loss, supply chain issues, and production failure. These exposures could lead to bankruptcy as a worst case scenario.

Without knowing which specific regulatory change is at hand, it is difficult to come up with specific risk mitigating measures. Two general aspects are overall important to manage regulatory change. The first of al is a frequent updated regulatory register. Industries often offer subscriptions for relevant regulatory changes. This can help the organisation plan for upcoming regulatory change. The second aspect is a commitment to resilience (an aspect form HRO). The company can become more resilient for regulatory change by diversifying its portfolio and by staying flexible, so that it can quickly implement the changes necessary to stay compliant.

2. New suppliers

New suppliers has an impact on the risk exposure of the company. Depending on the company and its suppliers risks could be; production failure, health and safety risks

and reputational failure.

To mitigate the risks, the company should consider to perform third party audits. In a third party audit, the company reviews its suppliers. In this way, the company can confirm that the supplier will be able to provide consistent quality. Another mitigating method might be to build up relations with a diverse network of suppliers, so that the company can switch suppliers if needed.

3. New technology

New technology has an impact on the risk exposure of the company. The main one being that not implementing new technology could cause the loss of an competitive edge. But implementing new technology can also cause risk exposure, for instance information security risks. In order to manage these risks, companies should implement new technology in the right way.

The company should first of all keep updated on new technology. For instance by attending conferences, or inviting representatives, to determine which technology can help the company improve and keep its competitive edge. Secondly the company should implement a system for the integration of new technology where risks are addressed. This system should consider a system approach, where the impact of adopting new technology is assessed on the whole organisation.

Task 3

1.

A. Phishing and supply chain vulnerabilities pose security treats.

Phishing is a method of stealing login credentials. This could for instance be done by redirecting employees to a fake login page. By an successful Phishing action, malicious actors can gain access to digital systems. This could have a wide spectrum of possible negative consequences. In an extreme case, this could cause a shutdown of all company operations.

Supply chain vulnerabilities are weaknesses linked to suppliers. Almost all enterprises make use of digital systems from other enterprises. This causes a vulnerability. It could for instance be that a supplier (intentionally) builds in a 'back door' in there software. This means that they could gain access to the system, even after it has been sold to another enterprise.

B. The NSM principles can be used to protect the company against these treats. First of all it is important to identify values and treats. What aspects are important values to the company and what does the company use in order to live up to these values? This long list can then be used to identify the possible treats that can affect these values. Which is done in a treat assessment. These treats can be addressed by coming up with preventive and mitigating security measures. What type of technical, operational and orgnisational barriers can the company implement in the attack vector (pathway) so that events don't occur, and if the occur the consequences don't materialise. Lastly the company should continuous update and improve its protocols in order to detect treats and stay updated with the latest best available technology and information.

C. The PDCA cycle forms the bases of most management systems. It is useful concept for continuously improve cybersecurity practices.

In the Planning phase, the company outlines goals and how to reach them. For effective continuous improvement it is important that these goals are formulated Specific, Measurable, Acceptable, Realistic, and Time bound (SMART). An example of a SMART cyber security

goal could be; We want to have less than 1 percent of employees pressing on the phishing links send by the information security consultants in 2026.

In the Do phase, the company does the work necessary to reach the goal. For the formulated goal, this could be launching an cyber security awareness campaign.

In the Check phase, the company checks wether it is still on track to reaching its goals. For the formulated goal, this would be checking if the awareness campaign contributes to reaching the goal. What aspects of the campaign are working, which aspects are not contributing?

In the Act phase, the company embeds the aspects that contribute to the goal in the organisation. If for example having a recurring information security test helps reach the goal, than the company should embed this in the organisation by allocating resources, such as time and money to continuously perform this task.

2. John Hart's active credentials even though he has left the company provides a security treat, because he might not share the same company values anymore. Maybe he works for a competitor now that can use the information John has access to gain a competitive edge. This could for instance be information on pricing.

Words: 2301