**Guidance in the risk assessment of information security**

Version 1.0

xx. mmm 20nn

# Purpose

This guide describes an overall method for assessing the company’s critical information risks when you do not have a complete framework for how the management handles IT security (management system for information security also called Information Security Management System or ISMS). The accompanying spreadsheet is built around this method.

The guide presents a simple model that provides an introduction to what risk assessment is, how it is carried out and how to use it. The main objective is that small and medium-sized companies can get started with a simple and practical use of risk assessment and build up their experience within this area and that of risk management. When the company’s need for risk management grows, it has the option to switch to more advanced models and methods.

The method is aimed at small and medium-sized companies that have a reasonably simple IT application in the form of approx. 3-5 crucial IT systems that are necessary for the company to function. These 3-5 IT systems can either be managed by the company itself or purchased as an IT service from an IT supplier.

If you already have a risk assessment method in place, you can continue to use it. Larger companies and/or companies with an established IT/security department can advantageously use the Agency for Digital Government’s method and tool for risk assessment[[1]](#footnote-2) or look at DS/ISO/IEC 27005:2018.

**About risk assessments**

Good IT security/information security is basically about ensuring the availability, confidentiality and integrity of information all at the same time. *Availability* means that information is available to those who need it, when they need it. *Confidentiality* means that unauthorised persons cannot gain access to the information. *Integrity* is about information being correct and trustworthy and that, for example, it has not been changed by unauthorised persons.

Risk management is a central part of the work with IT and information security, which enables the management to decide on, and prioritise, the necessary investments and initiatives in relation to the company’s willingness to take risks. The starting point for this is a risk assessment.

In this context, a risk is considered as an unwanted event with adverse consequences for availability, confidentiality and/or the integrity of information security.

The purpose of the risk assessment is to make risks comparable by, for example, expressing risks as a numerical value. A high risk for the company is shown as a high numerical value and correspondingly a low risk is expressed as a low numerical value.

The risk is measured by assessing how likely it is that a threat can exploit a vulnerability and what and how big the consequences would be for the company. An example is that the company loses a laptop (threat) that is not encrypted (vulnerability), which makes it possible for unauthorised persons to access company emails and the like on the computer (consequence).

On the basis of the risk assessment, the company must assess the need for, and identify, any additional security measures that ensure the necessary availability, confidentiality and integrity. In the aforementioned example, this could be the need to encrypt laptops. That assessment forms part of a risk management plan.

Four types of risk management are generally used:

* Risks are accepted
* Risks are managed
* Risks are shared (such as through insurance)
* Risks are avoided

One way to manage risks is to split risks into categories such as low, medium and high, indicated with different colours, typically green, yellow and red. It is the company’s management that determines the categories based on the company’s willingness to take risks. The management’s willingness to take risks is a term describing what the management is willing to risk.

If there is a low willingness to take risks, there will be many numerical values that cannot be accepted without further action (i.e., red values). This applies, for example, if you are very dependent on your information. If there is a medium willingness to take risks, the numerical values for green, yellow and red will be more evenly distributed. If the willingness to take risks is high, there will be many numerical values that are acceptable for the company (green values). For example, you can work fine without your own servers and you only have very little personal data,

If a high/red risk cannot be reduced, the risk must be avoided. This could mean, for example, that the company might have to stop carrying out a task. However, the company’s senior management can always decide that the company can live with a red risk if the risk is monitored and managed as soon as possible. See more about the practical use of this in Section 2.1.

# Risk management method

The risk management process proceeds as follows:

1. The security officer and senior management have to decide when a risk assessment should be carried out, how the consequences should be assessed, which risks can be accepted and which must be handled (willingness to take risks)   
     
   Typically, you start with an annual risk assessment, and you choose to express the consequences and probabilities on a numerical scale from 1 (low) to 5 (high). The risk is then the product (probability x consequence) of the two values, i.e., ranging from 1 (lowest) to 25 (highest). See the scales below in points e) and f).
2. The security officer assesses, preferably together with managers who have a knowledge of the business, which business-critical information, processes and IT systems the risk assessment must be carried out on. For example, you can look at which processes are critical for the delivery of a certain service or the production of certain products, as well as which information and IT systems these processes depend on.

Typical topics are customer data, financial system and any customer-facing services and employee data.

1. Once the critical systems, data and processes have been identified, a risk owner must be appointed for each of them. The risk owner is the person who can recommend to management that a specific risk be accepted or reduced/handled.   
     
   The risk owner is typically a finance manager, operations manager or IT manager. It can also be the director.
2. The security officer and risk owner and other IT and business experts together identify the threats which, through the use of existing vulnerabilities, could break the availability, confidentiality and integrity of the chosen processes, data and IT systems and thus pose a risk.

Typically, you start by looking at what such breaches might actually be. For example, it could be the risk that the customer database is revealed to a competitor (a threat) because an employee doesn’t know how to process emails correctly (the vulnerability).

Appendices C and D in DS/ISO/IEC 27005:2018 contain lists of possible threats and vulnerabilities that can be used as a starting point. If you have a higher level of ambition, you can work with a threat terminology, such as The OCTAVE model[[2]](#footnote-3) . The OCTAVE model reviews all conceivable threats divided into three main categories: Human threats, systemic threats and threats beyond the company’s control.

Human threats can come from internal employees or from people outside the company. It may be deliberate/intentional actions or accidents. In this main category we find, for example, corrupt employees, employees who forget their laptop, hackers, and suppliers or partners who make a mistake.

Systemic threats exist, for example, when there is a built-in logical error in a program, such as when the “Heartbleed” vulnerability was discovered in 2014.

Threats beyond the company’s control are, e.g., riots or torrential rain storms flooding the server room.  
  
Another source for identifying relevant threats is the European Union Agency for Cybersecurity (ENISA), which published a threat overview in 2016*[[3]](#footnote-4)*.

1. The security officer determines the consequences of these risks, possibly together with someone from the management, and assesses its impact on the company. The consequences are indicated in levels on the following scale:

1 - Very small consequence – it is really of no significance  
2 - Small consequence – it can be handled as part of the operation  
3 - Some consequence – extra resources will probably have to be found  
4 - High consequence – it has an impact on the bottom line  
5 - Very large consequence – the company is threatened

An example of a consequence assessment is that the disclosure of information about important customers’ discount agreements or of such information about a larger number of customers can negatively affect turnover (High consequence).

1. The security officer assesses, in discussion with any other IT and business experts, the likelihood that the risk in question will, based on experience, appear as an actual security incident. The probabilities are also determined in levels on the following scale:

1 - Rare or unlikely  
2 - Will hardly occur  
3 - Is possible  
4 - Must be expected to happen  
5 - Will be exploited

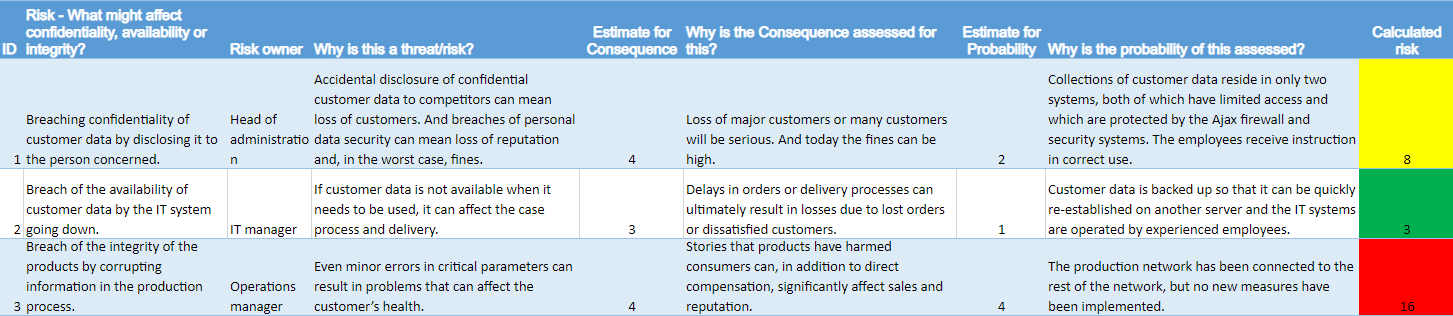
When assessing the probabilities, account must be taken of the administrative and technical security measures already in place, which can help reduce the experience-based probabilities. If you train, e.g., employees in the correct use of systems and tools, as well as in general security, this can reduce the likelihood of information about customer discount agreements being disclosed. The same applies if you have restricted access to employees with a business need.

**NOTE!**It is important that you describe and note the relevant risks and the justification for both the consequence and the probability in the fields “Why is the consequence/probability of this assessed?” in the risk assessment sheet. Partly so that the risk assessment can be made available to the management and partly so that you can later follow up on whether there are changes in the risk picture (threats, vulnerabilities, consequences and/or new subjects that need to be assessed).

## 2.1 The result

The calculated risk that has been found above, with the current security measures, is also called the residual risk.

The residual risk is coloured/grouped based on the company’s willingness to take risks, so that you can see which risks the management can immediately live with and when something needs to be done to deal with them, such as by implementing new measures. See, for example:



In the accompanying sheet, the willingness to take risks is expressed in a colour scale, based on the categories low, medium and high. This means that the calculated risk from 1-25 is split into intervals, as shown in the model’s column Q:

* Green is a low risk, of 5 or below, where risks can be immediately accepted by the management.
* Yellow is a medium risk, from 6 to 9 inclusive. Here, the management assesses from time to time whether the risk can be accepted or whether something will be done to reduce it, such as by introducing extra measures.
* Red is a high risk, of 10 or more. This is when something should be done to manage the risk.

This division reflects a suitably low willingness to take risks, where the company can live with very large consequences (5), as long as the probability is low (1). If the probability increases to 2, the risk becomes 10 and is therefore unacceptable (marked in red). It is also pleasing if, for example, you have a risk with a possible (3) probability of a high consequence (4). Then the risk becomes 12 and cannot be accepted either.

If you want a different distribution of the values in relation to the colours (the willingness to take risks), you can change this by specifying other numbers in column Q for the individual colours. For example, if you have a high willingness to take risks, yellow could be set from 8 to 14 and red could be 15 or more. Green is then 7 or below.

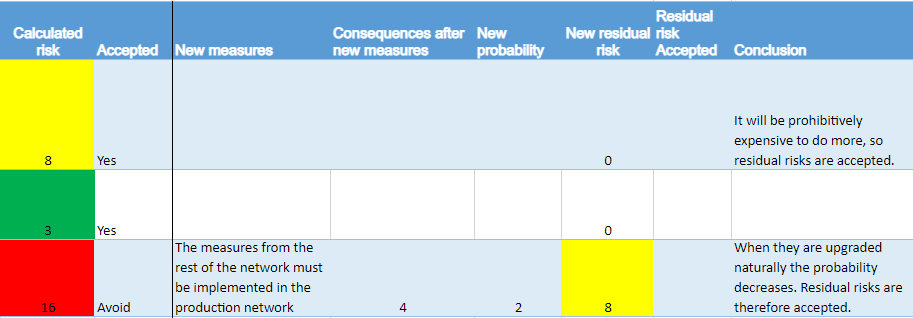
Considerations about which risks need to be addressed and what needs to be done are documented in a risk management plan.

## 2.2 Risk management plan

Based on the risk assessment, it is assessed whether security is at an acceptable level, or whether more security measures must be implemented to reduce the probability of the individual threat to the individual asset. This will depend on whether it is financially viable. You can also consider ceasing the risky activities, if possible. Finally, you can consider whether you can share the remaining risk with suppliers or insure yourself out of it.

In the above example, it will clearly be necessary to do something about risk No. 3. For instance, that at least the same security is implemented in the production network as in the rest of the network.  
You can consider whether there is anything you can do extra to reduce the probability of risk No.1. Risk No. 2 can be accepted.

The risk management plan can either be described in a separate document or incorporated as extra columns in the spreadsheet used for the risk assessment. In the accompanying spreadsheet, the last columns (JO) can be used. Here you can indicate whether residual risks are acceptable or whether something must be done about them. In the event that something needs to be done, the new measures are noted and what new probability, and thus new residual risks this results in. See, for example:



## Maintenance

The risk assessment and risk management plan are not static documents which, after management approval, can simply be “put in a draw”.

In addition to the risk management plan having to be implemented, including updates of, e.g., the contingency plan, you must follow up on whether there are changes to the risk picture (threats, vulnerabilities, consequences and/or new topics that need to be assessed). If there are, the process must be repeated for the changes in question.

Ideally, this should be done continuously, e.g., in the event of major changes in the company’s IT or processes and whenever new threats are discovered. You should make sure that it happens regularly, e.g., at least once a year, with a frequency based on how dynamic the company’s world is.

If red risks are identified, you should follow up and report on these more frequently. If, on the other hand, there are risks that are repeatedly green, you can perhaps do it a little less often for these, e.g., every two years.

There should also be a process that informs the management of major changes in the risk picture and assessments. As a minimum, the security officer should bring it up at the next management meeting.

1. <https://digst.dk/sikkerhed/hjaelp-til-sikkerhedsarbejdet/vejledninger-til-sikkerhedsarbejdet/risikovurdering/> [↑](#footnote-ref-2)
2. <http://www.cert.org/resilience/products-services/octave/>. [↑](#footnote-ref-3)
3. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file> [↑](#footnote-ref-4)