Whitepaper Information Security Risk management

January 2016, GÉANT SIG-ISM

Author: Rolf Sture Normann
Review: Alf Moens, Alessandra Scicchitano, Fotis Gagadis, James Davis
Version 1.0

Traditionally, IT and information security risk has been a responsibility of IT departments. Systems however, are becoming more complex and integrated and frequently connected to third parties. Risk management should therefore not only be performed by IT personnel, but include all stakeholders and different kinds of users and roles to ensure that every aspect of risk is addressed, including hardware, software, employee awareness, users and business processes. Risk management is one of the key activities in information security management.

Every business, business process and system should go through a process of risk management to inform the organisation of the risks it is facing. Mitigation activities should be provided for all risks that are higher than the management's risk attitude (acceptable risk). Risk can be *mitigated (reduced), accepted, avoided(removed) or transferred.*

This whitepaper is about how to manage information security risk by performing risk assessments in a National Research and Education Network (NREN) organisation or not-for-profit organisations such as universities. The scope of this white paper is only information security: discussions around disaster recovery and continuity planning are considered out of scope. However, it should be mentioned that disaster recovery and continuity plans should coexist with risk assessment.

Risk assessment in everyday activity

We actually assess risk every day: when we go to work we face the risk of a number of incidents. We accept this risk, and we still go. We take the car to go to work because we believe that the risk is acceptably low, considering the risk reducing controls that are in place, eg. brakes, airbags etc. This is actually a type of risk assessment, but of course not a documented one that follows a formal process.

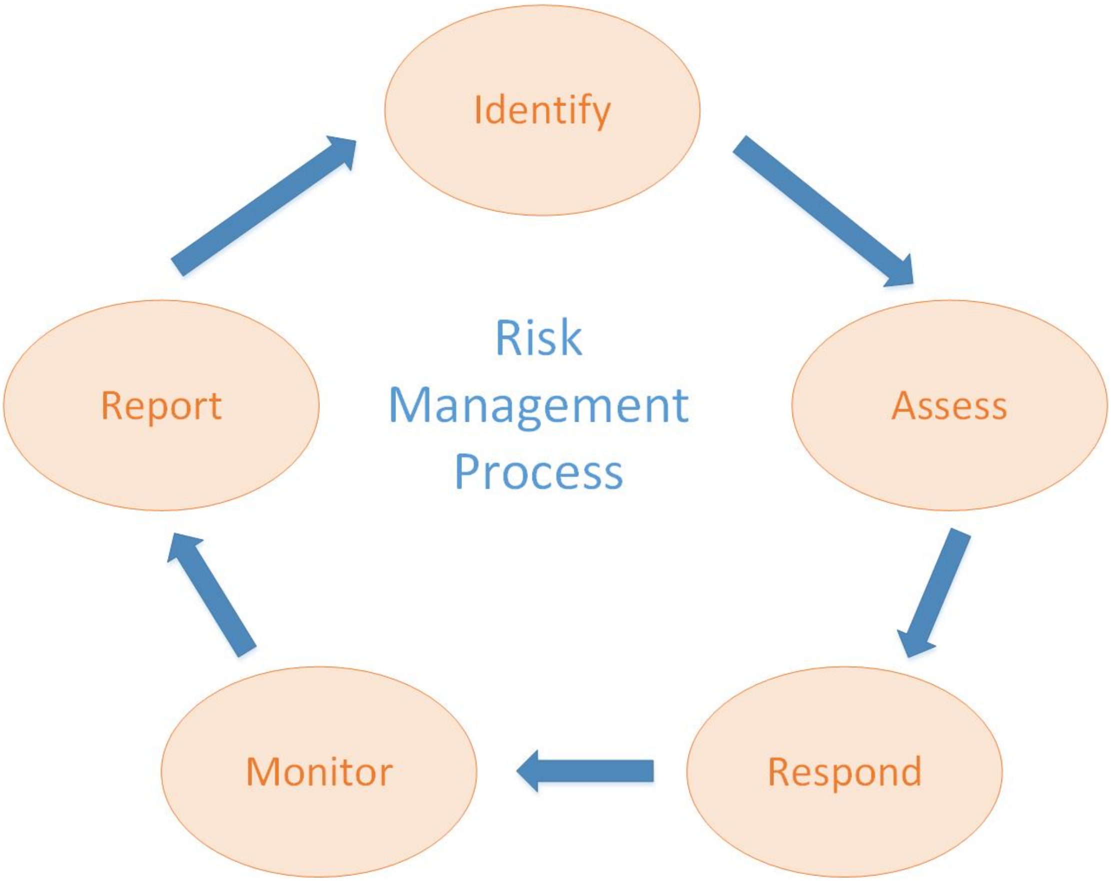
A documented and formal risk management process is important to be able to respond to risks in a repeatable and reliable way.

Audience

This whitepaper is meant for security leaders such as Chief Information Security Officers (CISO) or Chief Security Officers (CSO), security professionals and senior information managers. The paper can be used as a guide for building a risk-based approach to information security in an organisation as it covers all aspects of risk assessment and treatment. This whitepaper is loosely based on the ISO standard on security management, ISO 27001:2013 'Information security management systems' and ISO 27005:2005 'Information security risk management'.

What is risk management?

When we manage risk, we have to identify, assess and prioritise activities to minimise the effect of unwanted incidents. Risk management's objective is to reduce the impact of uncertainty on the business's ability to meet its objectives.



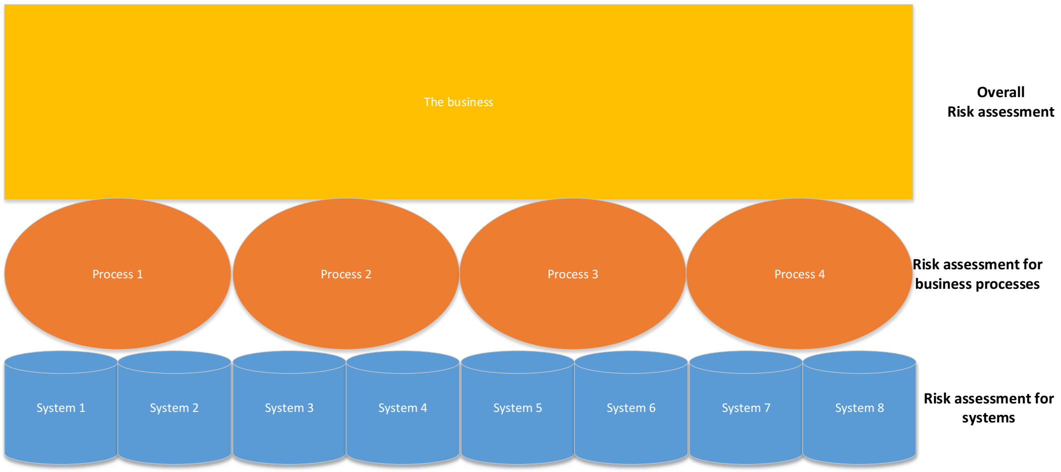
Risks can arise from uncertainty in financial markets, threats from project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary, or events of uncertain or unpredictable root cause.

Strategies to manage risks typically include transferring the risk to another party, avoidance of the risk, reducing the negative effect or probability of the risk, or even accepting some or all of the potential or actual consequences of a particular risk. Risk can also be positive, and give some important possibilities. This will not be discussed here.

Risk management and risk assessment

Risk assessment can be done for different parts of the organisation with different levels of detail and focus, but it is also important to undertake an overall risk assessment for the business to find which risks are most critical to the business overall.

Business processes and systems



Risk assessments can look at the overall business, business processes and also individual systems:

Overall risk assessment

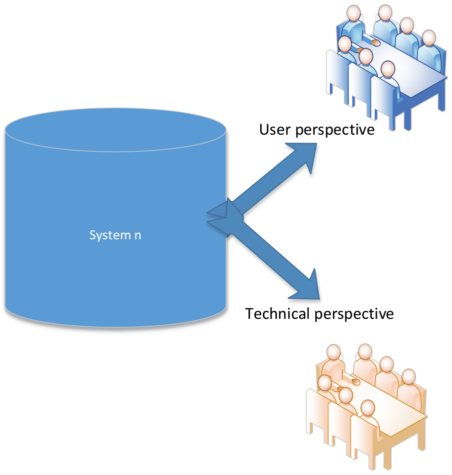
You need to take a helicopter view and look at risk at an overarching level. Which inherited risk is this organisation facing by being in this sector, area or type of business. Is there any specific risk on an overarching level that the organisation needs to assess and manage, will be a typical question.

Risk assessments for business processes

Business processes involve users, routines, procedures and different kinds of hardware and software to support these processes. Performing a risk assessment of the process can be very useful. In this case, you are not specifically looking into any hardware or software, but the process itself and the delivery of the services this process should provide. Much experience that is needed for systems (hardware/software) or routines will be discovered during this type of assessment.

Risk assessments for business systems

Every organisation uses different systems to support business processes. They could be accounting systems, HR systems, systems for storing sensitive data, ticketing systems, timesheets, mobile equipment and other hardware. These systems have users and operators. It is good practice to divide the assessment between the users and the operating staff of the systems, simply because there will be different persons and competences to invite to the assessment workshop.



It is important that, where risk assessments are being performed at different levels within an organisation, the results are consistent and comparable across levels. It would not be useful if an assessment of an individual system accepted risks that would not be acceptable at a higher level.

Information security risk management starts with an inventory of the most important assets for an organisation, assessing threats, quantifying risk and assigning responsibilities. Security managers then evaluate what measures to implement, enhance or improve to reduce the risks to an acceptable level. In the latter case the organisation can look to roll off the risk with extra insurance or decide to run down the activity that causes this big risk.

There are several methods for risk analysis, risk methods and risk treatment. Choose one that is consistent with your organisational culture and habits. Being too precise in quantifying risk isn't necessary, you need to have a clear idea of the risks and the costs but not necessarily a precise one.

Most methods focus on two dimensions, the likelihood of the incident occurring and its corresponding impact. Some methods also involve the value of the asset to calculate the risk. The first step is to find the scope and boundaries regarding what is going to be assessed. Then try to find suitable participants for a workshop (brainstorming) on what incidents could happen. The calculating of impact and likelihood will vary from institution to institution, as even similar organisations will place different values and business requirements on the same asset. In Appendix A, we suggest one method that is often used.

Performing a risk assessment

Management support and policy

It is important to involve your management. The management of the organisation should support a policy that states that information security should take a risk-based approach. Typically, an information security leader (CISO) is responsible for ensuring that risks assessments are carried out and that the results of them are acted upon. The status should be reported to the management, to ensure that the management can decide corrective actions and support continual improvements in the information security management system.

Planning a risk assessment workshop

When we plan a risk assessment in either the overview, process or system area it is important to describe the scope.

The scope: What are we going to assess the risk for?

Normally this is easier for the overview than for the systems. The nature of systems is that they are often integrated with other systems, and can be difficult to set the scope. Nevertheless, it is really important that this is done. Every participant in the assessment workshop should know what the boundaries of the risk assessment are.

Workshop participants

Choosing the right participants for the workshop is important in order to get the best results out of the risk assessment. It should be a group of people who represent all aspects of the organisation, process or system that are going to be assessed. Divide the risk assessment for a system into user perspectives - where you can find unwanted incidents based on a user's point of view - and a technical perspective, where operating staff and super-users attend. Often regular users have no knowledge of the technical issues that can happen and the technical personnel do not fully understand how the system is used in practice.

Preparing information

Normally it is useful to provide the participants of a risk assessment workshop with some information in order to prepare for the workshop. You can provide information about the area (process, system or organisation) and the scope. In addition, you should prepare them with some short description of risk assessment methods used. Provide them with a couple of examples of risks that are typical for this assessment so that they are prepared for the workshop. Often people fear that they do not have the right competence for a risk assessment, so it can be helpful to explain them that their presence is important as a 'user of the system' etc.

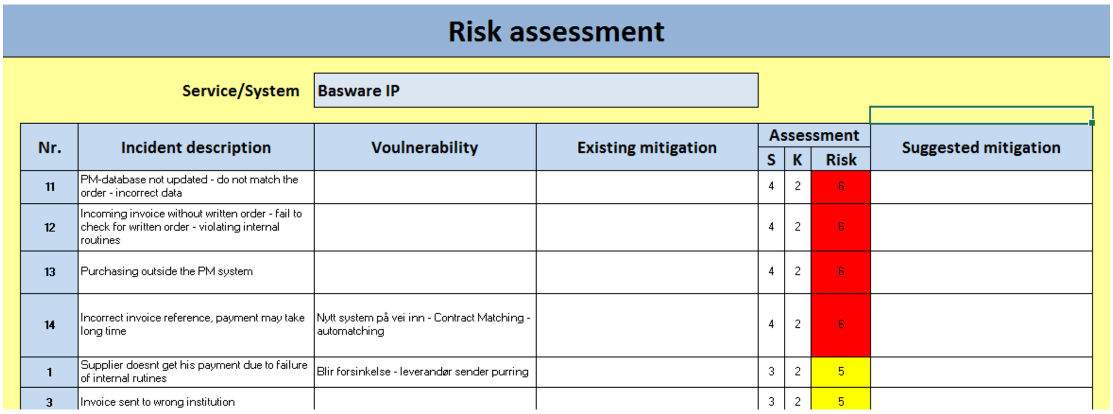
Workshop

Start with a short presentation of risk assessment methodology and the scope. Then take the prepared information and discuss the examples that were provided. That will often start an open discussion and lead people to participate. Write down the risks that come up during the session. The facilitator should try to lead the discussion during the workshop and write down the incidents that the group agrees can happen.
Also you need to discuss whether you will be assessing residual or inherent risks, that is with or without taking already implemented measures into account.

For example, the risk of damage through fire might be assessed as very small because you have smoke and fire detectors and fire suppression systems in place, but the risk might be much higher if these existing controls are not to be considered.

Assessment of likelihood and impact

After the discussion it is time to assess the likelihood and consequence of the risks that the group discussed earlier. ISO/IEC FDIS 27005:2011, E.2.1 provides an example matrix with predefined values.
There are varieties of different methods used in risk assessment to assess and evaluate the risk. Here is an example.

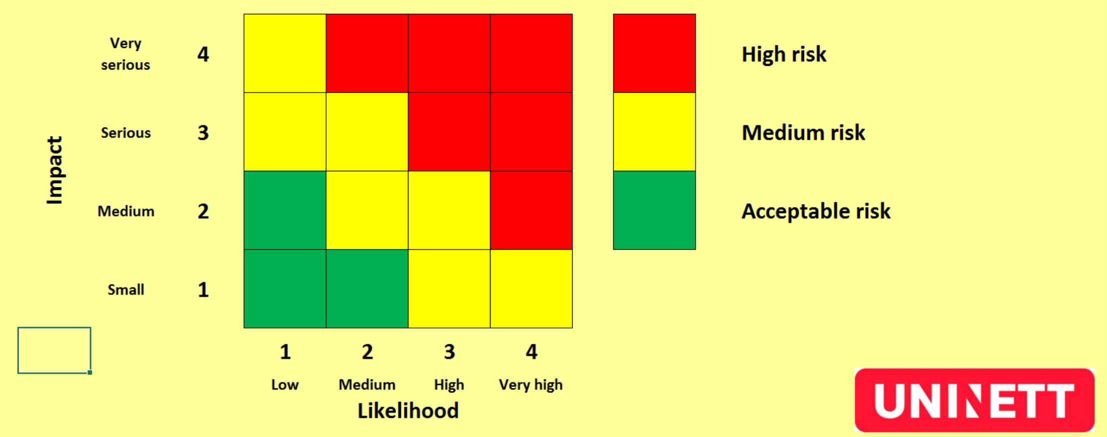


Risk assessment

Service/System: Basware IP

Nr.	Incident description	Voulnerability	Existing mitigation	Assessment			Suggested mitigation
				S	K	Risk	
11	PM-database not updated - do not match the order - incorrect data			4	2	6	
12	Incoming invoice without written order - fail to check for written order - violating internal routines			4	2	6	
13	Purchasing outside the PM system			4	2	6	
14	Incorrect invoice reference, payment may take long time	Nytt system på vei inn - Contract Matching - automatching		4	2	6	
1	Supplier doesnt get his payment due to failure of internal rutines	Blir forsinkelse - leverandør sender purring		3	2	5	
3	Invoice sent to wrong institution			3	2	5	

Risk matrix:



Impact		1	2	3	4
Very serious	4	🟨	🟥	🟥	🟥
Serious	3	🟨	🟨	🟥	🟥
Medium	2	🟩	🟨	🟨	🟥
Small	1	🟩	🟩	🟨	🟨
		Low	Medium	High	Very high
		Likelihood			

🟥	High risk
🟨	Medium risk
🟩	Acceptable risk

Examples of likelihood:

When assessing the likelihood of a risk occurring, you most likely use the expected frequency. In rare cases where you don't have any historical data or knowledge about the frequency, you could also use other indicators such as ease of access and motivation.

	1 Low	2 moderate	3 High	4 Very high
Frequency	More seldom than every 5th year	More seldom than yearly	More often than once a year	More than once every 6 months
Ease of access	There are existing relevant controls in place. Can be compromised by persons with privileged user rights who know what controls are in place. External parties cannot compromise the system without help from insiders.	There are existing relevant controls in place. Can be compromised by persons with normal access rights who know what controls are in place. External parties need knowledge of the system and controls.	The controls in place do not function as required. Employees can work around these controls without any special knowledge. External parties can compromise the system with normal knowledge of the system.	No controls are in place. The system can be compromised by internal or external users without any special resources or knowledge.
Motivation	Employees with privileged access and special knowledge need to act with purpose. External parties need special knowledge and must cooperate with employees to compromise the system.	Employees with knowledge of the controls that are in place need to act with purpose. External parties must have special knowledge of the controls in place, and have a planned approach for breaking in.	Employees can violate security by accident or through a failure. External parties must have some knowledge and act with the purpose of breaking in.	Both employees and external parties without any special knowledge can compromise the system accidentally or through a failure.

Examples of impact:

Impact is more difficult to assess than likelihood, especially across different types of risks. Impacts are often about economy or reputation, and different people may be comfortable with different measures depending on their role in the organisation. It is important though, that the impact can be reduced to a common base (for example, a financial figure, or an impact level).

	1 small	2 moderate	3 serious	4 catastrophic
Economic	Loss up to [VALUE]	Loss up to [VALUE]	Loss up to [VALUE]	Loss up to [VALUE]
Reputation	Considered bad judgement	Unacceptable behaviour locally	Unacceptable regionally	Careless behaviour

It can be hard to measure the impact of an event. Some organisations could also use a table like the following:

	1	2	3	4
Confidentiality	Lack of logging of access to personal information.	Exposal of personal information of a small number of individuals.	Exposal of a large amount of personal information or of few, but sensitive, personal information.	Exposal of a large number of sensitive personal information.
Integrity	Unclear when non critical information was updated.	Uncompleted non critical information	Lack of or wrong important information.	Critical information is not present or not correct.
Availability	Up to one working day.	Up to five working days	Up to three weeks.	More than three weeks

Risk treatment

Risk management is not only about assessing the risk: the risks discovered also have to be treated in some way. Evaluating the risk using a matrix will give you an idea of which risks should be prioritised.

After a risk assessment workshop a report should be written for the risk owner. The risk owner needs to discuss and agree mitigating activities; either organisational or technical controls should be implemented to lower the risk to an acceptable level. The risk owner should set up an implementation plan and send to the CISO for follow up. This is to ensure that the plan is followed, and that managers are aware of any gaps between planned and implemented controls. This allows them to take any necessary corrective actions to improve the management system.

Standards

Iso 27005:2011, RISKIT (COBIT5), NIST, CRAMM

References

ISO 27001
ISO 27005
COBIT5 (RISKIT)
ISF