Risk Assessment Report - Skyri Municipal's Archive

ROGER LARSEN & ERNST KRISTIAN HENNINGSEN
Project - IMT4762 Risk Management I
Gjøvik University College
2011 Fall

Document Classification: RESTRICTED.

Tuesday 27th September, 2011

Risk Assessment Document Review History

Date	Author	Version
2011-09-07	Roger Larsen & Ernst K Henningsen	Initial Document
2011-09-09	Roger Larsen & Ernst K Henningsen	Structural changes
2011-09-15	Roger Larsen & Ernst K Henningsen	Text tuned to lower technical level on response from Mrs Ann Ready.
2011-09-19	Roger Larsen & Ernst K Henningsen	Classification of document in dialogue with Mrs Ann Ready; Restricted
2011-09-23	Roger Larsen & Ernst K Henningsen	Restructured (removed some tables)
2011-09-27	Roger Larsen & Ernst K Henningsen	Minor errors. Recommendation done.

Table 1: Risk Assessment Document Review History.

Chapter 1

Executive Summary

Skyri Municipals have for a while experiences several unwanted events related to computer information systems/IT. We where hired by City Manager Mr. Roger Fast to do a Risk Assessment Report on Skyri Municipal. We have participated in several meetings with Skyri Project participants and got a broad overview of the situation in the municipal. The actual unwanted events are documented and taken care of in this report. We have under the whole project had an open,active and inclusive participation from Skyri Municipal – which is very important in this kind of work.

We start this report by giving general motivation to risk management. Further we inform about the typical threats that exists and some statistical figures to understate this. We also explain common ways of dealing with these threats. Then we explain how IT risk management can be approached using ISACA RISK IT FrameWork as a basic methodology for this work [3].

We limit/scope our risk assessment to adapt Mr. Fast's inputs. We focus only on risk category; operation and the risk areas; (i) Productivity, (ii) Public reputation, (iii) Legal. We evaluate and analyse the unwanted events and recommends the response to these events. Finally we conclude on what actions to prioritize.

Skyri municipal have started working with risk management because of many unwanted events lately (events that perhaps challenged legal aspects). This job may now be seen on as a enormous job, and it may well be – but with a great deal of planning and a good information plan (include every employees) with proper methodology you will soon see the fruits of this important job.

Contents

Chapter 2

Introduction

2.1 Background/Purpose of this report

Skyri Municipals have for a while experiences several unwanted events. This generates in short term negative effects; (i) bad service level to the citizen of Skyri, (ii) wasting time and money, (iii) breaking laws regarding citizen privacy violation. The negative effects in long term may be; (i) a change in the political elected board, (ii) higher employee turnover, (iii) bad reputations. We have based the Risk Assessment on The Risk IT Framework by ISACA [4].

2.2 The task from Skyri

We got the job from City Manager Mr. Roger Fast and here is his general Project Description (quoted);

> This report should result in an overview of the situation, a broad threat picture, and most important which security measures should be prioritised.

2.3 Motivation

"What you risk reveals what you value."
- Jeanette Winterson

Accidents happens – whether we try to hide in our bedrooms or we are active practising bungee jumping. Organisations that do not accept this fact are in danger of breaking a lot of laws, experiencing financial loss, or what is worse; human injuries of even death. Risk Management deals with proactive, operative and reactive actions to avoid events and at least minimise the consequences of the event when it happens. We need to evaluate the cost/benefit to what is most efficient regarding these three stages. By executing good risk management one can achieve being a more robust organisation and can bear the fruits as e.g:

- Archive predictable service levels to inhabitants
- Be able to improve cost control and to follow cost plans (budgets)
- Be able to fulfil the elected politicians promises
- Can ensure that the suppliers' contracts fulfil our expectations
- Can start measure Skyri's effectiveness
- Will be a much more flexible/learning organisation

Chapter 3

Information Security Threats

3.1 Information Security in General

Computer security is a phrase often used together with many difficult words. We often associate computer security with cryptology and large passwords together with the not so social group of people with thick glasses (nerds). Today many of us are overrun by information about computer security. Nowadays the technological approach using computer systems are in every organisation. Municipals are often challenged regarding computer security in their broad needs of computer systems. Municipals archive services touches every other service and activity in their own organisation. We have in this Risk Assessment Project documented some unwritten routines and suggested some new. We have found some areas that may need some more attention and suggested improvements in physical hardware. The concrete findings can in the short run help you get the grip on computer security - but in the long run you need to continuously work with risk management to keep yourself at a stable risk level.

3.2 Information Security Threats Today

During the last years there have been several cases regarding malicious attacks either directly directed against various neighbouring municipalities, or indirectly. There have also been reported several virus attacks in the police and hospitals in Norway. This means nothing less than that the threats are out there, and they are close. One thing one can be sure about, is that it will, eventually, happen against the municipality Skyri. Though, when this time comes, one can be prepared by having reviewed security-holes in ones own system. Security-holes can be in a technical aspect, in regard of firewalls and alike, but it can also be in regard to bad routines, for example in the handling of sensitive information.

Dark figures of computer crime / Statistics are found in the The Norwegian Business and Industry Security Council (NSR) report dated 2010-09-15 (latest version). These statistics show that 30% of all Norwegian organisations have been victims of computer crime and 56% of them had systems break-down for up to one day in 2009 for same reasons [1].

Chapter 4

Risk Assessment in General

4.1 Risk Defined

Risk is the output of the two factors; **probability** (how likely will this event happen?) and the **consequences** (what impact does this event cause?). Short version; Risk = Probability $*$ Consequences. In this context we like to measure both values, so the more practical way ; **Risk = Frequency** $*$ **Magnitude**. The typical illustration is found in figure 4.1.

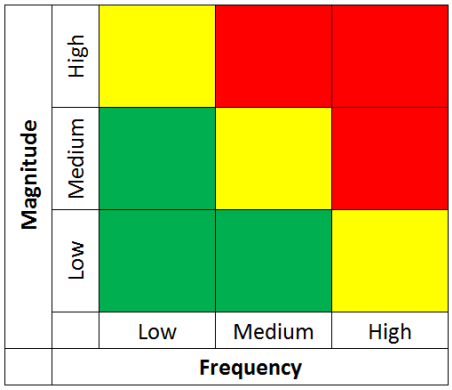

Figure 4.1: Illustrating Risk = Frequency $*$ Magnitude.

4.2 The Risk IT FrameWork

We have good experience in using *The Risk IT Framework* by ISACA. Risk IT FrameWork is based on COBIT ®(also an ISACA brand). ISACA (from Information Systems Audit and Control Association) is a global non-profit, independent organisation with 95.000 members in 160 countries founded in 1969. They are a leading provider of knowledge, certification, advocacy and education on IT systems. ISACA have been an active part in the development of international information systems auditing and control standards. The Risk IT framework is based on the principles of enterprise risk management (ERM) standards/frameworks such as ISO 31000 (from International Organization for Standardization) [5] and provides insight on how to apply this guidance to IT. [4]. Please checkout figure 4.2 on next page that graphically illustrated the main parts of the processes in IT Risk Management.

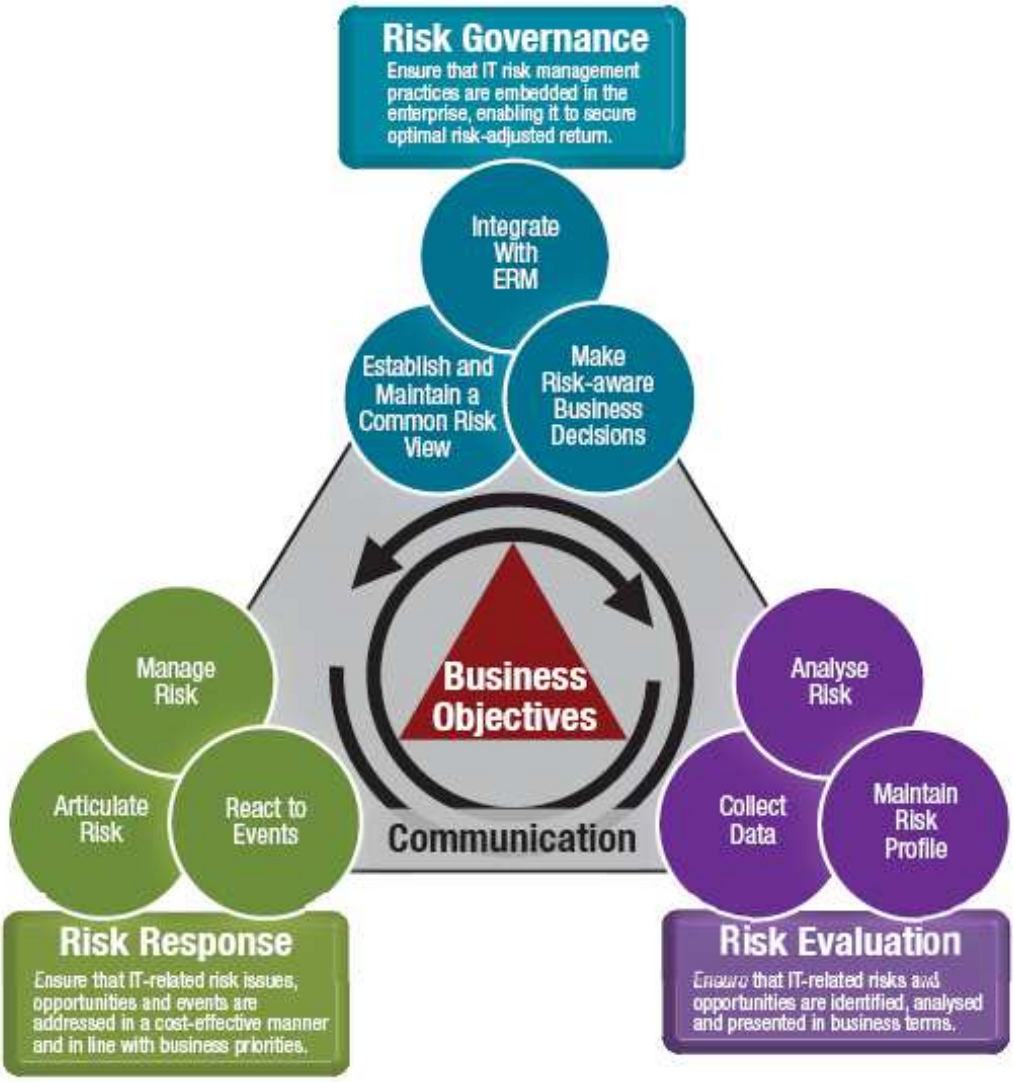

Figure 4.2: The IT Risk FrameWork Process Model Overview.

Source: ISACA RISK IT FrameWork [3].

Chapter 5

Risk Assessment in Skyri Municipal

5.1 Scoping/Limiting the Risk Assessment Project

In this section we narrow down/scope the Risk Assessment Project.

General assumptions:

- Skyri is supposed very knowledgeable within what laws they are affected of. The reason for not complying to these laws is not having control.
- We are only looking at the archive, as Skyri has hired several other consultants for the other areas of Skyri. Their work is going parallell with ours. Skyri wants to get a grip on their situation as fast as possible. The challenge here is that every department in Skyri municipal are supposed to archive, thus they are all influenced by any bad archive service.
- At the City Manager Mr. Fast's request, this report should result in an overview of what key-services doesn't work of today. As of this, a thorough analysis of all risks will not be performed. This is due to limited amount of resources, both financial and in regard to timeline.
- The Archive law demands that any signed agreement where Skyri is involved must be filed physical. We do not focus on physical security in this risk assessment report, but it is mentioned some places.
- We focus on operational challenges in Skyri. There exists no IT strategy in Skyri.
- We limit our Risk Analysis Areas to; (i) Productivity, (ii) Public reputation, (iii) Legal.

Please find more details in table 5.1.

5.2 The IT Risk Assessment Form - Description/Facts

We have had several meetings with Skyri municipal. Table 5.1 describes the facts regarding our risk assessment project.

IT Risk Assessment Form – Description	
Entity	Skyri Municipal, Archive
Entity strategic role and objectives	A complete system for preserving both working-documents and documents for storage. It should be easy reaching the system for extracting information, but also for adding new information. Focus should be on efficiency but at the same time secure handling of sensitive information
Assessment date	2011-09-08
Assessor(s)	Roger Larsen, Ernst Kristian Henningsen
Responsible at main entity	City Manager, Mr Roger Fast
Contact persons at entity	Head of Archive, Mrs Ann Ready
Major business processes	Quality Assurance of Archive regarding Information Security
IT infrastructure and applications supporting major business processes	Network equipment, File-/Terminal-/Print- Servers, General Office Applications
Document Security Classification	The Risk Assessment Report are classified as *RESTRICTED*
Project Extent	Risk Assessment Report are welcome in the size of 15 pages (ex. frontpage, index, references and appendix etc.)
Project Communication	We will have Mrs Ann Ready as our contact in Skyri and copy every written correspondence (emails, letters etc) to Mr. Roger Fast.
Project Meetings	Every Friday 09:00 is a status meeting in Skyri's administration building, meeting room A-110. Other meetings will be communicated and set up as needed. Minutes of meetings are written and communicated after every meetings.

Table 5.1: IT Risk Assessment Form, Description.

5.3 Skyri's Archive

Today Skyri have one physical archive within each department, but in the building department each employee have their own archive system.

Input from meetings show that Skyri actually have a centralized Archive system, but it is not used because of lack of availability, training and maintenance of archive-scanners and other relevant multi-functional machines. Beneath is an visualisation of how this is supposed to work, figure 5.1

Documents scanned is also brought to the administrations office, which puts them into their physical archive.

ITAll is delivering Skyri's centralized archive-system. If Skyri's internet-connection goes down, they will loose all communication towards this system. Servers used should be installed within Skyri's network, but serviced by ITAll through the VPN-connection. If the internet-connection goes down, Skyri will still have an functioning Archive-system. Though it will probably be less secure against internal attacks.

No SLA with ITAll - ITAll can do whatever they want (though Gordon had the impression that they were "good guys"..)

As the building department had to move to another building, every employee put their archive-documents into boxes which they put in their hallway. The "moving-people" (some teenagers hired from Adecco) picked them up and brought them to their moving-truck. Because of some moving trouble at the place they were moving all equipment (the former renter had problems getting some stuff out) they had to store the boxes in the truck outside for some days. After this, they were put just inside the entrance to the building, where everyone is allowed walking.In the new building the

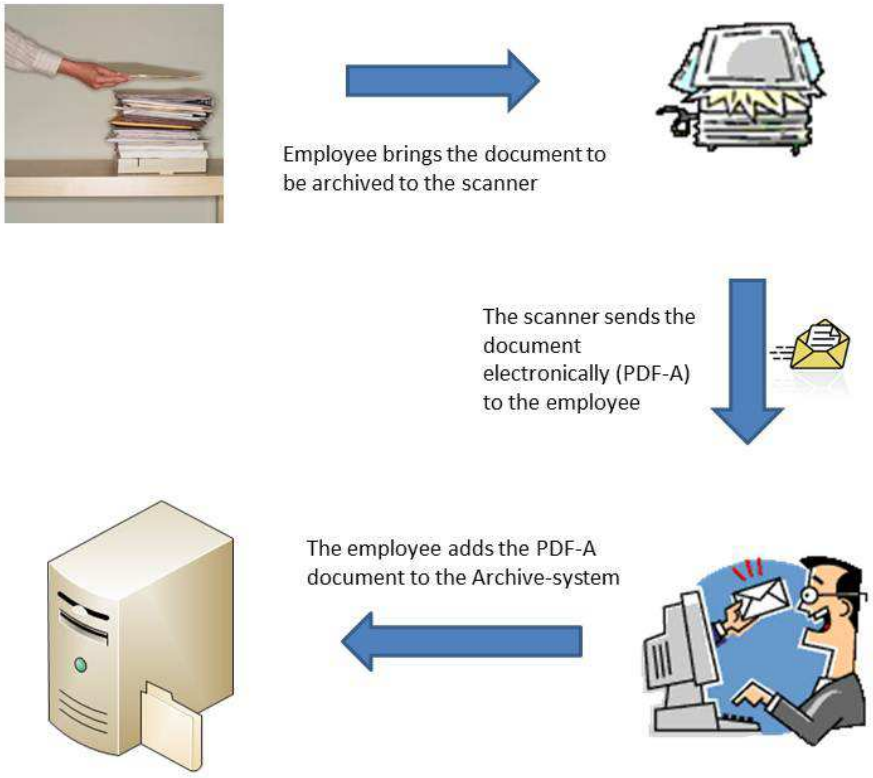

Figure 5.1: The Archive's scanning process.

building application department now is in, they share entrance with NAV.

5.4 Responsibilities and Accountability in Skyri

Responsibilities and Accountability for IT Risk Management										
Role Definition		**Risk Governance**			**Risk Evaluation**			**Risk Response**		
Role	**Suggested Definitions**	**Common Risk View**	**Integrate With ERM**	**Risk-aware Decisions**	**Collect Data**	**Analyse Risk**	**Maintain Risk Profile**	**Articulate Risk**	**Manage Risk**	**React to Events**
Municipal Board	The head board of the Municipal	R	R							
Mayor	Elected leader of the Municipal	A	A							
City Manager	The Administrative Manager	A	A	R	R	R	R	R	R	R
Head of Archive		A	A	A	A	A	A	A	A	A
Head of IT		A	A	A	A	A	A	A	A	A
Legend: **Red** = Responsibilities, **Blue** = Accountability										

Table 5.2: Responsibilities and Accountability for IT Risk Management.

We have here identified how Skyri are working regarding responsibilities and accountability in the organisation. This is important and helps us to see how the organisation works. Show table 5.2.

5.5 Risk Appetite

5.5.1 Risk Appetite in General

When performing a deeper analysis on a certain subject or potential happening, it is important to have in mind that the rating is strongly attached to what the organisation, in this case the municipality Skyri, think of as risks. For example, if the IT system goes down in an carpenter company it will most possibly have much less consequences compared to if it goes down for Facebook [1] [2]. As of this, it is important/practical to have some concrete units to measure a consequence against (this is not straight-forward/possible for all analysis).

Risk Appetite are important to document as a later baseline for the Risk Response.

5.5.2 Skyri's Risk Appetite

As of our second meeting with the Municipality Skyri we went through and tried establishing a common risk-view of happenings that could occur, and what degree of consequences it would have. Make a note that these degrees of consequences are what Skyri finds as risks compared to their own service-level

[1] One of the largest Social Networks on Internet. They have over 800 millions of active users. 50% of them log on every day.

towards their inhabitants. In this process one will force oneself to take an high-level decision on what is most prioritised spending resources on to fix, and what is not prioritised. Note that an happening regarded as 'accepted' doesn't mean that is nothing wrong with an happening of this sort; it means that one is not able to spend precious resources on doing something to prevent/mitigate it.

This is also called the "Risk appetite". Please find our results in figure 5.3.

Risk Scenarios and Risk Appetite		
1	Sensitive information of 1 inhabitant accessible for unauthorised users	Acceptable
2	Sensitive information of >1 & $\leq$ 10 inhabitant accessible for unauthorised users	Unacceptable
3	Sensitive information of >10 & $\leq$ 50 inhabitant accessible for unauthorised users	Really Unacceptable
4	Archive System unavailable <15 min. each day	Acceptable
5	Archive system unavailable >15 & $\leq$ 60 min. in one day	Unacceptable
6	Archive system unavailable >60 min. in one day	Really Unacceptable
7	Archive system unavailable >5 hours in one week	Really Unacceptable
8	Bad news article $\leq$ 1 each year	Acceptable
9	Bad news article >1 & <5 each year	Unacceptable
10	Bad news article >5 each year	Really Unacceptable

Table 5.3: Risk Scenarios and Risk Appetite.

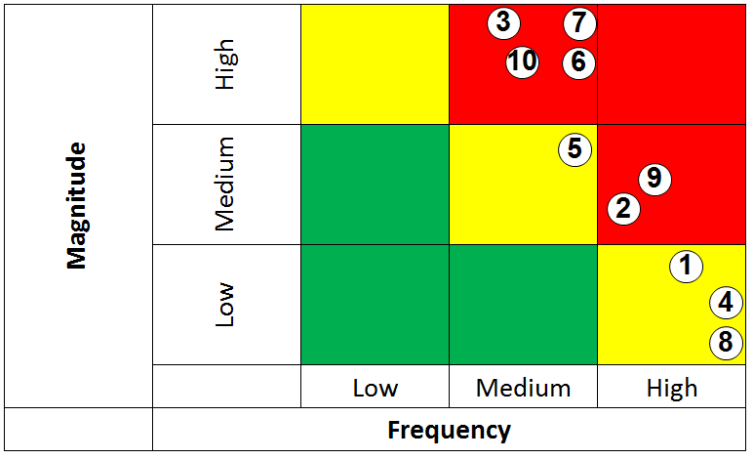

Figure 5.2: Risk Map indicating Risk Appetite.

5.6 Risk Culture

Skyri have exposed some critical risk culture. Some examples are listed here:

- Very relaxed to the "rumour" that it had been virus in the archive system.
- The Building Application department do not bother contributing to the central (physical) archive system
- The loss of sensitive information was not frightening
- Employee talk about clients in lunch - seemingly not aware of that others may listen in

5.7 Risk Communication

In this section we usually describe how communication regarding risks flow through the organisation, by using a table. Risks in this regard could be that a particular door is often unlocked, a window at first level always open, or violations of internal policies. It is very practical having this flow formally set, so that one know who to contact about a matter. However, in Skyri there does not exist this kind of formalities. We have talked with several employees to get a picture of how this is working as of today, who contacts who and so on. The general feedback is that the employees do not know who to contact. They often just speak to each other, when they sporadically meet - and conclude that this is probably already noticed by the people "higher up" in the system. They seem a little sceptical about reporting this kinds of information, in that they may feel it embarrassing if reporting something not suitable. This is a risk culture that is quite unfortunate, because one miss alot of useful input. Please find a suggested communication flow in appendix A table A.1.

5.8 Risk Analysis

5.8.1 Risk Analysis in General

Here we analyses the risks we have found in our meetings with the project group. Please find our limitations in section 5.1. We have used the Risk Register Entry as shown in appendix B to conclude on the risk factors. The Risk Acceptance Criteria we agreed on are defined in this document. Please find the risk map in figure 5.3.

We focus on operational challenges in Skyri. There exists no IT strategy in Skyri.

5.8.2 Risk Analysis Results

Analysing Known Risk Incidents					
Risk	Risk Factor	Description	Frequency	Magnitude	Result
1	Archiving not done centrally	Building Application Department file their documents in every employees office and do not scan&send them to central archive	High	Medium	High
2	Virus in archive system	There has been rumour about virus in the archive system last year in neighbour municipals	Low	High	Medium
3	Bad availability to IT-system	The general IT system are in periods unavailable in daytime, several times a week	High	Medium	High
4	Missing routines	All departments are missing routines in how to discard sensitive documents	Medium	Medium	Medium
5	Lack of rules and solutions in exchanging data	All departments lack rules and solutions in how to exchange sensitive information within and to each other	High	Medium	High
6	Lack of rules and solutions in reading email on Smart Phones	All departments lack rules and solutions in how to use Smart Phones regarding work (email)	Low	Low	Low
7	Lack of role regarding information security	Skyri municipal lack the role regarding information security	High	High	High
8	Lunch-talk about clients - relentlessly of others that may be listening in	Sensitive information about inhabitants may be revealed to unauthorised people, though usually employees of the municipality itself	Low	Low	Low
9	Ethernet cable physically squeezed door	Several cables is not installed professionally - they are led through doors. This results in the cable getting weakened each time it is squeezed by the door, again resulting in it finally not working	Low	Low	Low
10	Mail server reachable from world wide web	When analysing risk concerning the checking of email on Smart Phones, this revealed itself. This makes it possible, if an adversary were to get email-addresses and passwords, to retrieve sensitive information.	High	High	High

Table 5.4: Analysis of Known Risk Incidents.

5.8.3 Risk Analysis Risk Map

This risk map indicates illustrates our conclusions regarding the unwanted events when analysed.

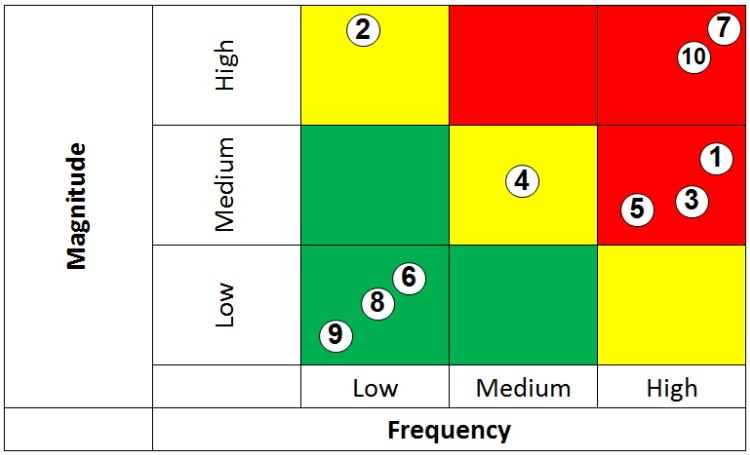

Figure 5.3: Risk Map of Risk Analysis.

5.9 Risk Response

5.9.1 Archiving not done centrally

As Skyri already has a system for centralizing the Archive, they should approve resources to get this up and running. We have observed several areas that would need to be addressed;

- Malfunctioning scanners - should be fixed and set up by ITAll - Lack of training - Make an easy-to-read training-program/document that people can rely on after they have had an introductory lecture about how it works. (ITAll should probably have something to say here). At the start one must maintain a low threshold for asking question. Questions, and possible problems should be directed to the Head of Archive (Mrs. Ann Ready) which will be the contact-point between users and the archive-system in general. If/when this is done, one will have a centralized Archive-system that permits very efficient ways of both extracting and adding information, complying to the whole idea of the Archive. We also identified an possible coming problem when starting to use this new system. The server for the Archive system is stationary at ITAll's site. This means that if the Internet-connection goes down, Skyri is unable to use this system. They must then attend to the physical archive. We recommend making ITAll installing this Archive system server at a local environment at Skyri's internal network, so one are able to reach it despite the internet connection going down.

This is considered being a high risk, as it is quite inefficient for the employees, resulting in less man-hour, which again results in less service for the inhabitants. One must also presume higher employee turnover because of annoyance.

5.9.2 Virus in archive system

A thorough analysis show that this is a two-sided case. Most employees didn't use the the electronic Archive system (the centralized one that didn't functioning properly). There were only a couple ones that sometimes used it, when it for some reason worked. We took the deliberty of requesting an anti-malware scan of the Archive to potentially unveil time-critical risks. Fortunately the scan turned out negative (no match for malicious content). Though, because of unclear policies (and people at all not complying to the clear ones) regarding the use of private usb-keys it was possible injecting malicious pdf-documents to the Archive, which would infect other vulnerable users when they would

extract it at a later time. One could of course bypass usb-keys and send a malicious pdf through email, but this is checked and blocked by the mail washer (a system for checking emails for malicious content). To combatant the possible injection of bad content to the Archive system, an up-to-date anti virus application should be present and therefore installed (together with a host firewall) on the archive server. This server should automatically update it's virus-definitions. This, like all other traffic, should only reach the internet through a designated proxy for maximum protection.

According to the Risk map in figure 5.3 this is classified as medium, as there was no malware in the Archive system per day. Despite that it is possible getting malicious content into the Archive rather easily, it must be done from within the network, either by an mole, or by a machine hijacked by an outside adversary. If this would be the case, there are several other areas that probably should be prioritised before the Archive system when facing an internal attack/threat.

5.9.3 Bad availability in IT-system

This have a high impact on both the employees efficiency and on their happiness at work. Analysis show that Skyri in general have a downtime for about 40minuts each day on average. Some days over one hour, some days nothing at all (but that is quite rare). As of our earlier Risk Appetite statements, this comply to being an Really Unacceptable risk (High). There is not much Skyri themselves can do about this however, as IT-services is outsourced to ITAll. This is under the responsibility of ITAll. Though as far as we can see, no-one has been able to show us an Service Level Agreement (SLA) agreed upon with ITAll. On contact with ITAll they have been rather silent about the matter. It seems as their have been some kind of verbal, diffuse agreement that ITAll should try their best to keep the network up and running satisfactory. When running a municipality this just don't cut it. One need to sit down with ITAll and discuss an acceptable limit of downtime (for starters this should be less than 15min each day, complying to risk appetite set earlier) and if ITAll exceeds this, ITAll's bill to Skyri's will get smaller depending on the majority of the downtime, and what has been agreed upon beforehand.

5.9.4 Missing routines in handling sensitive information

Archive from building application department left public

Risk appetite state that sensitive information of 10 or more people being accessible to unauthorised persons should be looked upon as an Really Unacceptable (High) risk. It is clear here that information to more than 10 (probably more than 50 as well) individuals of Skyri has been accessible by other. First hand by the movers, then by possible theft (though it didn't happen) of the truck, and last but not least when they were placed publicly at the entrance.

To deal with situation like this it is important to have good routines. If able to get the centralised Archive System up and running, this particular problem should arise less frequently. But that doesn't mean that one should accept it silently. Routines for handling of sensitive information must be made and learned. In an unclear situation one designated person should step up and make sure that everything is done according to routines.

Securing memorysticks/USB-dongles: [9].

5.9.5 Lack of rules and solutions in exchanging data

During interviews with various employees it became quite clear that Skyri lacks a particular method for sending and receiving sensitive information to each other, not only within a department, but also to other department on requests. One could argue for using the central electronic Archive System for this purpose as well, but the information exchanged is not what one would consider final documents - more like work documents, therefore they will/should never enter the Archive in the first place. An

disturbing example of coarse mishandling was actually with the building application department. A couple of employees had understood that it was not effective at all performing local archiving (as mentioned earlier in this report). They therefore tried starting a process of centralizing their archive-documents. The problem was that they sent this both through fax and email (unencrypted), not directly because of the sending-method (although there exist more secure methods for sending this sort of information), but because they managed to send the documents to unauthorised receivers, both internally at the municipality and externally. The receivers have (seemingly) handled this quite ethically and contacted Skyri municipality at once - though a few others have resulted in negative press articles. This is just one example, but majority of the employees did not know how to answer "How do you send sensitive information securely to others?" We believe this is something that would need to be addresses rather quickly, as it has quite an impact (medium) on the legal and public reputation areas which defined earlier. As this happens rather often we conclude with this being an high risk as of today. To remove or mitigate this problem, one should contact ITAll and ask about what they potentially could deliver of services of this kind. A simple solution could example be encrypting of email with white listing of email addresses. White listing means that the mail server would only accept designated receivers for this particular kind of information (for example only internal users - no outgoing emails of this kind)

5.9.6 Lack of rules and solutions in reading email on Smart-Phones

We understood that there were employees checking and reading email on Smart-Phones. After performing a survey about this, it turns out that there was only a couple of employees doing this. Being allowed to check emails (with possible sensitive information) from ones own Smart Phone should be a violation of IT policies. This is because if not using a system designed particularly for this purpose, Skyri's IT department do not have control of security mechanisms installed on the Smart Phone. None of the particular employees checking email on their Smart Phones had taken steps to secure their devices in any way (not even connecting through VPN) (we were able to get in contact with these employees at their own request, as they were unaware of the possible security threat they posed and were curious - very good!). Employees have the possibilities of checking their email at home through a designated VPN-connection, though this should be done from designated computers destined for work purposes.

As this account for just a few employees the frequency is quite low. There is also limited possibilities (compared to a real computer) regarding what could be done. We therefore classify this totally as low risk. (But note that checking emails on Smart Phones should not be allowed and should be stated so in IT Policy.

5.9.7 Lack of role regarding information security

Having a designated person for being responsible for Information Security is very important. If one have had this already, Skyri would by all predictability not be in the situation which it is in now. This is a clear total risk of High. Recommendation is to appoint someone to this role immediately. This person should also be involved on every active response to this risk assessment.

5.9.8 Lunch-talk about clients - relentlessly of others that may be listening in

At the coffee-machine and especially at lunch, employees talk about cases they are handling, often mentioning inhabitants directly by names. Asking for opinions and alike should be OK, but this is possible without exposing the inhabitant's identity. The magnitude of this is low, since there mostly is employees in the municipality which have signed a non-disclosure agreement. Nevertheless, sensitive information should be handled on the need-to-know basis.

5.9.9 Ethernet cable physically squeezed in doors

In lack of better (cheap) ways of installing network cables, they are put through doors and other rather creative areas (example hanging from lamp to lamp in the ceiling). When closing and opening these doors, they will eventually wear out the cables. Though this happen quite seldom, it have an high instantaneous impact on network efficiency. But it is rather visible on central network devices, as one can see that it do not have contact anymore. One then can just replace the faulty cable very fast (since it already has been put so conveniently easy-to-reach. Because of this fast fix, the impact is considered low. Total risk of low.

5.9.10 Mail server reachable from world wide web

When the employees checked emails using their Smart Phones, they did not go through a VPN-connection, but were able to reach and check emails from the world wide web. This is quite concerning and should by restricted immediately. It allows adversaries a method for brute forcing email-accounts and possible get access to sensitive information (without compromising any other computer on the network). It may as well have happened already. Services exposed to the internet is constantly scanned for vulnerabilities and is subject for brute force attacks. This make this a rather high chance for happening, and if it were to happen, it could reveal much sensitive information. Risk is a total of high.

Chapter 6

Conclusions / Recommendations

Skyri municipal have some general challenges regarding information security; both broad (organisational) and specific(technical). We will highly recommend Skyri municipal to invest time/money in working with risk management in the whole municipal. As stated in the limitations of this document; this assessment report may be seen on as an injector to cover the worst operating threats in archive and in the same time alert you in how important risk management in an organisation is.

6.1 Legal Obligations

It is important to remember that this Risk Assessment have not been performed in regard to what laws Skyri municipality have to comply to. An important step forward is therefore to make sure that one already have an detailed overview over what laws Skyri is subject to. Typical legal obligations for Skyri; *The Right to Privacy Act, The Archive Act, The Civil Service Act, The Working Environment Act et.al.*

6.2 Action List – Short Run

Below is an overview with topics/areas that prompt need to be addressed, prioritised from 1 to 5.

1. Point out an IT security responsible
2. Change settings on email server to avoid misuse
3. Start looking at reasons for bad availability on archive system
4. Start working towards a centrally functional electronic archive system
5. Start creating routines for dealing with sensitive information

6.3 Action List – Long Run

- Evaluate less critical events we have analysed and take actions as needed
- Start working with an IT strategy
- Create/revise policy and rules regarding information security
- Make a plan in how to motivate all employees in information security work
- Make an risk communication flow table. Please find an example in appendix A table A.1

- Seek guidance in best practise regarding the computer technical challenges

6.4 Further Reading

The Norwegian Centre of Information Security (NorSIS) is a government founded initiative that are intended to help companies and personal people in securing their assets. They have really succeeded in producing several users guides, videos and games in struggle to educate in information security [7]. They are able to assist in risk assessments and/or guidance in managing information security work.

Norwegian National Security Authority NSM is a government founded supervisory authority within the protective security services in Norway. They monitor the security level and are the Norwegian CERT (Norwegian Computer Emergency Response Team (NorCERT)) [8]. They have produced several guides and can be asked to assist in computer security issues.

The Data Protection Agency is an government founded and independent service organisation. They work primarily with the enforcement of the Data Register Act of 1978, now made obsolete by the commencement of the Personal Data Act of 2000. They have produced several guides regarding computer security.

IT Infrastructure Library ITIL is a in general a framework of best practise methodologies in how to plan/make strategies/implement/test/operate/manage etc. IT/computer systems [6]. There are numerous computer companies that offers ITIL consultants/courses.

6.5 Risk Management is in general an organisational challenge

Risk Management is in large scale an management and organisational focus/project. When the leaders/government of an organisation understand that risk management is an important part of every organisation – half of the job are done! Further step is to motivate people to think risks in every corner of the organisation. Motivation is crucial for further success Risk Management.

Appendix A

Recommendation regarding communication

Input	Stakeholder	Output
Expectations towards risk awareness	Employee	Potential IT risk issues (including a not function IT system) to Head of IT
Risk Culture		Archive not working properly to the Head of Archive
Obligations according to the Personal Data Act	ITAll	System which satisfies issues regarding confidentiality, integrity and availability
Obligations according to the Service Level Agreement (SLA)		Periodic risk view report to Skyri - Head of IT
Potential IT risk issues		
Internal auditing of Risk (Skyri-related)		
Reporting of (IT) failure	Head of IT	Plan to fix or mitigate failure/IT Risk internally
Potential IT risk issues		Establish communication with ITAll
		Report IT risk issues to ITAll
		Follow up periodic risk view with ITAll
		Report of important IT Risks revealed this period to City Manager
Expectations for an efficient Archive system	Head of Archive	Efficient Archive system
Archive not working properly		Ideas for improving the Archive system to City Manager
		Contacting the proper people for problem-handling
Report of important IT Risks revealed this period	City Manager	Delegating of resources to handle new known IT Risks
Review ideas for improving the Archive system		Delegating of resources to set new ideas into life

Table A.1: Risk Communication Flow.

Appendix B

Template Risk Register Entry - Skyri				
Part I—Summary Data				
Risk statement				
Risk owner				
Date of last risk assessment				
Due date for update of risk assessment				
Risk category	☐ **Strategic** (IT benefit/value enablement)	☐ **Project Delivery** (IT program and project delivery)	☒ **Operational** (IT operations and service delivery)	
Risk classification (copied from risk analysis results)	☐ **Low**	☐ **Medium**	☐ **High**	
Risk response	☐ **Accept**	☐ **Transfer**	☐ **Mitigate**	☐ **Avoid**
Part II—Risk Description				
Title				
High-level scenario (from list of sample high level scenarios)				
Detailed scenario description—scenario components	Actor			
	Threat type			
	Event			
	Asset/ resource			
	Timing			
Other scenario information				
Part III—Risk Analysis Results				
Frequency of scenario (# times per year)	**LOW**	**MEDIUM**	**HIGH**	
	0.1<N≤1 ☐	**1<N≤10** ☐	**10<N** ☐	
Comments on				

Appendix B

Template Risk Register Entry - Skyri			
frequency			
Impact of scenario on business	**LOW**	**MEDIUM**	**HIGH**
1. Productivity	**Loss in man-hours**		
Impact rating	**< 1 HOUR IN 1 WEEK** ☐	**1 - 10 HOURS IN 1 WEEK** ☐	**>10 HOURS IN 1 WEEK** ☐
Detailed description of impact			
2. Public reputation	**Loss in public reputation**		
Impact rating	**1 NEGATIVE ARTICLE IN PRESS IN 1 YEAR** ☐	**2 - 5 NEGATIVE ARTICLES IN PRESS IN 1 YEAR** ☐	**>5 NEGATIVE ARTICLES IN PRESS IN 1 YEAR** ☐
Detailed description of impact			
3. Legal	**Regulatory compliance**		
Impact rating	**0 – 100 000NOK** ☐	**100 000 – 1000 000NOK** ☐	**>1000 000NOK** ☐
Detailed description of impact			
Overall Impact rating (average of four impact ratings)			
Overall rating of risk, obtained by combining frequency and impact ratings on risk map	☐ **Low**	☐ **Medium**	☐ **High**

Part IV—Risk Response				
Risk response for this risk	☐ **Accept**	☐ **Transfer**	☐ **Mitigate**	☐ **Avoid**
Justification				

Appendix B

Template Risk Register Entry - Skyri			
	Response Action	**Completed**	**Action Plan**
Detailed description of response (not in case of 'accept')	**1.**	☐	☐
	2.	☐	☐
	3.	☐	☐
	4.	☐	☐
	5.	☐	☐
	6.	☐	☐
Overall status of risk action plan			
Major issues with risk action plan			
Overall status of completed responses			
Major issues with completed responses			
Part V—Risk Indicators			
Key risk indicators for this risk	**1.** ***2.*** ***3.*** **4.** ***5.*** ***6.***		

Source: figure 36 *The Risk IT Practitioner Guide*.

Bibliography

[1] The Norwegian Business and Industry Security Council (NSR). Dark figures of computer crime. Technical report, NSR c/o NHO Scanning Postboks 5250 Majorstuen 0303 Oslo Norway, September 2010.

[2] Facebook. Statistics. URL, September 2011.

[3] ISACA. Homepage. URL. https://www.isaca.org/Pages/default.aspx.

[4] ISACA. *The Risk IT Framework*. ISACA, 2009. ISBN 978-1-60420-111-6.

[5] ISO - International Organization for Standardization. Iso-31000:2009. URL, September 2011.

[6] ITIL by APM Group Ltd and The Cabinet Office, UK. The Official ITIL Website. URL, September 2011.

[7] Norwegian Center og Information Security (NorSIS). URL, July 2011.

[8] Norwegian Computer Emergency Response Team. URL, September 2011.

[9] Norwegian Computer Emergency Response Team. Reccomondations regarding usb media. URL, September 2011.