Actions to enhance and support the information security risk assessment process in corporations

KAROLIN KARLSSON
Actions to enhance and support the information security risk assessment process in corporations

Karolin Karlsson

karok@kth.se

Degree project subject: Media Technology
Programme: Master of Science in Engineering in Media Technology, Master’s programme in Interactive Media Technology

Supervisor: Anders Lundström
Examiner: Haibo Li

2019-06-14
ABSTRACT
Information security is growing in importance as the world becomes more digital, at the same time the importance of usability implementation in software development is also growing. In this study, an evaluation was done on what affects usability and how important usability is in a reporting tool handling information security risk assessment (ISRA). The research question from which the study is based on: *What actions can enhance and support the information security risk assessment process in corporations?*

In order to investigate the research question a study was organized consisting of a survey (N=30) and a think-aloud usability test (N=7). As a part of the analysis process a usability heuristic analysis was performed.

According to this study, the ISRA process is complicated and creating a well-functioning supporting tool for it is complex. In order for the tool to facilitate for the users work, usability is an important aspect and should be taken in consideration early in the development process of a tool. Based on the findings in this study actions that can contribute to enhanced usability were discussed. The recommended actions are: 1) Include all types of roles in the ISRA process to determine the purpose of the tool and what it should support. 2) Implement clear guiding information in all parts of the tool, all people involved in the ISRA process should be able to understand the tool. 3) Keep an intuitive flow throughout the tool, the user should intuitively always know what the next step is and what to expect. 4) Have a search function that supports all aspects in the tool.

SAMMANFATTNING
Informationssäkerheten växer i betydelse i takt med att världen blir mer digital, samtidigt så ökar även betydelsen av implementering av användbarhet i mjukvaruutveckling. I denna studie gjordes en utvärdering av vad som påverkar användbarheten och hur viktigt användbarheten är i ett rapporteringsverktyg som hanterar informationssäkerhetsriskbedömning (ISRB). Den forskningsfråga som studien bygger på: *Vilka åtgärder kan förbättra och stödja informationssäkerhetsriskbedömningsprocessen i företag?*

För att undersöka forskningsfrågan organiserades en studie bestående av en enkätundersökning (N = 30) och ett användbarhetstest med ”Think-Aloud” (N = 7). Som en del av analysprocessen utfördes en användbarhets heuristisk analys.

Enligt denna studie är ISRB-processen komplicerad och att skapa ett välfunctionerande stödjande verktyg för att det är komplext. För att verktyget ska undlåta för användarnas arbete är användbarheten en viktig aspekt och bör tas i beaktning tidigt i utvecklingsprocessen för ett verktyg. Baserat på resultaten i dessa studie så diskuterades åtgärder som kan bidra till ökad användbarhet. De rekommenderade åtgärderna är: 1) Inkludera alla typer av roller i ISRB-processen för att bestämma syftet med verktyget och vad det ska stödja. 2) Implementera tydlig guidande information i alla delar av verktyget, alla personer som är involverade i ISRB-processen ska kunna förstå och använda verktyget. 3) Ha ett intuitivt flöde genom alla delar i verktyget, användaren bör intuitivt alltid veta vad nästa steg är och vad de kan förvänta sig. 4) Har en sökfunktion som stöder alla aspekter i verktyget.
Actions to enhance and support the information security risk assessment process in corporations

Karolin Karlsson
Media Technology
Royal Institute of Technology
Stockholm
karok@kth.se

ABSTRACT
Information security is growing in importance as the world becomes more digital, at the same time the importance of usability implementation in software development is also growing. In this study, an evaluation was done on what affects usability and how important usability is in a reporting tool handling information security risk assessment (ISRA). The research question from which the study is based on: What actions can enhance and support the information security risk assessment process in corporations?

In order to investigate the research question a study was organized consisting of a survey (N=30) and a think-aloud usability test (N=7). As a part of the analysis process a usability heuristic analysis was performed.

According to this study, the ISRA process is complicated and creating a well-functioning supporting tool for it is complex. In order for the tool to facilitate for the users work, usability is an important aspect and should be taken in consideration early in the development process of a tool. Based on the findings in this study actions that can contribute to enhanced usability were discussed. The recommended actions are: 1) Include all types of roles in the ISRA process to determine the purpose of the tool and what it should support. 2) Implement clear guiding information in all parts of the tool, all people involved in the ISRA process should be able to understand the tool. 3) Keep an intuitive flow throughout the tool, the user should intuitively always know what the next step is and what to expect. 4) Have a search function that supports all aspects in the tool.

Keywords
Information Security Risk Assessment; Usability; Risk Assessment; Risk Management; User Experience; UX; Intuitive; Human-Computer Interaction; HCI; Human-Computer Interaction and Security; HCISec; Interaction Design;

INTRODUCTION
Information security is growing in importance as the world becomes more connected and the number of electronically managed businesses are increasing [1]. Previous studies show that the implementation of usability in software development is important, and that the user plays a big part in a system being secure [16, 17]. For a company's survival, keeping information assets safe can be crucial and continuous risk assessments can mitigate and prevent the risk of information falling into wrong hands. The purpose of having a risk assessments process (Figure 1), is to prevent the company and its assets from being harmed and causing harm.

The connection between risk assessments and usability comes in the digitalisation of the process. During this project I have investigated how the employees at a global company experience the usability of a reporting tool intended for information security risk assessments. I have looked into the challenges and the problems that underlie for the employees when they are using the tool. The purpose of the tool is to ensure that the right actions is being made and implemented,
in order to mitigate risks. An example of an action can be restrictions on who is having access to the information asset. The tool also supports the follow-up process and traceability of past activities for the people responsible for the information asset. At the moment the tool is not used to the extent desired, and I am going to look into if the structure and design of the tool and the perceived usability of it could be a reason for it.

**Purpose and Research Question**

The purpose of this Master Thesis is to investigate how a reporting tool intended for information security risk assessments (ISRA) is used and how the usability of it affects the ISRA process. The goal is to see what actions can be done in order to enhance and support the ISRA process. The research question: *What actions can enhance and support the information security risk assessment process in corporations?*

**BACKGROUND**

**Usability**

Usability refers to the ease of using or accessing a product or system. It is part of the broader term user experience and has emerged from and replaced the expression “user friendly”. If the user achieves their goals with satisfaction, effectiveness and efficiency the product or system is usable, and usability is often achieved by having a user-centred way of designing and ensuring that the product incorporates attributes that support usability [14]. Satisfaction can be described as fulfilling a person's wishes, expectations or needs, or the pleasure that comes from this.

According to the official ISO standard 9241-11 the definition of usability is *“the extent to which a product can be used by specified users to achieve specific goals with effectiveness, efficiency and satisfaction in a specified context of use.”* [7]

**Information Security**

Information security consists of technical and administrative actions to protect information assets from intentional or unintentional acquisition, manipulation, damage, loss, exposure or misuse [3].

**Information Security Risk Assessment**

Information Security Risk Assessment (ISRA) is an important activity in information security management systems, as it is a method for identifying and assessing risks to information assets within corporations. The method is a continuous process of planning and performing risk assessments, reporting on activities and mitigating risks. Risk assessments are performed to understand the level of risk within a specific scope. Performing an ISRA gives the company the opportunity to analyse the information security risks to the company's business and operations as well as providing the basis for decisions on how to prioritize the mitigation of the risks. The importance of doing risk assessments in general at a company, is to prevent the company and its assets from being harmed and causing harm.

**Risk Assessment Process**

Risk assessment is commonly part of a process (Figure 1) and a workshop is typically organized with people responsible for the specific information asset that are being assessed. Following points describes the parts that are typically included in a risk assessment process [3].

1. *Determine vulnerabilities* - Investigate how the specific information asset is handled and if it is susceptible to an undesirable action.
2. **Risk assessment** - In this step an assessment is done on how damaging the risk is.
3. **Determine countermeasures** - Decisions are made about potential actions to address the vulnerability.
4. **Cost and benefit assessment** - Assess the costs for the actions (both financially and timewise) and assess if the actions actually reduces the risk.
5. **Compare cost and probability of the risk** - This step determines whether the vulnerability poses a sufficient risk to justify the cost of the countermeasures. If the cost is unacceptable or the benefit are too small, go back to step 3.
6. **Conduct Countermeasures** - When the countermeasures have been conducted, re-assess the risk for the information asset.

In order to maintain a consistent way of performing risk assessments throughout an organization, a reporting tool can be used. Such a tool can facilitate the dissemination of the actions to all concerned, contribute to an understanding of countermeasures and also facilitate the continuity of risk assessments [9].

**Context of this study**

This study is conducted at a large multinational company in networking and telecommunications. The company has around 95,000 employees spread around the world and risk assessment is crucial to be able to prevent the company's employees, products and information from being harmed or causing harm. This master thesis is done at the company's security department, in collaboration with the team that works with information security.

Currently, the company uses a web-based Risk Assessment Tool (RAT) (Figure 2) for reporting risk identification, risk assessment and action management. The tool was originally implemented to support their internal risk management processes and employees needs to be granted access to use it since it contains sensitive information. The system is a product developed by an external company.

**Usability Heuristics**

The following standard usability heuristics [15] describe principles for interaction design and can be seen as broad rules of thumb when talking about and evaluating usability.

*Visibility of System Status* - A system should always give the user relevant feedback and keep the user updated on what is going on.

*Match Between System and the Real World* - A system should follow real-world conventions and have information appear in a natural and logical order. Using concepts, words and phrases that are familiar to the users

*User control and freedom* - Possibility of undo and redo should be easy for the user and possible to do without having to go through extended dialogue

*Consistency and standards* - Standards ensure a consistent vocabulary and the users should not have to wonder whether different words, situations, or actions mean the same thing.

*Error prevention* - Even better than good error messages is careful design that prevents a error from arising. Either remove faulty conditions or control them and show the users a confirmation option before they commit to the action.

*Recognition rather than recall* - By showing things that the users can recognize, making things like options, objects and actions visible and having instructions for the system retrievable whenever appropriate, minimize the users memory load and improves usability.

*Flexibility and efficiency of use* - Allow users to tailor frequent actions can improve and speed up the interaction, mostly for frequent or expert users.

*Aesthetic and minimalist design* - All included information should be relevant to the users. All irrelevant information competes with relevant entities and reduces their relative visibility.

*Help users recognize, diagnose, and recover from errors* - The error messages should be expressed in a precise and non-coded way and suggest constructive solutions.

*Help and documentation* - It may be necessary to provide documented help and guidance, even if a system should be able to be used on its own. The documentation should not be too long, easy to search and focused on the user's tasks.

**Related Work**

Hvannberg et. Alt. describes a framework in their paper, this framework is for comparing evaluations methods to find usability problems [18]. Tiwana et. Alt. discusses the importance of risk assessments and the costs of failing in projects due to lack of risk assessments and risk management [19].

These two papers together highlights two important topics in this paper, the importance of both usability and risk assessments. In this project the two are combine and an investigation is done on what effects usability have on a reporting tool for risk assessments.

**METHOD**

In order to investigate my research questions a study was devised consisting of a survey (N=30) and think-aloud usability testing (N=7) in which the participants (Table 1) had to perform four tasks using the RAT. After the think-aloud an post semi-structured interview was conducted.
The purpose of the survey was to get insights in what the employees' opinions and experiences were regarding the RAT, what they think about the ISRA process and in what way the RAT contributes to the process. The usability tests purpose was to get a deeper understanding of how the users interact with the RAT, what they think about the usability and what functionality they think is important to maintain or enhance the usability. The semi-structured interview was aiming for understanding in what way the RAT supported the ISRA process.

Survey

The survey was hosted online using Google Forms and sent out to 102 RAT users registered in the system. In total 30 respondents completed the survey. The survey was divided into five parts. Having a survey divided into several parts with a progress bar has shown an increase in the number of respondents completing the survey, thus contributed to fewer dropouts [5]. This was something that was taken in consideration when creating the survey and inspiration was also taken from texts on survey methodology [6]. The survey includes both quantitative and qualitative questions. There are questions with different options to choose from (both multiple- and single-answer), open free text questions and also some questions where the participants are asked to answer on a scale from 1 to 10. The values on the scale vary depending on the question. Most of the questions are required for the participants to answer, but some are not.

To eliminate problems the survey was tested through a pre-study pilot [4] with four participants. In the pilot, the feedback was requested on the structure and the questions after they completed the survey. This test lead to several changes and a general quality enhancement.

The five different parts in the survey:

<table>
<thead>
<tr>
<th>Participant</th>
<th>Gender</th>
<th>Age</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Female</td>
<td>26</td>
<td>First time user, not involved in the ISRA process.</td>
</tr>
<tr>
<td>P2</td>
<td>Female</td>
<td>47</td>
<td>Have good insight into how RAT works and have performed a couple of risk assessments before and been part of documenting the ISRA process. This participant did succeed completing all the tasks.</td>
</tr>
<tr>
<td>P3</td>
<td>Male</td>
<td>47</td>
<td>Responsible for people working with reporting ISRA’s in RAT, but is not reporting anything himself.</td>
</tr>
<tr>
<td>P4</td>
<td>Female</td>
<td>60</td>
<td>Have used the RAT a couple of times to report an ISRA, not a frequent user. It was a while ago since the last use.</td>
</tr>
<tr>
<td>P5</td>
<td>Male</td>
<td>45</td>
<td>Good insight in the ISRA process and works with risk assessments. Not so frequent user of RAT but have used it a couple of times, now it was a while ago.</td>
</tr>
<tr>
<td>P6</td>
<td>Male</td>
<td>55</td>
<td>Have not reported any ISRA’s himself, but have looked into what others have added to RAT before.</td>
</tr>
<tr>
<td>P7</td>
<td>Female</td>
<td>42</td>
<td>Have used RAT a couple of times, but it was a while ago.</td>
</tr>
</tbody>
</table>

Table 1. Participants in Think-Aloud

Introduction - This part aimed to find out what kind of user the respondent was and also what their overall impression of the RAT was.

Starting to use the RAT - In this part the focus was on how the participants first interaction with the RAT was and if they explored it by themselves or if they got an introduction.

You as a RAT user - This part target what the respondent does as a RAT user and in what context they use the RAT. What part of the company they belong to, what they think about the process and how they think the RAT contributes to the ISRA process.

Your experience and interaction with the RAT - This part focused on the participants opinions about what they appreciate with the RAT, what they think is problematic, functionality they miss and if there is anything they want to change. It also focused on their experiences regarding structure, design, what they think about the RATs intuitiveness and how easy/difficult they think it is to use.

Final comments - This part was for final comments [13] and their potential participation in future usability testing.

Usability testing

Usability-testing means that the participant is performing some tasks in the tool, and usability inspection is the generic name for a set of useful ways of evaluating user interfaces in order to find usability problems [10].

Seven participants (Table 1) volunteered to participate in the usability test via the survey. All participants were located in Sweden and the tests were conducted in person.

Think-Aloud

According to Nielsen, using think-aloud while evaluating usability are convincing, flexible and robust [2]. During the usability testing session the participants were asked to
perform four tasks while they were thinking aloud about their experience. The reason why these four tasks were chosen was because they are common things that users do when using the RAT. They were encouraged to speak loudly about what they did, what they thought of the tool, and its usability. At the same time I recorded and observed how they performed the tasks and recorded task completion times.

The tasks during the think-aloud:

1. Log on to the RAT (with their own login details), start from the company's internal site
2. Find the ISRA with the name Master Thesis Project
3. Update the name on the same ISRA
4. Create a new ISRA

Task nr 2, 3 and 4 was performed in an test environment of the RAT.

The qualitative data collected during these sessions underlies for the observational findings that identify potential design and usability problems.

**Post Semi-Structured Interviews**

After the think-aloud, an semi-structured interview was conducted with the participants about how they experienced the tasks and the usability of the tool. Questions regarding how well the RAT supported the ISRA process was discussed along with if they think that something should be changed in the RAT or if they miss any functionality in order to make their workflow with the tool better.

**Data Analysis**

The collected data from the user studies was first evaluated with a bottom-up approach, with an open analysis aimed at detecting general impressions and recurring opinions from the participants. As a part of the further analysis process a usability heuristic analysis was performed using the standard usability heuristics [15].

The data that was collected from the user study was anonymised and the personal identifying information was not stored without consent from the participant. All the collected data connected to the participants was deleted after the evaluation and presentation of the master thesis project.

**RESULT**

The user study showed that the overall impression regarding the RAT was that the system does not suit the purpose and that it is too difficult to use. The user study also showed that the participants thinks that the information security risk assessment process is important. On the survey question “How important do you think the identification of information security risks are for the company's business or operations?”, where the participants answered on a likert scale from 1 (not important at all) to 10 (critically important), 17 participants responded 10, eighth responded 9, four responded 8 and one responded 5. The one respondent that answers 5 (neutral), is a person that do not use the RAT any longer. So 29 of the 30 respondents thinks that identifying information security risks are important or critically important.

“Highly inadequate and user-unfriendly. Not fit for purpose”

- Not so frequent user, Survey

Many (18/30) of the participants in the survey expressed dissatisfaction regarding the ISRA process. Some things the participants uttered was that the current ISRA process is unclear and that it has to become more elaborate and informative. The RAT does not facilitate the employees to report and manage the ISRA process. Some of the recurring words and phrases that the participants used when describing the RAT was: not intuitive, complicated, user-unfriendly, difficult to use, too complex and confusing.

**Usability Heuristic**

In this section I present the users' experiences and opinions about the RAT in relation to six of the ten standard usability heuristics [15].

**Visibility of System Status**

From the interviews and observations it became obvious that the RAT does not provide sufficient information to the users about what is possible to do in the tool and how to actually do it. For instance, the start page (Figure 1) contains very little information about the functions available in the system. This can be associated with the fact that many participants (5/7 in the semi-structured interview) stated that users needs to know the RAT beforehand to be able to do things in it. This makes it difficult for a first time users to understand how to do things and where to find what they are looking for. Numerous participants (10/30 in the survey) also expressed that it is complicated process to get the right access for using the system and that this is something that hinders them from starting to using it in the first place.

Not surprisingly, many participants also wished for a tool that guides them to do things correctly, and helps them put in the right information in the right place. The majority of the participants (26/30 in the survey, 7/7 in the semi-structured interview) think that the tool needs to be changed or replaced, because at the moment it is too complicated to use and it does not help them in their ISRA processes as the RAT mainly contributes in making the process hard and cumbersome. Here is one illustrative example response:
“An information page would help. Because now when you enter the tool, you are expected to know everything.”

- P1, during usability testing

Furthermore, in addition to the lack of informative texts, the think-aloud further highlighted that the complicated structure of the RAT makes the users confused. Five out of the seven participants in the think-aloud got stuck on a task and did not know how to continue, as the tool itself could not help them to proceed they gave up.

During the semi-structured interviews, the participants talked about their expectations on the RAT and how they wished it to be like. In order to get proper ISRA reports that can give the possibility for people to follow and handle the ISRA’s in an efficient way, it was stated that it is important that all the parts of the process is reported correctly in the RAT. One reason for this that was mentioned was that more people than those who work with reporting into the RAT are involved in the ISRA process, and they wished that it would be easier for them to be able to see the reported ISRA’s and the information regarding it. Many of the RAT users are only interested in seeing the information reported about the ISRA’s. These users typically rarely use the RAT. Many of them have only logged in once (9/30 in the survey) or 2-5 times (8/30 in the survey), and because they failed to find what they were looking for, they never returned to the RAT.

To prevent this from happening, the participants wanted the RAT to attract first-time users and that it should be easy for the users to find the right path.

Recognition Rather than Recall

On the start page of the RAT (Figure 2), there is no information on what the RAT is and what could be done in the tool. The participants (22/30 in the survey, 5/7 in the think-aloud) expressed that it is non intuitive and that they would like to have clear information of how to do different things directly when they are entering the tool. The think-aloud showed that the one participant (P2) that has used the RAT many times before could perform all of the task with no trouble at all. She recalled her previous usage of the RAT, and remembered how to click and do to succeed with all the tasks.

Five (P3, P4, P5, P6, P7) of the seven participants in the think aloud did not manage to do task 3, a very basic task to edit the name of an ISRA. Four (P3, P4, P5, P7) of them came to a view of the ISRA were there was no possibility to edit or change anything (Figure 4). All of them tried different commands, such as right-clicking, but did not succeed to edit the name. The two (P1, P2) participants that manage to do task 2, found a way to another view of the ISRA where it was possible to update (Figure 3). One participant (P6) failed with all the tasks, except login in, despite that P6 had used the RAT a couple of times before. He said that his

![Figure 3. View of ISRA, found through navigation under Action Management](image1)

![Figure 4. View of ISRA, found through search](image2)
expectations on the tool was that it should be possible to put it in the hands of anyone, and they would be able to use it, but that he does not believe that it is so right now.

“You have to be an expert in order to use it.”

- P3, during interview

**Match Between System and the Real World**

According to the participants in the user study, the RAT does not appeal to new users or infrequent users. Although those who have used the RAT several times feel that it is possible to learn the language and structure of the RAT over time. According to 24 of the 30 participants in the survey, they think that the RAT is not easy to use and that it is hard to understand the RAT and its structure. Mainly because of the lack of information in the RAT making it difficult to understand how to do things in the tool.

One participant (P7) said that a possibility to work more creatively and free in the tool could enhance the experience and lead to better ISRA reports. She thought that the tool was too strict and steered them too much. For instance, she wanted the tool to be more intuitive to use with drag and drop functions, like working on a whiteboard. She believed that a more creative approach would lead to better data and better results from the ISRA process.

In the RAT, users have to do three clicks from the start page in order to come to the Risk Assessment page, where they can find all the existing ISRA’s (Figure 5). On the Risk Assessment page (Figure 6), the user can see all the ISRA’s they have access to, update or edit ISRA’s and create new ISRA’s. In order to be able to perform all these activities, the user have to come to this Risk Assessment page that are located under the title Action Management, a title that not obviously led on to risk assessment.

**Consistency and Standards**

In the RAT there are uncertainties when it comes to the titles on different pages. Two participants (P1, P5) in the think-aloud commented on the titles that they did not understand what it means and that it is very vague what to expect. The users do not feel that they know what to expect when they click on certain things and enter a new page in the tool. Overall indicating fundamental problems with naming and structure in the tool.

The participants think that it is unclear what happens when they were about to confirming certain things. One example from the think-aloud, when the three participants (P1, P2, P7) that succeeded performing task 4 (create a new ISRA). When they were done typing in the info for the new ISRA they had the option to click Perform or Update. All three of them expected a save button, or similar. They all choose to click on Perform. After loading for a couple of seconds, an information box was shown saying that an email had been sent to a person. This action was unexpected to all participants when clicking Perform. They thought that it would have been good to know that when they clicked Perform, it meant that they both saved and also that an email will be sent to that person.

---

**Figure 5. Click path to the risk assessments**

**Figure 6. Risk Assessment page**
“Right now we as users need to adapt to the tool, instead of the tool being adapted to us and the ISRA process.”

- P6, during interview

Flexibility and Efficiency of Use

The RAT cannot be customized for any user, the look of it is static. However, users with different accesses have different rights to do and access things. The look is the same for everybody, but the users possibilities are different. Two participants (one from survey, P6 from semi-structured interview) said that they think that the RAT should be able to customize and appear differently depending on type of user and type of access. They think that a more user-focused UI can lead to better interaction and more essential and accurate data reporting. Two participant (P6, P7) said during the semi-structured interviews that users can get lost in the RAT, because of all the unclear possibilities and options. That the user risk to stare blindly at different fields and strange words and that it can affect the quality of the information that they reports in the tool.

A wish for the possibility to do smart analyses was also expressed by one participant (P7). She wanted to take advantage of the work with reporting ISRA’s to the fullest, and use it to find potential correlations between different ISRA’s independent on who have reported the information.

Error prevention

During the first task in the think-aloud, when all of the participants were asked to log into the RAT, everybody got an error. The RAT does not support single sign on when entering from the company’s internal site. The users had to type in their login details at least three times before entering the RAT successfully. This caused confusion for the users and they all got a bit annoyed when they had to type in their login details that many times. The RAT does not keep the user informed of all things that happen when the user clicks on certain buttons. I now also refer to the aforementioned problem with an email (in consistency and standards) that was sent away without the user knowing it in advance, the RAT did not give the user an option the email was just sent.

“What I miss most is probably a functionality that prevents you from doing wrong.”

- P2, during interview

DISCUSSION

In this report a tool, intended for risk assessments, has been evaluated by analysing a survey, a think-aloud and interviews through the lens of usability heuristics. The focus have been on the users and the usability of the tool. According to this study, fundamental usability issues are prevalent in their current tool that needs to be addressed in order to support ISRA processes. It is obvious that the current system suffers from 1) poor visibility of system status, 2) relies heavily on recall rather than recognition, 3) forces the ISRA process to adapt to a dysfunctional system rather than to support ISRA processes, 4) have poor and inconsistent naming and structure, 5) does not adapt to users roles and needs, and 6) has poor error preventions and behave in unexpected ways.

In a future implementation all these usability aspects should be taken in consideration early in a development process of a new system aiming for a high usability standard and good user experience. This is important to support new and occasional users returning to the system as today many visit once and is reluctant to ever use it again, which is potentially harmful to the company as it may overall affect the important ISRA process. A new system needs to support different users and roles and be, simple, intuitive and guiding. I will now proceed to discuss these issues in more detail.

Out of the usability heuristics problems identified in this study, visibility of system status and recognition rather than recall is two of the most important ones. Because if a user knows intuitively how things should be done, the occurrence of problems will probably be minimized and the usability perceived as good. If a system relies on that the users are able to recall to previous use, errors will most likely occur for many users and contribute to low usability.

That the RAT is lacking on information about what is possible to do in the tool and how to do it, is a clear recurring problem for many users. The fact that many participants in the think-aloud did not manage to perform as simple tasks as finding an ISRA, shows that the tool is non-intuitive and not self-explanatory. By not giving the users clear information or guidance, confusion arises and lower the level of usability a lot.

The fact that even frequent users did not manage to do all of the tasks easily further highlights the degree of these issues and hence it not surprising that new or infrequent users struggle even harder. Overall, this indicates clearly that the RAT relies on the user being able to recall how to use it at all levels, including navigating to and performing tasks. This is in opposition to fundamental usability recommendation that the system should support recognition and guiding the user rather than forcing them to remember all details. Although this system probably needs a complete makeover, the usability could possibly be improved greatly by adding informative texts and guidance in the RAT. This could also be in the format of a manual if it is not possible to change the tool itself, although manuals are generally to be avoided
since they tend to be unread. Nevertheless, clear instructions is needed and also wanted by the participants.

As regards recognition rather than recall, the user get different views of the ISRA depending on where they access it from. This may be a potential reason for some of the confusions for the users. This also violates the usability consistancy and standards.

The fact that the search function do not lead the user to the view were the user are actually able to edit or do anything is problematic and misleading. This problem becomes particularly problematic in relation to the general problems of navigating the system since the think-aloud showed that most of the participants started the task using the search bar to find a the relevant page for the task. In such a dysfunctional and complex system it appears crucial to have a well-functioning search function as a work around for navigating. This may also be a natural path for many users today who are used to search for things directly using (e,g,) Google, instead of looking for it were they think that it may be.

During this project I have got the impression that if you are a frequent user of a system, you will be able to learn how to use it, regardless its lack of usability, user experience design and user friendliness. A user can make it work if it puts time and effort to learn how to use a system, product or tool. However, still they do not appear to really enjoy using the tool and report dissatisfaction. If the user have to use the poor designed tool, because of the duty at work for example, this duty risks to becoming a task that is not appreciated and it may affect the quality of the reporting and hence also the overall values provided by ISRA processes. If the tool instead would have a high level of usability and ease the work of performing the task, then most likely, the user will appreciate the tool and enjoy using it for higher quality ISRA.

That the employees had to type in their login details at least three times before entering the RAT properly, is one thing that I think can lead to that some user drop of already here. Although all of the participants continued to try even when they got an error, this may not be the case under real conditions outside of a study. I think that a person who is trying to log in by themselves have a bigger chance of giving up if facing an error, than a person attending a think-aloud with an observer.

Having the functionality of being able to customize a tool is something I absolutely think can be good, but I do not think that it is a crucial thing in order for a tool to have good usability. I think this can be a feature that more advanced and frequent user could appreciate. The possibility of adding shortcuts to frequently visited pages or being able to mark ISRA’s which they want easily accessible, this could both enhance the usability. But on the other hand, I think all of the basic functionalities and pages should be easy accessible, and not hidden behind incomprehensible titles.

**Design Implications**

The main problem with the RAT is that it is not made for its purpose at the company, with the ISRA process, the employees, and their workflow in mind. The employees have to adapt to the tool, instead of that the tool helps and facilitates their work. This causes confusion and frustration, and makes the employees duties that includes using the RAT feeling tough and something that they avoid as much as possible. The RAT has to ease their work if they are to use it, not complicate it. The design in form of colors and shapes, are not so important in this case as the users want something that works and something that helps them. It does not have to be fun using the tool, but it has to be helpful.

Based on the results in this study, these four suggested actions could be a step in the right direction in order to enhance or create good usability in a reporting tool intended for information security risk assessments.

1. All different types of roles involved in the ISRA process should be included early in the development process to determine the purpose of the tool and what it should support. This could be done through participatory design or by creating personas representing the different user groups.
2. Implement or add clear guiding information in all the parts in the tool. All the people involved in the ISRA process should be able to understand the structure and language of the tool.
3. Keep an intuitive flow throughout the tool, the user should intuitively always know what the next step is and what to expect. Even a person new to the ISRA process should be able to report an risk assessment.
4. Have a search function that supports all aspects in the tool. Such as both finding their way to different parts in the tool, but also find information and help on how things should be done in the tool. A good search function is probably not as important in a good designed system, as it is in a poor designed one.

These suggested action could be applicable on other types of tools and systems in order to enhance the usability.

**Method Reflection**

Generally, the methods used in this study complemented each other in a good way. The survey gave a broad insights
of the problems, and the usability testing gave more in depth insights about the users experiences, opinions and expectations.

The usability heuristic analysis gave a clear picture on what was problematic and dysfunctional with the RAT. I started with all ten of the usability heuristic standards and ended up to choose six, since I found them most applicable to the data and this specific tool.

As Nielsen claims [4], using surveys is a flexible and easy method for gathering data, and it felt that for my type of user study, that was a good place to start from. Since I had the opportunity to reach out to user spread out in the company with different locations in the world, I thought that survey was a suitable option. I feel that it also turned out to be a good method for me since it resulted in qualitative and detailed answers. The survey contained mostly free text questions, I choose to have that because I wanted them to think freely and not be misled or limited by predetermined options. I was a bit worried that the questions were too open, and that it would lead to people not completing the survey, and contribute to too few responses. But since my goal was to get at least 20 responses and I finally received 30, I am pleased and believe that the survey turned out to contribute with a lot of engaging and detailed answers, that contributed with qualitative data for the user study.

If I would have the possibility to do something different with the survey, it would be to ask questions about the users expectations on the tool. During the think-aloud I found out that it was a good question to ask, in order to get dedicated and detailed answers. I would also have included more questions where the answers would be on a scale. I think questions with answers like that can give a quick understanding of what specific things that the users think is important and not.

The think-aloud gave good insights in how they use the tool and clearly highlighted obvious obstacles and problems. The directly followed interview turned out to contribute with a lot of qualitative data that supported the observations I did during the think-aloud.

As an observer during the think-aloud I learned that it is important to not only listen to what they are thinking, but also look at what they are doing. Because all participants did not tell about every single detail of what they did and thought. The recordings I made during the test contributed to my focus being on observing their actions in the tool. Although participants succeeded with a task, they were able to express dissatisfaction with how the interaction worked.

I thought that it would be good to ask them questions when they had the interaction, user experience and user interface of the RAT fresh in mind. Therefore I choose to directly after the think-aloud have the semi-structured interview. The answers contributed to deeper understanding of their experience and opinions. Since the questions came right after the participants interacted with the tool, I think that it made the questions more reliable, than if the user had to think back to maybe several weeks or even months ago when they last used the RAT.

The thing that I would have done differently if I were to do the usability testing again, is try to get more participants and a greater variety of users. Since it is a global company, the logistics regarding location made it complicated to meet people in person.

CONCLUSION

What actions can be done to support the information security risk assessment process in corporations?

From the findings in this study, it could be determined that in order for a tool to properly support the ISRA process and facilitate for the people working with it, it is important that the tool is intuitive, self-explanatory, clearly structured and includes guiding information. To achieve this and to maintain good quality in the ISRA reporting, it is important to understand all users’ needs and expectations, and make the tool support them in the process. All different end-users should be included during the development stage to achieve good usability for all users.

Looking at the problem on a larger scale, I believe that the effects that can come from lack of usability in a tool such as RAT, is that risk management can be affected. If the people who are responsible for a specific information access cannot follow the process and use the tool to the extent expected, it can lead to the information becoming vulnerable and exposed to risks.

ACKNOWLEDGMENTS

Firstly, I want to say thanks to the company and my manager for giving me the opportunity to conducting this thesis. A big thank you to all the participants that took the time and share their valuable information and opinions. Finally, I am truly grateful to my supervisor at both KTH and at the company for always supporting and guiding me through this process.
REFERENCES

[17] Adams, A. Sasse, M.A. “Users are not the Enemy” 1999