Abstract

Various risk management methodologies have been developed to help the organizations define, analyze, evaluate and mitigate the most relevant and critical risks to the information security in an organization. How useful are the information security risk assessments to the organization? To what degree are acknowledged risk assessment methodologies used in practice, and which factors determine the benefit of doing risk assessments? The current use of Information Security Risk Management methodologies will be examined in this master thesis.

The perceived usefulness of doing risk assessments, how and to what extent the different risk assessment methodologies are used in practice will be surveyed. Various studies have reviewed risk assessment methodologies with the purpose of presenting new methods for risk assessment, and taxonomies for risk assessment methodologies have been developed with the purpose of helping organizations to choose the most suitable risk assessment methodology.

This study is based on a survey of risk and information security experts, and interviews with four risk managers and information security experts, in addition to review of scientific articles on risk assessment case studies, comparisons and risk assessment methodology taxonomies. The survey was distributed by The Norwegian Business and Industry Security Council (NSR) to their newsletter recipients, and followers of NSR LinkedIn and Facebook pages. The language in the survey and interviews is Norwegian.

The findings in the risk assessment survey and the interviews indicates that the well acknowledged risk assessment methodologies, COSO and IRAM2, ISO/IEC 27005, NIST 800-37 and NSM's risk assessment methodology are known and used, while OCTAVE, CRAMM, EBIOS and TRA are not as well-known by the information security experts and risk managers as the scientific articles give an impression of. However, responses from both participants and interview subjects indicate that organizations do perceive the risk assessment as useful.

Comparing findings from the survey and interviews with the papers on risk assessment, and the taxonomies giving an overview of the risk assessment methodologies indicate that perceived usefulness does not imply that the factors determining the usefulness of risk assessment were present, and that the success criteria for risk assessment were present. If top management, information security experts and risk managers became aware that there exists inventories of risk assessment methodologies, taxonomies and other resources, this could contribute to increasing the usefulness of the risk assessment process, and ensure success factors of the risk assessment process were present.

Oppsummering

Ulike risikostyringsmetoder er utviklet for å hjelpe organisasjonene med å definere, analysere, evaluere og behandle de mest relevante og kritiske risikoene for informasjonssikkerheten i en organisasjon. Hvor nyttige er risikovurderingen av informasjonssikkerhet for organisasjonen? I hvilken grad er anerkjente risikovurderingsmetodologier brukt i praksis, og hvilke faktorer bestemmer fordelen ved å gjøre risikovurderinger? Den nåværende bruken av risikostyringsmetoder for informasjonssikkerhet vil bli undersøkt i denne masteroppgaven.

Den opplevde nytten av å gjøre risikovurderinger, hvordan og i hvilken grad de forskjellige risikovurderingsmetodikkene blir brukt i praksis vil bli undersøkt. Ulike studier har gjennomgått risikovurderingsmetodologier med det formål å utvikle og presentere nye metoder for risikovurdering, og det er utarbeidet taksonomier for risikovurderingsmetoder for å hjelpe organisasjoner å velge den mest passende risikovurderingsmetodikken.

Denne studien er basert på en spørreundersøkelse med eksperter på risiko og informasjonssikkerhet, og intervjuer med fire risiko- og informasjonssikkerhetseksperter, i tillegg til gjennomgang av vitenskapelige artikler om risikovurderinger, casestudier og taksonomier for risikovurderingsmetodikk. Spørreundersøkelsen og intervjuene foregikk på norsk, ble distribuert av Norsk Næringslivets Sikkerhetsråd (NSR) til deres nyhetsbrevmottakere, og følgere av NSR på sosiale medier.

Funnene i risikovurderingsundersøkelsen og intervjuene antyder at de godt anerkjente metodene for risikovurdering, COSO og IRAM2, ISO / IEC 27005, NIST 800-37 og NSMs risikovurderingsmetodikk er kjent og brukt, mens OCTAVE, CRAMM, EBIOS og TRA er ikke så godt kjent av informasjonssikkerhets- og risikoeksperter som de vitenskapelige artiklene gir inntrykk av. Svar fra både deltakere og intervjuobjekter indikerer imidlertid at organisasjoner oppfatter risikovurderingen som nyttig.

Sammenligning av funn fra undersøkelsen og intervjuer med avhandlingene om risikovurdering samt taksonomier som gir oversikt over risikovurderingsmetodikkene, gir indikasjoner på at opplevd nytteverdi ikke medfører at faktorene som angir høy nytteverdi av risikovurderingen eller suksesskriteriene for risikovurdering var til stede. Dersom toppledelse, informasjonssikkerhets- og risikoeksperter kjente til at det fantes oversikter over risikovurderingsmetodikker, taksonomier og andre ressurser kunne dette bidra til å øke nytten av risikovurderingsprosessen, og sikre at suksessfaktorene i risikovurderingsprosessen var til stede.

Acknowledgment

I would like to thank my supervisor dr.philos. Einar Snekkenes, for all his good advice, interesting discussions and constructive feedback during the work with this thesis.

I would like to thank Arne Røed-Simonsen, senior consultant in The Norwegian Business and Industry Security Council (NSR) for all his help and advice regarding the distribution of the survey, and for the results and reports related to the Norwegian Computer and Data breach survey 2018 and Norwegian Crime and Security survey 2019. As a service towards Norwegian students in information security-related programs, The Norwegian Business and Industry Security Council (NSR) offer their results and reports to use in their studies.

I would like to thank the interview subjects who shared your time, knowledge, experience and opinions, your contribution to this thesis is highly appreciated.

I would like to thank my colleagues at Watchcom Security Group for their interesting discussions, moral support, sporty attitude, and constructive feedback as “guinea pigs”.

I would like to thank my husband for all his patience, calm, moral and practical support during the work with this thesis, and previous semesters with papers, exams, and deadlines. I would also like to thank my boys for enduring their boring-nerdy-, always-writing-on-her-laptop-mum, and I would like to thank the fabulous Mormor, Bestefar, Farmor and Farfar for taking the boys out and have some fun while mum study.

Content

List of figures xi

List of tables xi

Abbreviations/symbols xii

1 Introduction.................... 13

1.1 Problem description.................... 14

1.2 Research questions: 14

2 Related work 15

3 Research methodology 23

3.1 Planning the research 23

3.2 Implementation of research methodologies 25

3.2.1 The survey on risk assessment methodologies 25

3.2.2 The interviews 28

3.3 Analysing the results 29

3.4 Evaluating the research methodologies.................... 31

4 Analysis 34

4.1 To what degree are well-established methodologies for risk assessment used by organizations?.................... 36

4.2 Which factors determine the choice of risk assessment methodologies? 40

4.3 To what degree are risk assessments perceived as useful? 43

4.4 Which factors determine the usefullness of risk assessments?.................... 47

4.5 Have organizations defined any success criterias for risk assessments? 51

5 Discussion 56

5.1 To what degree are risk assessment methodologies used by organizations? 56

5.2 Which factors determine the choice of risk assessment methodologies? 59

5.3 To what degree are risk assessments perceived as useful? 62

5.4 Which factors determine the usefulness of risk assessments?.................... 64

5.5 Have organizations defined any success criterias for risk assessments? 67

6 Further research.................... 70

7 Conclusion.................... 71

References 74

Attachments 77

List of figures

Figure 1 - Classification of Risk assessment methods(22) 20
Figure 2 - CURF taxonomy of risk assessment methodologies(28) 22
Figure 3 - Branches represented in the survey... 35
Figure 4 - When the participants last took part in risk assessment 37
Figure 5 - The use of risk assessment methodologies 38
Figure 6 - Definition of risk.. 38
Figure 7 - Assessment of threats 39
Figure 8 - Level of education 41
Figure 9 - The level of usefulness in risk assessments.................................. 44
Figure 10 - Experience with information security incidents........................... 45
Figure 11 - Severity of incidents 45
Figure 12 - Types of consequences 46
Figure 13 - Preparedness for incidents 47
Figure 14 – How participants describe usefulness 48
Figure 15 - The greatest benefit of doing risk assessments 49
Figure 16 - Processing of risk assessment 50
Figure 17 - Success criteria of risk assessments 52
Figure 18 - Number of participants in risk assessment 53
Figure 19 – The survey participants role in risk assessment 54
Figure 20 - Other roles present in risk assessment 54
Figure 21 - Methodologies mentioned in taxonomies and papers 57
Figure 22 - Branches represented in the crime and security survey(33) 60

List of tables

Table 1 - Overview of the use of terms and definitions in Risk Assessment methodologies 30

Abbreviations/symbols

ISMS	Information Security Management System
PDF	Portable Document Format
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	The National Institute of Standards and Technology
NSM	The Norwegian National Security Authority
NSR	National Business and industry Security Council
ENISA	European Union Agency for Cybersecurity
EBIOS	Expression of Needs and Identification of Security Objectives
CRAMM	CCTA Risk Analysis and Management Method
CCTA	British Central Communication and Telecommunication Agency
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
MEHARI	MEthod for Harmonized Analysis of Risk
TRA	Harmonized Threat and Risk Assessment Methodology
IRAM2	Information Risk Assessment Methodology 2
TREsPASS	Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security
CBA	Cost-Benefit-Analysis
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
Difi	Norwegian Digitalisation Agency (Previous: Norwegian Agency for Public Management and e-Government)

1 Introduction

This master thesis examines the current use of Information Security Risk Management methodologies, the perceived benefits of doing risk assessment and what the success factors for doing risk assessment are. To what degree are risk assessment methodologies used in practice? And how are they chosen?

ISO 27000(1) defines risk assessment as the process of risk identification, risk analysis and risk evaluation, whereas risk is defined as the effect of uncertainty on objectives, while risk analysis is the process to comprehend the nature of risk and to determine the level of risk. Thus, Risk management is defined as the whole process of risk identification, analysis, evaluation and risk treatment. NIST 800-37(2) defines risk management as "The program and supporting processes to manage risk to agency Operations(…) and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time".

This master thesis focus on the part of the risk management regarding the risk assessment process. It has been observed that the process of doing risk assessments can be unnecessary comprehensive, resource demanding and time consuming and not operationalized by the organization, or as Barak Engel (3) states about risk assessment reports: "It seems like nobody actually wants to read it, let alone fix anything".

Various risk assessment methodologies provide guidance in the process of identifying, analyzing, and evaluating and treating the risk. This thesis will examine to which degree 10 of the well-acknowledged risk management methodologies are known and used by organizations, and which factors determined the choice of methodology. These ten risk management methodologies are ISO/IEC 27005(4), NIST 800-37(2), COSO(5), IRAM2(6), OCTAVE(7), CRAMM(8), EBIOS(9), MEHARI(10), TRA(11) and the Norwegian methodology NSM risk assessment handbook(12). How useful the risk assessments are perceived, the factors that determine the degree of usefulness and the success-factors of risk assessments will be analyzed and discussed in this study.

Several studies have been written about the risk management methodologies, reviewing the characteristics in case studies, examining the differences between them, their suitability for different types of organizations, and there are several studies presenting taxonomies of the most acknowledged risk assessment. methodologies, with the purpose of being an aid to decide the most suitable methodology for an organization.

This study is based on a survey of risk and information security experts, and interviews with four risk managers and information security experts, in addition to review of scientific articles on risk assessment case studies, comparisons and risk assessment methodology taxonomies. The survey was distributed by The Norwegian Business and Industry Security Council (NSR) to their newsletter recipients, and followers of NSR LinkedIn and Facebook pages. The language in the survey and interviews is Norwegian, and the members of NSR are Norwegian organizations the participants represent which are members of NRS are Norwegian,

The master thesis consists of five chapters, the first chapter includes the introduction, problem description, research questions and terms and definitions. The second chapter includes related work on risk assessment experience, comparisons and taxonomies, the third chapter consists of descriptions and discussions regarding the research methodologies used in this study. The fourth chapter cover the analysis of results from the survey and interviews, and the fifth chapter holds the discussion of the findings, compared with reports from related studies and related articles.

1.1 Problem description

The well acknowledged risk assessment methodologies are not as well-known by the information security experts and risk managers as the scientific articles give an impression of, meanwhile organizations do not perceive the risk assessment as useful

1.2 Research questions:

1) To what degree are well-established methodologies for risk assessment used by organizations?
2) Which factors determine the choice of risk assessment methodologies
3) To what degree are risk assessments perceived as useful?
4) Which factors determine the usefullness of risk assessments?
5) Have organizations defined any success criterias for risk assessments?

2 Related work

The current research on risk assessment methodologies will be reviewed in this chapter. There are mainly case studies of the implementation of risk assessment methodologies and presentations of risk assessment methodology taxonomies. However, a study has been examined where the failed attempt to survey the actual use of risk assessment methodologies due to low response rate was discussed. Another contribution was the study on other papers on risk assessment methodologies, discussing the meta-aspect of reviews.

In an essay by Barak Engel(3) the experiences of a risk assessment process was described. The essay was not a scientific article, but with a lighter look on risk assessment process Engel described how risk assessment was perceived to be time-consuming and resourse-demanding, however, “While we feel good about producing such a valuable and well-considered document, it seems like nobody actually wants to read it, let alone fix anything”. Engels proposed a closer connection to business processes and making sure the risk is relevant to the business, and concluded that presenting the risk assessment in a form and language top management understood was the key to getting the risk communicated, understood and operationalized by the organization.

In a study by Pan and Tomlinson(13) over 80 research papers published between 2004 and 2014 related to information security risk assessment were examined and systematically reviewed to find the information security risk assessment methods which are mostly studied and the current categories of research. The study presented a framework of the research papers, classified by seven types, to help researchers get an overview over the research areas of risk management.

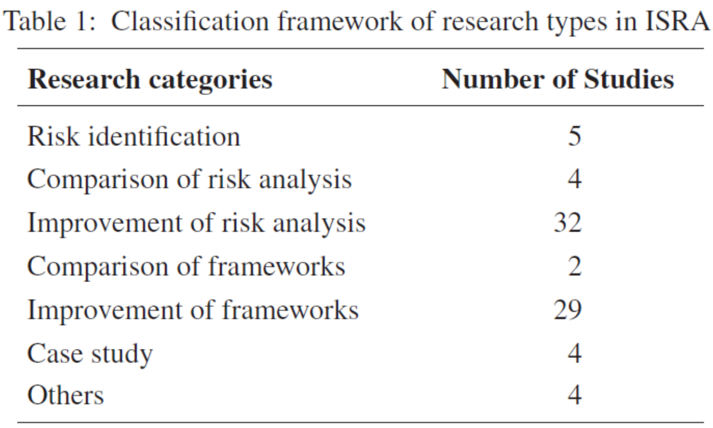


Table 1: Classification framework of research types in ISRA.

Research categories	**Number of Studies**
Risk identification	5
Comparison of risk analysis	4
Improvement of risk analysis	32
Comparison of frameworks	2
Improvement of frameworks	29
Case study	4
Others	4

Pan and Tomlinson conclude that the collecting and managing of information in the risk management context are rarely mentioned in the reviewed papers, and that the “real-world” data is insufficient. Therefore, there is a need for increased research on this is area in information security risk assessment to gain knowledge of the variety of methods to collect and analyze the input data effectively and efficiently.

Andrew Kotulic and Jan Guynes Clark (14) did the study “Why there aren’t more information security research studies” on security risk management in organizations and observed that organizations were reluctant to give away information about their risk management procedures, and thus a lack of empirical research related to risk management. The hypothesis was related to executive managements involvement in security risk management compared to perceived usefulness of the risk management program, and the connection between severity in security breaches and security risk management, based on the definition of risk that it is “the perceived extent of possible loss”.

Kotulic and Clark struggled to present a valid result of the research, with the response rate for the survey being too low. This led to another survey on the reasons for organizations not to participate in a survey on risk management. The conclusion was that research on information security in organization was an intrusive type of research, and therefore an overall mistrust of any attempt to examine the actions of information security officers.

Case studies has therefore been another approach to examining the implementation and practice of risk assessment methodologies. Corland Gordon Keating(15) has done a case study on the use of OCTAVE allegro. Ladislav Beranek(16) did case studies with various small and medium organizations, where CRAMM and octave were considered, but risk assessment procedures based on FRAP and BITS methodology was developed and presented. Dorna Dehkhoda(6) developed a new method based on IRAM2 and cost-benefit analysis. Odd Busmundrud et al. (17) examined two approaches to risk, defined in respectively Norwegian standards NS 5814 and NS 5832. The methodology developed by NSM, is based on NS 5832.

In a paper by Keating(15), the challenges related to information security risk assessments in small-sized colleges and universities were addressed by using the OCTAVE Allegro risk assessment methodology. In the case study at a small-sized university it was observed that the complexity of many risk assessment methodologies required highly qualified and experienced security experts to be completed successfully. The conclusion was that it was relatively easy for the users to understand OCTAVE Allegro, and it provided the case organization with the ability to document the requirements, identify and evaluate their concerns, and prioritize the information system security measures.

Beranek(16) did a study where various risk assessment methodologies successfully applied by Czech small and medium enterprises were examined. It was observed that small and medium enterprises have a little or no IT personnel dedicated to information security and the budgets do not allow premium expenses for risk assessment methods. Previous experience with CRAMM and

OCTAVE methodologies were examined, and findings related to combining FRAP and BITS methodologies were presented.

In a study by Dehkhoda(6) the practical use of the risk assessment methodology IRAM2 in combination with cost-benefit-analysis(CBA) was examined. The purpose was to increase the level of knowledge on cost-benefit analysis within risk management that was observed in previous information security research. IRAM2 is known for being a holistic, practical and simple yet rigid risk assessment method, but as with many risk assessment methods, cost-benefit analysis was not included in this risk management method either.

By combining a Cost-Benefit-Analysis with the IRAM2 risk assessment method, the study examined whether this merge provides a more valuable result. CBA analysis could be implemented into any of the phases of risk management, dependent on the suitability of the CBA analysis results related to activities of the phase. Cost-effective and correct decisions require the organization to know the value of assets and the cost to protect them, and the risks of each asset. Dehkoda concluded that a combination of IRAM2 and CBA-analysis included all those aspects.

In a report by Busmundrud et al.(17) the objective was to examine the use of risk assessment methodologies in Forsvarsbygg, and compare the risk assessment approach based on the Norwegian Standard (NS) 5814: 2008 with the approach based on the standard NS 5832: 2014. The strengths and weaknesses of the two approaches where the definitions of risk respectively was an "the combination of likelihood and consequences of an unwanted event" and "the relationship between threats towards a given asset and this asset's vulnerability to the specified threat".

The report concludes that the approach based on NS 5814 where risk is defined as likelihood x consequences were easier to understand and to use than NS 5832 where risk is asset x threat x vulnerability, although this model defines risk more accurately, since it is not based on people's perception of likelihood, but the value, threat and vulnerability assessments. However, there is no agreed best practice, internationally or nationally, for security risk assessment.

In addition to case studies on various risk assessment methodologies, there are also several papers on the comparisons between different risk assessment methodologies, some of which present taxonomies on risk assessment methodologies. These papers examine the most relevant features of acknowledged risk assessment methodologies and contribute to the discussion of the usefulness of risk assessment.

In 2006 Enisa(18) presented their report "Inventory of risk assessment and risk management methods" where they presented a consolidated view of risk management and risk assessment. The purpose of the report was to increase the awareness of Risk Management activities in both public and private organizations, provide a common set of risk management terms to simplify communication between stakeholders, and examine the use of existing tools, methods and practices.

It was observed by that risk management procedures have been implemented, but risk assessments have not been adequately performed in some cases. Raising the awareness, the performance of risk assessments and providing good examples to facilitate the use of risk assessments became therefore Enisas objectives.

Enisa found that the comparability of methods and tools needed to be improved, by adding more characteristics and detailed properties. Combinations of methods which could fulfill organizational requirements should be identified and elaborate on combinations of methods that are suitable within a sector. Enisa should develop awareness material and demonstrators for using the methodologies, with examples on how to use the methods and tools. Continuity and emerging risks are important in information security risk management and should get more focus. Enisa should develop a software base of tools, methods and applications and performance of risk assessments to improve the hands-on competence at Enisa. Integration of Risk Management with other processes/disciplines should be exemplified to integrate Risk Management and Risk assessment to the operational processes of organizations.

In the report, ENISA presented an inventory of 13 Risk Management and Risk Assessment methods, which is accessible and updated on the Enisa website(19). Each method in the inventory has been described with 21 attributes that describe characteristics of a method. Enisa states that "Identification, analysis and evaluation" of the threats and vulnerabilities is crucial to understand and measure the consequences of the risks and implement appropriate measures to manage the risks.

A study by Stefan Fenz et al.(20) gave an overview of current risk management methodologies and compared their commonalities and differences based on 6 defined challenges decision-makers struggle with, and how risk management methodologies meet these challenges. These challenges were related to asset and countermeasure inventory identification, asset value assignment, risk prediction, the overconfidence effect, knowledge sharing and risk vs. cost trade-offs.

By evaluating the risk assessment methodologies by these challenges Fenz et al. observed that management should be able to compare opportunities, operational costs, and risks in different dimensions to make good decisions. To do this, Fenz observe the need for measurements that can estimate vulnerability mitigation when countermeasures are implemented, which includes factors capable of defining threats, collecting impact data and loss and can provide estimations on the mitigations of vulnerability.

The master thesis of Dan Ionita(21) examines the risk assessment methodologies and tools that are considered State-of-the-art, and compare them to find the "the key differences and commonalities" with the focus on scope, target users of the methods and intended stakeholders. Ionita's master thesis is a contribution to the TREsPASS project, where the purpose of the project is to improve the holistic view of information security by integrating technical, digital and social domains. To get insight into how these domains are connected in information security is crucial to identify potential weak points within an organization or infrastructure.

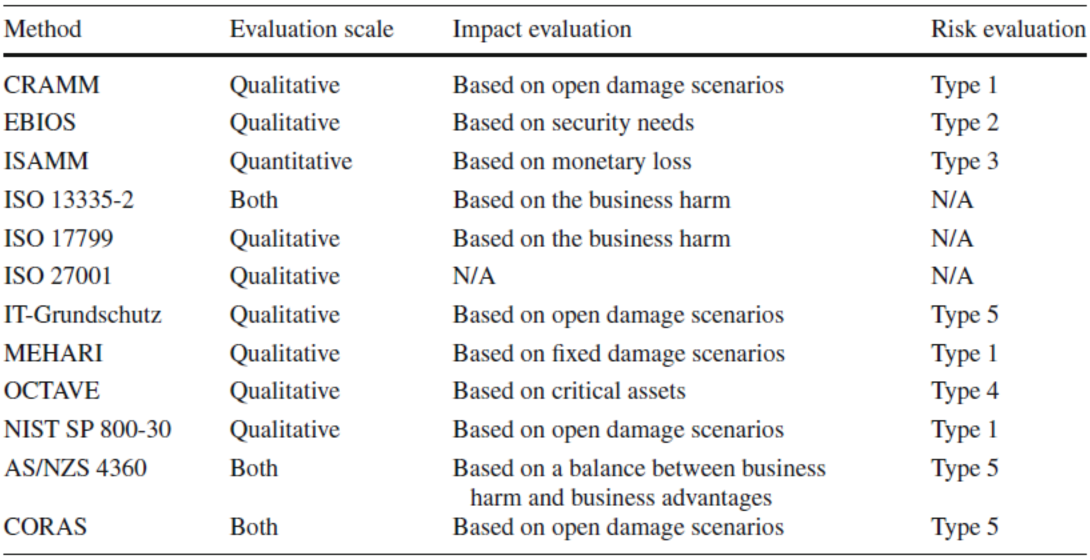
Ionita examined different concepts of risk presented in the frameworks, methodologies and tools evaluated in this study. How assets, vulnerabilities, threats, risk, impacts and measures are defined and implemented is a part of the concepts of the methodologies and make the basis for how they are measured, operationalized and processed to assess and evaluate risk. The contribution is a schematic presentation of the methodologies, how risk is defined, how many phases are included, which users and the level of skills are required and what organizations the methodologies are suitable for, to get an overview of functionalities to decide which tool, framework and methodology to use, to satisfy security requirements, and level with the skills and knowledge of the analysis team and financial considerations.

Ionita examined how risk assessment could be used to derive security requirements in the risk management process and identified three different relations between risk assessments and security requirements. Security requirements could be retrieved within the risk management process with asset values and threats, the risk related to compromise of security requirements could be evaluated by using risk assessments, or comparing defined security requirements to state of security controls by using gap analyses.

A study by Emmanuele Zambon et al.(22) presented a new model for qualitative assessment of availability risks, the qualitative time dependency (QualTD) model, as an alternative to general techniques like Fault Tree Analysis or Attack graphs that were considered too expensive or time consuming to be adopted in most risk assessments. The model visualized the propagation of availability incidents in an IT architecture and was supposed to be used with the initial phases in standard risk assessment methods.

Zambon found that it was possible to embed the model without requiring too much time or unavailable information, and defined factors to determine the usefulness of risk assessment, since Zambon found that the model delivered more accurate and intersubjective results, compared to other methodologies based on dependency graphs that required information that is unavailable or that required too much time to be extracted. The QualTD model was applied to a risk assessment method in one of the stages of the risk assessment process, however the definition of scope for risk assessment, business impact assessment, risk identification, risk evaluation and risk prioritization for availability risks could all be suitable for using the QualTD model.

Zambon developed a taxonomy of the most common risk assessment methodologies that was presented and discussed under which circumstances theQualTD model could be used in combination with them. Both the choice of risk assessment methodologies and the characteristics in this taxonomy was a basis for developing the survey and the discussion of the research questions.



Method	Evaluation scale	Impact evaluation	Risk evaluation
CRAMM	Qualitative	Based on open damage scenarios	Type 1
EBIOS	Qualitative	Based on security needs	Type 2
ISAMM	Quantitative	Based on monetary loss	Type 3
ISO 13335-2	Both	Based on the business harm	N/A
ISO 17799	Qualitative	Based on the business harm	N/A
ISO 27001	Qualitative	N/A	N/A
IT-Grundschutz	Qualitative	Based on open damage scenarios	Type 5
MEHARI	Qualitative	Based on fixed damage scenarios	Type 1
OCTAVE	Qualitative	Based on critical assets	Type 4
NIST SP 800-30	Qualitative	Based on open damage scenarios	Type 1
AS/NZS 4360	Both	Based on a balance between business harm and business advantages	Type 5
CORAS	Both	Based on open damage scenarios	Type 5

Figure 1 - Classification of Risk assessment methods(22)

In her doctoral thesis, Siv Houmb(23) examined an approach to help choose the best suited security solution based on relevant security, development, project and budget. The security solution decision support framework was called the Aspect-Oriented Risk Driven Development (AORDD) framework. In the 5th chapter, Houmb presents the methodologies AS/NZS 4360, and the methodologies CRAMM and CORAS. Houmb examined the way Australian/New Zealand Standard for Risk Management AS/NZS 4360:2004 a generic risk management framework, and elements from this standard was incorporated into ISO/IEC 27005. The difference between CORAS and the AS/NZS 4360 risk management process is that the CORAS risk management process is asset-driven and therefore the CORAS risk management process is extended by relevant activities for asset identification and valuation.

Houmb divides risk assessment methodologies into three types, rule based, risk based (probabilistic) and judgment based (expert judgment). Rule based risk assessment covers all approaches where the system is evaluated against a checklist or set of criteria based on guidelines given by standards. However probabilistic risk assessment focuses on identifying and assessing the probability of both known and unknown undesired risks. Houmb concluded that Cost benefit analysis method would focus on the investments organization should make to maximize gains and minimize risks and offers “a set of techniques for assessing the uncertainty of the judgments involved in assessing costs and benefits for each alternative architecture.”

Other papers presenting new taxonomies with the purpose of helping organizations choose the most suitable or useful risk assessment methodologies was reviewed to give an overview of other researchers' descriptions of various risk assessment methodologies. These articles took on a systematic approach to the characteristics of risk assessment methodologies, and in that context, they define what is considered useful in a risk assessment methodology, and they indicate what is considered to be the most used risk assessment methodologies.

In a study by Alireza Shameli-Sendi et al.(24) a taxonomy of security risk assessment based on 125 papers published from 1995 to May 2014 was presented, and what key features of risk assessment the information security management system should consist of was discussed.

Organizations of different size are having problems with selecting appropriate risk assessment methods. Although many risk-based approaches have been proposed, rapidly changing technologies and the attackers knowledge level increases the need for the process of considering and applying the important criteria in risk assessment because they are mostly based on the old taxonomy.

Shameli-sendi et al. conclude that organizations do not fulfill the risk assessment requirements because of the variety of methodologies and frameworks. The challenges caused by the lack of "Lack of attention to discussed questions in the risk assessment process causes many challenges: the number of non-critical resources, the effect of the threat could not be accurately calculated, the output of the risks is extremely close to each other and makes it hard to detect significant risks, and the evaluation of the risk is too imprecise, and this leads to a lack of proper risk management in the next step."

In a paper by Palaniappan Shamala(25) six risk assessment methodologies are compared and analyzed to suggests a conceptual "framework of info-structure" for information security risk assessment. These six methodologies were compared by the main features; developer, user group, risk assessment approach and risk model/phases. All methods required similar kind of information features, however, with some variation in form.

Shamala concluded that there a large variety of risk assessment methodologies, therefore organizations are reluctant to choose the most appropriate methods for them. Nevertheless, information security risk assessment is an important method to identify and prioritize information assets and to identify and monitor the specific threats to an organization, which in turn leads to concern and interest in information security.

In a paper by Nan Feng et al.(26) a security risk analysis model (SRAM) was proposed and a risk analysis model to visualize and identify the relationships between causes of risk factors was presented. This visualization technique could be helpful when analyzing the complexity and uncertainty of vulnerability propagation. In the SRAM, a Bayesian network was developed to define the causal relations between risk factors, based on the knowledge from observed cases and security experts.

Gaute Wangen et al. (27) evaluated risk assessment methodologies and proposed the Core Unified Risk Framework (CURF) as a complete approach to comparing information security risk assessment methodologies, where other methods compare the methods based on a predefined set of criteria. CURF is further developed by adding tasks and issues to the model from newly reviewed methods.

The criteria for being included in this taxonomy were that the methodology must have fifty citations in the academic literature, it must be industry best practice, include documentation of risk identification, estimation, and evaluation steps, the methodology must have been developed after 2002 and thus not older than 15 years at time of review and it must have been published in English or Norwegian.

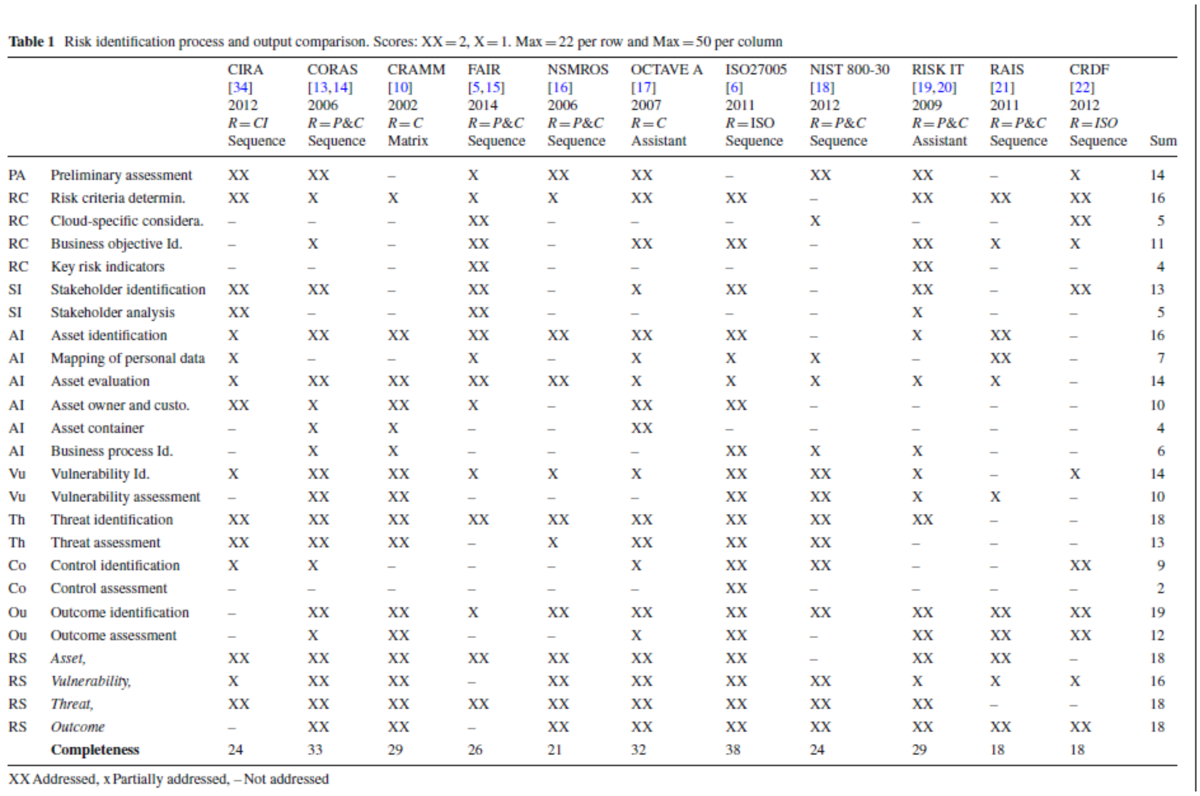


Table 1 Risk identification process and output comparison. Scores: XX = 2, X = 1. Max = 22 per row and Max = 50 per column

		CIRA [34] 2012 *R = CI* Sequence	CORAS [13,14] 2006 *R = P&C* Sequence	CRAMM [10] 2002 *R = C* Matrix	FAIR [5,15] 2014 *R = P&C* Sequence	NSMROS [16] 2006 *R = P&C* Sequence	OCTAVE A [17] 2007 *R = C* Assistant	ISO27005 [6] 2011 *R* = ISO Sequence	NIST 800-30 [18] 2012 *R = P&C* Sequence	RISK IT [19,20] 2009 *R = P&C* Assistant	RAIS [21] 2011 *R = P&C* Sequence	CRDF [22] 2012 *R = ISO* Sequence	Sum
PA	Preliminary assessment	XX	XX	–	X	XX	XX	–	XX	XX	–	X	14
RC	Risk criteria determin.	XX	X	X	X	X	XX	XX	–	XX	XX	XX	16
RC	Cloud-specific considera.	–	–	–	XX	–	–	–	X	–	–	XX	5
RC	Business objective Id.	–	X	–	XX	–	XX	XX	–	XX	X	X	11
RC	Key risk indicators	–	–	–	XX	–	–	–	–	XX	–	–	4
SI	Stakeholder identification	XX	XX	–	XX	–	X	XX	–	XX	–	XX	13
SI	Stakeholder analysis	XX	–	–	XX	–	–	–	–	X	–	–	5
AI	Asset identification	X	XX	XX	XX	XX	XX	XX	–	X	XX	–	16
AI	Mapping of personal data	X	–	–	X	–	X	X	X	–	XX	–	7
AI	Asset evaluation	X	XX	XX	XX	XX	X	X	X	X	X	–	14
AI	Asset owner and custo.	XX	X	XX	X	–	XX	XX	–	–	–	–	10
AI	Asset container	–	X	X	–	–	XX	–	–	–	–	–	4
AI	Business process Id.	–	X	X	–	–	–	XX	X	X	–	–	6
Vu	Vulnerability Id.	X	XX	XX	X	X	X	XX	XX	X	–	X	14
Vu	Vulnerability assessment	–	XX	XX	–	–	–	XX	XX	X	X	–	10
Th	Threat identification	XX	XX	XX	XX	XX	XX	XX	XX	XX	–	–	18
Th	Threat assessment	XX	XX	XX	–	X	XX	XX	XX	–	–	–	13
Co	Control identification	X	X	–	–	–	X	XX	XX	–	–	XX	9
Co	Control assessment	–	–	–	–	–	–	XX	–	–	–	–	2
Ou	Outcome identification	–	XX	XX	X	XX	XX	XX	XX	XX	XX	XX	19
Ou	Outcome assessment	–	X	XX	–	–	X	XX	–	XX	XX	XX	12
RS	*Asset,*	XX	XX	XX	XX	XX	XX	XX	–	XX	XX	–	18
RS	*Vulnerability,*	X	XX	XX	–	XX	XX	XX	XX	X	X	X	16
RS	*Threat,*	XX	XX	XX	XX	XX	XX	XX	XX	XX	–	–	18
RS	*Outcome*	–	XX	XX	–	XX	XX	XX	XX	XX	XX	XX	18
	Completeness	24	33	29	26	21	32	38	24	29	18	18	

XX Addressed, x Partially addressed, – Not addressed

Figure 2 - CURF taxonomy of risk assessment methodologies(28)

In this study, CURF has been the basis for developing the survey and presenting an overview of the risk assessment methodologies, however, the CURF could also be useful for risk managers making a choice of the appropriate risk assessment methodology, although it is admitted that understanding and utilizing the CURF taxonomy require a certain level of knowledge and experience.

3 Research methodology

There is a variety of research methodologies that could be suitable to examine the research questions in this thesis, and paper reviews, case studies, interviews and surveys are considered most relevant. These will be reviewed and discussed in the first part of these chapter. The second part of the chapter will discuss how to prepare for and perform the data collection by the chosen research methods, and the third part will discuss the reasonings and considerations to account for when analysing and discussing the results.

The discussion regarding choice of research methods is based on the papers reviewed in the previous chapter, where case study, document reviews and surveys were described. The papers are also basis for preparation for data collection, as the taxonomies presented in the papers give an overview of the methodologies and useful when forming questions for the data collection process, in addition to the experiences described in the study where a survey about risk assessments was attempted.

3.1 Planning the research

This part describes the process of planning which, how and when to use the research methods most suitable to answer the research questions in this study. The factors relevant when defining a target group for the research, the preferred level of competence and experience will be discussed in this part.

The research methods chosen in this study should fulfill the purpose to examine whether well acknowledged risk assessment methodologies are as well-known by the information security experts and risk managers as the scientific articles give an impression of and examine whether organizations perceive the risk assessment as useful. The research methods should provide the discovery of any success factors for doing risk assessments.

The methods should therefore involve data collection from practical use of risk assessments, and from those who have experience with conducting risk assessments in practice. The evaluation of this master thesis does however set other criteria. The data collected shall be accessible to the sensors and others to validate the analysis and discussion, and anonymizations shall be avoided as much as possible.

It could be possible to withhold sensitive organizational data from publishing, however, the reluctance in organizations to release information about risk assessment procedures, as documented by Kotulic(14), set some restrictions to choice of methods and the premises for data collection. The limitations related to resources is another factor, as this thesis is conducted by one person, over a year, as a part time study. This would imply that time-consuming and resource demanding research methods set limitations for data collection.

Document reviews is a common research method in other master thesis to compare and discuss the suitability of risk assessment methodologies in organizations. The results have often been presented as taxonomies of risk assessment methodologies, or new risk assessment procedures based on the researched methodologies. The document reviews, comparisons and taxonomies from related studies will also be used in this study, but as basis for further data collection, and discussions.

To study one or more cases where risk assessments are performed, routines and reports from the process are collected, in dept interviews are performed and observations are documented, could give extensive amounts of information about the risk management processes in a small number of organizations. Gerard Guthrie(29) defines Case studies as "the examination of one or, possibly, two or three particular cases in-depth and holistically" that could last for months or years. This would be a suitable method for answering the research questions related to the factors determining the choice of risk assessment methodology, and factors determining usefulness and success factors more that the degree of use of risk assessment methodologies and the degree of perceived usefulness.

To find organizations willing to participate in case studies where extensive amount of sensitive data about the vulnerabilities and assets in an organization and the risk management process could be difficult, and if any organizations was willing to participate, the case study would take up much of the organizations time and the data obtained would have to be accessible only to the sensors. Exclude information related to this master thesis from the public, would defeat the purpose of the thesis which is sharing knowledge about information security risk management.

In this study a new attempt at conducting a survey is made. Based on the experiences from Kotulic and Clark(14), the overview provided by the taxonomies presented in related work-chapter, and the criteria for data collection defined above, a survey is developed and distributed to risk managers and experts, and information security experts in Norway. The results will be compared and discussed based on to findings from reports and papers. This chapter will review the methodologies the research planning, implementing and analysis.

A survey is a quantitative research method, and Gerard Guthrie(29) describes survey as a method that is used for developing generalizations about populations. In this study the purpose is to collect data from as many participants as possible for analysing the results to answer the research questions statistically. The research questions in this study are mainly formulated to answer them with quantitative studies, however, they also require a deeper analysis of correlations between the research questions.

Defining the target group in this survey is important to ensure the level of difficulty of the questions are coherent with the level of competence and experience with the target group. To answer the research questions by doing a survey, the survey questions are at a relatively advanced level, and this could require a target group with risk assessment experience and competence. Questions about the usefulness of risk assessment in an organization, require the participant to have roles and responsibilities in the organization giving them sufficient understanding of the objectives of the organization.

This could make the target group small, and the risk of getting an insufficient sample size could be high. Reducing the level of difficulty in the survey could therefore be a way to increase the target group, and thus the sample size in the study. This could increase the surveys validity, but the chance of getting useable answers for the research questions could be reduced. The participants in this survey should therefore be a representative sample of risk managers and risk assessment participants in different types of organizations, small, medium size and large organizations, as well as both public organizations and private companies. This way the validity of the results could be increased.

An interview is a qualitative research method to examine the in-dept answers to the research questions by giving the subjects opportunity to answer the questions with their own words and elaborate on topics by using follow-up questions. In Guthrie's definition, the ustructured interview "generate qualitative data by raising issues in conversational form. The interviews can go in-depth into a topic and are appropriate for obtaining sensitive information." In this study, this would imply the reasons for choice of risk assessment methodology, the experiences with risk assessments and reasons for perceived usefulness and how usefulness is determined.

The subjects are mainly information security experts who had comments and questions about the survey and volunteered to participate as interview subject. In the article with the invitation to about the survey was contact information the participants could use if they had questions about the survey or the master study. Interview subjects in this study are risk assessment experts with experience and opinions on risk assessments and who volunteered to be interviewed about information security risk assessments.

3.2 Implementation of research methodologies

3.2.1 The survey on risk assessment methodologies

This survey was distributed to the members of National Business and industry Security Council (NSR). Norwegian business and industry security council (NSR) occasionally help doctorate- and master students in information security by distributing their surveys to their members. This contribution of endorsing the survey in an article on their website, distributing the article and survey in their weekly newsletter and on social media like LinkedIn and Facebook, ensure the survey reaching the target group of risk managers, information security experts and chief information security officers. The members of NSR are 310 private and public organizations and their newsletters are sent to ca 3000 recipients. NSR's group on Facebook had 2185 followers, and their group on LinkedIn had 1706 followers by 1. February.

This survey was primarily distributed by NSR newsletter, and the article with link to the survey was posted on their LinkedIn and Facebook group, to help increase participation after a week. This reminded newsletter-recipients and reached new relevant participants on social media. If these measures still were insufficient to increase the participation to at least over 30, other actions were planned as well.

The survey could be translated to English and distributed on several risk management and information security groups on LinkedIn. It was also considered to distribute an English version of the survey to several international organizations, addressing their risk management experts, chief information security officers and managers. However, this is suggested as an issue for further research.

Even if a survey has a clear and simple language, misinterpretations can happen and lead to lacking or wrong results. The analysis of the survey results must account for differences in the participants interpretations of the questions, and differences in understanding of the topic. However. Schaeffer(30) states in The science of asking questions that: "Seeing the questions in a self-administered form rather than hearing them read by an interviewer, to take another example, may mitigate the effects of question order or make it easier for respondents to use the full range of categories in rating scales" when examining different types of questionnaires.

To reduce misunderstanding and lower the bar for participating in this survey it will be developed and distributed in Norwegian, the language of most of the NRS-newsletter-recipients. The questions will be formulated with the members of NSR in mind, requiring some experience with risk management. There will therefore be used terminology and definitions known to information security officers.

The choice of survey tool for this survey was based on price, information security, previous experience and user-friendliness. Limesurvey, Questback, surveygismo and Nettskjema have been considered. Both Questback and Surveygismo have been used in previous projects at work, but the tool Nettskjema(31) was recommended by NTNU. This tool was provided by The University of Oslo, which NTNU had an agreement with, and has user-friendly functionality for radio-button-questions, dropdown-menu-questions and multiple answers-checkboxes were used. The radio button matrix was used for question about the level of experience with several risk assessment methodologies.

The first draft was made in Word, and here the structure of the survey was outlined, and the initial multiple-choice questions stated. These questions were then copied in to the first Nettskjema-draft, and the survey was developed further in Nettskjema. The second draft was tested on other information security consultants. Useful feedback on alternatives in the multiple choice questions, and suggestions on rephrasing of some of the questions made the basis for further development of the survey, where new questions were added and other questions rephrased as well. The third draft was reviewed by two of the information security consultants, before the final edition was ready for distribution by NSR.

The structure in the survey and the order and type of questions is important to make the participants answer the questions as honestly and accurate as possible. The survey consists of 3 parts. The first part consists of generic questions about the participants' age, experience and workplace, and questions about their workplace, the size of the organization and type of branch. The demographic questions are at a minimum to ensure the participants as much anonymity as possible.

The second part consists of questions about the participants experience with risk assessment, how many participants took part in the risk assessment, how long the risk assessment took, and the roles of the risk assessment participants, whether the risk assessment was useful or useless. and the last part consists of one page with questions about the participants experience with information security incidents and one page with questions about the usefulness of risk management.

The demographic questions in the survey is about the participants age, education, work experience and experience with information security activities. These are easy questions to get the participants started. They will say something about the relation between experience and the choice of risk assessment methodology and usefulness of risk assessment. Questions about the size of the organization and the type of branch the organization are compared to the findings from the Norwegian computer and data breach survey 2018(32) and Norwegian Crime and security survey 2019(33) and the do discuss relation between size and type of organization and use of risk assessments.

The second part of the survey consists of questions about the last risk assessment performed by the participants. How long time the risk assessment took, how many participants took part in the risk assessment and which roles they had were questions to compare with questions about usefulness and eventually what factors make the risk assessments not useful. Questions about risk acceptance and risk treatment will also be compared with the questions about usefulness, in addition to the questions about risk assessment methodologies.

In addition to the questions about the level of knowledge and experience with the ten well-acknowledged risk assessment methodologies, the participants are asked about terms and definitions on risk and likelihood and how they assess threat and use any risk assessment tools. These questions are compared to validate the responses and examine the relations between risk assessment methodologies and choice of usefulness.

The reference to NIST frameworks differs from the survey and the taxonomies, where the taxonomies reviewed in Related work-chapter refer to the risk assessment guideline NIST 800-30(34), and the survey refer to the risk management framework NIST 800-37(2). This framework has similar scope as the ISO 27005(4) other risk management frameworks. However, the possibility that the survey participants are unaware of the difference between these two NIST methodologies will be accounted for.

The questions regarding definitions of risk and likelihood have been developed based on the papers on comparisons of risk assessment methodologies, and studies of risk assessment methodologies including descriptions and analysis. The list of ten risk assessment methodologies in the multiple choice matrix are thus based on the taxonomies presented in the studies presented in Related work.

The last part of the survey consists of questions about the participants experience with information security incidents. Like the questions about risk treatment, these are questions that are basically out of scope, but they can amplify the importance of answers to the questions about the perceived usefulness and use of methodology, especially if they have experienced incidents and have perceived the risk assessment as useful. In that case, it is also useful to relate this to the last question on what success factors the participants consider most significant in regard to risk management.

3.2.2 The interviews

When the survey was distributed, some of the participants contacted the student with an offer to elaborate on the subject in a meeting or phone call. This offer of participating in an interview was taken, and interviews with 4 participants with several years of experience and knowledge related to risk management and information security was conducted. Three of the interviews were conducted on the phone, over 2-3 days, and one of the interviews were a meeting close to the participants workplace.

There were 4 questions prepared for the interviews, but the interviews had a free form, where the subjects spoke freely, and follow-up questions and elaborating questions were only asked to keep the subjects on topic. This gave the opportunity for the subjects to give insights on their experience that could not have been prepared for, but also the possibility that some questions were not covered.

The questions prepared for the interview were:

1. Which risk assessment methodology do you prefer, or base your risk assessment procedure on, and why?
2. In what way is the risk assessment useful for your organization?
3. Which success-criteria do risk assessment have to you?
4. Have you experienced any information security incidents?

3.3 Analysing the results

The results from the surveys was downloaded as an excel-file and a tab-separated text-file, and the results were analyzed in Excel. Single submissions could be viewed online, and all submissions could be viewed and downloaded in a web report. Part of testing the draft was testing different reports and how to conclude from the results.

All numbers in the report was imported as text-strings and was converted to numbers to be processed further in the data analysis tool for calculation of mean square error and Chronberg’s alpha. Some of the numbers were also replaced with the corresponding text-alternative in the survey, to be processed further in pivot-diagrams. The survey was in Norwegian, and the results were then translated to English before further processing in Excel, using the functionality of pivot-tables and diagrams.

Analyzing the answers on participants level of experience with risk assessment methodologies by comparing them to the answers on the use of terms and definitions of risk, threat, likelihood and the use of risk assessment tools was done to validate the answers on experience on risk assessment methodologies, and to reveal some experience on risk assessment by participants claiming they don’t know or use any of the mentioned risk assessment methodologies. Making an overview of terms and definitions used in risk assessment methodologies makes this comparison easier to do, and to explain the reasoning in the discussion afterwards. This overview is based on risk assessment taxonomies, case studies and descriptions of the methodologies by the institutes that developed them, as presented in related work.

	Use of terms and definitions in methodologies			
	Risk	**Likelihood**	**Threat**	**Tool**
Octave	Asset x Threat x Vulnerability x Consequence for the organization	Not relevant	We design threat scenarios based on the form in the risk assessment method	Filling out form on paper
CRAMM	Vulnerability x Threat x Asset	Threat agent's capacity x vulnerability	They are defined in the risk assessment system	Program/system on PC
NSM	Vulnerability x Threat x Asset	Not relevant	We design threat scenarios based on the form in the risk assessment method	Excel sheet
TRA	f(Value, Threat, Vulnerability)	Not relevant	We design threat scenarios based on the form in the risk assessment method	Program/system on PC
NIST 800-37	Likelihood x Impact	Number of events per year/month/week or Threat agent's	We design threat scenarios based on the form in the risk assessment method	Excel sheet

		capacity x vulnerability		
EBIOS	Likelihood x Impact	The system finds the likelihood	They are defined in the risk assessment system	Program/system on PC
Mehari	Likelihood x Impact	Number of events per year/month/week	We design threat scenarios based on the form in the risk assessment method	Filling out form on paper
COSO	Likelihood x Impact x Vulnerability x Speed of Onset	Number of events per year/month/week Percentage calculation	We design threat scenarios based on the form in the risk assessment method	Excel sheet
IRAM2	Likelihood x Impact	Likelihood of initiative x Strength of threat x Strength of Measure	We design threat scenarios based on the form in the risk assessment method	Program/system on PC
ISO/IEC 27005	Likelihood x Impact	Number of events per year/month/week	We design threat scenarios based on the form in the risk assessment method	Excel sheet

Table 1 - Overview of the use of terms and definitions in Risk Assessment methodologies

The responses from questions about the perception of usefulness, the factors determining usefulness and the success criteria was compared to the demographic questions, the questions about the risk experience, incident experience, responses, and questions about activities initiated after a risk assessment. This was used to validate the responses, and to give an indication to what the perceived level of usefulness was based on. The participants responses to the questions about the usefulness of risk assessment was compared to their experience with incidents, responses on actions taken in the aftermath of the risk assessment, in addition to the free text answers on how the risk assessment was perceived as useful.

To analyze and visualize the frequency of terms or keywords in large amounts of text, Angela Roe(35) proposes the use of a word cloud to introduce vocabulary, compare tests and summarize survey results. The use of word cloud has also been discussed by John D. Lee(36) as a visualization technique to highlight the important terms in a field of study. Lee compared word clouds to word networks and observed that word networks could offer more insights but were less accessible that word clouds.

In this study the tool Wordclouds.com(37) is used to visualize the responses in the free-text answers related to usefulness of risk assessments, so that the most frequent keywords can be analyzed and compared with the responses on factors to determine usefulness, and success criterias for risk assessments. In the discussion about to which degree risk assessment methodologies are in use, a visualization of frequency of representation for the risk assessment methodologies in taxonomies. The word cloud could be made manually, but to reduce the possibility of counting and copy-paste-errors, the wordclouds.com was used. The list of words generated in the word cloud tool was cleaned, so variants of the same word were merged, and the most insignificant words were removed.

The interviews were semi-structured, and the interview subjects talked freely, therefore the summaries from the four different interviews differ in structure and content, and how they cover the research questions. The interviews were summarized and translated to English shortly after the interviews had taken place, and excerpts from the summaries were placed in the relevant parts of the analysis-chapter.

All the interviews were conducted before the results from the survey was analysed, to avoid the results from the survey to influence the questions and answers from the subjects. One of the interview subjects volunteered to participate in the interview on the condition that the subject would be anonymous. This is respected, and therefore all the subjects interviewed for this study will be kept anonymous.

3.4 Evaluating the research methodologies

There is a possibility that risk assessment methodology is a topic that risk managers and security experts are reluctant to be participants in a survey, since the survey requires participants with risk and information security experience. Reluctance to reveal information about the organizations risk assessment routines and strategies could be a reason for not participating in the survey. The validity and reliability in this survey will therefore depend on the number of participants attending this survey.

Mohsen Tavakol and Reg Dennick (38) defines reliability as "The ability of an instrument to measure consistently" as opposed to validity as "the extent to which an instrument measures what it is intended to measure." In this case, the risk assessment survey will be this instrument. Tavakol and Dennick examine Cronbach's alpha as an index of reliability, where the value of alpha is increased when items in a test are correlated to each other. The length of the test could also influence Alpha, therefore a high alpha does not always indicate a high degree of internal consistency.

However, Tavakol and Dennick warned that incorrect use of Cronbach's alpha could cause cases where a test or scale was rejected, or the test was disapproved of for being insufficiently valid. Cortina(39) also stated that the "acceptance of a>.70 is adequate is implied by the fact that a>.70 usually goes uninterpreted. It is merely presented, and further scale modifications are seldom made" and warns that alpha should be interpreted with caution. Chronberg's alpha could however be useful to determine the sufficient sample size for a survey. In a study by Halil Yurdugul(40) on validity and the size of the sample is examined. It has been claimed in previous studies on sample size and validity, that the size of a sample should be over 500 or 300 for a study to be valid. Yurdugul claims that 30 participants could be sufficient in a survey, based on simulations on generated data with sample size 500, 300, 100, and 30 where Cronbach's alpha is calculated.

The survey was distributed to ca 3000 NSR newsletter recipients, 1500 LinkedIn-followers and 1800 Facebook-followers, and received only 40 answers. With the sample in this survey being as small as 40 people, the population is considered infinitely high. Based on the results from the questions related to knowledge and experience with risk assessment methodologies in this study the findings were that the Cronbach’s alpha was 0,62. The survey included a variety of other questions, therefore the Chronbachs alpha will not be emphasized in the assessment of validity.

The sample size calculator(41) by Creative research systems have been utilized to calculate and give an indication of the required sample size, and the confidence intervals. Calculating the margin of error will only give an indication validity of the survey, where the population in this survey will be the number of newsletter recipients and the sample size will give an indication of the required the number of participants in this survey(41). The calculations are based on the formula(42). This calculator indicates that with a population of 3000 and the confidence interval of 5, the required sample size should be 341. By this standard, the sample size of 40 was smaller than the sample size calculator required, but could still be useful as indications, as long as the numbers are considered to be just that.

Other methods to validate the results of surveys will therefore be used. In this survey similar questions will be asked in different contexts, to compare the answers before and after the main part of the survey. Asking control questions about the responses in the main questions will also be validation factors. Comparing the results from the survey with results from the Norwegian crime and security survey and the Norwegian computer and data breach survey is also a validation method, including demographic questions and questions about the frequency of risk assessments and observed incidents. However, with a low response rate in this survey, the results will be considered indications of the current state, and suggestions to further research will be to extend the survey to other countries and other professional environments.

Validity in interviews is based on the experience and knowledge the subjects have related to risk assessment. The interview subjects have higher education and several years of experience with risk management. Besides, as volunteers to these interviews they have clear opinions of the risk management practice in organizations.

The tone and mood of the conversation in the interview and how the subjects are able to speak freely about the topics is also a validation factor. For one of the subjects, this depended on the possibility to remain anonymous, given that the subject is a risk expert in a large essential public organization, therefore, all the subjects will remain anonymous in this thesis.

4 Analysis

In this chapter the research questions are answered by presenting and analysing the findings from the survey on risk assessment methodologies and interviews with four information security experts. The survey was distributed to ca 3000 NSR newsletter recipients, 1500 LinkedIn-followers and 1800 Facebook-followers, and received 40 responses. This is a small sample

The participants in the survey were mostly in their 40's and 50's, and while nearly half of them worked in government, the branches Communications/IT and Counselling was also well represented, and all the branches mentioned in the survey was represented. The participants were highly educated, with over half of them having a master's degree, and all of them had one or more years in university or vocational college. All of the participants had experience with risk assessment, and one or more years of experience with information security related work.

In this survey 45,0% of the participants were between 40-49, 27,5% of the participants were between 50-59 years old. 10,0 % of the participants were under 29 years old, 10,0 % were between 30-and 39 years old and 7,5% of the participants were above 60 years.

Public and private organizations are represented evenly in this survey with half of the participants working in public organizations and the other half in private organizations. However, 40% of all participants worked in government, while healthcare, education, transportation, industry and wellness/adventure each are represented with just 2,5% of the participants.

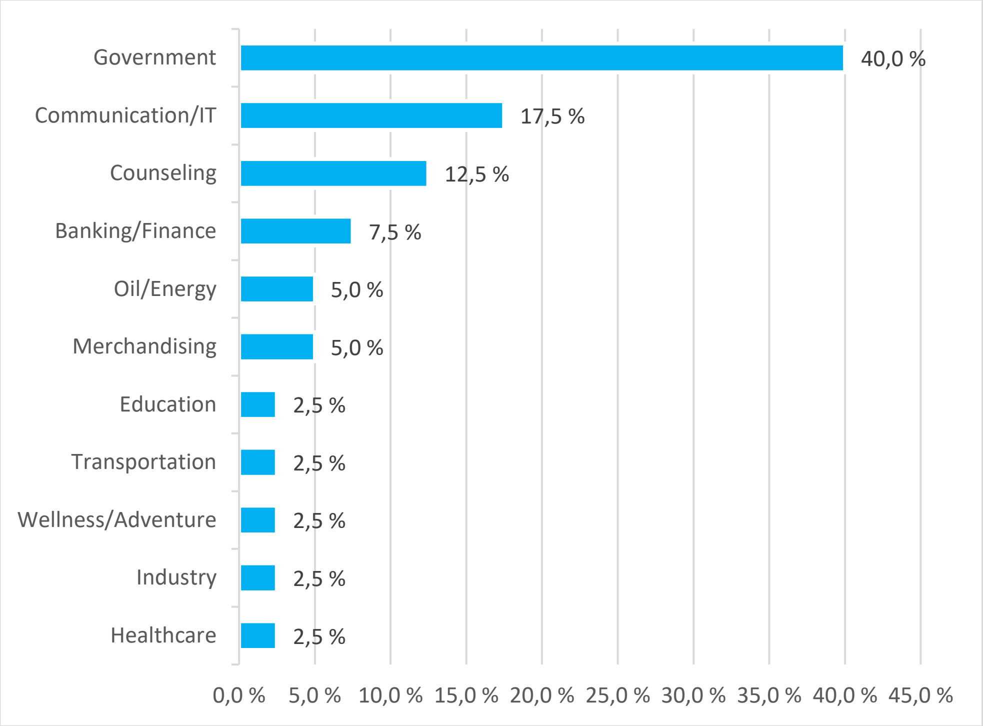
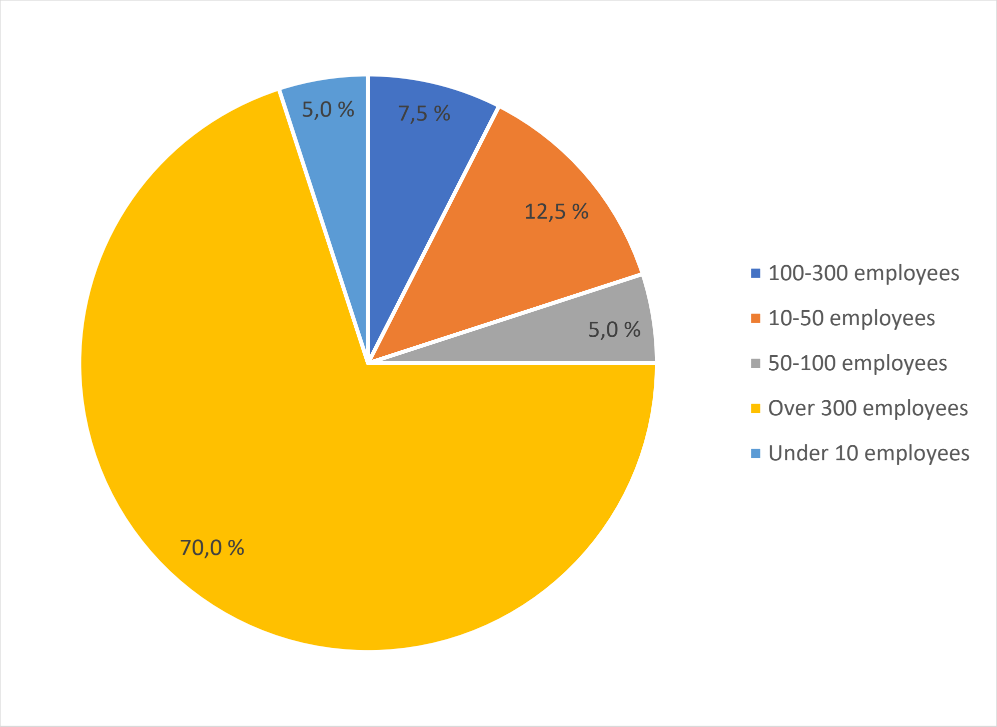


Figure 3 - Branches represented in the survey

The participants came mainly from large organizations. 70% of the participants were from organizations with over 300 employees, while 7,5% came from organizations with 100-300 employees. 17,5% of the participants, however, came from small organizations under 50%, whereas 5% were also under 10 employees.



The interview subjects were receivers of the newsletter from NSR, volunteering to contribute with their experience and opinions on the subjects as they had more knowledge to share than would be absorbed by a survey. They are all security experts and risk managers with 15-20 years of experience from both private and public organizations. They do risk assessments for their own organization, and one of the subjects do risk assessments in other private companies and public organizations.

The subjects:

- Subject 1 is an information security consultant in a counselling company. She has 15 years experience with risk assessments from both public and private organizations.
- Subject 2 is an advisor in a government organization. He has 20 years' experience from various companies as a consutant, and the last 5 years as a security advisor in a governmental organization.
- Subject 3 is a security manager in a government organization. He has 25 years' experience with security and risk assessments from the military and other government organizations.
- Subject 4 is an auditor and risk manager in car retail company. She has 15 years' experience with safety and security from both private companies and public organizations.

4.1 To what degree are well-established methodologies for risk assessment used by organizations?

To examine the spread and practical use of the ten often reviewed risk assessment methodologies, the survey included questions about the last risk assessment experience and the level of knowledge and experience with ten different methodologies. The participants use of the terms and concepts, what definition of risk the organization used, how likelihood was defined in the organization, and whether the organization used any tools when conducting the risk assessment. These results were used for validating the participants answers on risk assessment methodology experience against the known characteristics of methodologies, but also to determine whether participants actually use elements from known risk assessment methodologies without them being aware of it.

All the survey participants had done risk assessments no longer than 2 years ago, thus none had answered that they never had participated in a risk assessment. Over half of the participants, 57%, had done risk assessment the last month, and 27 % had done risk assessment the last year. Only 15 % of the participant had done risk assessments 1-2 years ago.

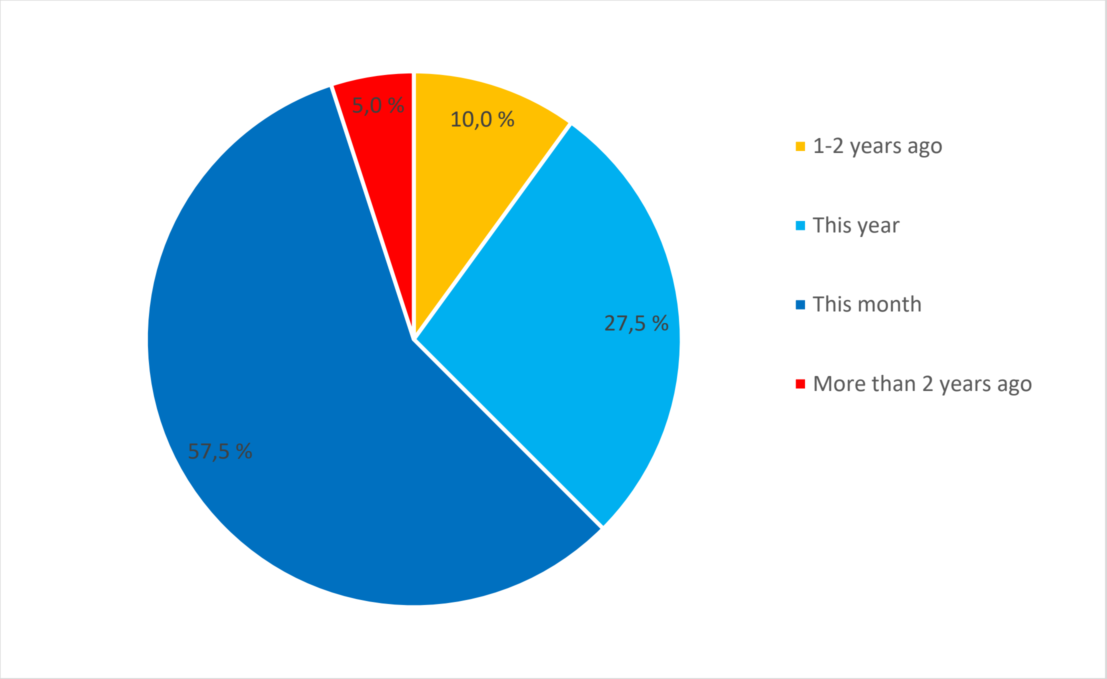


Figure 4 - When the participants last took part in risk assessment

The participants were asked about the knowledge and experience with the ten often reviewed risk assessment methodologies. None of participants were familiar with the methodologies OCTAVE, CRAMM, TRA, EBIOS and Mehari. Some of the participants had used or were using elements from Coso, Iram2, NIST 500-37, ISO/IEC 27005 and NSM risk assessment methodology. However, only three risk assessment methodologies were preferred by the participants, 22,5% participants preferred ISO/IEC 27005, the NSM developed methodology was preferred by 10% of the participants and 2,5% of the participants preferred NIST 500-37 and as their risk assessment methodology. This indicates that 33,5% preferred one or two of the methodologies, while 45,0% of the participants used elements from one or more of the methodologies in their own risk assessment procedure. However, of the 33,5% who prefer one method, 53,8% did also use elements from the other risk assessment methodologies. This means that preferring a risk assessment methodology before others, does not necessary imply that the risk assessment methodology is in use, as is.

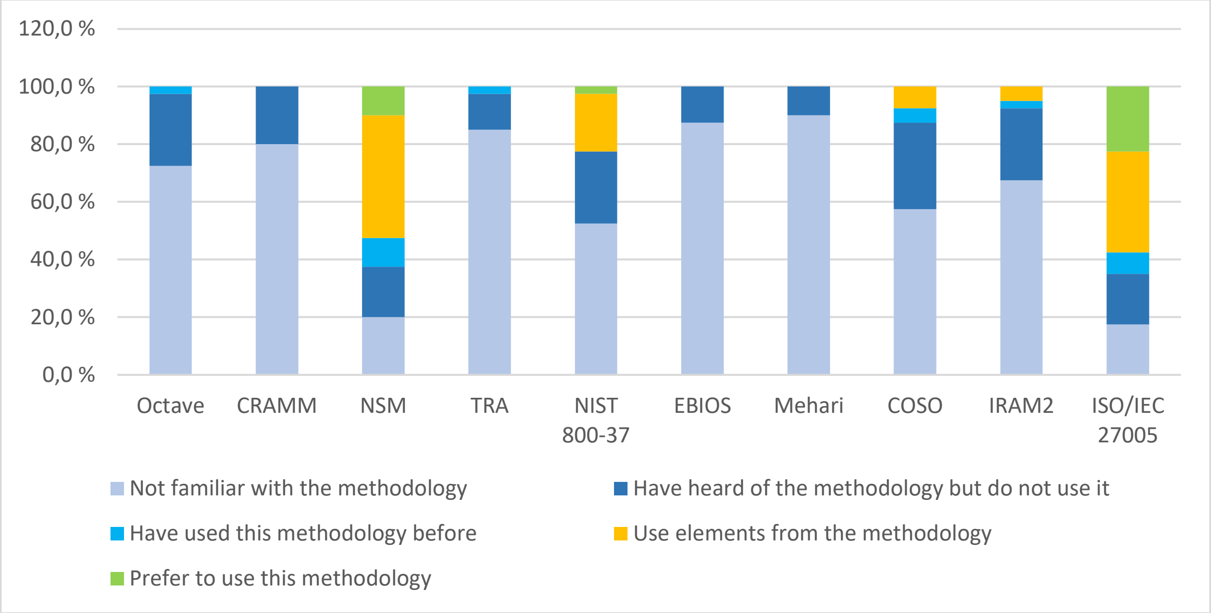


Figure 5 - The use of risk assessment methodologies

The definition of risk and likelihood and the assessment of threats are main characteristics of risk assessment methodologies. Therefore, the participants were asked what definition of risk and likelihood was used in the organization. They were also asked how threats were found in the organization, and which tools were used when doing risk assessment.

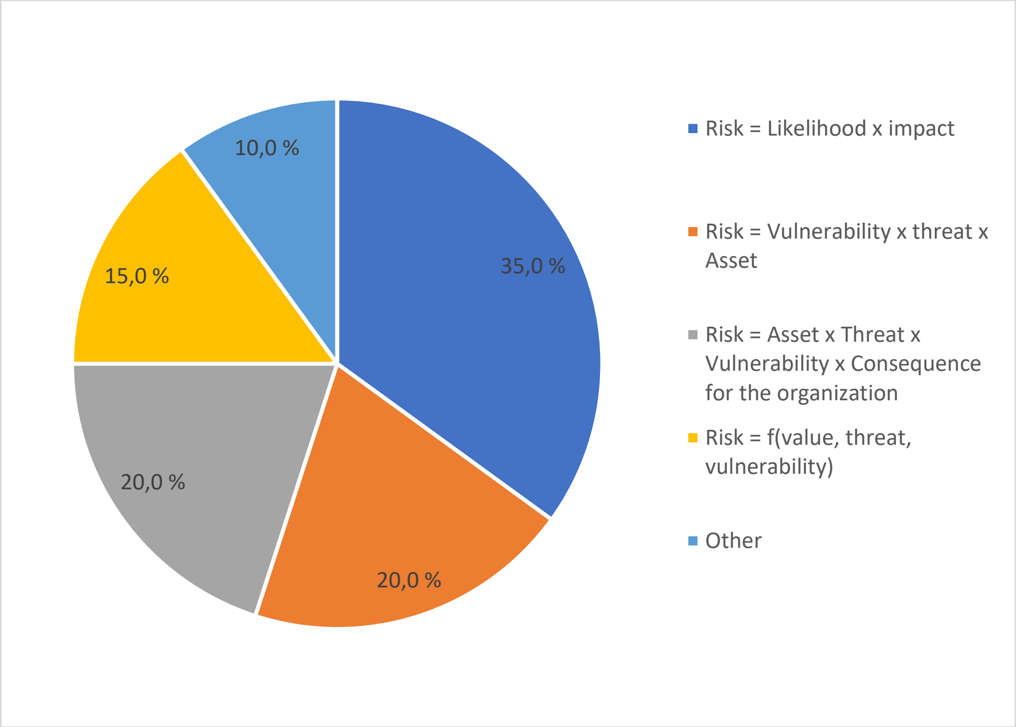


Figure 6 - Definition of risk

The definition of likelihood is characteristic for several risk assessment methodologies, but irrelevant to a few.

The threat assessment is characteristic for all methodologies, and a significant part of the processes described in the methodologies. The survey also gave the participants the option to give their own definition of likelihood.

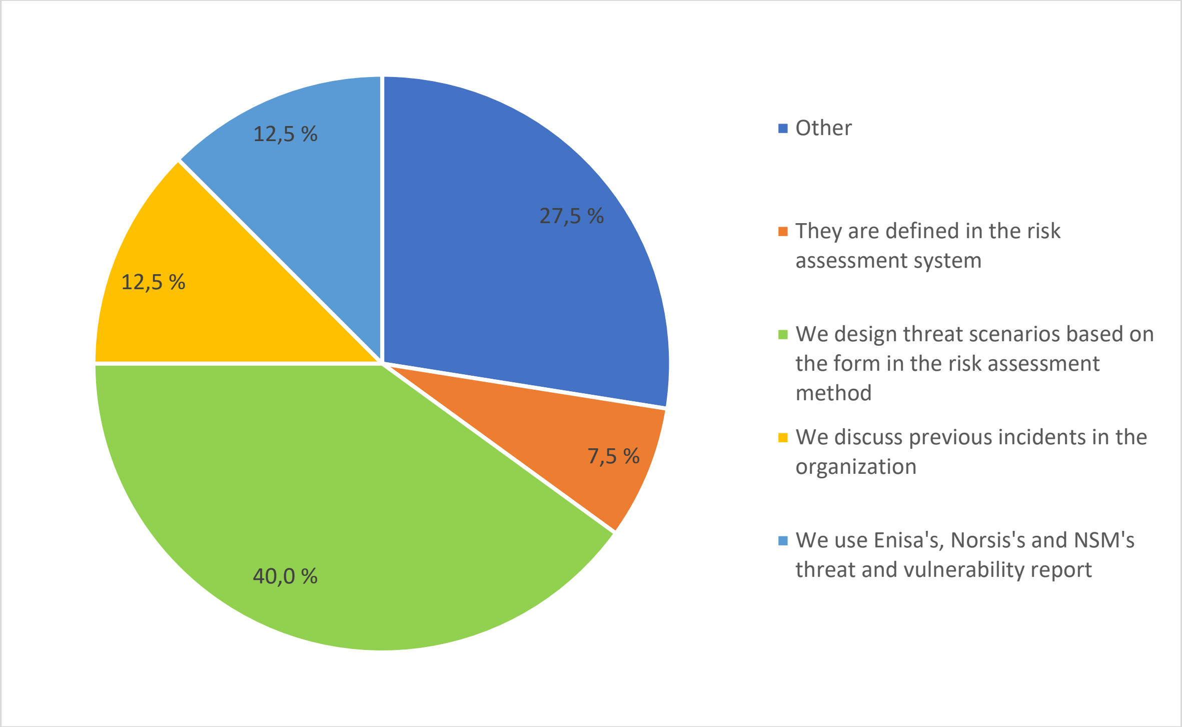


Figure 7 - Assessment of threats

5% of the participants were not familiar with any of the mentioned methodologies in this survey, and 12,5% of the participants had heard of the methodologies but not used any of them, and 5% of the participants had used one or more of the methodologies before. Their answers on risk and likelihood definitions and threat assessment indicates however that they do use elements from the methodologies mentioned. ISO/IEC 27005 defines risk as Likelihood x impact, and this is also how 4 of the participants define risk. 2 of the participants define risk as Assets x Vulnerability x Threat, this is also how risk is defined in the NSM methodology. One of the participants define risk as Assets x Vulnerability x Threat x impact for the organization, which could indicate that the participant use elements from COSO.

The relation between the participants level of experience with risk assessment methodologies and their definitions on risk and likelihood and threat assessment, have also been examined in the cases where participants answered that they prefer a methodology and the characteristics for that methodology. This applied to only two risk assessment methodologies, the NSM-developed methodology and ISO/IEC 27005.

In the NSM-developed methodology, preferred by 10% of the participants, risk is defined as Vulnerability x Threat x Asset. 5% of the participants who preferred this methodology answered that the organization defined risk this way, 2,5% of the participants preferring NSM methodology defined risk as Asset x Threat x

Vulnerability x Consequence for the organization, and 2,5% defined risk otherwise, that they “distinguish between natural and intended events and use a suitable model for this”. Likelihood is not relevant in NSM methodology, still, likelihood is defined as Threat agent's capacity x vulnerability by 5% of the participants who also prefer NSM methodology.

ISO/IEC 27005 defined risk as Likelihood x Consequence, and 22,5% of the participants prefer this methodology. However, 15,0% of the participants who preferred ISO/IEC 27005 used this definition of risk. 5% of the participants, however, defined risk as Vulnerability x threat x Asset, and 2,5% defined risk as f(value, threat, vulnerability).

The interview subjects were asked which risk assessment methodology they preferred and which methodologies the had experience with. Subject 1 preferred Iram2 and Difi methodology, a methodology based on information security management system standard ISO/IEC 27001, and customized for Norwegian public organizations. Subject 2 use the methodology developed by NSM, The Norwegian National Security Authority, a methodology described in the risk management handbook. Subject 3 used the standard NS 5832 on Societal security in previous , but developed a framework tailored to the organization, and which the NSM-methodology which the three-factor risk definition is based on. In his current workplace a customized risk assessment methodology based on this standard had to be simplified, and the element of likelihood had to be included for the methodology to be operationalized by the organization. Subject 4 has experience with HazOP and Good Manufacturing Practice (GMP) safety management systems, in addition to the security standard NS 5832 from previous workplaces. In current workplace the risk assessment methodology ISO/IEC 27005 is used.

Both the interviews and survey indicate that many of the acknowledged and often reviewed risk assessment methodologies are unknown or unused by most participants and subjects. However, ISO/IEC 27005, NSM-methodology and NIST 800-37 were the three risk assessments that were preferred by 35,0% of the participants and interview subjects. Elements from these three methodologies were used in participants own risk assessment procedures, as were elements from COSO and IRAM2.

4.2 Which factors determine the choice of risk assessment methodologies?

To choose a suitable risk assessment methodology for the organization, there are some factors that influence this choice. To examine possible factors, the interview subjects answers to why the particular risk assessment methodology was chosen were analyzed, and the survey participants response to questions about education, branch, work experience and information security work experience were combined with the responses regarding risk assessment methodology knowledge and experience in the analysis.

The participants were asked about their background, education and work experience. All the participants in the survey had higher education, whereas over half, 55%, of the participants had a master's degree or higher and over a quarter, 27% of the participants had a bachelor's degree. Comparing the education and the level of knowledge and experience with risk assessment methodologies show little connection between education and choice of methodology. The methodologies preferred by participants, NSM, NIST 800-37 and ISO 27001 had one-year programme in university, bachelor's or master's degree. The methodologies that are scarcely known amongst the participants as a whole are also scarcely known amongst the masters and bachelors. However, the participants with master's degree use elements from different methodologies more than bachelors and other participants.

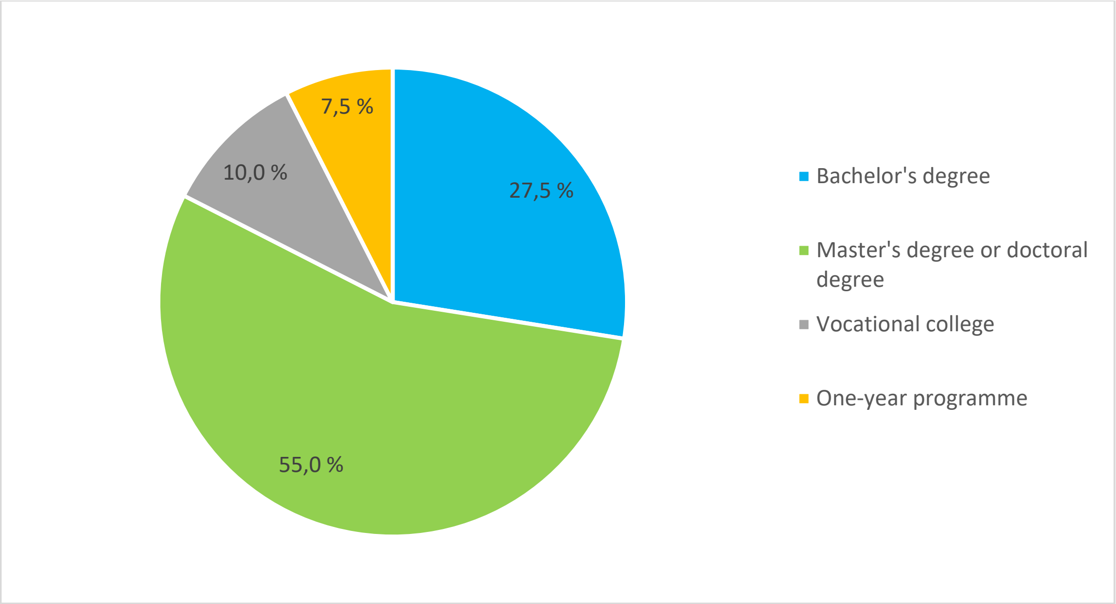


Figure 8 - Level of education

As requested, in the announcement of the survey in the NSR newsletters and on social media, all the participants had some experience with information security related work. 25,0% of the participants had over 30 years of work experience, however, only 5,0 % of the participants have over 30 years' experience with information security related work. 52,5% of the participants in this survey has 15-30 years' work experience, but 27,5% of the participants have 15-30 years' experience with information security related work. 40% of the participants have worked with information security for 6-15 years, while 27,5% of the participants in this survey has under 5 years' experience with information security work.

The participants who preferred the three risk assessment methodologies NSM, NIST 800-37 or ISO 27005 had work experience related to information security in the range from 1-6 years to over 30 years. There was neither a significant difference in experience where elements from the methodologies, or where the participants had heard of the methodology, have used the methodology or never heard of the methodology.

The participants represented all the types of types of branches in the survey, and there was a vague relation between type of branch and level of knowledge and experience with the preferred methodologies, NSM, NIST 800-37 and ISO 27005. 22,5% of participants from the government branch use elements from NSM-methodology in their own procedures, also participants from Communications/IT, banking/finance, counselling, healthcare, industry and oil/energy do this. However, NSM-methodology is the preferred risk assessment methodology for 10% of participants which from communication/IT, governance and transportation.

NIST 800-37 is preferred by 2,5% of the participants, and come from Communications/IT. However, 20% of the participants which comes from Banking/Finance, Communication/IT, Counseling, Government and Merchandising use elements from NIST 800-37 in their own risk assessments.

22,5% of the participants prefer ISO 27005 as their risk assessment methodology, and they come from Communication/IT, Counseling, Government, Healthcare and Oil/Energy. Communication/IT, Counseling and Government are also represented amongst participants who use ISO 27005 in their own risk assessment procedures, in addition to the branches Banking/Finance Industry, Merchandising.

The interview subjects who had experience with different workplaces and different types of organizations were asked what factors determined the choice of risk assessment methodology, and all the subjects answered that they used the methodology that were already implemented in the organization. All subjects have stated that the choice of risk assessment methodology is insignificant if one is used consequently.

Subject 1 preferred the IRAM2 methodology, but also said she was pragmatic in choice of methodology. The reason IRAM2 was chosen by the organization was the holistic focus in the methodology, but risk assessment on a new area created the need for less rigid, more easily adaptable risk assessment methodology, thus the methodology developed by Difi was implemented. Subject 2 experienced that small and medium-sized enterprises are not aware of the methods they use and how risk assessment should be utilized in the business. Risk assessment become a paper exercise not handled further by management. Subject 2 observed that a few large companies have good risk management routines, but even though top management in both large and medium size organizations are focused on risk they don’t know how to do it. In the risk assessment methodology subject 3 used at his previous workplace, the organization wanted to implement the likelihood into the risk assessment. Therefore, a new method was developed, where likelihood has also been included.

The factors that determined the choice of methodology was for both interview subjects and participants connected to the branch they were in, more than the participants education and previous experience. The risk assessment methodologies used by interview subjects were the same as the three risk assessment methodologies preferred by survey participants, NSM-methodology, NIST 800-37 and ISO 27005. However, both the interview subjects and survey participants with master's degree used elements from known methodologies when developing risk assessment procedures and standards. The risk assessment methodologies were unknown or unused by survey participants regardless of experience and education.

4.3 To what degree are risk assessments perceived as useful?

To what degree risk assessments are perceived as useful by risk assessment participants could be related to the participants awareness of the risk assessment process. Most of the participants perceived the risk assessment as useful or very useful but the next two parts will also analyze how the participants measure this usefulness, and which factors must be present for the risk assessment process is a success.

The participants were asked whether the last risk assessment they participated on was perceived as useful, very useful, a little useless or very useless and dependent on the answers, they were asked why they perceived the risk assessment as respectively useless or useful. Most of the participants found the last risk assessment useful or very useful, but there were 7,5% who found the last risk assessment not useful.

By comparing the participants answer about usefulness with their answers on the further processing of the risk assessments, the answers on usefulness could be validated in the way that participants who had experienced an incident and perceived the risk assessment as useful could be more significant than the participants who had not exoerienced any incidents.

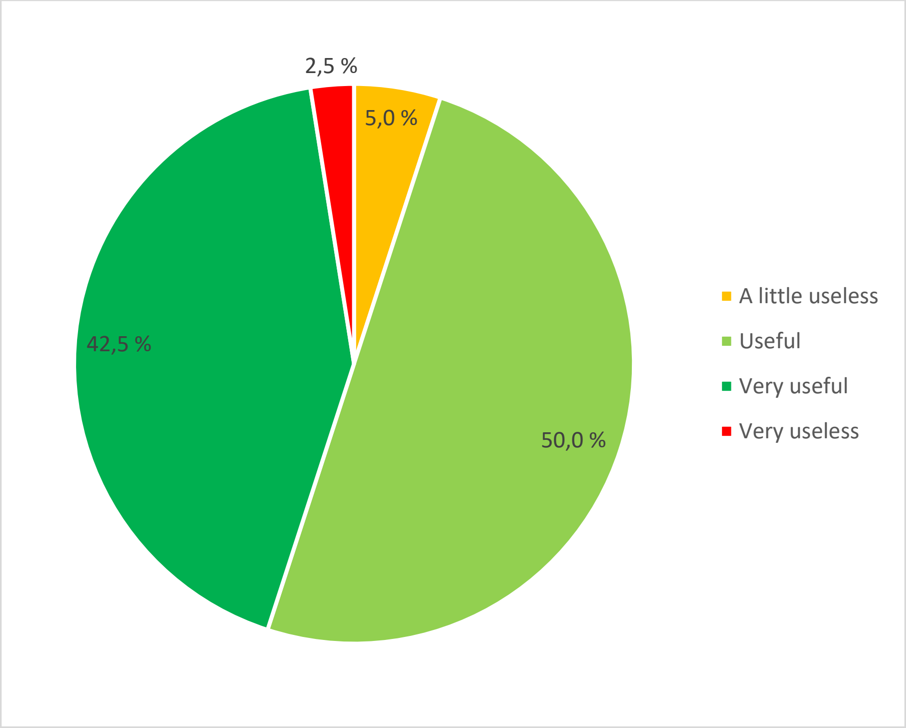


Figure 9 - The level of usefulness in risk assessments

The participants were asked whether the they had any experience with information security incidents, and in that case how severe the incident was. 65% of the participants had experienced information security incidents, while 15,0% of them did not know if they had experienced any incidents. Of the 92,5% participants who had found the risk assessment useful or very useful, 62,2% had experienced information security incidents. However, 16,2% of the participants did not know if they had experienced an incident. All of those 7,5% who found the risk assessment not useful, had experienced information security incidents.

61,5% of the participants who had experienced an incident had done risk assessment the previous month, while 23,1% had done a risk assessment the previous year. However, 20,6% of the participants who had done risk assessment the same year, including those who had done risk assessment the same month, had not experienced any information security incidents.

Risk assessments are mainly perceived as useful, even for those participants who have experienced information security incidents. However, over a quarter of the participants experienced that the risk assessments were not further processed, while under half of the participants perceived that a proposed actionplan had been introduced, which was the purpose of a risk assessment, according to ISO/IEC 27000.

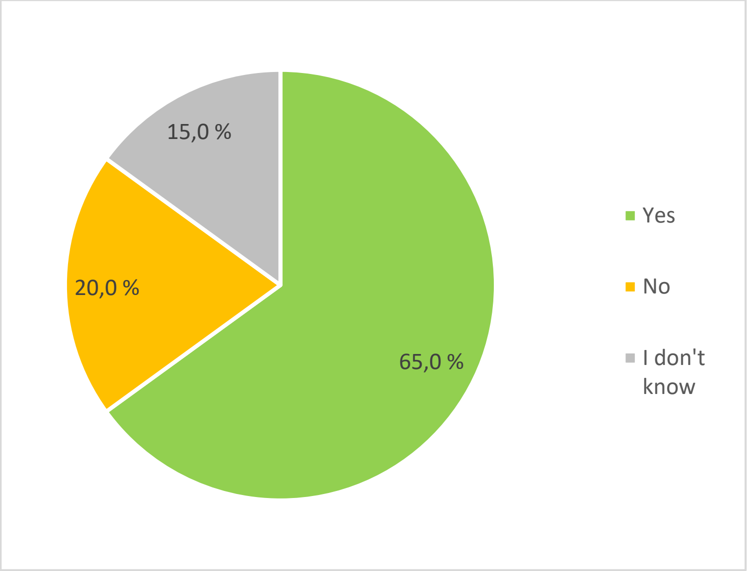


Figure 10 - Experience with information security incidents

Of those who answered that they had experienced an information security incident, equal parts characterized the incident as severe and not so serious, and 4% responded that the incident was completely insignificant. Of those who characterized the security incident as severe, 12,0% had responded that the latest risk assessment was useless or very useless.

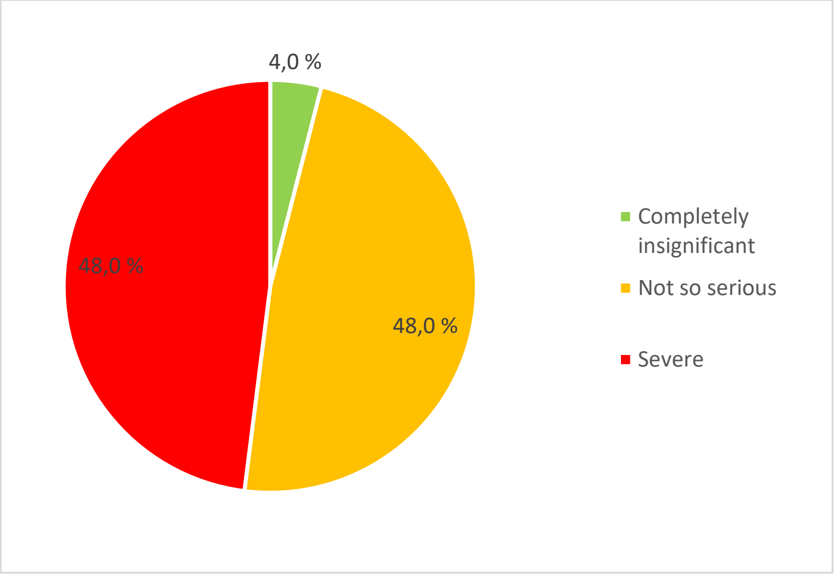


Figure 11 - Severity of incidents

In addition to the level of severity, the participants were asked about which types of consequences the information security incidents had, and the participants were allowed to give multiple answers. Loss of income and working hours, the inaccessibility of network central systems and loss of confidential information were the most responded consequences. Loss of reputation and encrypted or lost data were also on the top five list of consequences.

Of all those who had loss of confidential information, 33,3% considered this severe consequence, but also experienced the last risk assessment as useless or very useless. 44,4% of those who experienced a useful risk assessment considered the loss of confidential information not so serious. However, those participants who experienced very useful and very useless risk assessments, 11,1% oconsidered loss of confidential information severe.

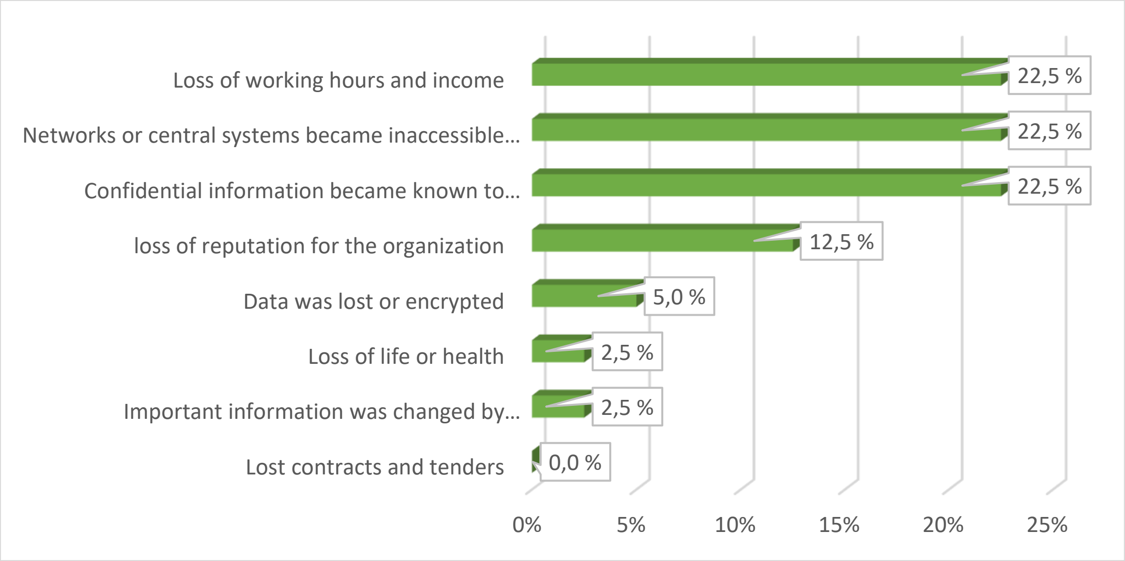


Figure 12 - Types of consequences

The participants who had experienced an information security incident were asked how well prepared they were for the incidents, and over half of the participants answered that they were very well or well prepared for the information security incident they experienced.

All 48,0% who answered that they were very well prepared had also answered that the last risk assessment was useful or very useful. However, those who said they were unprepared for an incident did also answer that the last risk assessment was useful. The 8,0% participants who were very unprepared for an incident did also answer that the last risk assessment was useless.

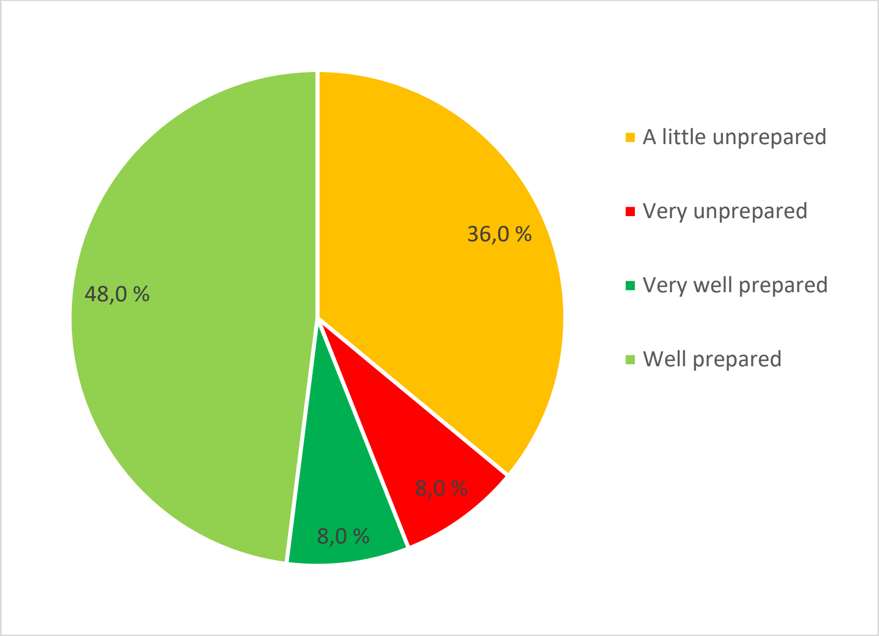


Figure 13 - Preparedness for incidents

All the interview subjects have stated that the risk assessment they have participated in can be useful, however, subject 1 also observe that risk assessments often are done due to legal requirements, and that organizations are not concerned about the answer risk assessments give. Subject 2 observe that risk assessments are mainly performed in relation to outsourcing of service functions, and rarely during the systems lifecycle. Subject 3 wrote in an email before the interview where he stated that "Risk assessment is an integral part of business management. If the business is not oriented towards this, a risk analysis is likely to have limited value and at the same time be wasted effort."

Both interview subjects and most of the survey participants perceived the risk assessments as useful, but further treatment of the results from risk assessments and the incident experience indicated that the perceived usefulness of risk assessment should not be the only indicator of usefulness.

4.4 Which factors determine the usefullness of risk assessments?

Most of the participants perceived the risk assessment as useful, however they have different opinions to what a useful risk assessment is, and how it can be measured. The level of perceived usefulness in comparison with questions related to the organization's further treatment of risk assessments, could indicate the level of risk awareness in the organization.

The survey participants who responded that the last risk assessment was useful or very useful, were also asked "In what way did you find the risk assessment useful?" where they could answer in their own words. The responses were processed in Wordclouds.com and visualized in the figure below where the most frequent words have the largest font size. The most insignificant words have been removed, and variants of the same word have been merged.

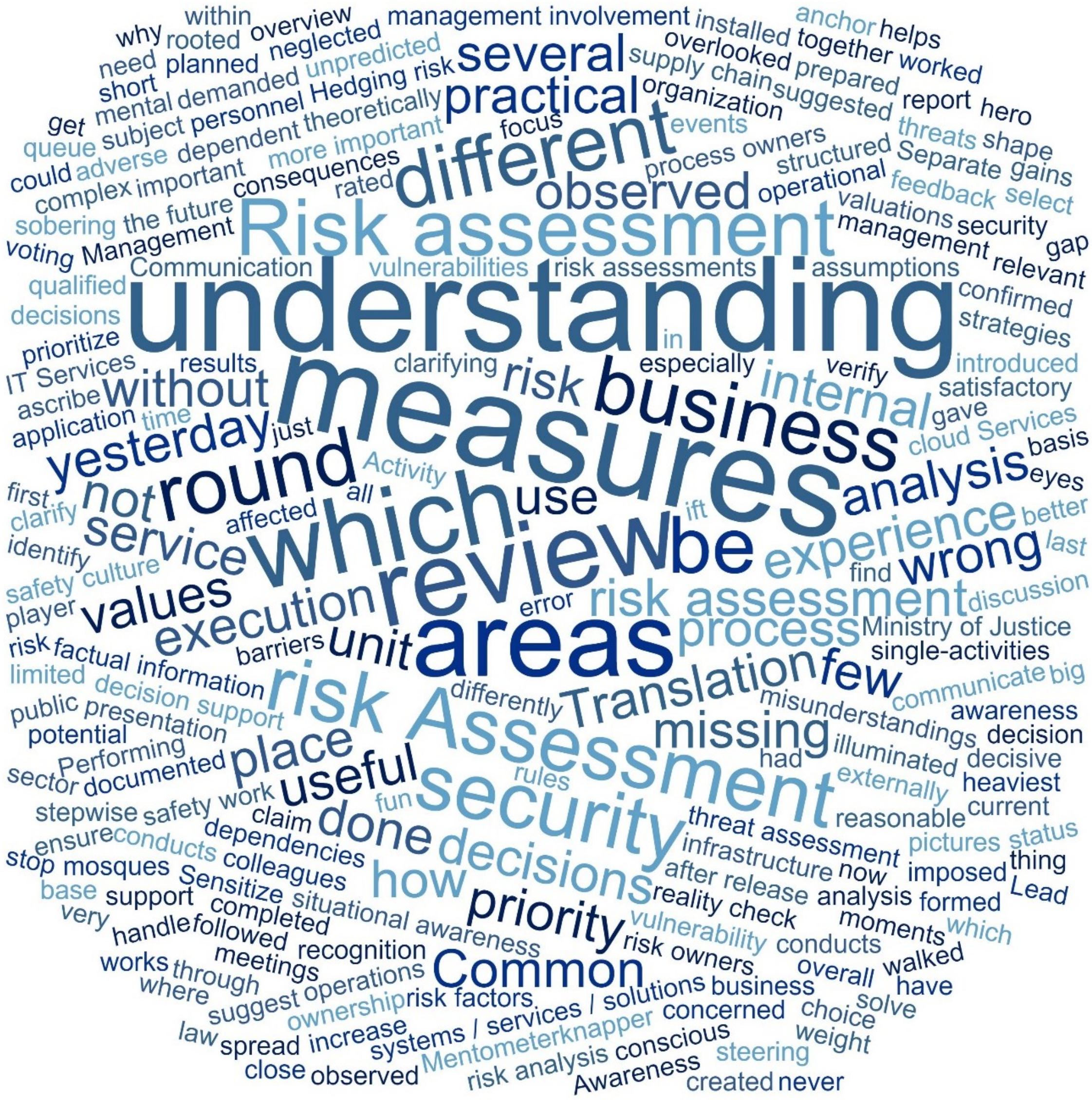


Figure 14 – How participants describe usefulness

The most frequent answers about the usefulness of risk assessments were related to increased awareness and understanding of risks, that it gave a better basis for decisions, the involvement of management and compliance with internal requirements. Some of the participants also answered that a structured process provided overview, and that risk assessments are a clarifying process.

The question about perceived usefulness of risk assessments came early in the survey and awareness, however, the participants were asked about the greatest benefit of doing risk assessments as one of the final questions. 45,0% of the participants responded that the greatest benefit of doing risk assessment was that they take action to avoid incidents or limit the impact, while 37,5% of the participants responded that they raised the awareness of information security and 7,5% of the participants do exercises on relevant events.

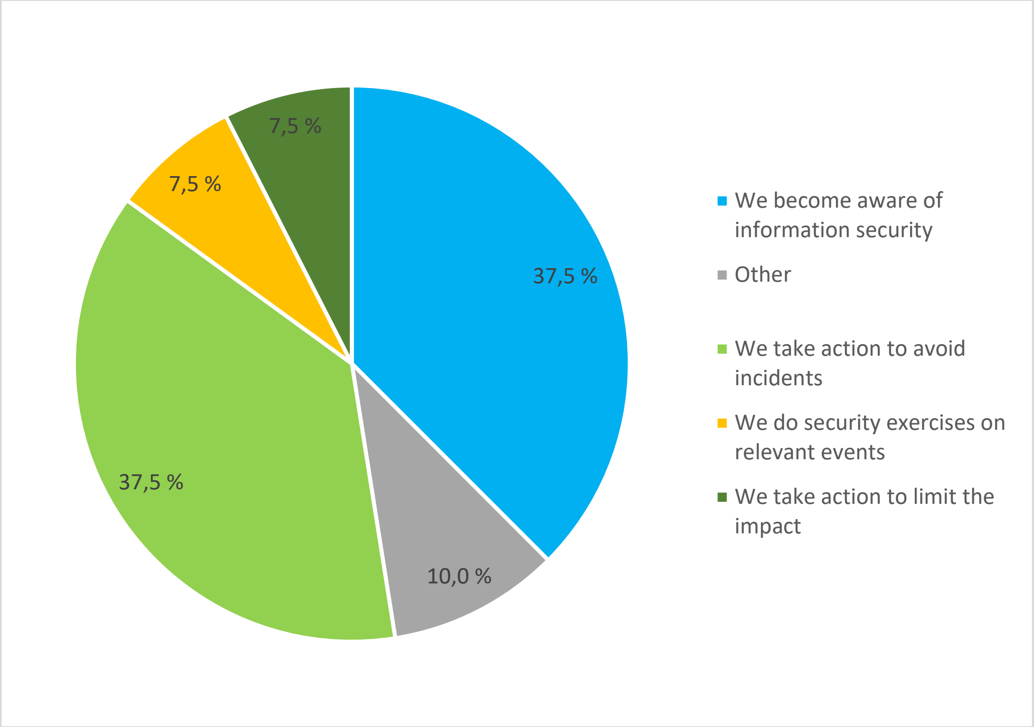


Figure 15 - The greatest benefit of doing risk assessments

None of the participants chose the alternative answer that the greatest benefit was to cut costs for unnecessary measures or to act in accordance with the legislation. However, 10,0% of the participants formulated their own answers. The answers was "Provides a decision-making process so that good decisions can be made in relation to trade-offs between security and other considerations", "To have a basis for prioritizing measures (cost / benefit), as well as giving an overview of residual risk" and "We make sure that the company can fulfill its mission", while one answer was that several of the alternatives were relevant.

The participants were asked what happened further with the risk assessment reports, and the participants could choose more than one alternative. 27,5% of the participants answered that the risk assessments were not further processed, however an action plan had been introduced in risk assessments done by 42,5% of the participants, management had approved the risk assessments for 40% of the participants, and the report was the starting point for a security exercise for 7,5% of the participants. 15% of the participants had both the managements approval and introduced an action plan, and 2,5% of the participants had a security exercise based on the risk assessment as well.

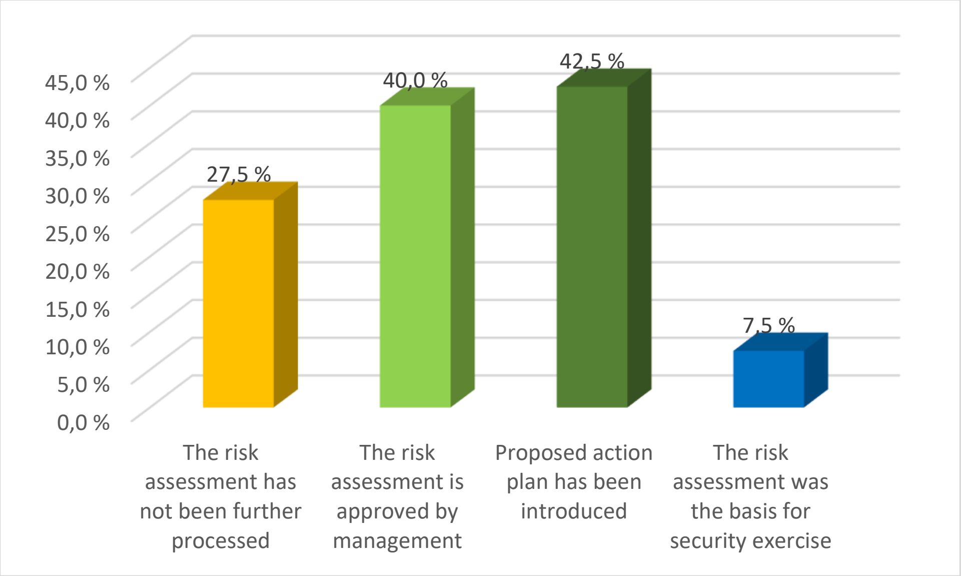


Figure 16 - Processing of risk assessment

Of all those who had introduced a proposed action plan, 41,2% responded that the greatest benefit of risk assessment was to avoid incidents or reduce impact, however, increasing awareness of information security was the greatest benefit for 47,1%, while 5,9% do security exercises on relevant events. Of those who used the risk assessment report as basis for security exercise 33,3% also responded that doing security exercise on relevant events was the greatest benefit of risk assessment.

The perceived usefulness compared with the knowledge of the various risk assessment methodologies, when 92,5% of all participants perceived the risk assessment as useful or very useful indicated no relation between methodology and usefulness.

Comparing the experience and knowledge of the methodology with processing of risk assessments and which factors determine the usefulness, of those who take action to avoid incidents or limit the impact, 33,3% use elements from NSM and 5,6% prefer this methodology, 22,2% use elements from NIST 800-37 and 5,6% prefer this methodology, 27,8% use elements from ISO/IEC 27005 and 22,2% prefer this methodology while 5,6% use elements from COSO and 5,6% use elements from IRAM2. This indicate a somewhat weak relation between participants who prefer a risk management methodology or use elements from one and also define actions to avoid incidents or limit the impact as factors that determine usefulness.

When the interview subjects were asked how useful they experienced risk assessments, they answered that this depended on whether management was involved in the process, that the proposed measures were implemented, and that in the risk assessment participants represented different parts of the organization.

Subject 1 observed that Risk assessment often was done without the planning and implementation of measures and controls afterwards. She stated that managers in Norway do not realize that they are responsible for the residual risk. Therefore, managers must take the effort to read risk assessment reports and security reports and focus on security needs to reach top management. Risk assessments are important and require action.

Subject 2 observed that both large and small organizations lack expertise and resources. Companies do mainly desktop exercises where there is no interaction between the risk assessment participants and the IT technicians. Subject 2 proposed to do risk assessment at the right level, participants must have ICT competence, and knowledge of the area to be risk assessed.

Subject 3 observed the same as Subject 1, when a thorough organizational risk assessment was carried out in 2010, the result was a long document that was not read by the organization. In 2018, a new organizational risk assessment was conducted, and all departments throughout the organization participated in the value assessment. The initial involvement from all departments lead to increased interest in the results of the risk assessment.

Involvement from the organization is also a factor according to Subject 4. She states that risk assessment is a process of people in which there must be room for trust and dialogue. It is important to involve expertise on all areas to ensure risk management, control management and supplier management is sufficient. All participants must understand the process from risk assessment to implementing measures.

Findings from the survey and the interviews indicate that actions taken to limit the impact or avoid the incidents, increased awareness regarding information security and approvement from management are the main factors that could determine the level of usefulness. The findings from interviews also indicate that management being aware of their responsibility for the residue risk and risk management are factors that could determine the usefulness, however involvement from the whole organization is both a factor to determine usefulness and a success criteria for risk assessment.

4.5 Have organizations defined any success criterias for risk assessments?

The questions about success criteria for risk assessments can give an indication of common success criteria for doing risk assessments, regardless of methodology when comparing the responses to responses related to perceived usefulness, experiences with risk assessments and incidents, responses related to choice of methodology and terms and definitions related to risk and responses related incidents in combination with responses from the questions about success criterions for risk assessments.

The survey participants were asked think is the most important success criteria for risk assessments. The participants were asked to choose the 3 most important success factors from a list, and "That the proposed measures are followed up", "That we use a good risk assessment methodology" and "That the manager participates in the risk assessment" are what the participants responed most. That some of the participants have experience with risk assessments, and that the participants are familiar with the threat image is also important success factors for the participants.

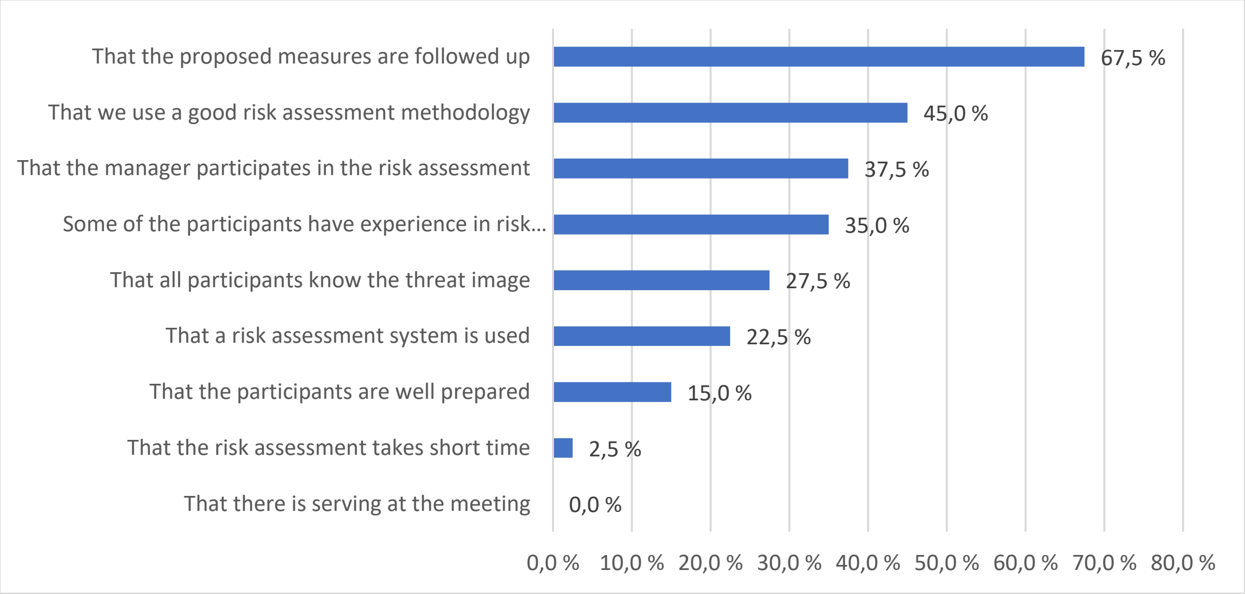


Figure 17 - Success criteria of risk assessments

Of the 67,5% participants who responded that the proposed measures are followed up as a success criterion, 40,7% had also answered that the proposed action plan has been implemented, while 29,6% of the participants had answered that the last risk assessment has not been processed further. However, 11,1% of the participants found the risk assessment useless or totally useless. This would indicate that the participants expect a follow up of the risk assessment to be useful. Although some participants observed that the risk assessments had not been followed up, they mainly perceive the risk assessments to be useful nevertheless.

Using a good risk assessment methodology, was a success criterion for 45,0% of the participants. While 16,7% of the participants preferred ISO/IEC 27005, 44,4% of the participants based their risk assessment procedures on elements from NSM-methodology, 27,8% use elements from ISO/IEC 27005, 22,2% use elements from NIST, 5,6% use elements from respectively COSO, and IRAM2. This could indicate that although a good risk assessment methodology is a success criterion, the participants mainly utilize elements from the well-known methodologies to develop their own risk assessment procedures.

That the management is present in the risk assessment was a success criterion for 37,5% of the participants, and of these were 26,7% managers themselves.

46,7% of the participants had the manager present as a participant in the risk assessment. However, of all the participants who answered that the manager took part in the risk assessment, only 29,1% answered that this was a success criterion for risk assessment. This could indicate that management involvement and follow-up not necessarily imply taking part in the risk assessment personally.

27,5% of the participants responded that "The participants are familiar with the threat image" is a success criterion. 72,7% of these participants define Risk as *Asset x Threat x Vulnerability x Consequence* or *Asset x Threat x Vulnerability*. 54,5% of the participants design threat scenarios based on the form in the risk assessment method or use the threat scenarios defined in the risk assessment system, while 18,2% of the participants base threat scenarios on incidents in the organization and 9,1% based the threat assessment on Enisa's, Norsis's and NSM's threat and vulnerability report. 18,2% of the participants responded that they base their threat assessment on another source.

Findings when comparing the number of participants with the perceived usefulness could indicate a relation between participants and perceived usefulness and determine if number of participants is a success factor. However, of all the participants who found the risk assessment useful or very useful, 67,6% were 3-6 participants, while 18,9% were 6-10 participants and 13,5% were under 3 participants. These numbers are similar to the number of participants in general, and this could indicate that number of participants is not a particular success factor based on the survey findings.

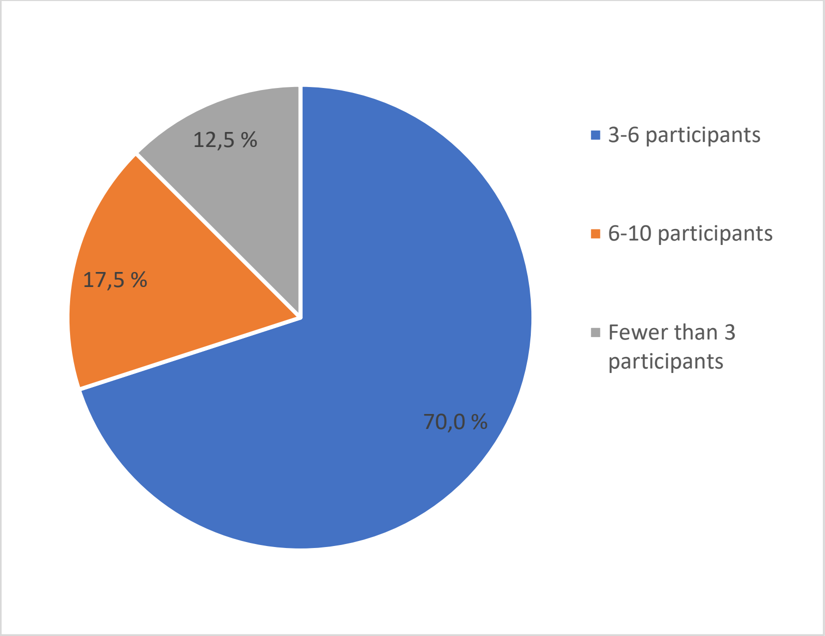


Figure 18 - Number of participants in risk assessment

Of the 35% participants who responded that "having a participant with experience with risk assessment" was a success criterion, as many as 92,9 % have experience with risk assessments themselves. Half of the participants have 6-15 years of experience with information security, while 14,3% have only 1-5 years information security experience.

The survey participants were mainly risk experts or security experts, but 17,5 % of the participants were managers. Other roles were also present in risk assessments, and 36,9% of the participants responded that managers were present at the risk assessments.

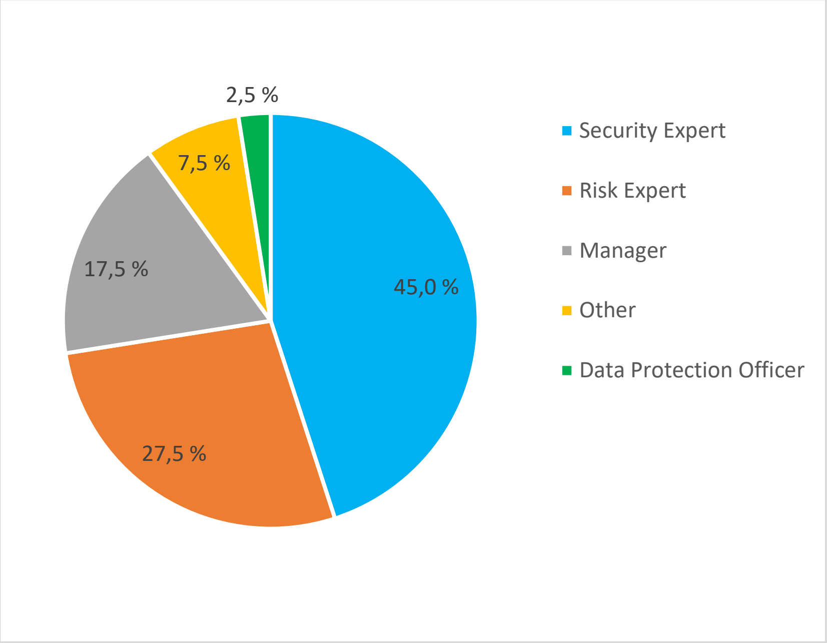


Figure 19 – The survey participants role in risk assessment

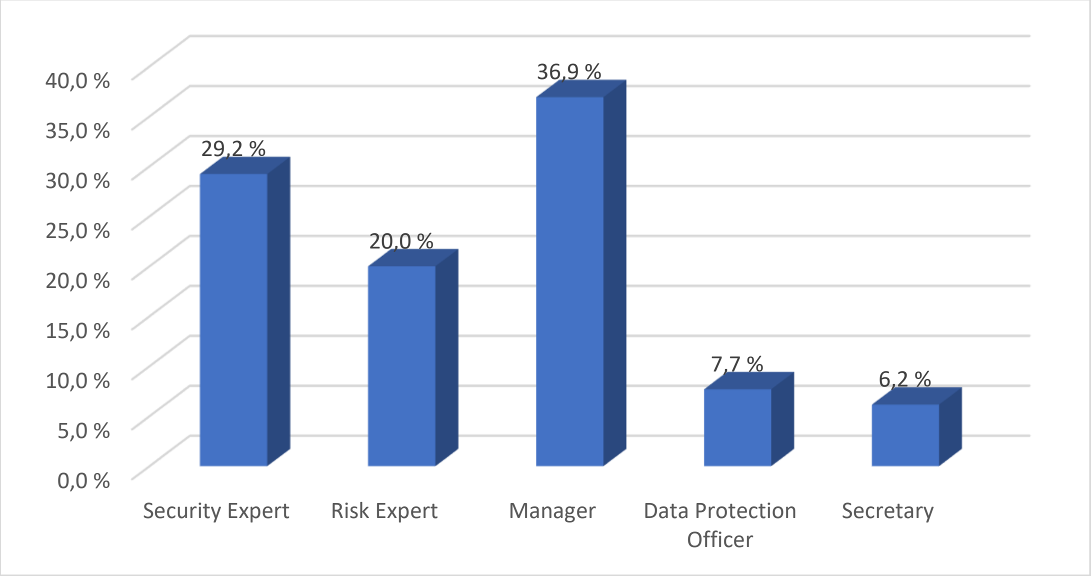


Figure 20 - Other roles present in risk assessment

The 7,5 % who found the risk assessment useless, got questions related to the reason for the perceived uselessness. They answered that they there were too few participants on the risk assessment workshop, and that there was a lack of follow-up from management. The last risk assessment they did was more than a year ago, and took under 6 hours. Those who answered that the risk assessment was totally useless did the risk assessment in under 1 hour. These could also be contributions to defining the success criteria for risk assessment.

The interview subjects were asked to define success criterias for risk assessment and the involvement of both management and employees were mentioned by all subjects. Subject 1 focused on the risk managers role in the risk assessment workshop, that they must have social skills and be able to understand the employees' lack of risk assessment to offer guidance in the risk assessment workshop. Subject 1 also states that the risk manager should not underestimate the job of selling risk analysis and action plan to management. The management need to be informed at a high level.

Subject 2 observed that top management had a different focus than IT-people and spoke a different language. He recommends IT departments to acquire the language and focus of top management, and use terms and concepts such as profit, cost, profit to get top management’s attention. Subject 3 stated that the guidance and involvement of everyone in the organization is more important than the methodology used.

Subject 4 had observed that courage, skills, and experience are important to communicate with top management. The challenges of combining digitization and innovation with security management, risk management and audit management requires a more agile way of approaching risk management, using Lean methodology. Gaining the confidence of the development teams by communicating with the development teams and asking the right questions subject 4 stated.

Both the survey participants and the interview subjects seemed to have a clear understanding of which success criteria that should be present in a useful risk assessment. The follow-up of proposed measures, the use of a good risk assessment methodology and the presence of management in the risk assessment process were the most significant responses, and management and organizational involvement was the crucial success criteria. However, the results also indicate that the success criterias were not always fulfilled in the risk assessments the participants had taken part in, but still the risk assessments were perceived as useful.

5 Discussion

The findings from the survey and interviews is discussed and compared to the results from the FFI report, the NSR reports and other related work in this chapter. The structure of the chapter will mirror the research questions in this study. In the first part the findings on which risk assessment methodologies are used the most will be compared with findings from related work and discussed. The factors that determine the choice of methodology will be discussed in the second, based on the findings from the survey and interview, and articles on taxonomies and cognitive complexity. The third part will examine the level of usefulness of risk assessments, while the fourth part will discuss which factors determine the usefulness of risk assessments. The last part will discuss which success criterias that should be present when doing risk assessments.

5.1 To what degree are risk assessment methodologies used by organizations?

Various information security risk assessment methodologies have been developed to help the organizations define, analyze, and evaluate the most relevant and critical risks to the information security in an organization. Whether organizations have used any of these risk assessment methodologies will be discussed in this part. These methodologies have been examined, reviewed, and compared in various studies to provide risk assessment taxonomies with the purpose of helping organizations to choose the most suitable risk assessment methodology. The studies have selected risk assessment methodologies based on the number of other reviews, papers, references, case studies and the risk assessment methodology developers own documentation.

Enisa(18) made an inventory of methods, where 13 methods have been considered. Wangen(27) developed a taxonomy of risk assessment methodologies, the Core Unified Risk Framework (CURF), which give an overview of risk assessment methodologies, and where 11 risk assessment methodologies qualified. Shameli-Sendi(24) present a taxonomy of security risk assessment drawn from 125 papers published from 1995 to May 2014, and examines the most reviewed information security risk assessments.

In the master thesis of Dan Ionita(21) a list of 14 risk assessment methodologies were evaluated based on a set of criteria. In a study by Fenz(20) challenges in security risk management are examined by studying 8 risk assessment methodologies, and in light of this, factors to determine the usefulness of risk assessment could be found. Zambon et al.(22) examined 12 risk assessment methodologies and discussed the compatibility with a model-based technique, QualTD, based on characteristics of the risk assessment methodologies.

The methodologies reviewed in these taxonomies and papers are presented in a Wordcloud where frequency of the various methodologies is indicated by the size of the fonts. The methodologies OCTAVE and CRAMM, NIST 800-30, ISO/IEC 27005 and CORAS, followed by EBIOS, FAIR, MEHARI and IT-Grundschutz. NSMROS, The methodology developed by NSM is only mentioned in one taxonomy.

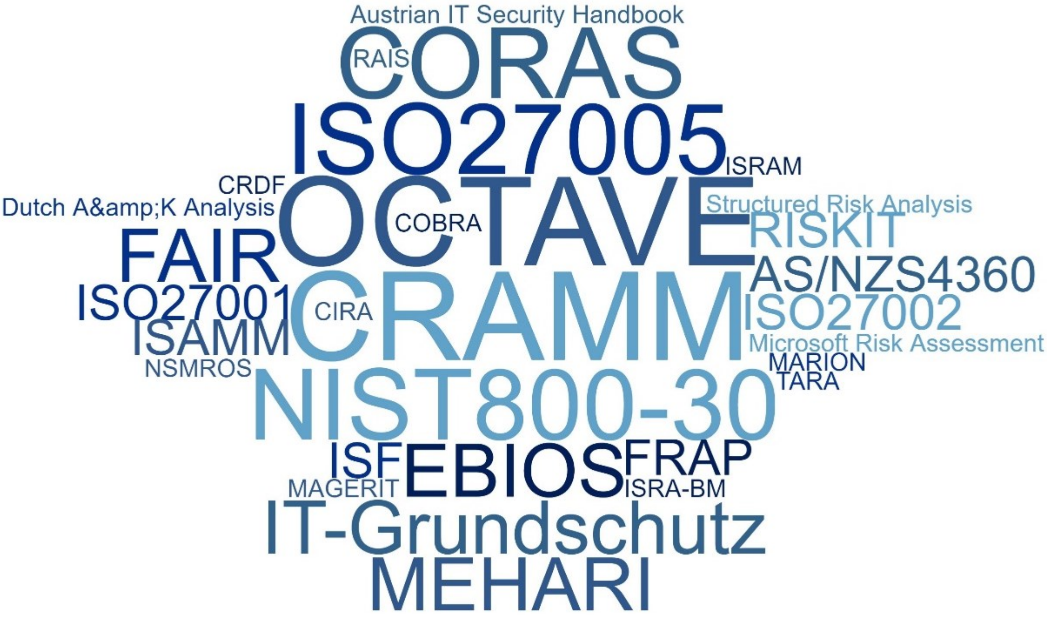


Figure 21 - Methodologies mentioned in taxonomies and papers

The findings from this thesis survey and interview, however, indicate that of all the methodologies presented and analyzed in the papers and studies, there are only three methodologies that were preferred by participants and interview subjects, ISO/IEC 27005, NIST 800-37 and NSM, the methodology called NSMROS in the study by Wangen(27). It should be noted that preferring a methodology does not imply that the methodology is implemented as is, since several of the participants also responded that they also used elements from other methodologies. In the survey, the participants were asked about the risk management framework NIST 800-37, as opposed to the risk assessment guideline NIST 800-30 described in mainly all taxonomies reviewed.

Elements from COSO and IRAM2 as well as ISO/IEC 27005, NIST 800-37 and NSMROS are used by 45,0% of the participants in their own risk assessment methods, while 33,5% of participants preferred one of the methodologies. However, findings indicated that risk assessment methodologies reviewed by several of the papers OCTAVE, CRAMM, TRA, EBIOS and Mehari were not used, or not known by the participants.

The findings from the interviews indicated that the interview subjects also preferred and used the same methodologies as the survey participants, ISO/IEC

27005, IRAM2, and NSM was preferred amongst interview subjects, although one of the subjects stated that she also used the methodology developed by Difi.

In the Core Unified Risk Framework (CURF), a taxonomy of risk assessment methodologies, developed by Wangen et al.(27), ISO/IEC 27005 was described as the most complete risk assessment methodology. The CURF framework was based on the risk management process of ISO/IEC 27005, and other methodologies have been added to the taxonomy and comparisons made based on the core activities of ISO/IEC 27005, Risk identification, risk estimation and risk evaluation to provide a measure of completeness. The second most complete risk assessment methodology was CORAS, however NIST 800-30 was the 6th and NSMROS was the 8th most complete methodology. This could indicate that although the CURF taxonomy could be a useful help for organizations to choose the most complete and suitable risk assessment methodology, it does not give an indication of the current use of risk assessment methodologies.

Enisa reported that organizations mainly used one single method for Risk Management but used various methods in parallel for Risk Assessments depending on the nature of the subjects of assessment. However, the findings in this thesis indicate that more

Of all the methodologies examined in the master thesis of Ionita(21), ISO/IEC 27005 stand out from the rest. Ionita found that this framework gives a thorough description of how to implement and maintain Information Security Risk Managements, including how to perform Risk Assessments. Most other tools and methodologies refer or comply to these guidelines, as Ionita states, "all generic tools and even some of the specialized tools are compatible with the ISO/IEC Information Security standards."

In a study on the practical use of OCTAVE, Corland Gordon Keating(15) found that in USA, although the number of higher education institutions that perform information security risk assessments has increased over the last five years, 42% of the small colleges and universities performed information security risk assessments on central administrative systems and data, while 68% of the largest colleges and universities performed risk assessments.

Most of the methodologies described in these studies have been unknown to the participants, with the exception of NSMROS, NIST 800-37 ISO/IEC 27005, IRAM2 and COSO. What case studies, Enisa and other taxonomies have found is coherent with the findings from the analysis, that organizations use different elements from a variety of methodologies and develop their own methodology, or procedure, They also use different risk assessment methodology in different contexts, even if they stick to one single risk management framework.

Studies where risk assessment methodologies are reviewed and the methodologies classified according to a variety of characteristics, the intention was to help organizations choose the most suitable methodology for their use. However, findings from analyzing the results of the survey and interviews indicate that only a few of the most acknowledged risk assessment methodologies are used in practice in organizations. As the report from Enisa describes, it is more common for organizations to use elements from different risk assessment methodologies in the development of the organizations own risk assessment routines.

5.2 Which factors determine the choice of risk assessment methodologies?

An important task in the implementation of an information security management system is for the organization to choose an appropriate risk assessment methodology. In addition to the inventory developed by Enisa, various risk assessment taxonomies have been developed and proposed to help the organizations make this choice. The findings from the survey and interviews indicate that other factors could determine this choice of risk assessment methodology, and the survey indicates that many risk managers don't choose a methodology at all, but select elements from various methodologies to develop their own information security risk assessment procedure.

The findings from the interviews indicated that the factors determining the choice of risk assessment methodology is connected to previous experiences by the risk manager, or information security expert. The choice of method was often made in organizations long before any of the participants of the risk assessments was a part of the organization, and for a hired consultant, this required a pragmatic view on the choice of methodology. The participants also use elements from risk assessment methodologies to make their own risk assessment procedure, rather than to completely utilize one of the risk assessment methodologies.

The survey questions related to knowledge and experience with different risk assessment methodologies did not include an explanation for the answers. The basis for participants' answers could however be extracted from answers on other areas. The results related to work experience, education, and experience with risk assessment, in addition to type of branch, have been analyzed to give an indication to the choice of methodology, the type of branch same can type of industry.

The branches are differently represented in this survey compared to the Norwegian crime and security survey(33), where government is overrepresented, and education and healthcare is underrepresented. However, the Norwegian crime and security survey have not examined the type of risk assessment methodologies in use in the organizations.

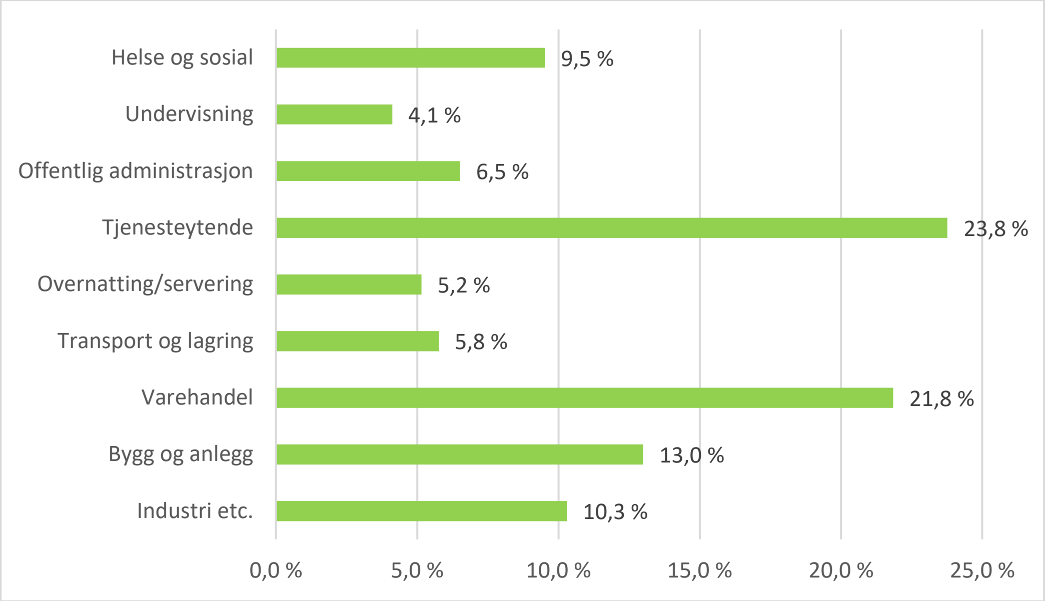


Figure 22 - Branches represented in the crime and security survey(33)

Most of the participants in the survey had either a master's or a bachelor's degree, and the rest had either a one-year programme or education from vocational college. The knowledge and experience with risk assessment methodologies had no correlation to the difference in education. Those who preferred one of the three risk assessment methodologies NSM, NIST 800-37 or ISO 27005 had one-year programme, bachelor's degree or master's degree or higher from universities. However, the participants with master's degree use elements from different methodologies more than bachelors and other participants.

The findings from the analysis indicate that besides Communication/IT which was the only branch where participants preferred one of the methods, the type of branch the participants represented had little to say for the choice of methodology. Those who preferred the NSM-methodology was from Government, Communications/IT and transportation, while participants representing Communication/IT, Counseling, Government, Healthcare and Oil/Energy, and as mentioned, The participants preferring NIST 800-37 represented Communications/IT. The interviews subjects, however, related the choice of risk assessment methodology to the line of work they were in, and what risk assessment methodology the organization already had implemented.

Whether the risk managers and information security expert in charge of developing the organizations risk management system are aware of Enisa's inventory and the various studies that have provided taxonomies over risk assessment methodologies to help organizations choose the most suitable method for their needs, have not been questioned in this survey, and the taxonomies were not mentioned as determining factors by the interview subjects.

In Enisa’s(19) inventory, each method in the inventory was described using 21 attributes that describe characteristics of the methods, e.g fullfillment of the various phases of risk assessment, language, price, size of organization, skills needed licencing and certification. Raising awareness on risk management, give an overview of the different relevant alternatives and help the organizations make a qualified choice of methodology was the purpose of Enisas inventory, and in the study by Wangen(27) the degree of completeness was proposed as a factor to determine the choice of methodology, however, Wangen found that none of the risk assessment methodologies in CURF was complete. The most complete methodology is ISO/IEC 27005 which addresses 18 of 25 criteria.

Shameli-Sendi et al.(24) conclude in the study that the variety of available risk assessment methodologies makes the organizations unsure about which methodology is the most appropriate to their requirements. The objective is to provide organizations with an overview of the various techniques used to evaluate risks. This can help them conduct risk assessment successfully.

The factors that determine the choice of risk assessment methodology in the case study by Ladislav Beranek(16) were; the price of a possible support instrument, the transparency of individual steps of the analysis and the suitability for use in day-to-day management within the fast-changing environment of small and medium organizations, and CRAMM and OCTAVE were considered to complex and costly for the study case.

By combining two other methods BITS and TRA, the organization gained an “inexpensive tool which is easily edited and used for follow-up procedure” and thus got an acceleration of the risk assessment, particularly in the identification and asset evaluation phase, and the ability to generate simple spreadsheet tables to document the risk assessment.

Zambon et al.(22) have examined 12 risk assessment methodologies and discussed the compatibility with their developed model-based technique, QualTD, based on characteristics of the risk assessment methodologies. They found that QualTD could be combined with many of the “popular risk assessment methodologies”, in organizations not using the same risk assessment methodologies as in this study, Zambon concludes.

In the master thesis of Dan Ionita(21) a list of 14 risk assessment methodologies were evaluated based on a set of criteria. The methodologies shall be documented sufficiently, and in English, and the documentation shall be publicly available. The methodology should neither be restricted to high-level management users or technical issues and users, while Shameli-Sendi et al.(24) presented a taxonomy of security risk assessment drawn from 125 papers published from 1995 to May 2014, and examined the most reviewed information security risk assessments.

Shamala et al.(25) observed that there was an absence of one perfect one-size-fits-all risk assessment method for all organizations, no guidance system to help the organizations determine the most appropriate risk assessment methodology. There exists no standard information security risk assessment method and proposed an agreed reference benchmark or comparative framework for evaluating information security risk assessment methods.

Taxonomies are developed with the purpose to help organizations choose the most suitable risk assessment methodology for their use. The overview of characteristics and attributes of the methodologies could give an indication of what is considered useful in a risk assessment, and how the methodology could be suitable for an organization. However, the findings from the survey and the interviews indicate that the choice of risk assessment methodology is more pragmatic, and that the methodology already in use is the preferred choice of method. Regardless of the variety of suitable risk assessment methodologies, the findings from the survey are similar with the observations described in Enisa, that organizations use elements from several risk assessment methodologies as basis for their own risk assessment procedures.

5.3 To what degree are risk assessments perceived as useful?

The benefits of doing risk assessments have often been related to the costs of implementing controls in comparisons to the cost of impacts in risk assessment methodologies and standards. However, to what degree the risk assessments are perceived as useful in the organizations indicate a relation to the awareness of the risk assessment process, based on experience with information security incidents and the further treatment of risk assessment results.

The perceived usefulness was measured in this thesis' survey by asking the participants about their experience with the risk assessment. The findings indicate that risk assessments were perceived as useless or totally useless by only 7,5% of the participants, while 92,5% of the participants perceived the risk assessments as useful or very useful. Even if mostly all participants found the risk assessment useful, the perceived usefulness will be discussed against other criterias in this part.

According to Ionita(21), the purpose of doing risk assessment was to analyze the security of an infrastructure, identify the vulnerabilities and choose appropriate countermeasures. However, under half of the participants in this theses' survey, 42,5%, responded that an action plan had been introduced. This is not far from similar results from the Norwegian crime and security survey(33), where 47% of those who responded that they documented their risk assessments also answered that the risk assessment led to the implementation of measures to prevent criminal activity.

Findings from the analysis about the participants experience with information security incidents, shows that 62,2% of all the participants who found the risk assessment useful or very useful, also had experienced information security incidents. That these participants who had experienced incidents and still responded that the risk assessment was useful, could be interpreted as a more valid result than the results where the participants responded that the risk asessement was useful had not experienced any incidents.

On the other hand, 16,2% of the participants who found the risk assessment useful did not know if they had experienced an incident. Only 7,5% of the participates found the risk assessment not useful, and all of them had experienced information security incidents. However, those who had experienced incidents risk assessments and not found the risk assessment useful could also be considered more valid.

Norwegian computer and data breach survey(32) is a survey conducted by Opinion AS for The Norwegian Business and Security Council(NSR), examining the usefulness of information security management systems, presenting numbers of organizations having a ISMS and how many organizations having been exposed to information security incidents.

Results show that 61% of the organizations have an information security management system (ISMS), and of these 88% had found that the organization was in compliance with the security management system. Risk assessment methodologies were not the subject of that survey, although ISO 2700x and COSO were mentioned as examples of ISMS in the survey, and these examples of information security frameworks were considered as risk-based.

In another survey by NSR, The Norwegian crime and security survey(33) the focus of the study were to examine the effects crime have on organizations, what measures they are taking, and effective they are. In this survey 28% of the organizations responded they had a written risk assessment of crime in or against the organization. The study shows that 57% of the organizations with 100 employees or more have documented risk assessments, however, 14% of organizations with 4 employees or less and 27% of organizations with under 100 employees have documented risk assessments.

Neither of the NSR reports examine which risk assessment methodologies were used, but the results on how many documented risk assessments in the organizations have been compared to the findings in this thesis survey on the number of participants who have participated in risk assessment the previous month or the previous year, which were 85% of the participants.

Risk assessments are perceived as useful by mostly all participants in the survey and interview subjects. However, the definitions of risk assessments as parts of the risk management process defined by ISO/IEC 27005 and NIST 800-37, and the findings from the survey and interviews regarding factors that determine the usefulness of risk assessments, where follow-up by management and implementation of a risk handling plan are important, the degree of actual usefulness of risk assessment is lower.

5.4 Which factors determine the usefulness of risk assessments?

How the survey participants perceived usefulness and which factors they propose determine the usefulness of the risk assessment are compared to factors in that could determine the usefulness of risk assessments.in taxonomies and case studies, the requirements for being included in the taxonomies, and the characteristics of risk assessment methodologies. One of the purposes of this research question was also to determine if risk assessment methodology could be one of these factors.

The finding from the interviews and surveys show that the main factor that determine the usefulness of risk assessments is that actions have been taken to limit the impact or avoid the incidents, that there have been an increased awareness regarding information security and that exercises on relevant scenarios are done. Cutting costs for unnecessary measures or to act in accordance with the legislation were not chosen as a factor by any of the participants, however, the participants had the opportunity to formulate an answer themselves, and the risk assessment being "a basis for prioritizing measures (cost / benefit)" was one of these answers. The findings from interviews also indicate that approval from management, and that management being aware of their responsibility for the residue risk and risk management are factors that could determine the usefulness

The existence of a risk reducing action plan can be an indication of usefulness in risk assessments, especially if the risk assessment and action plan lead to a reduction in incidents, or that the organizations were better prepared for incidents and could reduce the impact. In the survey, 53,8% of the participants who had experienced an incident, answered that they were prepared or very prepared for the incident. Of these, 30,8% had done risk assessments the same month, and 15,4% had done risk assessments the same year.

Questions about the usefulness of risk assessments had been placed both at the start and the end of the survey, in addition to questions about how the risk assessments were further processed in the organization. The responses at the start and the end of the survey indicated similar responses, and this could imply that the participants had a clear perception of the factors that determine usefulness.

However, there was also a question about how risk assessments were processes further where 40,0% of the participants responded that management had approved of the risk assessment, and 42,5% responded that that an action plan had been introduced, This could indicate that even if the participants had a clear perception of factors that determine the usefulness of risk assessments, they were not necessary present in the risk assessments the participants had done, still, nearly all the participants had responded that they perceived the risk assessment as useful or very useful.

In the Norwegian computer and data breach survey(32) where 61% of the organizations responded that they had implemented an ISMS, 19% of the organizations answered that they were aware of the number of information security incidents the organization have had. The consequence of the incidents in the NSR survey was defined as "negatively affected the business in terms of financial losses or a weakened market position".

In this study however, the survey participants who responded that they had experienced incidents also answered a question about which type of consequences the information security incidents have had on the organization. The most frequent consequences were "Loss of working hours and income", networks and central systems became inaccessible over time", and "Confidential information became known to unauthorized persons". One of the participants however responded loss of contracts or tenders. In the Norwegian crime and risk study, however, 28% of the organizations had a documented risk assessment of crime in or towards the organization, whereas 47% of these had implemented measures as a result of the risk assessment.

According to Enisa(18), it is everyone's responsibility that Risk management becomes a part of the organizations philosophy, practices and business processes. Whether risk management would be effective, depends on whether it could become a part of organization's culture.

Siv Houmb(23), however, defined the purpose of risk assessment was to apply and maintain of an acceptable level of security. Risk assessment contribute to increased knowledge and insight into the system and the dependencies and inter-relations between the system and its environment. This motivates and increases the awareness of the importance of systematic security follow-ups. Houmb observed that quantification of security risks was less researched in academia. Although a change of focus, the importance of a structured and formalized security assessment and management is not appreciated.

Houmb examined the CORAS framework and observed that the framework provides support, guidelines and UML modelling elements which would increase the value of both system development and risk assessment activities. Enhancing the precision when describing the risk assessed system, communicating risk assessment process to stakeholders and document the risk assessment process and the results could therefore also be CORAS proposed factors that determine the usefulness of risk assessments.

Shameli-Sendi et al.(24) states that organizations need to identify security risks and to help them choose the best safeguards to reduce them. it is important that risks are managed in a way that gives confidence to all stakeholders. To identify all imaginable risks to the assets and do an accurate evaluation to find the appropriate measures to handle the risks. The objective of risk assessment according to Shameli-Sendi, was therefore, finding the vulnerabilities related to the assets, services and business process, and determine the related threats that could exploit them, is essential to safeguard an appropriate level of security for the organization’s information systems. The usefulness of risk assessment, depends on risk management processes to be possible to model, in addition to “repeatable, measureable, and auditable”.

In a study by Fenz(20) challenges in security risk management are examined, and in light of this, factors to determine the usefulness of risk assessment could be found. The risk assessment methodologies evaluated were NIST 800-30, ISO 27005, EBIOS, OCTAVE, CRAMM, FAIR, ISAMM and ISF, and these methodologies were compared by challenges related to asset and countermeasure inventory identification, asset value assignment, risk prediction, the overconfidence effect, knowledge sharing and risk vs. cost trade-offs. These challenges thus becomes Fenz’ proposed factors to determine usefulness of risk assessments.

Dorna Dehkhoda(6) proposed several factors that must be present in a comprehensive risk management: The definition of risk must be a function of assets, threats and vulnerabilities, decision-makers must be able to prioritize based on what is important to the organization, organizational issues related to the use of computing infrastructure to meet the business objectives of the organization and technological issues related to the configuration of the computing infrastructure, the method should therefore be so flexible that can be uniquely tailored to each organization.

In the study by Zambon et al.(22) it was observed that IT risk assessments often are based on the intuition and expertise of the auditor and could lack certainty in terms of objectivity and replicability of the risk assessment results. Zambon developed a model for qualitative assessment of availability risks, without requiring too much time or unavailable information, and defined factors to determine the usefulness of risk assessment, since Zambon found that the model delivered more accurate and intersubjective results, compared to other methodologies based on dependency graphs that required information that is unavailable or that required too much time to be extracted

Taxonomies are developed with the purpose to help organizations choose the most suitable risk assessment methodology for their use. The overview of characteristics and attributes of the methodologies could be the factors that determine usefulness in a risk assessment. However, the standards ISO 27005 and NOST 800.37 define the benefit of risk assessment as the cost of implementing measures being lower than the cost of an impact. Meanwhile, the survey and interviews also indicate that both taking actions to avoid incidents and reduce impact, and increasing the level of awareness of risks and incidents are the most important factors that determine the usefulness of risk assessments.

5.5 Have organizations defined any success criterias for risk assessments?

The purpose of doing risk assessments have been defined in the methodologies and standards, and the degree of usefulness have been discussed in the previous part. In this part which factors need to be present for the risk assessments to fullfill this purpose and to safeguard usefulness of risk assessments will be discussed. The participants have been asked what factors need to be present for the risk assessment to be perceived as a success, and these findings are compared to response from FFI(17) and NRS reports, taxonomies and case studies.

The findings from the analysis indicate that the organizations have defined success criterias for risk assessments, where the follow-up of proposed measures, the use of a good risk assessment methodology and the presence of management in risk assessment were the most responded alternatives, and management and organizational involvement was the crucial success criteria were the most significant.

The interview subjects proposed the involvement of both management and employees were success factors for risk assessments. The social skills of the risk manager and be able to understand the employees' lack of risk assessment to offer guidance, was also mentioned as a success factor. Using the same terms and concepts as management level, such as profit, cost and profit to get top management’s attention, was also mentioned as a success factor. The findings from the survey indicated that using a good methodology was a success factor, was also found in the interviews.

It could be argued that the managements handling of risk assessment results should rather be considered a factor to determine usefulness, but it would also be a success-factor, since the expectations of management to approve and act on the risk assessment report could inspire and motivate the risk assessment participants in the process.

The case in the Dehkhoda(6) study did originally not use any common risk management methodology, therefore the quality of the results relied on those in charge of the risk management and their choice of methods. The lack of a common risk management methodology also made it difficult to communicate with management regarding investments as a result of risk assessments.

In that case study IRAM2 have been problematic adapting, therefore a simplified IRAM2 was considered to make the risk assessment process easier when a new method was developed. In addition to identify and analyze risks and vulnerabilities, the risk management method should be used to show the mitigations that are financially beneficial.

The study by Kotulic(14) defined success criteria for risk management to be that the risk management should be cost-effective and nontechnology driven, and it should “contribute to the overall effectiveness of the organization”. The role management has in risk management was emphazised, when making the right decisions based on risk assessments and interpret them into strategic choices. The concern related to lack of communication between management level and security functions were also described in this study, making a negative impact on the security risk management program effectiveness.

In the FFI-report by Busmundrud et. al (17) several success factors for risk assessments were proposed. To enhance and strengthen the risk assessments the process should be structured and conducted by a group with broad expertise. Mapping the knowledge level in the working group and make sure the group has knowledge of the system is crucial to the process, and having a holistic perspective and being concrete, is essential. It is also important to be able to communicate risks and uncertainties is important to make sure the risk assessment is transparent, traceable, and verifiable.

In the report on risk management, Enisa (18) defined success factors for the effectivity of ISMSs, which will be relevant in a risk assessment context as well. The support and commitment from top management must be continuous, visible and consistent, and a common strategy and policy across the organization must be managed centrally. As an activity defined in the ISMS, information security risk assessment must reflect the organizations approach to risk management, control objectives and degree of assurance. As with ISMS, risk assessment must be integrated in the overall management of the organization, to avoid waste of valuable resources and superfluous control, and to prioritize only necessary tasks. The awareness and training of employees, and not sanctions and disciplinary measures, should be the basis for ISMS which should be “a never ending process”.

The most significant success criteria for risk assessments are that proposed measures from the risk assessment are followed up, using a good risk assessment methodology and that management is participating in risk assessments. That the risk manager is able to offer guidance in the risk assessment process, and the importance of using the same terms and concepts as management level, such as profit, cost and profit to get top management’s attention, was also mentioned as a success factors. Communicating risks and uncertainties to management and within the organization to present the measures that are financially beneficial was also proposed by papers presenting taxonomies of risk assessment methodologies.

That risk assessments should be cost-effective and nontechnology driven, and that the risk assessment process should be structured and conducted by a group with broad expertise, and make sure the risk assessment is transparent, traceable, and verifiable was also success factors proposed in the papers on risk assessment methodologies. The findings from the survey and interviews indicate, however that even if the participants and interview subjects can identify success factors of risk assessments, it does not follow that the success factors are present in the current risk assessments performed, even if the participants responded that the risk assessment was perceived as useful.

6 Further research

In this study, the participants in the survey was security experts and risk managers, a few managers and data protection officers. Although they have a clear opinion of how risk assessment should be useful, other studies could examine the CFO’s and CEOs attitude towards risk assessment and their requirements for a useful risk assessment. They would perhaps have different opinions on the usefulness of risk assessments, the factors that determine usefulness and which risk assessment success criteria should be present in a risk assessment process.

In this study the survey was distributed to recipients in the Norwegian information security community, and in Norwegian. A possible next step could be to distribute the survey to the international information security community. The purpose could be to determine if Norway is similar to other countries when it comes to risk analysis, and to examine if the results indicated in this analysis are similar on a larger scale, and in other environments.

During the work with this study, the Covid-19 epidemic broke out and the world went into lock-down. This has led to other ways to work, communicate, and hold meetings. It has led to increased phishing activity and management freud, but the question is if it also has provided another perspectives on risk assessments. In a year or two, the aftermath of the epidemic will show if the way we do workshops and risk assessments have been influenced by the new everyday routine. To examine if there are more effective and useful ways to do risk assessments, and to what degree management will be involved, can be another possible research question.

7 Conclusion

In this study, the perceived usefulness of information security risk assessment has been examined by interviews with risk assessment experts and conducting a survey with Norwegian risk experts, information security experts and managers on risk assessment methodology and usefulness. The frequency of risk assessment methodologies in organizations and the practical use of the methodologies and elements from them have been examined, which indicates that only a few of the acknowledged risk assessment methodologies are in use in the organizations.

Only three risk assessment methodologies were preferred amongst the information security risk experts; ISO/IEC 27005, NIST 800-35 and the methodology developed by NSM. However, elements from other risk assessment methodologies,COSO and IRAM2, have also been implemented in the organizations own risk assessment methods, and that the three methodologies were preferred, does not follow that the methodologies were implemented as is.

Which factors determine the choice of methodology and to which extent characteristics from risk assessment methodologies have been in practical use have been examined, and various taxonomies of risk assessment methodologies in addition to Enisas inventory of risk assessment methodologies have been reviewed. The purpose of the inventoty and taxonomies is to help organizations choose the most suitable risk assessment methodology for their use, However, there seem to be a pragmatic view on choice of methodology. The interview subjects state the choice was made before they entered the organization, and the survey results indicate a vague connection between branch, experience and education and the choice of methodology.

The degree of perceived usefulness has been examined, and risk assessment is perceived as useful by most of the participants in the survey and by the interview subjects. However, findings from the survey and interviews on factors that determine the usefulness in risk assessment indicate that both taking actions to avoid incidents and reduce impact, and increasing the level of awareness of risks and incidents are the most important factors that determine the usefulness of risk assessments. The interview subject also added involvement by management as a crucial factor for determining usefulness. However, the standards ISO 27005 and NOST 800.37 define the benefit of risk assessment as the cost of implementing measures being lower than the cost of an impact.

The most significant success criteria for risk assessments are that proposed measures from the risk assessment are followed up, using a good risk assessment methodology and that management is participating in risk assessments. That the risk manager is able to offer guidance in the risk assessment process, and the importance of using the same terms and concepts as management level, such as profit, cost and profit to get top management's attention, was also mentioned as a success factors. Communicating risks and uncertainties to management and within the organization to present the measures that are financially beneficial was also proposed by papers presenting taxonomies of risk assessment methodologies.

The findings in the risk assessment survey and the interviews indicates that the well acknowledged risk assessment methodologies are not as well-known by the information security experts and risk managers as the scientific articles give an impression of. However, responses from both participants and interview subjects indicate that organizations do perceive the risk assessment as useful. Comparing findings from the survey and interviews with the papers on risk assessment, and the taxonomies giving an overview of the risk assessment methodologies indicate that perceived usefulness does not imply that the factors determining the usefulness of risk assessment were present, and that the success criteria for risk assessment were present. This could be mitigated, if top management, information security experts and risk managers became aware that there are inventories of risk assessment methodologies, taxonomies and other resources free and accessible that could contribute to increasing the usefulness of the risk assessment process, and ensure success factors of the risk assessment process were present.

References

1. ISO. ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/: the International Organization for Standardization; 2018.
2. NIST. NIST Special Publication 800-37. Risk Management Framework for Information Systems and Organizations: National Institute of Standards and Technology; 2018.
3. Engel B. Why Risk Assessments Fail. EDPACS. 2017;56(4):1-6.
4. ISO. ISO/IEC 27005:2018(en). Information technology — Security techniques — Information security risk management. https://www.iso.org: the International Organization for Standardization; 2018.
5. LLP DT. Risk Assessment in Practice. The Committee of Sponsoring Organizations of the Treadway Commission (COSO); 2012 1. October 2012.
6. Dehkhoda D. Combining IRAM2 with Cost-BenefitAnalysis for Risk Management: <em>Creating a hybrid method with traditional and economic aspects</em>. 2018.
7. Caralli R, Stevens J, Young L, Wilson W. Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012). CARNEGIEMELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST. 2007.
8. Yazar Z. A qualitative risk analysis and management tool–CRAMM. SANS InfoSec Reading Room White Paper. 2002;11:12-32.
9. d'information Andlsds. EBIOS risk manager. ANSSI; 2019.
10. Clusif. MEHARI 2010 : Risk analysis and treatment guide. https://clusif.fr: Club de la Sécurité De L'information Français; 2010.
11. Canada Go. Harmonized Threat and Risk Assessment (TRA) Methodology. Government of Canada, , Communications Security Establishment/Royal Canadian Mounted Police 2007.
12. NSM. Risikovurdering for sikring. Håndbok. https://www.nsm.stat.no/: The Norwegian National Security Authority; 2016.
13. Pan L, Tomlinson A. A systematic review of information security risk assessment. International Journal of Safety and Security Engineering. 2016;6(2):270-81.
14. Kotulic AG, Clark JG. Why there aren't more information security research studies. Information & Management. 2004;41(5):597-607.
15. Keating CG. Validating the octave allegro information systems risk assessment methodology: a case study. 2014.
16. Beranek L. Risk analysis methodology used by several small and medium enterprises in the Czech Republic. Information Management & Computer Security. 2011;19(1):42-52.
17. Busmundrud O, Maal M, Kiran JH, Endregard M. Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. Forsvarets forskningsinstitutt (FFI) FFI-rapport. 2015;923.
18. Enisa. Inventory of risk assessment and risk management methods. 2006.
19. Enisa. Inventory of Risk Management/Risk Assessment Methods and Tools: European Union Agency for Cybersecurity; 2020 [Available from: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory.
20. Fenz S, Heurix J, Neubauer T, Pechstein F. Current challenges in information security risk management. Information Management & Computer Security. 2014;22(5):410-30.
21. Ionita D. Current established risk assessment methodologies and tools: University of Twente; 2013.

22. Zambon E, Etalle S, Wieringa R, Hartel P. Model-based qualitative risk assessment for availability of IT infrastructures. Software & Systems Modeling. 2011;10(4):553-80.
23. Houmb SH. Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework. In: Norges teknisk-naturvitenskapelige u, editor.: Fakultet for informasjonsteknologi, matematikk og elektroteknikk; 2007.
24. Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers & Security. 2016;57:14-30.
25. Shamala P, Ahmad R, Yusoff M. A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications. 2013;18(1):45-52.
26. Feng N, Wang HJ, Li M. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences. 2014;256:57-73.
27. Wangen G, Hallstensen C, Snekkenes E. A framework for estimating information security risk assessment method completeness. International Journal of Information Security. 2018;17(6):681-99.
28. Wangen G, Snekkenes E. A Taxonomy of Challenges in Information Security Risk Management. Akademika Forlag; 2013.
29. Gerard G. Basic Research Methods: An Entry to Social Science Research. IN: IN: Sage Publications Pvt. Ltd; 2010.
30. Schaeffer NC, Presser S. The science of asking questions. Annual Review of Sociology. 2003;29:65.
31. UiO. User's Guide to Nettskjema: University of Oslo; 2020 [Available from: https://www.uio.no/english/services/it/adm-services/nettskjema/help/.
32. NSR. Norwegian Computer and Data Breach Survey 2018. The Norwegian Business and Industry Security Council; 2018.
33. NSR. Norwegian Crime and Security Survey 2019. The Norwegian Business and Industry Security Council; 2019.
34. NIST. NIST Special Publication 800-30. Guide for Conducting Risk Assessments. http://csrc.nist.gov/publications: National Institute of Standards and Technology; 2012.
35. Roe A. Generating Word Clouds. School librarian. 2018;66(1):19-.
36. Lee JD. Visualizing Human Factors and Ergonomics Publications: Word clouds and Word networks. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2014;58(1):355-9.
37. Zygomatic. Wordclouds.com: Zygomatic; 2020 [Available from: https://www.wordclouds.com/.
38. Tavakol M, Dennick R. Making sense of Cronbach's alpha. 2011. p. 53.
39. Cortina JM. What Is Coefficient Alpha? An Examination of Theory and Applications. Journal of Applied Psychology. 1993;78(1):98-104.
40. Yurdugul H. Minimum Sample Size for Cronbach's Coefficient Alpha: A Monte-Carlo Study. Hacettepe University Journal of Education. 2008;35:397-405.
41. Systems CR. Sample Size Calculator: Creative Research Systems; 2020 [Available from: https://www.surveysystem.com/sscalc.htm.
42. Systems CR. Sample Size Formulas for our Sample Size Calculator: Creative Research Systems; 2020 [Available from: https://www.surveysystem.com/sample-size-formula.htm.

Attachments

Attachment 1: Summary from interviews

Attachment 2: Survey form

Attachment 3: Web-report from survey

Attachment 4: Screenshot of article from NSR website

Attachment 5: RTF-report from survey

Attachment 1: Summary of interviews

Summary of interviews

Subject 1

Female, information security consultant in a Counseling company

On the usefulness of risk assessments

Subject 1 works mostly with risk assessments regarding transition to cloud services. She is pragmatic in relation to methodology. Preferably works with Difi and IRAM2, but the methodology must be adapted to the scope of the risk assessment.

Risk assessments are done because the authorities say so. The organizations do risk assessments but are not concerned about the answer.

Risk assessment is done without planning and implementing measures and controls. Managers in Norway do not realize that they are responsible for residual risk. Managers must take the effort to read risk assessment reports and security reports, and focus on security needs to reach top management. Risk assessments are important, but require action.

1) Which risk assessment method do you use? Why?

Subject 1 uses IRAM2 according to customer requirements. The customer's IRAM2 risk system has a holistic focus but was not suitable for a new area to be risk assessed, it was too rigid and could not be adapted to a new area that was to be risk assessed and instead used Difi.

2) What success criteria must be in place in a risk assessment?

Involve the employees

Guidance in the risk assessment workshop

The risk manager must have social skills and be able to understand the employees' lack of risk assessment

The risk manager should not underestimate the job of selling risk analysis and action plan to management. The management need to get the information at a high level.

Subject 2

Male, Advisor in a Government Organization

Subject 2 has a doctorate in Information Security v UiO

Subject 2 has been a consultant in various companies for 20 years, and since 2015 he has been an advisor in the current governmental organization, establishing the advisory department. They receive inquiries from small and large businesses and shall give advice and prioritize the large organizations when needed. This governmental organization has been in a gray area in terms of counselling until then. (?).

About risk assessments

The Norwegian Security Act has become risk-based. The Security Act now provides a functional approach to what is reasonable security. The mandate of the governmental organization where Subject 2 work is not to evaluate organizations risk assessments. The organization has however developed a security management-oriented Risk Handbook for private and public organizations to use.

Organizations information systems have more integrations and more cloud solutions. Few companies have done good risk assessments. Risk assessments are usually only performed in relation to outsourcing of service functions, and rarely during the systems lifecycle. However, Equinor and Telenor are two examples of Norwegian large companies that do risk assessments well.

The times are changing and there is an increased focus on security in Norway. The symbolic effect of having 4 ministers launching a digital strategy also helps. Top management in both large and medium size organizations are focused on risk but don't know how to do it. The organizations lack expertise and resources.

The GDPR also generates a willingness to change. It is wrong to say that GDPR is the same as Security, but if you have taken care of security, you have also taken care of GDPR. GDPR gives a boost to security awareness. Risk assessments has become important, especially related to cloud services.

Subject 2 concerns are what do the companies do to safeguard their values in the cloud? And what does society do when essential values lie in the cloud? There are geographical dependencies, and dependencies related to political stability. Level of security throughout the crisis vs maintaining essential society functions.

On risk assessment methodologies:

The mandate of the governmental organization is not to evaluate organizations' implementation and documentation of risk assessments, but based on inquiries and questions, the impression is that small and medium-sized enterprises are not aware of the methods they use and how risk assessment should be utilized in the business. Risk assessment become a paper exercise not handled further by management.

Increased awareness of risks related to outsourcing services is a consequence of the disclosures in public health organizations in Norway. In his work, subject 2 often gets asked whether it is safe to outsource service to e.g India, Bangladesh and other countries. It is emphasizes that their assessments of safe countries is just an input and the companies are responsible for doing their own risk assessments. Risk assessments help raise security awareness in the organization. The methods for risk assessment are difficult, resource intensive and require competence.

The companies only do desktop exercises (papirøvelser). There is no interaction between the risk assessment participants and the IT technicians.

In order to do risk assessment at the right level, participants must have ICT competence, and knowledge of the area to be risk assessed.

"Those responsible for risk assessment do not have a good enough ICT competence".

The arrows are pointing in the right direction. The Health organization and Hydro incident, among other things, generates a willingness to change.

"Cash is King".

«ICT security is investment in the absence of loss»

Top management has a different focus than IT people, and speak a different language. IT must acquire the language and focus of top management, and use concepts such as profit, cost, profit to get top management's attention.

"It boils down to the discomfort of management" and how the risk assessment and measures can be presented so that management wakes up. Those companies do not know what methods are used.

Risk management is lacking

There is a knowledge gap between management and risk assessment participants. NSM's Basic Principles v2.0 will be launched in March 2020 and will incorporate this and mitigate this gap.

The basic principles shall be an easier framework to implement and less difficult to understand.

Subject 3

Male, Risk Manager in a Government organization

20 years of experience in security work from the Norwegian Armed Forces as a security manager

Subject 3 has contact with private corporations and public organizations in both current and past jobs

He observes that other NATO countries are as good / bad at ISMS as they are in Norway. The Netherlands is the country most similar to Norway in regards of ISMS maturity.

Lack of focus on the vulnerability chain especially regarding IoT and smart cities

About risk methods

In the Norwegian Armed Forces, the Value-Threat Vulnerability (VTS) model was used, and here likelihood is irrelevant. Therefore, a new standard has been developed, where likelihood has also been included -> NS 5830 and NS 5832

This standard was used by the developers of the standard in Norwegian Armed Forces, but other organizations did not understand how to use it. Therefore, a risk assessment template has been developed in accordance with the safety act at current workplace, which should be easier and more understandable for departments to use.

A thorough organizational risk assessment was carried out in 2010, which resulted in a large document that was not read. In 2018, a new organizational risk assessment was conducted, and all departments throughout the organization participated in the value assessment. The initial involvement from all departments lead to increased interest in the results of the risk assessment.

2013 - The FFI survey supports that the whole organization is involved in risk assessment(?).

Mantra: "Everything is related to everything"

Subject 3 claims that the choice of methodology for risk assessment depends on what is to be expressed in the organization. Regardless, the guidance and involvement of everyone in the business is more important than the methodology used.

"Methodology has nothing to say - the most important thing is that risk assessment is done."

Statement from subject 3 on email:

«(The useability of risk assessments) It is entirely dependent on the business manager's awareness of his / her own values, knowledge of his / her own and collaborators' dependencies, and ability to manage the security need in order to gain sufficient profit.

Risk assessment is an integral part of business management. If the business is not oriented towards this, a risk analysis is likely to have limited value and at the same time be wasted effort. The risk analysis must be decision support for the management, which in turn must be responsible for the actual risk assessment based on hedging objectives and risk acceptance in order to achieve sufficient profit. If the line organization does not know or understand how to handle risk, the processes will often counteract each other.

In other words, the usefulness of risk assessment, and any methodology, depends on business management that contains a conscious relationship with the security needs and objectives of the business»

Subject 4

Female, CISO in a Car retail company

Telephone interview, 40 min.

Background:

Subject 4 is veterinarian and water supply safety specialist and has 15 years' experience with food safety in food industry as quality manager and as ISO 9001 certified auditor in Food Safety Authority. The focus on food safety in food industry and the introduction of new food safety regulations has resulted in implementation of HAZOP analysis methodology and Good Manufacturing Practice (GMP).

Subject 4 has also experience from The Norwegian National Security Authority (NSM) where ISO/IEC 19011 Guidance on management system audits, and ISO/IEC 27001 information security management system was essential.

On risk management:

In NSM she observed as an auditor that organizations struggled with the VST(asset-vulnerability-threat)-model developed by NSM and described in NS 5832, and experienced that diversity in risk assessment participants improved the quality in risk analysis.

Both in NSM and previous workplaces Subject 4 observed that long heavy risk assessment reports were not operationalized, which lead to the benefit of doing risk assessment was lost. Risk assessments requires follow-up by top management., and the challenge with the risk assessment process was that the report became outdated before it got operationalized. Subject 4 proposes to do risk assessment on changes as a solution, but this would require expertise in the organization, both on risk assessment, and on the subject of risk assessment.

Where risk assessments are done by external parties, this requires procurement expertise in the organization, and follow-up in terms of action plan and prioritized list of measures approved by management is important.

As a CISO in a large Norwegian motor company, she acknowledged the importance of gaining the trust of, and reporting directly to top management.

Courage, skills and experience are important in order to reach management. The challenges of combining digitization and innovation with security management , risk management and audit management requires a more agile way of approaching risk management, using LEAN methodology.

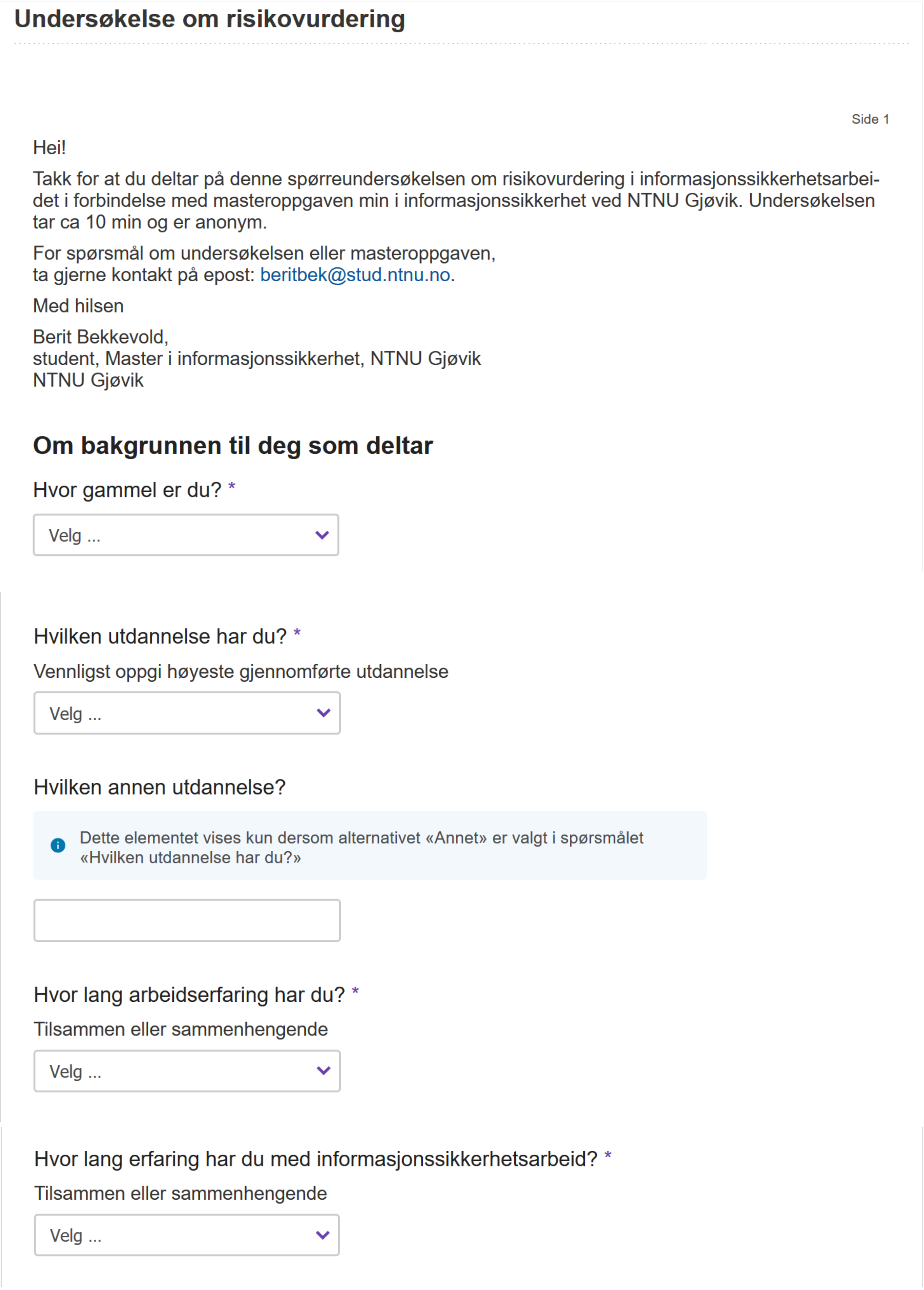
Gaining the confidence of the development teams, by communicating with the teams and asking the right questions: "What are your concerns?", Immediately place risks in the risk matrix and discuss how to move risk from red to yellow and green areas in the matrix helps understanding the risks and define measures. Leaving the DevOps team to work undisturbed, with follow-up after a few months, lead to DevOps teams taking the initiative and asking for assistance.

GDPR made the risk assessment demand situation clearer. GDPR requires that there should be a risk assessment but not how they should be done. However, a risk assessment methodology must be used consequently for the risk assessment to be compliant. It is also required to have implemented and operationalized policies.

Risk assessment is a process of people in which there must be room for trust and dialogue. It is important to involve expertise on all areas to ensure risk management, control management and supplier management is sufficient. All participants must understand the process from risk assessment to implementing measures. The expertise which the employees beholds is reflected in risk assessments. The synergy effect is self-confidence among participants of the risk assessment. Important success factors are motivation and competence.

ISO/IEC 27005 provides security in terms of experience, but Subject 4 recommends the procedure being simplified to include participants on all levels. For example, by using the concept of risk areas, introduce the risk matrix early in the assessment and divide into details. The alternative is having externsal parties doing risk analyzes, which requires sufficient follow-up by the organization.

Attachment 2: Survey form



Undersøkelse om risikovurdering

Side 1

Hei!

Takk for at du deltar på denne spørreundersøkelsen om risikovurdering i informasjonssikkerhetsarbeidet i forbindelse med masteroppgaven min i informasjonssikkerhet ved NTNU Gjøvik. Undersøkelsen tar ca 10 min og er anonym.

For spørsmål om undersøkelsen eller masteroppgaven,
ta gjerne kontakt på epost: beritbek@stud.ntnu.no.

Med hilsen

Berit Bekkevold,
student, Master i informasjonssikkerhet, NTNU Gjøvik
NTNU Gjøvik

Om bakgrunnen til deg som deltar

Hvor gammel er du? *

Velg ...

Hvilken utdannelse har du? *

Vennligst oppgi høyeste gjennomførte utdannelse

Velg ...

Hvilken annen utdannelse?

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilken utdannelse har du?»

Hvor lang arbeidserfaring har du? *

Tilsammen eller sammenhengende

Velg ...

Hvor lang erfaring har du med informasjonssikkerhetsarbeid? *

Tilsammen eller sammenhengende

Velg ...

Hva slags erfaring har du med informasjonssikkerhetsarbeid *

Velg en eller flere aktiviteter du har erfaring med

- □ Skrive retningslinjer
- □ Holde kurs og foredrag
- □ Gjennomgå logger og rapporter
- □ Sikkerhetstesting
- □ Risikovurdering
- □ Sikkerhetsrevisjon
- □ Planlegge og gjennomføre sikkerhetsøvelser
- □ Andre aktiviteter

Hvilke andre aktiviteter?

ℹ Dette elementet vises kun dersom alternativet «Andre aktiviteter» er valgt i spørsmålet «Hva slags erfaring har du med informasjonssikkerhetsarbeid»

Sideskift

Side 2

Om virksomheten du jobber i

Hvilken bransje hører virksomheten din til? *

Velg det alternativet som passer best

Velg ...

Hvor stor er virksomheten du jobber i? *

Velg ...

Er virksomheten offentlig eller privat? *

- ○ Offentlig
- ○ Privat

Sideskift

Side 3

Om risikovurdering i virksomheten

Når deltok du sist på en risikovurdering? *

○ Denne måneden

○ Dette året

○ 1-2 år siden

○ Mer enn 2 år siden

○ Har aldri deltatt på risikouvurdering

Hvor mange deltok på risikovurderingen? *

Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

○ Færre enn 3 deltakere

○ 3-6 deltakere

○ 6-10 deltakere

○ Flere enn 10 deltakere

Hvor lang tid tok risikovurderingen

Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

○ Under 1 time

○ 1-3 timer

○ 3-6 timer

○ 7-12 timer

○ Over12 timer

Hvilken rolle hadde du i risikovurderingen *

Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

○ Sikkerhetsekspert

○ Risikovurderingsekspert

○ Ansvarlig leder

○ Personvernombud

○ Sekretær

○ Annet

Hvilken rolle?

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilken rolle hadde du i risikovurderingen»

____

Hvilke andre roller var tilstede ved risikovurderingen

Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

□ Sikkerhetsekspert

□ Risikovurderingsekspert

□ Ansvarlig leder

□ Personvernombud

□ Sekretær

Hva ble risikovurdert? *

ⓘ Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

○ Et datasystem

○ En tjeneste

○ En del av virksomheten

○ Hele virksomheten

○ Annet

Hva annet ble risikovurdert?

ⓘ Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva ble risikovurdert?»

Hvordan ble risikovurderingen behandlet videre?

ⓘ Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

□ Risikovurderingen har ikke blitt behandlet videre

□ Risikovurderingen er godkjent av ledelsen

□ Foreslått tiltaksplan er innført

□ Risikovurderingen ble utgangspunkt for sikkerhetsøvelse

Hvordan opplevde du nytteverdien av å gjøre denne risikovurderingen? *

ⓘ Dette elementet vises kun dersom alternativet «Denne måneden», «Mer enn 2 år siden», «1-2 år siden» eller «Dette året» er valgt i spørsmålet «Når deltok du sist på en risikovurdering?»

○ Helt unyttig ○ Litt unyttig ○ Nyttig ○ Svært nyttig

Hva var grunnen til at du opplevde risikovurderingen som unyttig? *

ⓘ Dette elementet vises kun dersom alternativet «Litt unyttig» eller «Helt unyttig» er valgt i spørsmålet «Hvordan opplevde du nytteverdien av å gjøre denne risikovurderingen?»

- □ For tidkrevende
- □ For vanskelig
- □ For ressurskrevende
- □ For få deltakere
- □ For mange deltakere
- □ Manglende oppfølging av ledelsen
- □ Andre grunner

Hvilke andre grunner?

ⓘ Dette elementet vises kun dersom alternativet «Andre grunner» er valgt i spørsmålet «Hva var grunnen til at du opplevde risikovurderingen som unyttig?»

På hvilken måte opplevde du risikovurderingen som nyttig?

ⓘ Dette elementet vises kun dersom alternativet «Nyttig» eller «Svært nyttig» er valgt i spørsmålet «Hvordan opplevde du nytteverdien av å gjøre denne risikovurderingen?»

Svar med egne ord, gjerne i stikkordsform.

Sideskift

Om risikovurderingsmetoder

Hvilket verktøy bruker dere for å gjennomføre risikovurderinger? *

○ Excel-ark

○ Eget program/system på PC

○ Utfylling av skjema på papir

○ Egenutviklet skjema

○ Vet ikke

Hvordan definerer dere risiko i deres virksomhet? *

○ Risiko = sannsynlighet x konsekvens

○ Risiko = sårbarhet x trussel x verdi

○ Risiko = Verdi x trussel x sårbarhet x konsekvens for organisasjonen

○ Risiko = sannsynlighet x konsekvens x sårbarhet x effektens hastighet

○ Risiko = f(verdi, trussel, sårbarhet)

○ Risiko = f(sikkerhetskrav, trussel)

○ Annet

Hvilken annen definisjon av risiko bruker deres virksomhet

ℹ Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvordan definerer dere risiko i deres virksomhet?»

Hvordan finner dere sannsynlighet i risikovurderingen *

○ Det er ikke relevant

○ Antall hendelser i året/måneden/uka

○ Trusselaktørens kapasitet x sårbarhet

○ Sannsynlighet er en slags prosentregning

○ Systemet finner sannsynligheten

○ Sannsynlighet for initiativ x trusselens styrke x tiltakets styrke

○ Annen måte

Hvilken annen måte?

Dette elementet vises kun dersom alternativet «Annen måte» er valgt i spørsmålet «Hvordan finner dere sannsynlighet i risikovurderingen»

Hvordan finner dere aktuelle trusler? *

○ Vi drøfter tidligere hendelser i organisasjonen

○ Vi utformer trusselscenarier basert på skjemaet i risikovurderingsmetoden

○ De er definert i systemet for risikovurdering

○ Vi bruker Enisas, Norsis og NSMs rapport over trusler og sårbarheter

○ Annen måte

Hvilken annen måte

Dette elementet vises kun dersom alternativet «Annen måte» er valgt i spørsmålet «Hvordan finner dere aktuelle trusler?»

Hvilke risikovurderingsmetoder er du kjent med?

Her er en liste over de mest kjente risikovurderingsmetodene. Vennligst angi hvor godt du kjenner til dem.

	Er ikke kjent med metoden	Har hørt om metoden men bruker den ikke	Har brukt denne metoden tidligere	Bruker elementer fra metoden	Foretrekker å bruke denne metoden
Octave *	○	○	○	○	○
CRAMM *	○	○	○	○	○
NSM *	○	○	○	○	○
TRA *	○	○	○	○	○
NIST 800-37 *	○	○	○	○	○
EBIOS *	○	○	○	○	○
Mehari *	○	○	○	○	○
COSO *	○	○	○	○	○
IRAM2 *	○	○	○	○	○
ISO/IEC 27005 *	○	○	○	○	○

Sideskift

Om Hendelser

Har virksomheten opplevd noen informasjonssikkerhetshendelser eller avvik de siste 3 årene?

○ Ja

○ Nei

○ Vet ikke

Hvor alvorlig var hendelsen?

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har virksomheten opplevd noen informasjonssikkerhetshendelser eller avvik de siste 3 årene?»

○ Helt ubetydelig ○ Ikke så alvorlig ○ Alvorlig ○ Svært alvorlig

Hva førte hendelsen til?

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har virksomheten opplevd noen informasjonssikkerhetshendelser eller avvik de siste 3 årene?»

□ Data gikk tapt eller ble kryptert

□ Konfidensiell informasjon ble kjent for uvedkomne

□ Nettverk eller sentrale systemer ble utilgjengelig over tid

□ Viktig informasjon ble endret av uvedkomne

□ Dårlig omdømme for virksomheten

□ Tapte kontrakter og anbud

□ Tap av arbeidstid og arbeidsfortjeneste

□ Tap av liv eller helse

Hvor godt forberedt var dere på hendelsen som inntraff?

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har virksomheten opplevd noen informasjonssikkerhetshendelser eller avvik de siste 3 årene?»

○ Svært dårlig forberedt ○ Litt dårlig forberedt ○ Godt forberedt

○ Svært godt forberedt

Sideskift

Side 6

Om nytteverdien av risikovurderinger

Hva mener du er den største nytteverdien av å gjøre risikovurderinger? *

○ Har ingen nytteverdi

○ Vi blir bevisst på informasjonssikkerheten

○ Vi setter inn tiltak for å unngå hendelser

○ Vi setter inn tiltak for å begrense skadene

○ Vi kutter kostnadene til unødvendige tiltak

○ Vi gjør sikkerhetsøvelser på relevante hendelser

○ Vi handler i tråd med lovverket

○ Annet

Hvilken annen nytteverdi?

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva mener du er den største nytteverdien av å gjøre risikovurderinger?»

□

Hva mener du er de tre viktigste suksesskriteriene for risikovurderinger? *

□ At risikovurderingen tar kort tid

□ At noen av deltakerne har erfaring med risikovurdering

□ At vi har forberedt oss godt

□ At lederen deltar på risikovurderingen

□ At forslagene til tiltak blir fulgt opp

□ At vi bruker en god metode for risikovurdering

□ At alle deltakere kjenner trusselbildet

□ At det er servering på møtet

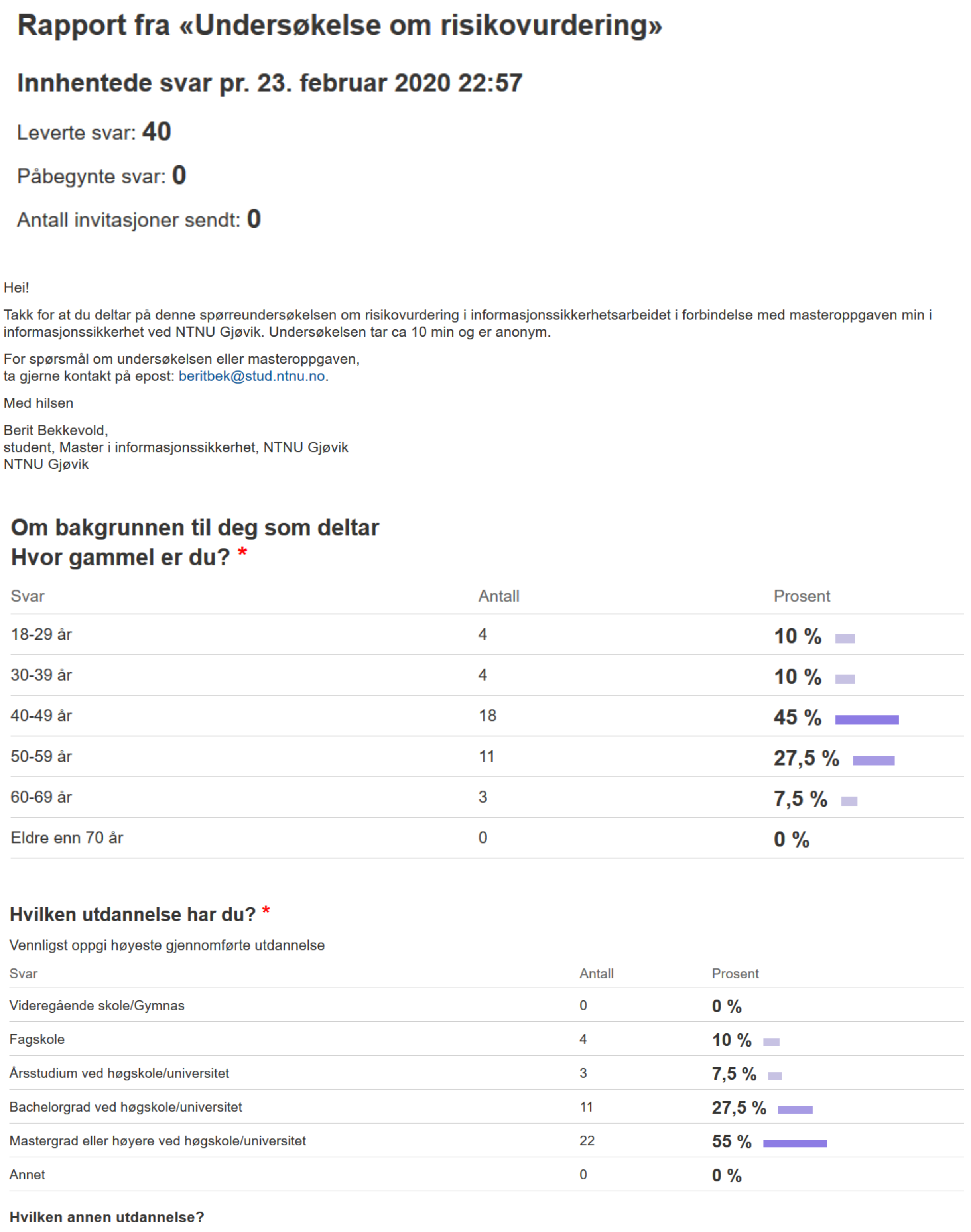
□ At vi bruker et system for risikovurdering

□ Annet

Hvilket annet suksesskriterie for risikovurdering?

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva mener du er de tre viktigste suksesskriteriene for risikovurderinger?»

Attachment 3: Web-report from survey



Rapport fra «Undersøkelse om risikovurdering»

Innhentede svar pr. 23. februar 2020 22:57

Leverte svar: **40**

Påbegynte svar: **0**

Antall invitasjoner sendt: **0**

Hei!

Takk for at du deltar på denne spørreundersøkelsen om risikovurdering i informasjonssikkerhetsarbeidet i forbindelse med masteroppgaven min i informasjonssikkerhet ved NTNU Gjøvik. Undersøkelsen tar ca 10 min og er anonym.

For spørsmål om undersøkelsen eller masteroppgaven,
ta gjerne kontakt på epost: beritbek@stud.ntnu.no.

Med hilsen

Berit Bekkevold,
student, Master i informasjonssikkerhet, NTNU Gjøvik
NTNU Gjøvik

Om bakgrunnen til deg som deltar
Hvor gammel er du? *

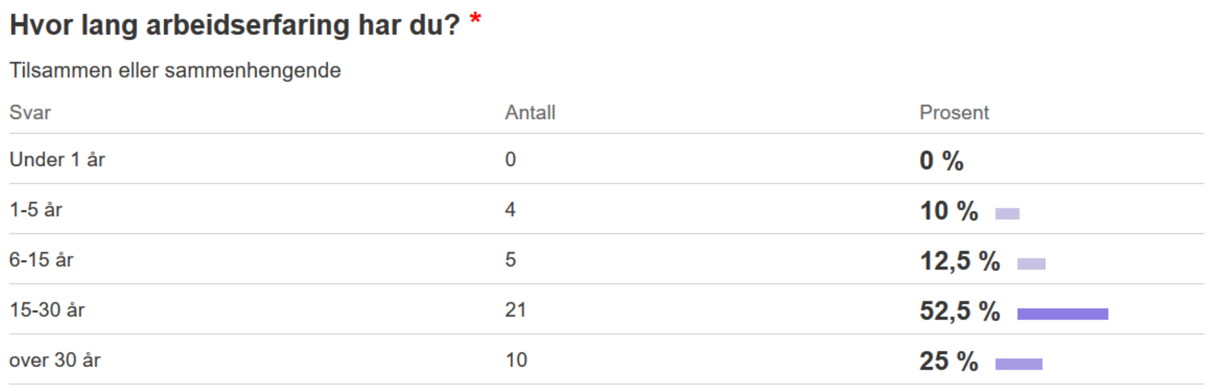
Svar	Antall	Prosent
18-29 år	4	**10 %**
30-39 år	4	**10 %**
40-49 år	18	**45 %**
50-59 år	11	**27,5 %**
60-69 år	3	**7,5 %**
Eldre enn 70 år	0	**0 %**

Hvilken utdannelse har du? *

Vennligst oppgi høyeste gjennomførte utdannelse

Svar	Antall	Prosent
Videregående skole/Gymnas	0	**0 %**
Fagskole	4	**10 %**
Årsstudium ved høgskole/universitet	3	**7,5 %**
Bachelorgrad ved høgskole/universitet	11	**27,5 %**
Mastergrad eller høyere ved høgskole/universitet	22	**55 %**
Annet	0	**0 %**

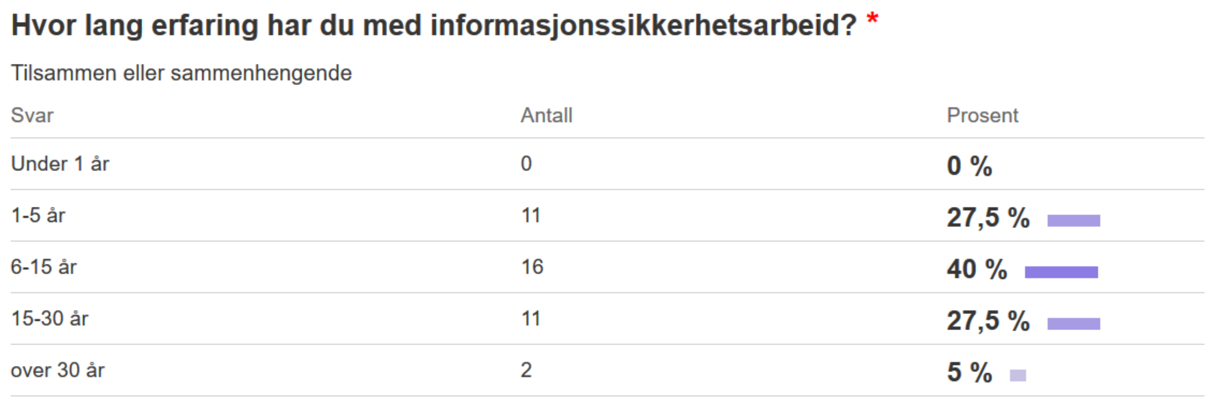
Hvilken annen utdannelse?



Hvor lang arbeidserfaring har du? *

Tilsammen eller sammenhengende

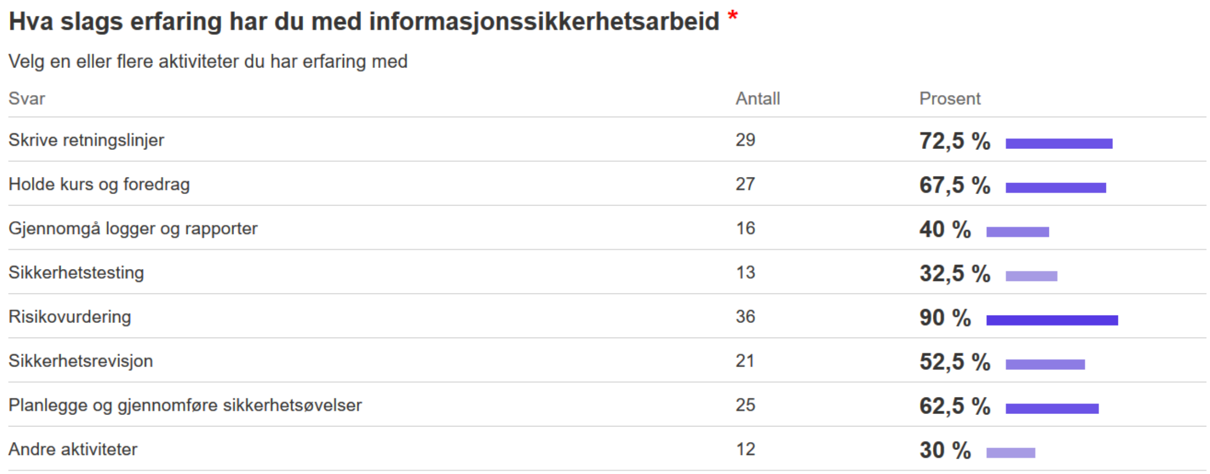
Svar	Antall	Prosent
Under 1 år	0	**0 %**
1-5 år	4	**10 %**
6-15 år	5	**12,5 %**
15-30 år	21	**52,5 %**
over 30 år	10	**25 %**



Hvor lang erfaring har du med informasjonssikkerhetsarbeid? *

Tilsammen eller sammenhengende

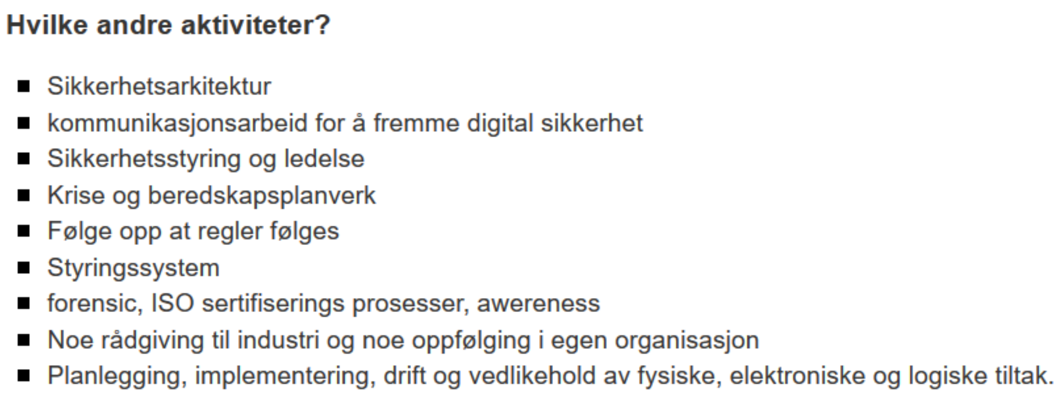
Svar	Antall	Prosent
Under 1 år	0	**0 %**
1-5 år	11	**27,5 %**
6-15 år	16	**40 %**
15-30 år	11	**27,5 %**
over 30 år	2	**5 %**



Hva slags erfaring har du med informasjonssikkerhetsarbeid *

Velg en eller flere aktiviteter du har erfaring med

Svar	Antall	Prosent
Skrive retningslinjer	29	**72,5 %**
Holde kurs og foredrag	27	**67,5 %**
Gjennomgå logger og rapporter	16	**40 %**
Sikkerhetstesting	13	**32,5 %**
Risikovurdering	36	**90 %**
Sikkerhetsrevisjon	21	**52,5 %**
Planlegge og gjennomføre sikkerhetsøvelser	25	**62,5 %**
Andre aktiviteter	12	**30 %**



Hvilke andre aktiviteter?

- Sikkerhetsarkitektur
- kommunikasjonsarbeid for å fremme digital sikkerhet
- Sikkerhetsstyring og ledelse
- Krise og beredskapsplanverk
- Følge opp at regler følges
- Styringssystem
- forensic, ISO sertifiserings prosesser, awereness
- Noe rådgiving til industri og noe oppfølging i egen organisasjon
- Planlegging, implementering, drift og vedlikehold av fysiske, elektroniske og logiske tiltak.

Om virksomheten du jobber i
Hvilken bransje hører virksomheten din til? *

Velg det alternativet som passer best

Svar	Antall	Prosent
Industri	1	**2,5 %**
Bygg/anlegg	0	**0 %**
Transport	1	**2,5 %**
Hotell/restaurant	0	**0 %**
Rådgiving/konsulent	5	**12,5 %**
Varehandel	2	**5 %**
Undervisning	1	**2,5 %**
Helse/omsorg	1	**2,5 %**
Kommunikasjon/IT	7	**17,5 %**
Velvære/Opplevelser	1	**2,5 %**
Bank/finans	3	**7,5 %**
Myndigheter	16	**40 %**
Olje/Energi	2	**5 %**
Skipsfart	0	**0 %**

Hvor stor er virksomheten du jobber i? *

Svar	Antall	Prosent
Under 10 ansatte	2	**5 %**
10-50 ansatte	5	**12,5 %**
50-100 ansatte	2	**5 %**
100-300 ansatte	3	**7,5 %**
Over 300 ansatte	28	**70 %**

Er virksomheten offentlig eller privat? *

Svar	Antall	Prosent
Offentlig	20	**50 %**
Privat	20	**50 %**

Om risikovurdering i virksomheten

Når deltok du sist på en risikovurdering? *

Svar	Antall	Prosent
Denne måneden	23	**57,5 %**
Dette året	11	**27,5 %**
1-2 år siden	4	**10 %**
Mer enn 2 år siden	2	**5 %**
Har aldri deltatt på risikouvurdering	0	**0 %**

Hvor mange deltok på risikovurderingen? *

Svar	Antall	Prosent
Færre enn 3 deltakere	5	**12,5 %**
3-6 deltakere	28	**70 %**
6-10 deltakere	7	**17,5 %**
Flere enn 10 deltakere	0	**0 %**

Hvor lang tid tok risikovurderingen

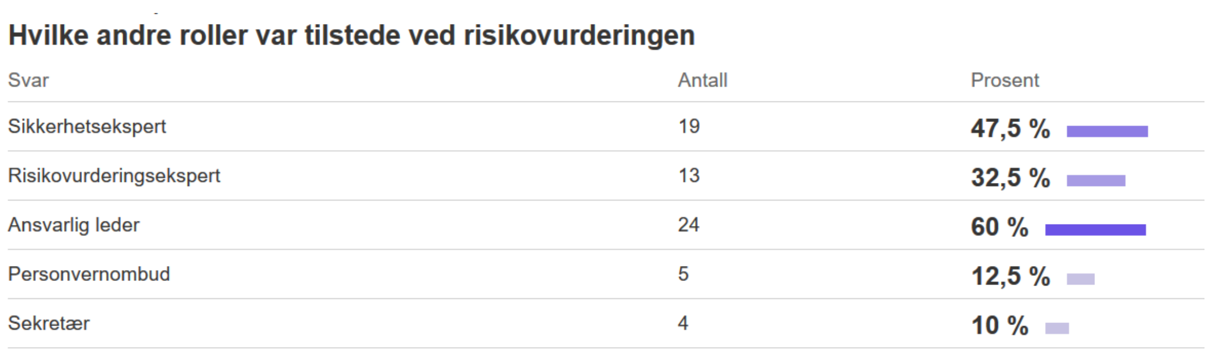
Svar	Antall	Prosent
Under 1 time	7	**17,5 %**
1-3 timer	8	**20 %**
3-6 timer	9	**22,5 %**
7-12 timer	1	**2,5 %**
Over12 timer	15	**37,5 %**

Hvilken rolle hadde du i risikovurderingen *

Svar	Antall	Prosent
Sikkerhetsekspert	18	**45 %**
Risikovurderingsekspert	11	**27,5 %**
Ansvarlig leder	7	**17,5 %**
Personvernombud	1	**2,5 %**
Sekretær	0	**0 %**
Annet	3	**7,5 %**

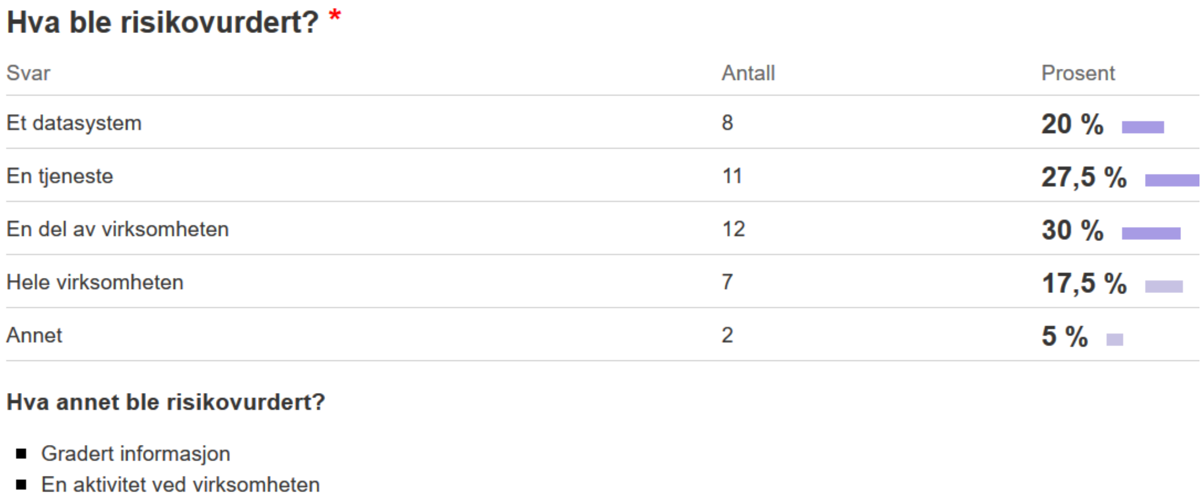
Hvilken rolle?

- Kommunikasjonsdirektør



Hvilke andre roller var tilstede ved risikovurderingen

Svar	Antall	Prosent
Sikkerhetsekspert	19	**47,5 %**
Risikovurderingsekspert	13	**32,5 %**
Ansvarlig leder	24	**60 %**
Personvernombud	5	**12,5 %**
Sekretær	4	**10 %**

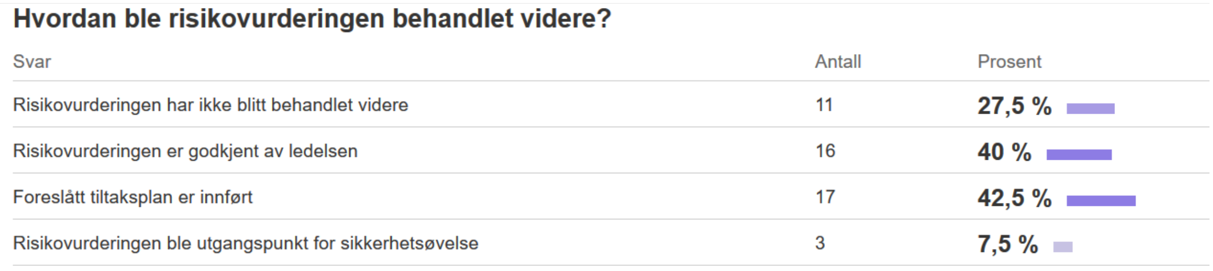


Hva ble risikovurdert? *

Svar	Antall	Prosent
Et datasystem	8	**20 %**
En tjeneste	11	**27,5 %**
En del av virksomheten	12	**30 %**
Hele virksomheten	7	**17,5 %**
Annet	2	**5 %**

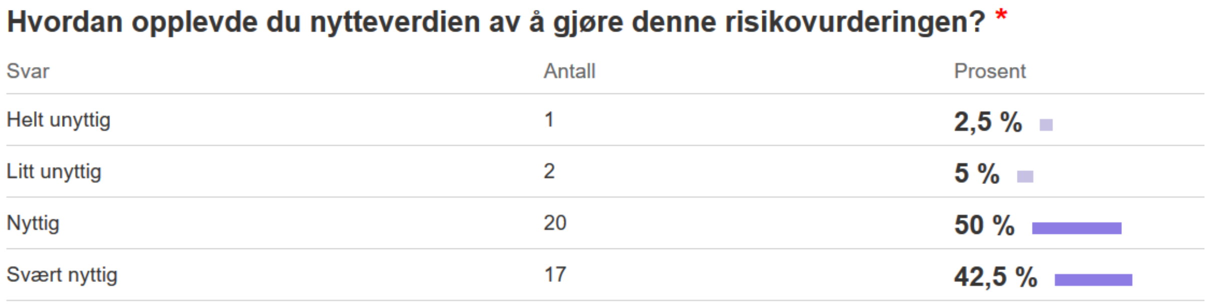
Hva annet ble risikovurdert?

- Gradert informasjon
- En aktivitet ved virksomheten



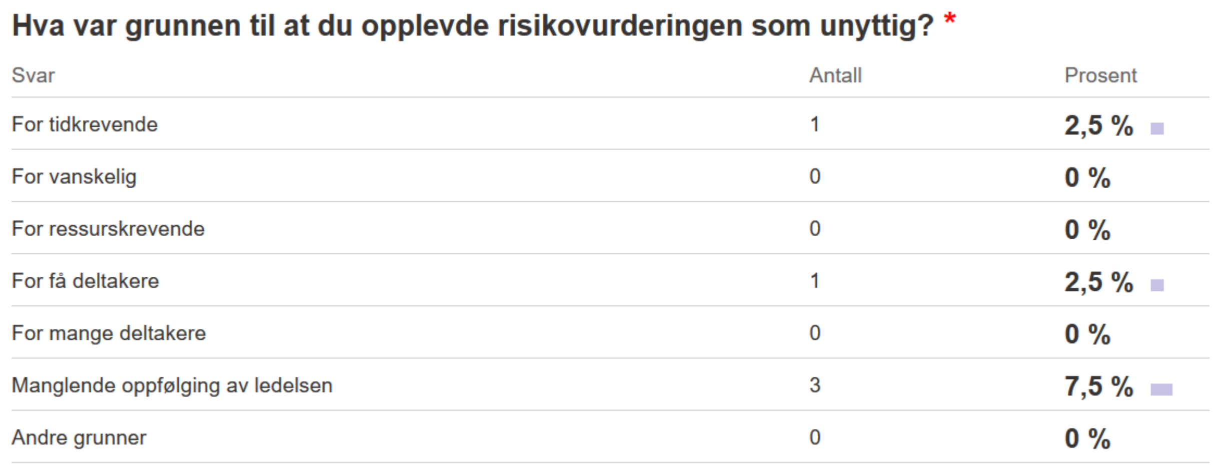
Hvordan ble risikovurderingen behandlet videre?

Svar	Antall	Prosent
Risikovurderingen har ikke blitt behandlet videre	11	**27,5 %**
Risikovurderingen er godkjent av ledelsen	16	**40 %**
Foreslått tiltaksplan er innført	17	**42,5 %**
Risikovurderingen ble utgangspunkt for sikkerhetsøvelse	3	**7,5 %**



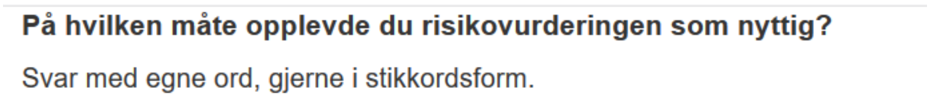
Hvordan opplevde du nytteverdien av å gjøre denne risikovurderingen? *

Svar	Antall	Prosent
Helt unyttig	1	**2,5 %**
Litt unyttig	2	**5 %**
Nyttig	20	**50 %**
Svært nyttig	17	**42,5 %**



Hva var grunnen til at du opplevde risikovurderingen som unyttig? *

Svar	Antall	Prosent
For tidkrevende	1	**2,5 %** ▪
For vanskelig	0	**0 %**
For ressurskrevende	0	**0 %**
For få deltakere	1	**2,5 %** ▪
For mange deltakere	0	**0 %**
Manglende oppfølging av ledelsen	3	**7,5 %** ▬
Andre grunner	0	**0 %**



På hvilken måte opplevde du risikovurderingen som nyttig?

Svar med egne ord, gjerne i stikkordsform.

- Dannet et beslutningsgrunnlag for risikoeiere
- Risiko og sikkerhetsarbeid skal ha med hele verdikjeden - og det å kommunisere intern og eksternt om dette på ulikt vis er viktig for å sikre etterevelse av tiltak
- Stegvis prosess. Flere korte møter. God forankring og forståelse hos ledelsen. Skille risikovurderingen fra beslutninger om tiltak. Vurderingen viktigere enn en stemmegivning. Mentometerknapper er gøy, men fungerer ikke uten at det har vært en diskusjon og presentasjon av potensielle risikofaktorer og hvorfor akkurat dette kan være en risiko.
- Klargjørende
- Man får frem beslutningsunderlag. Kunne være forberedt på uforutsette ting
- Gjennomfører teoretisk - med flere «øyne» Så gjennomfører det praktisk - finne feil/ mangler i det vi har gått igjennom. Se om vi har oversett noe.
- Felles forståelse. Oppklare regler og misforståelser. Sette fokus på sikkerhet
- Risikovurderinger- og styring er i min sektor først og fremst pålagt og forankret i både lov og organisasjon. Men det er også en veldig fornuftig aktivitet som kan spre gevinster til ulike områder.
- Har erfaring med å gjøre analyse, vurderinger og foreslå tiltak. Denne gangen fulgte jeg også opp drift av en operasjonell enhet. Observerte hvordan tiltak var blitt innført, sikkerhetskultur, hvordan de jobbet med det og observerte mangler ift bruk av ulike "installerte" barrierer. Gav tilbakemelding i form av en rapport med bilder på status, og hva som burde gjøres for å lukke observerte gap. Nyttig fordi: utførelsen og praktisk bruk av en risikovurdering er helt avgjørende for å hindre uønskede hendelser å skje. Min erfaring er at vi tillegger mye vekt på analyse, vurdering, foreslåtte tiltak, mens det er utførelsen som kan være den tyngste å få på plass. Utøvende enhet må ha eierskap og forståelse til risikovurderingen.
- Førte til kvalifisert beslutning.
- Dette var en realitetsorientering for bedriften, og en erkjennelse av risikovurdering var et forsømt område, som for fremtiden må prioriteres.
- En del av spørsmålene dine over mangler alternativer som gjør det vanskelig å få frem relevant informasjon. RV var nyttig fordi den skapte et bedre beslutningsgrunnlag innenfor et komplekst område.
- Nyttig for virksomheten å få denne gjennomført og dokumentert.
- Internt krav til alle IT-tjenester, skytjenester, og IT infrastruktur
- Vi fikk antakelser vi hadde bekreftet med faktainformasjon.
- Fikk belyst områder som krevde tiltak for å ha en tilfredstillende sikkerhet.
- For å tydeliggjøre hvilke konsekvenser det vil ha om noe går galt, samt hvilken plass i køen tjenesten bør ha om alt går galt og en må velge hvilke systemer/tjenester/løsninger som må prioriteres.

- De to siste store var å risikovurdere moskeer, planlagte tiltak er avhengig av offentlig støtte. Justisdepartementet ville aldri vurdert en søknad uten en risikovurdering.
- Ledelse har forståelse for sikkerheten rundt tjenesten.
- Bevisstgjøring av kolleger. Felles mental situasjonsforståelse.
- At flere spiller inn momenter rundt risiko, ikke kun personell som har sikkerhet som fag
- Risikovurderingen var nyttig, men virksomheten har begrenset forståelse for resultatene og behovet for tiltak.
- Grunnlag for å identifisere/ prioritere /verifisere tiltak Kommunikasjon Ledelseforankring
- Bevisstgjørende og avklarende særlig når det gjaldt trusselvurdering og verdivurdering
- Det ga en strukturert prosess hvor (Sikringsrisiko) analysen ga god oversikt og forståelse for verdier, trusler og sårbarhet i virksomheten, sammen med valg av ulike strategier og relevante tiltak.
- Den aktuelle vurderingen tar utgangspunkt i virksomhetens helhetlige risikoanalyse, og bidrar til å øke bevisstheten rundt verdier som berøres av enkelt-aktiviteter. Prosesseiere blir bevisst hvilke avhengigheter de har og hvilke sårbarheter de må håndtere.

Om risikovurderingsmetoder
Hvilket verktøy bruker dere for å gjennomføre risikovurderinger? *

Svar	Antall	Prosent
Excel-ark	14	**35 %**
Eget program/system på PC	6	**15 %**
Utfylling av skjema på papir	1	**2,5 %**
Egenutviklet skjema	19	**47,5 %**
Vet ikke	0	**0 %**

Hvordan definerer dere risiko i deres virksomhet? *

Svar	Antall	Prosent
Risiko = sannsynlighet x konsekvens	14	**35 %**
Risiko = sårbarhet x trussel x verdi	8	**20 %**
Risiko = Verdi x trussel x sårbarhet x konsekvens for organisasjonen	8	**20 %**
Risiko = sannsynlighet x konsekvens x sårbarhet x effektens hastighet	0	**0 %**
Risiko = f(verdi, trussel, sårbarhet)	6	**15 %**
Risiko = f(sikkerhetskrav, trussel)	0	**0 %**
Annet	4	**10 %**

Hvilken annen definisjon av risiko bruker deres virksomhet

- Vi skiller på natur- og tilsiktede hendelser og benytter dertil egnet modell.
- Det avhenger av analyse. Security, blir det gjerne R = en kvalitativ funksjon av V, T og Sårbarhet. Ellers defenerer vi stort sett R = usikkerheten knyttet til en konsekvens.
- trussel - sårbarhet - konsekvens
- Kan ikke velge enten eller på dette spørsmålet. Vi bruker både to-faktor og trefaktor i min virksomhet, samt andre modeller avhengig av behov

Hvordan finner dere sannsynlighet i risikovurderingen *

Svar	Antall	Prosent
Det er ikke relevant	4	**10 %**
Antall hendelser i året/måneden/uka	11	**27,5 %**
Trusselaktørens kapasitet x sårbarhet	7	**17,5 %**
Sannsynlighet er en slags prosentregning	0	**0 %**
Systemet finner sannsynligheten	1	**2,5 %**
Sannsynlighet for initiativ x trusselens styrke x tiltakets styrke	5	**12,5 %**
Annen måte	12	**30 %**

Hvilken annen måte?

- flere av disse, avhengig av type
- Varierer. Men stort sett er sannsynlighet kunnskapsbasert kvalitativ vurdering. Men for enkelte hendelse kan man bruke statistikk/erfaring.
- Gjennom avvik, rapportering og ansatte sine tilbakemeldinger
- Erfaringsbasert synsing
- En skjønnsmessig subjektiv vurdering av 1) modus operandi og 2) målvalg. Sannsynlighet brukes indirekte for å redusere antall scenarioer som skal vurderes. Sannsynlighet brukes ikke i beskrivelsen av risiko
- kommer an på hvilken type analyse som gjennomføres
- Kombinasjon av flere vurderinger, slik som kapasitet, sårbarhet, geopolitisk situasjon, etc.
- kvalitativt
- PST Trusselvurdeing Ugradert/KONFIDENSIELT
- Sannsynlighet, konsekvens og usikkerhet (kunnskapsstyrke)
- Sammen med selve risikovurderingen, legger vi også ved grunnfrekvenser for hvor ofte cenarioet inntreffer nasjonalt.
- Sannsynlighet behandles som et uttrykk for usikkerhet knyttet til den enkelte risiko. Sannsynlighet vil som regel ikke være relevant i seg selv, da konsekvensen må være hovedkriterie, men graden av usikkerhet sier noe om hvor mye vi må jobbe med sårbarhetene.

Hvordan finner dere aktuelle trusler? *

Svar	Antall	Prosent
Vi drøfter tidligere hendelser i organisasjonen	5	**12,5 %**
Vi utformer trusselscenarier basert på skjemaet i risikovurderingsmetoden	16	**40 %**
De er definert i systemet for risikovurdering	3	**7,5 %**
Vi bruker Enisas, Norsis og NSMs rapport over trusler og sårbarheter	5	**12,5 %**
Annen måte	11	**27,5 %**

Hvilken annen måte

- Trusselbildet, tidligere hendelser med mer.
- Egen enhet ansvarlig for trusseletterretning
- Gradert informasjon.
- Etterretning: innhenter informasjon om alle relevante forhold som, tidligere hendelser (egne og andres), vurdering av hvem som kan ha direkte/indirekte interesse av å ramme våre verdier.
- Alle beskrevet over
- Trusselvurdering
- Vi baserer oss på Nordic Financial CERT trusselrapporter
- PST Trusselvurdeing Ugradert/KONFIDENSIELT
- når de skjer.
- Rapporter fra PST, POD, E-tjenesten, Fylkesmannen m.fl.
- Basert på egne, eller innhentede trusselvurderinger, utarbeider vi trusselscenarier

Hvilke risikovurderingsmetoder er du kjent med?

Her er en liste over de mest kjente risikovurderingsmetodene. Vennligst angi hvor godt du kjenner til dem.

Svar fordelt på antall

	Er ikke kjent med metoden	Har hørt om metoden men bruker den ikke	Har brukt denne metoden tidligere	Bruker elementer fra metoden	Foretrekker å bruke denne metoden
Octave *	29	10	1	0	0
CRAMM *	32	8	0	0	0
NSM *	8	7	4	17	4
TRA *	34	5	1	0	0
NIST 800-37 *	21	10	0	8	1
EBIOS *	35	5	0	0	0
Mehari *	36	4	0	0	0
COSO *	23	12	2	3	0
IRAM2 *	27	10	1	2	0
ISO/IEC 27005 *	7	7	3	14	9

Svar fordelt på prosent

	Er ikke kjent med metoden	Har hørt om metoden men bruker den ikke	Har brukt denne metoden tidligere	Bruker elementer fra metoden	Foretrekker å bruke denne metoden
Octave *	72,5 %	25 %	2,5 %	0 %	0 %
CRAMM *	80 %	20 %	0 %	0 %	0 %
NSM *	20 %	17,5 %	10 %	42,5 %	10 %
TRA *	85 %	12,5 %	2,5 %	0 %	0 %
NIST 800-37 *	52,5 %	25 %	0 %	20 %	2,5 %
EBIOS *	87,5 %	12,5 %	0 %	0 %	0 %
Mehari *	90 %	10 %	0 %	0 %	0 %
COSO *	57,5 %	30 %	5 %	7,5 %	0 %
IRAM2 *	67,5 %	25 %	2,5 %	5 %	0 %
ISO/IEC 27005 *	17,5 %	17,5 %	7,5 %	35 %	22,5 %

Om Hendelser
Har virksomheten opplevd noen informasjonssikkerhetshendelser eller avvik de siste 3 årene?

Svar	Antall	Prosent
Ja	26	**65 %**
Nei	8	**20 %**
Vet ikke	6	**15 %**

Hvor alvorlig var hendelsen?

Svar	Antall	Prosent
Helt ubetydelig	1	**4 %**
Ikke så alvorlig	12	**48 %**
Alvorlig	12	**48 %**
Svært alvorlig	0	**0 %**

Hva førte hendelsen til?

Svar	Antall	Prosent
Data gikk tapt eller ble kryptert	2	**5 %**
Konfidensiell informasjon ble kjent for uvedkomne	9	**22,5 %**
Nettverk eller sentrale systemer ble utilgjengelig over tid	9	**22,5 %**
Viktig informasjon ble endret av uvedkomne	1	**2,5 %**
Dårlig omdømme for virksomheten	5	**12,5 %**
Tapte kontrakter og anbud	0	**0 %**
Tap av arbeidstid og arbeidsfortjeneste	9	**22,5 %**
Tap av liv eller helse	1	**2,5 %**

Hvor godt forberedt var dere på hendelsen som inntraff?

Svar	Antall	Prosent
Svært dårlig forberedt	2	**8 %**
Litt dårlig forberedt	9	**36 %**
Godt forberedt	12	**48 %**
Svært godt forberedt	2	**8 %**

Om nytteverdien av risikovurderinger
Hva mener du er den største nytteverdien av å gjøre risikovurderinger? *

Svar	Antall	Prosent
Har ingen nytteverdi	0	**0 %**
Vi blir bevisst på informasjonssikkerheten	15	**37,5 %**
Vi setter inn tiltak for å unngå hendelser	15	**37,5 %**
Vi setter inn tiltak for å begrense skadene	3	**7,5 %**
Vi kutter kostnadene til unødvendige tiltak	0	**0 %**
Vi gjør sikkerhetsøvelser på relevante hendelser	3	**7,5 %**
Vi handler i tråd med lovverket	0	**0 %**
Annet	4	**10 %**

Hvilken annen nytteverdi?

- flere av disse
- Opplyser en beslutningsprosess slik at gode beslutninger kan tas knyttet til avveininger mellom sikkerhet og andre hensyn.
- Å få grunnlag for å prioritere tiltak (kost/nytte), samt gi oversikt over restrisiko.
- Vi sørger for at virksomheten kan løse oppdraget sitt

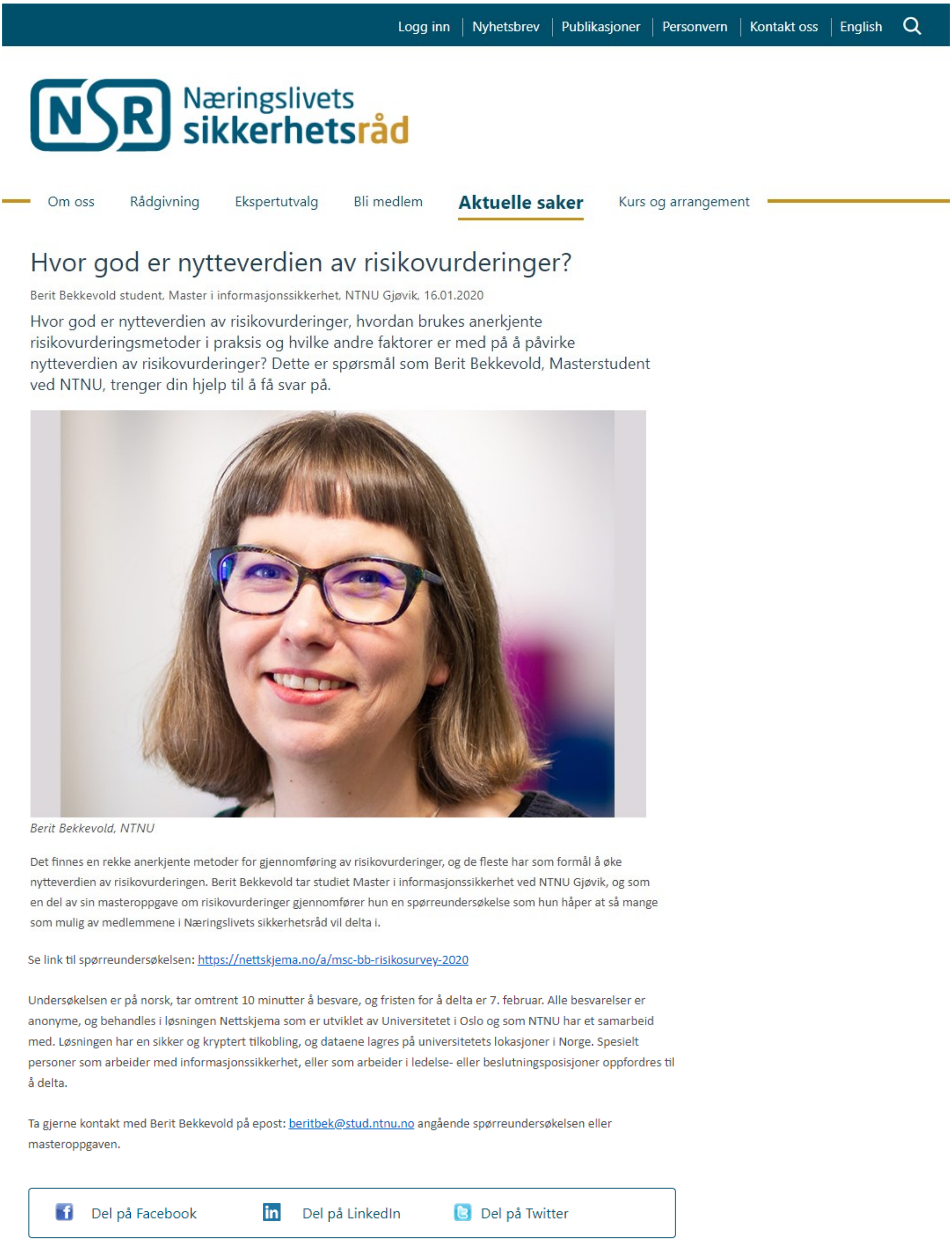
Hva mener du er de tre viktigste suksesskriteriene for risikovurderinger? *

Svar	Antall	Prosent
At risikovurderingen tar kort tid	1	2,5 %
At noen av deltakerne har erfaring med risikovurdering	14	35 %
At vi har forberedt oss godt	6	15 %
At lederen deltar på risikovurderingen	15	37,5 %
At forslagene til tiltak blir fulgt opp	27	67,5 %
At vi bruker en god metode for risikovurdering	18	45 %
At alle deltakere kjenner trusselbildet	11	27,5 %
At det er servering på møtet	0	0 %
At vi bruker et system for risikovurdering	9	22,5 %
Annet	4	10 %

Hvilket annet suksesskriterie for risikovurdering?

- kjennskap til truslene, kjennskap til verdiene, kjennskap til sårbarhetene, eierforrankring, kompetent analysegruppe, transperens, kritisk tenkning og tverrfaglighet
- At risikovurderingen brukes aktivt i virksomhetens risikostyring (ikke bare at tiltak blir fulgt opp)
- Strukturert prosess og fasilitering av noen som kan metoden
- 1. At ledelsen (CEO) tar eierskap. 2. En verdivurdering som involverer hele linjeorganisasjonen. 3. Bruk en metode de ansatte forstår og evner å delta i.

Attachment 4: Screenshot of article from NSR website



Hvor god er nytteverdien av risikovurderinger?

Berit Bekkevold student, Master i informasjonssikkerhet, NTNU Gjøvik, 16.01.2020

Hvor god er nytteverdien av risikovurderinger, hvordan brukes anerkjente risikovurderingsmetoder i praksis og hvilke andre faktorer er med på å påvirke nytteverdien av risikovurderinger? Dette er spørsmål som Berit Bekkevold, Masterstudent ved NTNU, trenger din hjelp til å få svar på.

Berit Bekkevold, NTNU

Det finnes en rekke anerkjente metoder for gjennomføring av risikovurderinger, og de fleste har som formål å øke nytteverdien av risikovurderingen. Berit Bekkevold tar studiet Master i informasjonssikkerhet ved NTNU Gjøvik, og som en del av sin masteroppgave om risikovurderinger gjennomfører hun en spørreundersøkelse som hun håper at så mange som mulig av medlemmene i Næringslivets sikkerhetsråd vil delta i.

Se link til spørreundersøkelsen: https://nettskjema.no/a/msc-bb-risikosurvey-2020

Undersøkelsen er på norsk, tar omtrent 10 minutter å besvare, og fristen for å delta er 7. februar. Alle besvarelser er anonyme, og behandles i løsningen Nettskjema som er utviklet av Universitetet i Oslo og som NTNU har et samarbeid med. Løsningen har en sikker og kryptert tilkobling, og dataene lagres på universitetets lokasjoner i Norge. Spesielt personer som arbeider med informasjonssikkerhet, eller som arbeider i ledelse- eller beslutningsposisjoner oppfordres til å delta.

Ta gjerne kontakt med Berit Bekkevold på epost: beritbek@stud.ntnu.no angående spørreundersøkelsen eller masteroppgaven.

Attachment 5: UTF-report from survey

See file.