Assessing Information Security Risks of AMI
What Makes it so Difficult?

Inger Anne Tøndel, Maria B. Line and Gorm Johansen
SINTEF ICT, Trondheim, Norway

Keywords: Advanced Metering Infrastructure, Information Security, Risk Assessment.

Abstract: A rich selection of methods for information security risk assessments exist, but few studies evaluate how such methods are used, their perceived ease-of-use, and whether additional support is needed. Distribution system operators (DSOs) find it difficult to perform information security risk assessments of Advanced Metering Infrastructure (AMI). We have performed a case study in order to identify these difficulties and the reasons for them. Our findings indicate that the risk assessment method in itself is not the main challenge. The difficulties regard competence; more specifically, insight in possible information security threats and vulnerabilities, being able to foresee consequences, and making educated guesses about probability. Improved guidelines can be a valuable aid, but including information security experts as participants in the process is even more important.

1 INTRODUCTION

Risk assessments are an essential part of the overall work on information security[1] in organisations. During a risk assessment process an organisation's key assets are identified, potential threats and vulnerabilities are evaluated, and the probability and consequences that the assets are harmed in potential incidents are estimated. Knowledge of which assets that need to be protected and the level of threat experienced is essential in order to achieve cost-efficient security.

Several research papers propose new and improved information security risk assessment methods, but few provide systematic evaluations of such methods or compare methods based on empirical studies (Sulaman et al., 2013). Limited information is available on how organisations perform risk assessments and their key challenges. This paper contributes to improved understanding of the challenges faced for one specific type of system: Advanced Metering Infrastructure (AMI)[2].

For Distribution System Operators (DSOs), the introduction of AMI represents a shift in technology towards increased use and dependence on Information and Communication Technology (ICT). This shift provides us the opportunity to study challenges that DSOs face when introducing new information security and privacy risks in their risk assessments. Regulations (NVE, 2013) require DSOs to secure their systems, including communication infrastructures, from unauthorized access. Each DSO is advised to perform a risk assessment of AMI (Skapalen and Jonassen, 2013). Even though the DSOs are used to perform risk assessments in several areas, we experience that they ask for assistance and aid in performing risk assessments of AMI. Several of these DSOs are small organizations with limited resources to perform these sorts of activities.

As part of the national research project DeVID[3], we have developed a guideline for information security risk assessments of AMI that describes the high-level process and provides support material (Line et al., 2013). This guideline builds on existing national and international risk assessment guidelines and standards, and in particular a general risk assessment guideline provided by NVE (NVE, 2010). Main additions to this national guideline include:

- Emphasising information security and privacy as a topic worthy of special attention, possibly in a separate risk assessment.
- Recommending that assets are identified prior to the identification of unwanted incidents.
- Providing support material in form of checklists

[1] Information security concerns preservation of confidentiality, integrity, and availability (ISO/IEC, 2005).

[2] AMI is also commonly referred to as *smart meters*.

[3] DeVID is partly funded by the Research Council of Norway, grant no 217528, http://www.sintef.no/Projectweb/DeVID/

Tøndel I., Line M. and Johansen G..
Assessing Information Security Risks of AMI - What Makes it so Difficult?.
DOI: 10.5220/0005228900560063
In *Proceedings of the 1st International Conference on Information Systems Security and Privacy* (ICISSP-2015), pages 56-63
ISBN: 978-989-758-081-9

that provide an overview of relevant assets, incidents and countermeasures when it comes to information security and privacy in AMI.

To evaluate our guideline, we have studied risk assessments performed by Norwegian DSOs. Our study was motivated by the following research questions:

- *RQ 1:* Why do DSOs state that assessing risks in AMI is difficult, i.e. what makes AMI so different from other objects that DSOs are already assessing the risks of?
- *RQ 2:* How well does our guideline support the DSOs when assessing the risks of AMI?

This paper is structured as follows. Section 2 presents related work on methods for risk assessment. The research method for our study is described in Section 3, and findings from the documentation study, interviews, and participant-observations are summarised in Sections 4, 5, and 6, respectively. Section 7 discusses the results, and Section 8 provides concluding remarks.

2 RISK ASSESSMENTS

A large number of standards, guidelines and research papers suggest different methods for risk assessments. Though they have their differences, the methods tend to include similar steps: characterisation of the system, threat and vulnerability assessment, risk determination, control identification, and evaluation and implementation of controls (Fenz and Ekelhart, 2011; ISO/IEC, 2011a). There is however limited empirical evidence regarding how the available standards and guidelines are used and what kind of support is considered most important. In a study by Jourdan et al. (Jourdan et al., 2010) 25% of information security professionals stated that risk analyses were actually never, or at best rarely, performed. Shedden et al. (Shedden et al., 2010) concluded that the risk assessment standards are not easy to use, and that they are actually difficult to comprehend and understand.

In 1999, the United States General Accounting Office (GAO) performed a study of information security risk assessment methods in four organisations (GAO, 1999). These organisations had organisation-wide information security risk procedures that were considered practical and useful, and they had used these procedures for at least one year. The study identified critical success factors for efficient and effective implementation of information security risk assessment programs:

- Obtain senior management support and involvement
- Designate focal points
- Define procedures
- Involve business and technical experts
- Hold business units responsible
- Limit scope of individual assessments
- Document and maintain results

The main challenges identified were related to estimation of likelihood and cost of information security risks. It was claimed that it is more challenging to reliably assess information security risks than other types of risks. This has to do with limited data available, as well as constantly changing risk factors. This challenge has also been put forward by other researchers (Fenz and Ekelhart, 2011; Cybenko, 2006; Gerber and von Solms, 2005; Rhee et al., 2012), who added that information is an intangible asset where it is *"extremely difficult if not impossible to determine precise value"* (Gerber and von Solms, 2005), and that the current situation is that *"many losses are never discovered and others are never reported"* (Rhee et al., 2012). Although this lack of information was considered a challenge, the organisations in the GAO study did not believe this to preclude understanding and ranking of information security risks.

3 METHOD

To address the research questions, we performed a case study (Yin, 2009), where information was collected through documentation, interviews and participant-observation. This choice of research method was guided by our goal to improve understanding of why information security risk assessments are considered difficult (RQ1). We aimed at opinions and experiences that can improve future improvements in guidelines and other support initiatives (RQ2), rather than statistically significant results. We compared the results from two different types of risk assessments:

A. Risk assessments of AMI performed by the DSOs before our study started *without the support of our guideline* (assessments A1-A3). Process leaders were interviewed.

B. Risk assessments where we took part as process leaders and brought expertise to the assessments by *extensive use of our guideline* (assessments B1-B2).

Table 1: An overview of the risk assessments.

Case	DSO	Status of assessment	Process leader	Material received	Role of interviewee	Other participants in the process
A1	1	In progress	Internal	Documented risk matrices	Proj.mgr AMI/ process leader	Communications, IT, IT manager, AMI, consultants
A2	2	Completed	Consultant	Final report and risk matrices	Proj.mgr AMI	Technical, specialists, commercial; AMI and IT
A3	3	Completed	Internal	Final report and risk matrices	Grid analyses/ process leader and infosec officer	AMI, IT
B1	4	Completed	We	(na)	(na)	IT, IT security, automation systems, AMI
B2	3	Completed	We	(na)	(na)	IT security, AMI owner, AMI responsible, technical experts

3.1 Development of Guideline

The Norwegian Water Resources and Energy Directorate (NVE) have provided recommendations on general risk assessments for the Norwegian energy domain (NVE, 2010). They have organised the risk assessment activities in three phases: The *planning phase* (system characterisation, determining the scope, the likelihood scale, and consequence dimensions; organising the risk assessment phase, preparing checklists), the *risk assessment phase* (threat and vulnerability assessments and risk determination, control identification activities; presentation of results in a risk matrix), and the *risk treatment phase* (selecting controls and following up on implementation).

As these recommendations are already well-established in the energy domain, we aimed at extending these rather than developing some brand new and completely different methods. Therefore, our guideline (Line et al., 2013) follows the same structure as this existing guideline from NVE, with one important addition: We recommend to start the risk assessment phase by identifying information assets. This is motivated by recommendations in recognised risk management guidelines in the information security field, such as OCTAVE Allegro (Caralli et al., 2007). Furthermore, we provide explanations to several of the activities recommended by NVE, specifically tailored to information security needs. Checklists present possible system characterizations (for AMI), information assets, incident categories (based on ISO/IEC 27035 (ISO/IEC, 2011b)) and specific incidents, stakeholders, vulnerabilities (based on NISTIR 7628 (Group, 2010)), and countermeasures (based on ISO/IEC 27001 (ISO/IEC, 2005)). Our guideline introduces methods for information security threat modelling as well, but these were not evaluated in the case study.

Our guideline has been developed with the aim of supporting a lightweight risk assessment process that does not require an extensive amount of resources in time or personnel, as several Norwegian DSOs are small and have limited resources available for this type of activities.

3.2 Case Study Context

An overview of the different cases studied is shown in Table 1. The four participating DSOs were recruited from the DeVID project consortium[4]. The scope of the risk assessments A1-A3 were the overall project of *implementing* AMI. This includes financial, operational, and customer aspects, in addition to information security and privacy aspects, which then constitutes just a minor part of the complete analysis. Assessments B1-B2 considered information security and privacy risks in the AMI.

Note that assessment A1 was in progress. They had identified several incidents, but the identification of incidents were not completed, and further assessments of the risk associated with the incidents were in some cases missing. Though assessment A2 was considered to be finished, the accompanying documents specifically stated that further work included assessing likelihood and consequences of incidents, suggesting that the provided risk values are initial values only.

For assessments B1 and B2, expertise within IT, IT security, automation systems, and AMI, participated from each DSO (3, 4, c.f. Table 1). After agreeing on the scope of the assessment and ensuring a common understanding of the system, the participants engaged in brainstorming sessions to identify assets,

[4] One DSO contributed to two different assessments; A3 and B2. They had already performed one risk assessment without the use of our guideline, and we were used as process leaders in a second risk assessment with a different scope than the first one.

stakeholders and incidents. The group then assessed the risks of the identified incidents and discussed relevant controls for some of the high-risk incidents. For B1, some relevant controls were added by the participating researchers after the risk assessment session. Around-the-table evaluations concluded each workshop, where each participant reported his opinion on what was successful, what was difficult and/or did not succeed during the day. Two researchers participated in both assessments[5], and results of the assessments as well as participant evaluations were documented by the researchers.

4 FINDINGS FROM THE DOCUMENTATION STUDY

In this section we provide an overview of the risks assessments A1-A3 with respect to incident types, assets covered, estimated risk and the controls identified. Note that in the tables that provide an overview of the incident types and controls, the results from the assessments B1-B2 are also included to enable comparisons.

4.1 Types of Incidents Covered and Level of Detail

Table 2 provides an overview of the incidents identified in all assessments, categorised according to ISO/IEC 27035. In general, risks from a broad range of incident categories are included. However, the risk categories ”Technical failure”, ”Technical attack” and ”Compromise of information” receive the most attention. Note that several of the incidents have been placed in more than one category, as for example an information compromise can have a technical cause due to failure or an active attack.

Some of the incidents represent lack of routines, or weaknesses in routines, that do not necessarily lead to information security breaches in the short term, as *Lack of overview of AMI components* and *Lack of control of collected meter values* are examples of. The DSOs are worried that the complexity of systems might lead to a lack of competence and overview that can lead to incidents on a long term.

Most analyses (A1-A3, B2) are performed at the strategic stage of the AMI, hence the DSOs do not know yet what the system will look like. The threats are in general at a high level (e.g. someone will hack something, or someone gets access to communication).

4.2 Types of Assets Covered

In general, assets are not documented, although in some cases specific assets are mentioned in descriptions of incidents:

- Meter values providing information about power consumption, and used as a basis for invoice (C, I, A[6])
- The meter itself (I, A)
- The communication network (A)
- The HES and other systems at the DSO (I, A)
- Breaker commands (I, A)
- Meter updates (A)

Incidents can however impact other assets than those that are specifically mentioned. As an example, inability to communicate with meters impacts the availability of meter values, but it also impacts the ability to send commands, collect status information and to perform software updates. In several cases, the incident is not related to any specific asset in particular, e.g. *New technology - a lot of startup problems*.

4.3 Estimated Risk

In A3, consequences of incidents are assessed due to their impact on reliability of supply, privacy, economy and reputation. Probabilities are also assessed due to predefined criteria. In A1 and A2 however, it is not clear which criteria are used in the assessment of consequences and probabilities.

In A2, few incidents related to information security and privacy are assessed to be of high risk. These have to do with insufficient quality in the equipment delivered by vendors. In A3 several incidents are considered high risk when it comes to economy and reputation impacts. These have to do with lack of communication, meter errors, immature metering technology, lack of control with collected meter values, privacy breaches, IT system failure, and loss of control over control systems. In A1, some of the incidents are assigned a consequence and probability rating, but none of the incidents are categorised as low, medium, or high risk or put into any form of risk matrix.

4.4 Controls Identified

There are large differences in which controls are included and how they are presented in the different

[5] One researcher leading the process (assessment B1: MBL; assessment B2: IAT) and one documenting the results (GJ).

[6] C: confidentiality, I: integrity, A: availability

Table 2: Types of incidents identified in the risk assessments.

Category	*A1*	*A2*	*A3*	*B1*	*B2*	*Examples of incidents covered*
Natural disaster	1	1	0	0	0	Equipment damage due to extreme weather conditions
Social unrest	1	0	0	0	0	Equipment destroyed due to war activities
Physical damage	2	2	1	1	1	Substation break-in; Customer destroys meter by accident; Customer vandalises meter
Infrastructure failure	5	2	2	3	0	Instability in communication (e.g. in the GPRS network); Lack of communication between smart meter and HES; Power stability problems
Radiation disturbance	2	0	0	0	0	Power instability problems; EMP
Technical failure	7	3	9	2	2	Existing system cannot handle increased data load; Encryption reduces performance of solution; Software updates corrupted; Meter failure; Meter lifetime shorter than expected
Malware	1	1	0	1	0	Customer infects the AMI system with malware, e.g. to manipulate own energy consumption values
Technical attack	7	4	3	3	2	Software updates corrupted; HES is compromised; Meter is compromised; Competitor attack on product/system/data; Erroneous deactivation of power (breaker command) for several customers
Breach of rule	1	1	0	2	2	Insiders get access to systems; Insiders manipulate own energy consumption values
Compromise of functions	2	2	4	2	3	Insiders get access to the system; Vendor misuses access rights to manipulate energy consumption or increase their competitive advantage; Criminals pretend to be meter installers
Compromise of information	6	3	2	8	3	Manipulation of information during communication; Eavesdropping; Customers manipulate own meter values; Wrong price information to customer; Documentation, maps, passwords, keys astray
Harmful contents	0	0	0	0	1	Reactivation of power (breaker command) causes equipment failure or fire at customer
Other	0	2	0	2	1	Lack of info on suppliers' security and privacy practices; Customer does not accept collected meter values

risk assessments. A1 seem to have a balance between procedural (organisation and personnel) and technical (physical measures and infrastructure) controls. In A2, controls are identified for all critical incidents, although few technical measures are identified and they were not precise (e.g. *Addressed by the IT department*). We did not have access to A3's list of controls, only the figures in their summary, which shows that procedural controls are given priority.

Table 3 shows the number of procedural and technical controls identified in the five risk assessments respectively. Due to different presentations of the controls in the different assessments, the numbers are not comparable. However, the relation between procedural and technical controls are comparable for each assessment.

Table 3: Types of controls identified.

Category	**A1**	**A2**	**A3**	**B1**	**B2**
Procedures	32	58	4	8	21
Technical	58	8	1	12	18

5 EXPERIENCES AS REPORTED IN THE INTERVIEWS

5.1 Sources of Information

The guideline from NVE (NVE, 2010) was mentioned by A1 and A2 as being used during the risk assessment process as a support, inspiration, and knowledge base. Further, two different publicly available risk assessments was considered in A1 to be useful support on on how to systemise the process. A2 referred to a seminar on information security in AMI. All three respondents (A1, A2, A3) reported having used a general risk assessment for the introduction of AMI from Energi Norge AS (EnergiNorgeAS, 2012) as a basis.

A1 reported that there is a lack of information on actual experiences with information security incidents related to AMI. They hired an external consultant towards the end to get help with identifying risks within the area of IT and IT security.

The external consultants leading the process in A2 used an extensive checklist to make sure they included all necessary aspects. This checklist was perceived as comprehensive and sufficient. A2 stated that several guidelines and related reports were published in the industry during their process. This was perceived as confusing, as the recommendations were vague and uncoordinated.

A3 successfully relied on the knowledge of the well-experienced personnel participating in the process. External information sources were not used. However, they are familiar with recent risk assessment reports made publicly available and the guideline from the authorities.

5.2 Challenges Regarding Information Security and Privacy

A2 described the area of information security and privacy as extremely technological and difficult to fully grasp. Specialists are needed, who understand the technical aspects and all possibilities regarding vulnerabilities, attacks, and potential consequences. Identifying incidents are not too difficult; e.g. *Someone hacks into the system*, *Breach of confidentiality*, but finding appropriate countermeasures is difficult without having competent specialists in the team.

A1 responded that identifying all possible incidents felt like a challenge, partly due to the fact that AMI is new and there might be aspects that are difficult to foresee. They see that cooperating with other DSOs in exchanging experiences on incidents could be useful. Also, A1 found it challenging to estimate probabilities and possible consequences of incidents. The worst consequences might have extremely low probability for occurring, which makes it hard to know whether they should be included or not. Statistics from previous incidents are not available, and estimating what are the real and realistic risks is perceived as quite hard. The possibilities seem infinite.

5.3 Needs for Support

A1 would like to have a kind of recipe which guides them through the whole risk assessment process. They also wish for information on realistic probabilities and possible consequences, not only unwanted incidents. Knowledge and understanding of appropriate countermeasures are needed; as the DSO specifies system requirements for the suppliers and leave to the suppliers to describe how they address the requirements, the DSO is left with the challenge of considering the appropriateness of the suppliers' solutions.

A2, on the other side, did not feel the need for any other support than what is already available. They have an internal risk assessment method and they feel satisfied with the work they did, as they have specified all requirements regarding information security and privacy. The most important thing is to include the right people in the process, those who have the right competence and knowledge in order to identify where the risks are and which countermeasures should be implemented.

A3 asked for necessary and basic templates for risk assessments. Bullet lists suggesting countermeasures would be useful in that the DSOs could make selections based on their own needs.

6 PARTICIPANT OBSERVATIONS

In the risk assessments, several of the incidents identified (see Table 2) were considered to be of high risk. When it comes to reliability of supply, B1 considered virus infection, unauthorised access to breaker functionality and external control over network functions to be main risks. In addition to unauthorised control of breakers and other main systems, B2 considered firmware errors in breakers and damage (e.g. due to fire) to main systems to be of high risk. B1 assessed privacy consequences of incidents, and identified virus infections, as well as access to meter values for individuals to be of high risk in this respect. B2 assessed consequences regarding economy and reputation, and identified considered incidents regarding leakage of personal information, and also meter hacking and meter value manipulation to be important in this respect, in addition to the incidents that were estimated as high risk when it comes to reliability of supply.

In both B1 and B2 a large set of information assets were identified, but the cases did make similar priorities regarding the importance of the assets; meter value (meter ID and corresponding customer), power switch (possibility to affect power supply), and encryption keys (encryption keys and passwords) were given highest priority.

In the risk assessment process, we encountered challenges regarding system documentation. There was a need for assumptions as it was almost impossible to be sure of all details in the system. For B2, this was particularly a challenge, as the risk assessment considered a future implementation of AMI. In general, it is not a problem to make assumptions as long as all assumptions are well documented and actions are agreed upon in order to investigate further details after the workshop.

Initially, we planned to spend one day on each risk assessment process. However, B1 showed that two half days could be more appropriate. It was found to be difficult to identify all system properties in advance. The discussions in the meeting revealed aspects that should have been better investigated or documented. Further, the five hours assigned for the assessment was found not to be enough. Most people would find it easier to spend two half work-days than one whole day due to other pressing tasks. Also, having two half days would give room for processing some of the information before completing the work.

The checklists were used towards the end of each brainstorming session to make sure that we included all relevant issues. We did not present them to the participants before the brainstormings; this could have reduced the number and variety of issues identified during the creative process. The use of checklists did result in some additions to the lists of both assets and incidents.

In B2, risks per consequence dimension were discussed in smaller groups before risks were agreed on in a plenary discussion. This was considered valuable for the results as differing opinions became visible; the participants had made different assessments of the threats and thus the discussion could focus on these differences.

The feedback in the end of the workshops were in general positive. However, several participants indicated that the method should have been presented more clearly. Although we explained it at the beginning of the workshop to make all participants familiar with the intended work flow, we should have put more effort into explaining each step as the workshop evolved. They found it somewhat confusing to follow the steps during the process, although they considered the process leader as key to what they perceived as a successful session. The participants reported that assessing a future system, where the technical details are yet unknown, was challenging. Furthermore, both analyses considered AMI and adjacent ICT systems, which was perceived to be a too wide focus for experts familiar with parts of the system only. At the same time, participants considered this multidisciplinarity to be a strength.

7 DISCUSSION

We started out with the aim to investigate why risk assessments of AMI related to information security was considered difficult (RQ1) and to study whether the guideline we had developed would provide support to DSOs in this respect (RQ2). The interviews performed regarding the assessments A1-A3 point to lack of experiences, statistics and examples as a main challenge. As a consequence, estimation of probabilities is difficult. Information security is also considered extremely technological and different to grasp for non-experts. The fact that AMI is currently not implemented in many of these DSOs is also a challenge in the assessments.

It is not possible to overcome all these challenges with a guideline. As AMI is currently not widespread, limited statistics are available. However, a guideline may be able to aid with examples and also increase understanding of information security. The provided checklists on assets, incidents, vulnerabilities and controls could contribute to this. When comparing the results of the assessments performed with and without the use of our guideline, it is however not possible to state that the quality has improved with use of the guideline. There is no indication that use of our guideline led to coverage of more incident types. There are high variations in what risks are considered to be most important, but this is the case also with the support of the guideline. Feedback received from the participants in the assessments B1-B2 were in general positive. A focus on assets was considered useful. Further, the use of checklists did result in additional incidents and assets being identified in the meetings. However, the positive feedback may also be due to having an external facilitator rather than the content of the guideline.

7.1 Systematic Approach and need for Experts

A1-A3 show that the DSOs have tried to identify main privacy and information security issues, but they seem to lack systematic ways to approach this area, e.g. in the form of asset identification or the use of threat categories. In A2 they used external documents and a risk map to make sure all things are covered, and felt confident as this support was provided by experienced consultants. For the others, a more systematic approach could potentially increase confidence that the most important threats have been covered. We received positive feedback on our suggested focus on assets.

Personnel who know the technical details of the systems, and possible threats and their corresponding potential consequences, are invaluable to an organisation‘s risk assessment process. For non-experts it is almost impossible to make realistic assumptions on likelihood and consequences.

7.2 Limitations

Our study of A1-A3 comprised a documentation study and interviews, but we still do not know details about the discussions and the priorities made. We might do the assessments injustice by making statements about whether or not the important risks have been identified and assessed.

Participant observation poses the risk of bias due to the researcher's active role in the process. As authors of the guideline that was used as support, we might use it differently than an independent process leader, and we might be too supportive of our own suggestions.

8 CONCLUDING REMARKS AND FUTURE WORK

This case study shows that the DSOs need support for their information security risk assessments, as they experience challenges related to competence and understanding of information security issues. Checklists and a focus on assets may help in this respect. However, more studies are needed in order to identify what type of support will significantly ease the performing of risk assessments by DSOs. We do not have a sufficient base for claiming that the use of our guideline will increase the quality of risk assessments. Feedback from the participants indicated that they appreciated the process of identifying assets before considering threats and vulnerabilities, and they felt that our checklists added value to the process as well. We would like to stress that our guideline does not present a new method, but the Norwegian energy industry does not have traditions for including asset identification as part of their risk assessments, and this may be a valuable approach when information security and privacy constitute the main focus for these assessments.

Irrespective of availability of guidelines or other types of support material, it is still important that each organisation perform their own assessments based on their specific systems and priorities. Thus the competence of the participants in an assessment is likely to be more important than any guideline support.

ACKNOWLEDGEMENT

The authors would like to thank the DSOs that participated in our study.

REFERENCES

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). The OCTAVE Allegro Guidebook v1.0. Software Engineering Institute.

Cybenko, G. (2006). Why Johnny Can't Evaluate Security Risk. *IEEE Security & Privacy*, 4(1):5.

EnergiNorgeAS (2012). Overordnet risiko-og sårbarhetsanalyse for innføring av AMS. PT-1070549-RE-01.

Fenz, S. and Ekelhart, A. (2011). Verification, Validation, and Evaluation in Information Security Risk Management. *IEEE Security & Privacy*, 9(2):58–65.

GAO (1999). Information Security Risk Assessment: Practices of Leading Organizations. United States General Accounting Office (GAO).

Gerber, M. and von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, 24(1):16 – 30.

Group, T. S. G. I. P. C. S. W. (2010). Guidelines for smart grid cyber security.

ISO/IEC (2005). ISO/IEC 27001:2005 Information security management systems - Requirements.

ISO/IEC (2011a). ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management.

ISO/IEC (2011b). ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management.

Jourdan, Z., Rainer, K., Marshall, T. E., and Ford, N. (2010). An Investigation of Organizational Information Security Risk Analysis. *Journal of Service Science*, 3(2):33–42.

Line, M. B., Tøndel, I. A., Johansen, G. I., and Sæle, H. (2013). Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer (Norw.). Technical Report A24258, SINTEF. ISBN 978-8-214-053203.

NVE (2010). Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen (in Norwegian). Norwegian Water Resources and Energy Directorate.

NVE (2013). FOR 1999-03-11 nr 301: Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester.

Rhee, H.-S., Ryu, Y. U., and Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2):221 – 232.

Shedden, P., Ruighaver, A. B., and Ahmad, A. (2010). Risk Management Standards - The Perception of Ease of Use. *Journal of Information System Security*, 6(3):23–41.

Skapalen, F. and Jonassen, B. (2013). Veileder til sikkerhet i AMS (in Norw.). NVE.

Sulaman, S. M., Weyns, K., and Höst, M. (2013). A review of research on risk analysis methods for IT systems. In *Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering*, EASE '13, pages 86–96, New York, NY, USA. ACM.

Yin, R. K. (2009). *Case Study Research - Design and Methods, 4th ed.*, volume 5 of *Applied Social Research Methods*. SAGE Publications.