An Effect Analysis of ISO/IEC 27001 Certification on Technical Security of Norwegian Grid Operators

Øyvind Anders Arntzen Toftegaard*†
* *Norwegian University of Science and Technology*
† *Norwegian Energy Regulatory Authority*
0000-0002-9135-6891

***Abstract*—Digital vulnerabilities and the risk of cyberattacks against the electric grid are a concern for both governments and businesses. There are several opportunities for authorities to impose security measures on grid operators to reduce risks. German legislation requires grid operators to certify their information security management system according to the ISO/IEC 27001 standard. Some researchers have tried to measure various effects of ISO/IEC 27001 certification, but nobody has so far assessed the effect of certification on technical security performance. This study hypothesizes that ISO/IEC 27001 certification will lead to increased technical security performance for Norwegian grid operators. A Quasi-Experimental methodology based on Difference in Differences logic is applied to test the hypothesis. 11.010 technical security scores from 400 entities were collected through BlackKite's Technical Cyber Rating tool and Security Scorecard's Security Rating tool. The effect of ISO/IEC 27001 certification was estimated by taking the difference in technical security performance between uncertified Norwegian grid operators and certified German grid operators, and subtracting the difference between a control group of Norwegian and German banks. The analysis predicts a significant positive effect for small Norwegian grid operators, it is inconclusive for medium-sized grid operators, and it indicates a negative effect for large grid operators. Since the research was limited to externally identifiable security mechanisms only, more research is necessary to fully understand the effect of ISO/IEC 27001 certification on technical security performance.**

***Index Terms*—Security, Security Certification, Security Management, Information Security, Cybersecurity, Energy, Quantitative Research**

I. Introduction

As the traditional electric grid is developing toward a smart and digitally enabled grid, the digital risks become more prominent. Potential worst-case consequences of cyberattacks are electricity outages and blackouts, harmful personal information leakages, and devastating economic loss. Huge and instant power outages may cascade across large geographic areas, and large parts of society may be affected. Therefore, it is in both government's, society's, and grid operator's interest that grid operators maintain a high level of cybersecurity. The information security management system standard ISO/IEC 27001 [1] is a certifiable standard. Being certifiable, it has been used by digital industry players to create trust among stakeholders for more than one and a half decades. The standard was developed in cooperation between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). In Germany, all grid operators have been required by law since 31. January 2018 to certify their information security management system according to the ISO/IEC 27001 standard [2]. In 2021, the EU agency for energy, ACER, suggested certification, such as ISO/IEC 27001, in a new piece of legislation for the European power sector [3].

An information security management system as described in ISO/IEC 27001 ensures that the entity is maintaining a system of processes that are important for information security. Examples of such processes are recurring risk assessments, a system for incident reporting and handling, top management involvement, and continuous improvement of the management system itself. ISO/IEC 27001 mainly consists of 10 clauses and Annex A. The first 3 clauses are administrative for the standard, such as its scope and definitions. Clauses 4-10 are the only compulsory part of the standard and are summarized in Table I. Annex A lists non-compulsory control objectives and controls for information security, which the entity may implement based on its own risk evaluation. ISO/IEC 27001 certification can in this relation be described as written confirmation from an independent third party that an entity's management system fulfills the requirements of clauses 4-10.

TABLE I
Mandatory clauses (C) of ISO/IEC 27001

Nr	Mandatory clauses	Content of clauses
C4	Context of the organization	External and internal issues relevant for the scope
C5	Leadership	Commitment and information security policy
C6	Planning	Identify Risks, assess compliance and establish objectives and plans to achieve them
C7	Support	Resources, competence, awareness, communication, and documentation
C8	Operation	Planning and control, information security risk assessment and risk treatment
C9	Performance evaluation	Management system monitoring and review, internal audits, and management review
C10	Improvement	React to nonconformities and continuous improvement

In this paper, the terms security, information security, and cybersecurity are used interchangeably. The term management system is defined in ISO 19011 as a set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives [4].

978-1-6654-8045-1/22/$31.00 ©2022 IEEE

A management system usually covers systematic measures that should ensure that an entity's activities are being planned, organized, executed, and maintained in compliance with requirements set by authorities [5].

The question of whether ISO/IEC 27001 certification should be required, should be connected to how effective such certification will be as a tool to increase technical security performance. Certification of an information security management system shall in theory prove that cybersecurity measures have been implemented correctly within the entity. A natural assumption is that correctly implemented security measures will give a higher technical security performance than if measures were not correctly implemented. If not, such certification would be an unnecessary cost from a technical perspective. If it can be proved an effect of ISO/IEC 27001 certification on technical security performance, it may be helpful for policymakers, such as EU officials, when they shall decide whether or not such certification should be a compulsory measure.

The relationship between an objective and a measure within policy design can be called effect- or causal theory. Within the term lies the assumption that the objective of a policy will be reached through a number of proposed measures [6]. According to [6], implementation- and evaluation research documents that such assumptions are often wrong. The reason is often that policy design is based on a causal theory that is not valid. This shows the importance of a good understanding of the relationship between cause and effect before measures are implemented.

The German Federal Office for Information Security (BSI) regards ISO/IEC 27001 certification as a confirmation that BSI's basic requirements for information security have been implemented correctly [7]. Therefore, BSI does not find it necessary to conduct audit inspections of grid operators who can provide an ISO/IEC 27001 certificate. ISO/IEC 27001 certification has been used to establish trust among stakeholders for several years by many entities in different sectors. However, the effect of ISO/IEC 27001 certification on technical security performance has not been proved, neither by the industry nor by researchers. Examples of technical security are IT system security configuration and software vulnerability management such as patching.

Consultant bureaus are commonly used as certification bodies. ISO/IEC 27001 certification may cost 5.000,- to 24.000,- Euro, depending on the size of the entity [8]. This covers the certification fee to the certification body. An entity's internal costs for the process of becoming compliant with ISO/IEC 27001 standard requirements come in addition. The latter is probably by far the largest cost. It can be questioned if this is an optimal use of an entity's budget. It would be meaningless to spend large amounts of resources on management system certification if it does not have a considerable effect on the entity's technical security performance. Funds could alternatively have been used on technical measures, such as upgrading to advanced intrusion protection and detection systems, firewalls, or for targeted penetration testing looking for vulnerabilities in the IT systems. Larger entities may have enough funds for all, but smaller entities will probably have to prioritize.

This study's main contribution is to provide a best-effort prediction of the effect of ISO/IEC 27001 certification on externally measurable technical security of Norwegian grid operators. As ISO/IEC 27001 is widely used for establishing trust among stakeholders and as a substitute for government inspection audits, such knowledge is important for authorities with responsibilities within cybersecurity. Such knowledge is also important for single entities utilizing the ISO/IEC 27001 standard for internal cybersecurity management. When this research was conducted, no other studies were found to have investigated the effect of ISO/IEC 27001 certification on cybersecurity at all. Therefore, this study can be considered a first step toward understanding the effect of ISO/IEC 27001 certification in general.

A planned EU legislation called network code on cybersecurity is assumed to be agreed upon by the EU Parliament and Council during 2023. The network code builds on the framework guideline from ACER referred to at the beginning of this section, where ISO/IEC 27001 certification is proposed. Therefore, the results from this research may be valuable when discussing whether ISO/IEC 27001 certification should be a compulsory requirement or not. A short overview of the most relevant literature is given in section II, before an overview of our applied scientific design and methodologies is provided in Section III. In Section IV, the results are presented, and the results are discussed in Section V. Threats to validity are discussed in Section VI, and in Section VII the paper is concluded.

II. Previous Research

When this research was conducted, no information was found on any previous research assessing the effect of ISO/IEC 27001 certification on externally observable technical security. Further, no studies were found to have investigated the effect of ISO/IEC 27001 implementation or certification at all in relation to security in any sector. As a consequence, the previous research section focuses on studies that lay the ground for this research.

A. Non-academic Sources

In May 2021, the Norwegian Water Resources and Energy Directorate surveyed 121 entities' in the Norwegian energy sector on information security management [31]. According to the results, 57% of the entities did not have an information security management system and 6% were not sure if they had it or not. 56 of the participants in the survey were grid operators, which amounts to about 50% of the grid operators in Norway. Unpublished data from the survey reveals that none of the Norwegian grid operators participating was ISO/IEC 27001 certified [10].

In 2017, the EU agency for Cybersecurity (ENISA) conducted a mapping of security requirements for critical entities [11]. The mapping showed that the two most used standards in the European energy sector were ISO/IEC 27001 and

ISA/IEC 62443. The latter is a technical security standard series for automation and control systems. ENISAs mapping also showed that ISO/IEC 27001 was the most used standard for critical entities in EU states, independent of the sector. ENISA did not evaluate the effect of the standards and/or their certification.

B. Academic Sources

Storm, Hagen, and Selnes assessed the effect of legislation and security management audits on the implementation of intrusion detection controls of Norwegian grid operators [12]. Legal requirements for intrusion detection entered into force in Norway in January 2013. In 2015, security management audits of larger grid operators by national authorities showed that intrusion detection capabilities were missing among most auditees. In 2021, however, audit results showed a significant improvement in intrusion detection capabilities. The authors believed the audits in 2015 contributed to the increase in reported detection capabilities for the large grid operators.

The effect of security management audits reported in [12] could have been caused by technological development or other influences. Toftegaard, Hagen, and Hämmerli [15] assessed the relationship between security management maturity and technical security performance. The authors were not able to find any clear correlation and therefore concluded that results from audits targeting information security management systems should not be used as indicators of an entity's technical security performance. The authors did not however evaluate the effect of ISO/IEC 27001 certification.

Edwards, Jacobs, and Forrest used technical risk indicators from the risk rating vendor BitSight to investigate relationships between these indicators and botnet infections [16]. The risk indicators they used were connected to the entity's use of filesharing, their configuration of the Transport layer Security (TLS) protocol, and which network services the entities made publicly available. Their results showed that entities with more filesharing, protocol errors, and risk services showed a tendency towards more botnet infections. Risk indicators collected by BitsSight are comparable with those collected by BlackKite and Security Scorecard. The report showed that these types of technical risk indicators may be used successfully to estimate the likelihood of unwanted cyber events and thus cybersecurity performance.

No previous research was found on the relationship between ISO/IEC 27001 certification and security performance. However, Jacobsen and Thorsvik claim it is difficult to prove a relationship between an entity's business goals, visions, and strategies, and the entity's efficiency [17]. In this context, it can be assumed that efficiency refers to income. The authors explain that research on this topic seldom is able to identify a relationship between strategic planning and the performance of the entity. This may be partially transferrable to an ISO/IEC certification, since the standard aims to establish objectives and strategies for the entity's work on information security. Hsu, Wang, and Lu found that ISO/IEC 27001 certification did not have any influence on an entity's profitability [18]. This complements Jacobsen and Thorsvik's observations that it is difficult to find a relationship between strategic planning and the success of an entity.

III. Methodology

A. Research Question and Hypotheses

The goal of this study is to examine if ISO/IEC 27001 certification can be used to improve cybersecurity for grid operators. The applied research question is "How effective is ISO/IEC 27001 certification in improving cybersecurity?" The scope has been limited to the technical security performance of Norwegian grid operators. The assumption is that improved security processes following ISO/IEC 27001 certification will have a positive influence on technical security performance (see Fig. 1).

Fig. 1. Expected effect of ISO/IEC 27001 certification.

The H_1 hypothesis is that "ISO/IEC 27001 certification would increase the technical security performance of Norwegian grid operators." The H_0 hypothesis then becomes "ISO/IEC 27001 certification would have no effect on the technical security performance of Norwegian grid operators."

B. The Difference in Differences Technique

The core of this study's research design is a quasi-experimental methodology based on Difference in Differences (DiD) logic [13]. DiD is a statistical technique that estimates the effect of a measure by looking at the difference between an exposure group ($_E$) subject to treatment (T) and a control group ($_C$). In this case, the treatment is ISO/IEC 27001 certification. The difference between the exposure and control group is registered both before (X) and after (Y) the treatment. The control group is normally used to control for unknown factors of influence that would lead to different conditions for the exposure group before and after the certification. In this case, the DiD technique has been tweaked so instead of using before and after, Norwegian grid operators who are not ISO/IEC 27001 certified are compared with German grid operators who are certified. The control group, here banks, is then used to control for any differences between the conditions in Norway and Germany. The traditional DiD technique can be set up as in (1):

$$\frac{(A)/C: \quad X_E \quad T \quad Y_E}{A/C: \quad X_C \qquad Y_C} \tag{1}$$

Where A means the selection of the group was autonomous, and C means the selection was controlled. In this case, the selection of the pre-treatment groups was autonomous because all grid operators and banks from Norway with available data were included. For the post-treatment groups, the selection was controlled, as German entities with similar revenue as the

Norwegian entities were chosen. X_E represents the exposure group before treatment. Y_E represents the exposure group after treatment. *T* represents the measure used as treatment, in this case, ISO/IEC 27001 certification. X_C represents the control group at the same time as the exposure group before treatment. Y_C represents the control group at the same time as the exposure group after treatment. In this case, all the data was collected within the same month, as this study instead relied on differences between Norway and Germany.

The average effect of a measure, called the Average Treatment Effect (*ATE*), is calculated from the *X* and *Y* values in (1). The difference between *X* and *Y* between the two groups will be reflected by the ATE value. It is assumed the exposure group would have an outcome identical to the control group if there were no causal effect of the treatment. The calculation of *ATE* can be set up as in (2):

$$ATE = (Y_E - X_E) - (Y_C - X_C) \tag{2}$$

As few or no Norwegian grid operators are certified, but all German grid operators are, an equation can be set up as in (3). The result should show the effect of ISO/IEC 27001 certification on Norwegian grid operators' technical security performance.

$$ATE = (G_{Ger} - G_{Nor}) - (B_{Ger} - B_{Nor}) \tag{3}$$

Where *G* = grid operators, *B* = banks, and $_{Ger}$ and $_{Nor}$ refers to Germany and Norway. (3) was used to find ATE for all the 90 Norwegian grid operators, and to find ATE for groups of the same operators classified into small, medium, and large entity sizes.

C. Regression Analysis

Ordinary least square (OLS) regression was applied to estimate the standard error and probability value of differences between the groups used in this research design. The regression model is based on regression for DiD (4):

$$Y_{it} = \alpha + \beta_1 E_i * POST_t + \beta_2 E_i + \beta_3 POST_t + \epsilon_{it} \tag{4}$$

Where Y represents the effect value. α represents the control group score, in this case the average security score of Norwegian banks. β_1 represents the most important estimate in the model, namely the average treatment effect (ATE) as explained in (3). β_2 represents the average difference between, in this case, the Norwegian (non-certified) exposure group and the Norwegian control group. β_3 represents the average difference between the two control groups. *E* represents the exposure group and $_i$ is a binary dummy variable set to value 1 if the group belongs to the exposure group and 0 if the group belongs to the control group. POST represents, in this case, the German exposure and control groups. $_t$ is a binary dummy variable with value 1 if the group belongs to POST and otherwise 0. ϵ_{it} represents controls for any influences that the control group does not control. In this case, the regression model looks like in (5).

$$Y_{it} = \alpha + \beta_1 G_i * Ger_t + \beta_2 G_i + \beta_3 Ger_t \tag{5}$$

Where *G* = Grid operator and is used instead of exposure group (*E*). *Ger* = Germany and is used instead of *POST* to symbolize the state with certified grid operators. The α and β_1, β_2, and β_3 are illustrated in Fig. 5.

The regression analyses were conducted in Python by setting up a script using PyCharm. Pandas (Python Data Analysis Library) was called to organize the datasets and the statsmodels.formula.api was applied, which has the OLS function.

D. Exposure and Control Group

The two exposure groups in this study consisted of German and Norwegian grid operators. The reason for choosing grid operators from these two states was that ISO/IEC 27001 certification had been compulsory for German grid operators since January 2018 [2]. Further, it was known that less than 50% of the Norwegian grid operators were ISO/IEC 27001 certified in 2021 [10] and the Norwegian Water Resources and Energy Directorate were not familiar with any Norwegian grid operator being certified [19]. Therefore, Norwegian grid operators were treated as non-certified. Banks in Norway and Germany were chosen as control groups. German grid operators commonly operate energy production facilities and water supply in addition to power grids, therefore, such entities could not be chosen for control groups. As the banks did not have any requirement of being ISO/IEC 27001 certified it was not known how many of them were certified. A survey published by ISO in 2021 [20] reported however 51 German and 0 Norwegian entities in the electricity supply sector as ISO/IEC 27001 certified. In the financial and real estate sector it reported 2 German and 0 Norwegian entities as certified. Although the survey did not receive answers from all the certified entities, it indicates that the banks are more homogenous across Norway and Germany than the grid operators.

The most important legal requirements for the German and Norwegian grid operators and banks are summarized in Table II. The table shows that the exposure and control groups in both states have a sector-specific piece of legislation covering detailed cybersecurity requirements. In Norway, the detailed requirements are listed in the legislation itself, while in Germany, detailed requirements are provided in statutory catalogs. When comparing the security requirements for all four groups, they have small variances, but all of them impose traditional technical and organizational security measures. However, it is only the catalog for the German grid operators that impose ISO/IEC 27001 certification.

The Network and information security (NIS) directive [23] is implemented in Germany, but not in Norway. NIS provides high-level security requirements for critical sectors and therefore covers both the bank and energy sectors in Germany. GDPR [22] is implemented in both Germany and Norway and covers all entities that process personal information of

any kind. Therefore, GDPR covers all four groups. The use of banks as control groups will control for any differences between Norway and Germany caused by the NIS directive. There are however other standards targeting the bank sector only. One example is the SWIFT Customer Security Controls Framework [26] which is compulsory for all SWIFT users globally. Another is the TIBER EU framework [27], implemented in Norway as the voluntary TIBER NO and in Germany as the voluntary TIBER DE. Because these frameworks are equally enforced in both Norway and Germany, they should not impact the analysis performed in this study.

TABLE II
CYBERSECURITY RELEVANT LEGISLATION FOR THE ASSESSED GROUPS.

Group	Prominent legislation	Main content related to cybersecurity
Norwegian grid operators:	Energy contingency regulation [39]	Asset management, access control, user instructions, procurement, personnel, backup, and information system security covering both information- and operational technology.
Norwegian banks:	ICT-systems regulation [21]	Security planning and organization, risk assessment, quality objectives, ICT-system security, development and procurement, maintenance and operations, incident and change management, crisis management, supply chain and ICT related documentation.
German grid operators:	Energy act [24]	Mandates a catalog of security requirements and regulations for regular verification of compliance with the security requirements. The catalog imposes ISO/IEC 27001 certification of an ISMS covering the security requirements in the catalog [2].
German banks:	Banking Act [25]	Mandates the Minimum Requirements for Risk Management (MaRisk) and the Supervisory Requirements for IT in Financial Institutions (BAIT). MaRisk covers risk management and management system in general while BAIT covers technical and organizational resources for information security, continuity, and outsourcing.
German grid operators and banks:	Network and information security directive [23]	Germany updated the BSI Act in 2017 to transpose the NIS Directive into German law. The act provides minimum security requirements to entities in critical sectors, which include energy and banking.
All groups:	General data protection regulation [22]	Requires measures that meet the principles of data protection by design and by default, as well as data protection impact assessment.

The business intelligence tool Wer-zu-wem [28] was used to gather data about company size for German entities. For Norwegian entities, the equivalent Proff Forvalt tool [29] was used. These tools provided information about the revenue for size determination as well as the URL of the entities which was used in the security scoring tools. A list of Norwegian grid operators was collected from the Norwegian Energy Regulatory Authority (RME) and a list of German grid operators from the German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (BNetzA). A list of Norwegian banks was obtained through the Proff Forvalt tool and a list of German banks through the Wer-zu-wem tool.

The lists of Norwegian grid operators and banks were about 100 entities each, which was a lot less than the lists of German grid operators and banks. Therefore, the lists of Norwegian grid operators and banks were used as a starting point and German grid operators and banks of similar size were then selected. The main grouping variable was the use of business revenue. For some German entities, approximate revenue data only was available (0-10, 10-50, 50-100, 100-250, 250-500, and above € 500 M). In such cases, the number of employees was used to improve the mapping of German entities to Norwegian entities.

Norway had approximately 100 grid operators in total during the time of this study. However, a few Norwegian grid operators were removed as they did not have any internet domain or did not have any website functioning at the time. The same applied when selecting banks for this study.

After the data cleaning, the remaining entities were 90 Norwegian grid operators, 102 Norwegian banks, 105 German grid operators, and 103 German banks. The European Commission definition for the size of entities was applied, which is based on annual turnover [30]. Entities with turnover $\leq$ € 10 M were defined as Small and $\leq$ € 50 M as Medium. Entities with turnover $>$ € 50 M were defined as Large. It was assumed that turnover equals revenue for the entities studied.

E. Collection of Security Scores

To enable the analysis, a total of 11.010 technical security scores from 400 entities were collected during March 2022. 7.600 scores were received from 400 entities through BlackKite's (BK) Technical Cyber Rating tool [37], and 3.410 scores from 341 of the same entities through Security Scorecard's (SS) Security Rating tool [38]. According to Gartner, these two tools were among the five most evaluated tools by the energy and utility industry in August 2022, and the tools were rated by the users as within the top 9 for the purpose of cybersecurity rating [35]. Combined, the two tools returned scores for a total of 22 security categories as listed in Table III: 19 security categories from BlackKite and 10 security categories from Security Scorecard. Seven of these categories overlapped.

The scores for each category were collected non-intrusively through a passive evaluation. This means the data only describe the technical status which is observable from the internet outside of the entities' firewalls and internal IT networks. For example will patch status of devices that do not communicate over the internet, such as many components for industrial control systems, not be registered by such analysis. It is also unknown whether the data collected this way from the outside, is representative of the technical security of the internal systems which are not exposed over the internet. Table III describes how scores are collected for each technical category.

The scores from BlackKite were delivered as ordinal data in form of letter grades from F – A. The scores from Security Scorecard were delivered as continuous variables between 0 and 100. To enable the analyses, the letter grades were converted so that A=100, B=80, C=60, D=40, E=20, and F=0, which would then correspond with Security Scorecard's scale

TABLE III
TECHNICAL SECURITY CATEGORIES AND INDICATORS.

Nr	Technical categories	Category description	Indicators BK (entities'=400)	Indicators SS (entities'=341)
1	DNS Health	DNS performance and configuration of the entity's DNS settings and checks the history of malicious events [34]	Grade (F-A)	Numeric (0-100)
2	Email Security	Email security mechanisms and configurations based on open sources [33]	Grade (F-A)	-
3	SSL/TLS Strength	Whether internet traffic is encrypted [33]	Grade (F-A)	-
4	Application Security	Configuration of web applications [33], and related threat intelligence [34]	Grade (F-A)	Numeric (0-100)
5	DDoS Resiliency	Whether the network is configured to withstand a DDoS attack [33]	Grade (F-A)	-
6	Network Security	Unprotected network devices, critical ports, misconfigured firewalls, and service endpoints [33]	Grade (F-A)	Numeric (0-100)
7	Fraudulent Domains	Adversaries registering domains that may have commonalities with the target entity, with the intent of malicious activity [33]	Grade (F-A)	-
8	Fraudulent Apps	Adversaries registering applications that may have commonalities with the target entity, with the intent of malicious activity [33]	Grade (F-A)	-
9	Credential Mgmt / Information Leak	Leaked user credentials [33], [34]	Grade (F-A)	Numeric (0-100)
10	IP Reputation / Cubit Score	Checking public IP reputation lists [33], [34]	Grade (F-A)	Numeric (0-100)
11	Hacktivist Shares / Hacker Chatter	Collection and analysis of underground communication related to the entity [34]	Grade (F-A)	Numeric (0-100)
12	Social Network	Attack surface from engaging in social media [33]	Grade (F-A)	-
13	Attack Surface	Number of entry points into the entity's network [33]	Grade (F-A)	-
14	Brand Monitoring	Monitoring various online channels for reported security-related issues [33]	Grade (F-A)	-
15	Patch Management/Cadence	Whether the software on computers and network devices is updated [33] and how quickly such updates are installed [34]	Grade (F-A)	Numeric (0-100)
16	Web Ranking	Rankings such as speed tests and web content accessibility [33]	Grade (F-A)	-
17	Information Disclosure	Detection of leaked sensitive information connected to the entity [33]	Grade (F-A)	-
18	CDN Security	Detection of vulnerabilities in content delivery network (CDN) services like edge caching, SSL offloading and edge routing [33]	Grade (F-A)	-
19	Website Security	Code and server-level vulnerabilities observable from outside the entity's network [33]	Grade (F-A)	-
20	IP Reputation	Detection through sinkhole infrastructure [34]	-	Numeric (0-100)
21	Endpoint Security	Information extracted from metadata related to operating systems and web browsers with their active plugins [34]	-	Numeric (0-100)
22	Social Engineering	Potential susceptibility of an organization to a targeted social engineering attack, based on an analysis of data from social networks and public data breaches [32], [34]	-	Numeric (0-100)

of values between 0 and 100. A summary of the categories and indicators is shown in Table III.

IV. RESULTS

The stacked columns in Fig. 2 shows that this study mostly has a good representation of data from both BlackKite and Security Scorecard. The only exception is the scores for Norwegian grid operators collected through Security Scorecard, which only covers 54 operators. However, these 54 are part of the 90 grid operators covered by BlackKite. Another observation is that a larger proportion of the Norwegian grid operators are small compared with the German grid operators. The German grid operators have a larger proportion of medium-sized grid operators. Norwegian banks are also a bit over-represented by small-sized banks.

The frequency diagram in Fig. 3 illustrates how the dataset is skewed. The skewed score distribution shows that the entities assessed mostly have a high level of technical cyber-security.

The histogram in Fig. 4 shows average security scores for Norwegian and German grid operators. The scores are based on data set D_1 which is calculated as shown in (6).

Table IV lists the average treatment effect (ATE) when classifying the entities into small, medium, and large-sized entities, as well as for all sizes. In the first row, ATE has been calculated based on scores collected through BlackKite only, and in the second row, ATE has been calculated based on scores collected through Security Scorecard. In the third row, for data set D_1, all the separate scores collected through both BlackKite and Security Scorecard were used, calculated

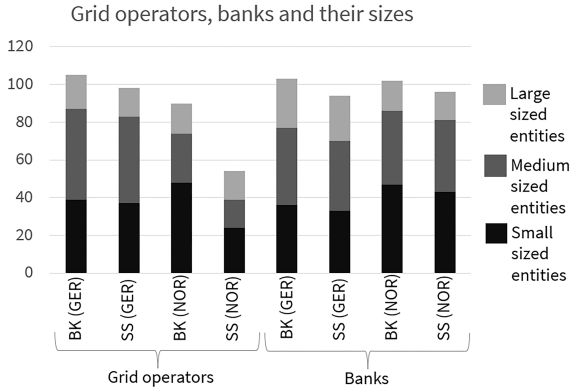

Fig. 2. Number of grid operators and banks of different sizes.

as shown in (6). The calculation establishes a total score (s) for each entity by combining the entity's overall average score from BlackKite with its overall average score from Security Scorecard.

$$\forall\, s \in D_1,\, s = ((\frac{1}{19}\sum_{i=1}^{19} BK_i) + (\frac{1}{10}\sum_{i=1}^{10} SS_i))/2 \quad (6)$$

BK represents an entity's score per category from BlackKite and SS represents its score per category from Security Scorecard. For the 59 entities with scores collected through BlackKite only, only the first half of (6) was applied, namely: $(\frac{1}{19}\sum_{i=1}^{19} BK_i)$. In the fourth row of table IV, for data

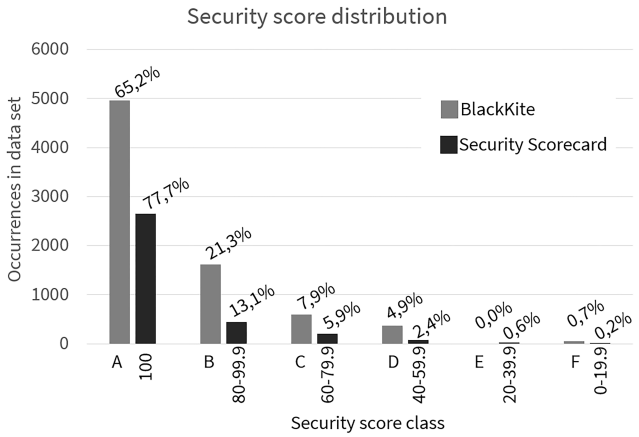

Fig. 3. Frequency diagram for the collected scores.

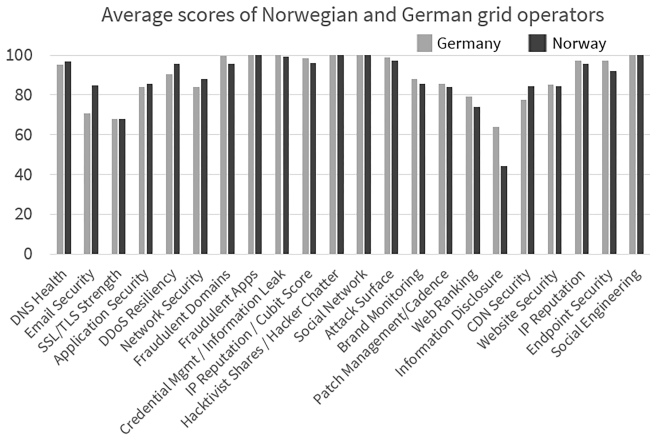

Fig. 4. Average scores from BlackKite and Security Scorecard combined.

set D_2, the values from BlackKite and Security Scorecard were combined for the 7 categories that overlapped, before calculating the average score as shown in (7). As a result, the calculation for data set D_2 is different than the one for data set D_1.

$$\forall\, s \in D_2,\ s = \frac{1}{22}\sum_{i=1}^{22}\left(\frac{BK+SS}{2}|BK|SS\right)_i \qquad (7)$$

Each entity's total score (s) which is an element of the data set D_2 is calculated as illustrated in (7). The symbol $|$ is used with the meaning "or". For the seven categories that overlapped the $\frac{BK+SS}{2}$ option is applied, for the twelve categories scored only by BlackKite, the BK option is used, and for the three categories scored by Security Scorecard only, the SS option is chosen.

By classifying grid operators and banks as small, medium, and large-sized entities as in Table IV, this study was able to identify a positive average treatment effect for small Norwegian grid operators. For medium-sized grid operators, the results were negative if based on the data from BlackKite and positive if based on the data from Security Scorecard. For large-sized entities, a negative average treatment effect is observed, which indicates a negative effect of ISO/IEC 27001 certification on technical security performance. For all entity sizes combined, a negative effect is found when based on scores from BlackKite and a positive effect when based on scores from Security Scorecard.

TABLE IV
AVERAGE TREATMENT EFFECT (AND ST. DEVIATION) PER ENTITY SIZE.

	Small	Medium	Large	All sizes
BlackKite	0.790 (1.176)	-1.571 (1.251)	-3.557 (1.874)	-1.100 (0.781)
Security Scorecard	2.066 (1.380)	2.669 (1.488)	-2.125 (2.181)	1.282 (0.904)
BK and SS Combined (D_1)	2.176 (1.089)	1.255 (1.151)	-3.135 (1.740)	0.707 (0.717)
BK and SS Combined (D_2)	1.839 (1.191)	-0.397 (1.068)	-3.678 (2.594)	-0.036 (0.803)

An average treatment effect at 0.707 was found when running the regression analysis for all entity sizes applying data set D_1. This effect is illustrated in Fig. 5, which also illustrates how the DiD technique as described in (3) and (5) works. In Fig. 5, β_3 represents the change in average security score for Norwegian grid operators if they were subject to German conditions but without ISO/IEC 27001 certification. The predicted average treatment effect for Norwegian grid operators of 0.707, if they should be subject to ISO/IEC 27001 certification, is represented by β_1.

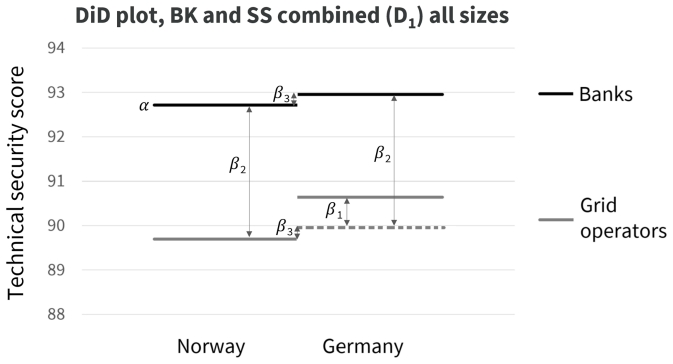

Fig. 5. Difference in Differences (DiD) plot based on data set D_1.

Probability (P) values were obtained to indicate the significance level of the results in Table IV. Table V shows that the positive effect predicted for small entities based on data set D_1 is statistically significant with a P-value <0.05. This means there is statistically strong evidence that small Norwegian grid operators would have a positive effect of ISO/IEC certification on their technical security performance.

TABLE V
RESULTS OF REGRESSION ANALYSIS (P-VALUE).

	Small	Medium	Large	All sizes
BlackKite	0.503	0.211	0.062	0.160
Security Scorecard	0.137	0.075	0.333	0.157
BK and SS Combined (D_1)	0.047	0.277	0.076	0.325
BK and SS Combined (D_2)	0.125	0.711	0.161	0.964

V. Discussion

The average treatment effect by combining security scores from all entity sizes, was 0.707 for data set D_1 and -0.036 for data set D_2. First, these are low numbers considering the range is from 0-100. Second, the standard deviations are higher than these values. Third, P-values show a low level of confidence in these results. Therefore, it cannot be claimed that certification has any effect on technical security performance, positive or negative, when not controlling for entity size. The low ATE-value supports the H_0 hypothesis, that ISO/IEC 27001 certification would have no effect on the technical security performance of Norwegian grid operators.

However, the analysis based on data set D_1 shows a significant positive effect of ISO/IEC 27001 certification for small grid operators. The H_1 hypothesis is that ISO/IEC 27001 certification would increase the technical security performance of Norwegian grid operators. This means that if the H_1 hypothesis is applied to small-sized entities only, it can be proved to be statistically true and subsequently the H_0 hypothesis can be rejected. However, the H_0 hypothesis can only be rejected for small-sized grid operators.

The reason why small-sized Norwegian grid operators would have a positive effect on technical security performance following ISO/IEC 27001 certification may be connected to resources. Their low revenue may not allow hiring dedicated security personnel unless forced. Therefore, a requirement to be certified may lead to small grid operators hiring their first dedicated security experts.

No clear effect in any direction is observed for medium-sized grid operators. However, for large-sized grid operators, the results indicate a negative effect. The predicted negative effect is not supported by a significant confidence level, but the P-value at 0.076 for data set D_1 does indicate a negative trend. The P-value gives a chance less than 10% that the H_0 hypothesis, saying there is no effect from certification, is true.

This study has identified three possible scenarios for why large Norwegian grid operators may have a negative effect from ISO/IEC 27001 certification. The first is that an enforced standard may kill motivation. According to [40], those who have taken a standpoint will feel a commitment to be consistent with that standpoint. Large operators may, because of their resources, have security experts in place already, who have clear standpoints on how to optimize their security processes. If told to change their preferred processes to follow a specific standard like the ISO/IEC 27001, it may be inconsistent with their standpoint and thus demotivating for the security experts.

The second possible reason is that an enforced management system may shift focus from daily security work to settling with becoming compliant with the security management system. A book on health-related management systems [14], points out that the most important is the daily work conducted by employees and how managers facilitate that work. A management system is only a tool providing structure for the work. Therefore, if employees are settling with becoming compliant with the management system, instead of focusing on daily technical security work, it may have a negative impact on technical security performance.

The third possible reason is that an enforced management system may emphasize the distance between employees working with security management and those working with technical security. The existence of such a distance was indicated in a recent study [15]. The authors were unable to prove any correlation between security management maturity and technical security performance among a number of entities in the energy sector. This shows that an increased focus on security management does not necessarily increase technical security performance. If ISO/IEC 27001 certification leads to the allocation of personnel working on technical security towards security management work, it may result in a decrease in technical security performance.

It should be emphasized that there are weaknesses in the study presented in this paper, which may have affected the outcome. Such weaknesses are discussed in the following section.

VI. Threats to Validity

As illustrated in Fig. 3, the assessed entities' turned out to have a quite homogeneous and high level of cybersecurity. The figure shows a striking skewness of the distribution of the entities' security scores towards the top scores. The lack of variation in the data makes statistical analysis challenging in general.

Construct validity reflects the extent that the indicators studied really represent what was intended and what is assessed according to the research questions [36]. In this case, whether the security scores are relevant for the relationship between ISO/IEC 27001 certification and technical security. As technical security scores were based on passive collection from outside the entities' IT networks, the security status of internal system components and software that are not observable from the outside is unknown. Access to scan or test IT systems on the inside could therefore have given different results.

A strength regarding the construct validity is that it was used two different tools to collect technical security scores to indicate technical security performance.

Internal validity is connected to whether there are other (third) factors affecting the indicators used than the factor the study assesses [36]. In this case, the first factor would be technical security, and the second ISO/IEC 27001 certification. Annual revenue was used to choose comparable groups of banks and grid operators from Norway and Germany. However, there may be other factors making them different, impacting the results found. For example, as German grid operators may also function as water utilities, they may be larger on water distribution than electricity, causing a measuring of security performance that is more representable for the water supply sector than the energy sector.

Further, German grid operators have only had a requirement of ISO/IEC 27001 certification since January 2018. The requirement had therefore only been active for 4 years and

3 months when data was collected for this project. How long time the grid operator has followed the ISO/IEC 27001 standard may have impacted the result. On the one hand, one would expect that 4 years and 3 months should be enough time for measuring any effect of ISO/IEC 27001 certification. On the other hand, it was shown by [12] that not much had happened two years after the introduction of a legal requirement imposing intrusion detection, while after 9 years there was a significant difference. This means that large grid operators, whose average treatment effect was found to be negative, might simply need more time to implement the ISO/IEC 27001 requirements well enough into their larger organizational structures.

Another weakness in this analysis is that more small grid operators from Norway have been included than from Germany, while more medium-sized grid operators are included from Germany. As the effect of ISO/IEC 27001 certification is observed as positive for small grid operators, but non-conclusive for medium-sized grid operators, this would mean that the ATE value for all grid operator sizes combined is influenced by the size difference between Norwegian and German grid operators.

A strength regarding internal validity is that all the data was collected using both tools during the same month. In a normal DiD analysis, the time aspect is used to trace the effect of treatment through a before-and-after evaluation. In this paper, however, differences between states were used instead of differences over time. Applying the DiD time aspect would potentially introduce more uncontrolled variables. Such other variables may be new legislation entering into force, a change in nature or number of digital attacks, technological development, and changes in the economy. All these variables may be external factors causing the security level to change independently of the ISO/IEC 27001 certification. As the technique used in this paper is based on DiD logic, but avoids the time aspect, these potential threats to internal validity are avoided. Comparing security scores between two different states and two different sectors do however introduce other potential sources of error. The use of a control group should control for most of the types of non-observable heterogeneity connected to the evaluation. Still, sources of error may be seen as connected to special legislation, supervision, or other cultural aspects that differ between the states and that are different between grid operators and banks.

External validity says something about to which extent results from a study may be generalized [36]. In this study, almost all the grid operators in Norway were included, and therefore it is not necessary to generalize for the Norwegian case. Whether these results may be generalized to another state is more difficult to say. There will probably be other legislation and security cultures in other states. However, the predicted effect of ISO/IEC 27001 certification should be the same for Norwegian grid operators if Germany was swapped with another state with certified grid operators. Still, if another state has conditions that are very similar to Norway, the results could indicate what effect certification would have for grid operators in that state.

Grid operators in Norway are subject to the energy contingency regulation. The regulation is built on several international standards [9] and requires grid operators to establish internal control for information security, which is comparable with requirements in the ISO/IEC 27001 standard. However, instead of certification, Norwegian energy authorities control compliance for a selection of businesses every year. This Norwegian regime may have caused the prediction of the effect of ISO/IEC 27001 certification to be lower for Norwegian grid operators than what it would have been for grid operators from other states. If this is correct, other states with less developed sector-specific legislation and supervision would see a more prominent positive effect of ISO/IEC 27001 certification.

The reliability aspect concerns the reproducibility of the research [36]. Using security rating tools, the technical security scores in themselves are not fully transparent concerning scoring methodology. As a result, it may be challenging to compare the scores. The scores of one entity, might not in reality be comparable with the scores of another entity. The reason is that qualitative variables such as different types of security configurations have been given quantitative scores by staff working for BlackKite and Security Scorecard.

VII. Conclusion

This study has examined the effect of ISO/IEC 27001 certification on the technical security performance of Norwegian grid operators. The overall result of the analysis supports the H_0 hypothesis, that ISO/IEC 27001 certification would have no effect on the technical security performance of Norwegian grid operators. However, by controlling for entity size, the data show a significant positive effect of ISO/IEC 27001 certification for small grid operators, no clear effect in any direction for medium-sized grid operators, and indicate a negative effect for large grid operators. Therefore, for small-sized grid operators, the H_0 hypothesis can be rejected and the H_1 hypothesis, that ISO/IEC 27001 certification would increase the technical security performance, can be accepted. The indication of a negative effect for large-sized grid operators is also interesting.

This research provides a best-effort study on the effect of ISO/IEC 27001 certification on Norwegian grid operators' technical security performance. The results may support authorities' policy-making processes when considering to enforce ISO/IEC 27001 certification. Further, the study may also be useful for entities considering certification. Last, this study may stimulate more research on the effect of ISO/IEC 27001 certification.

There is a weakness connected to construct validity that should be highlighted, namely that technical security performance has been observed from outside of the firewalls and IT systems only. Further, considering internal validity, it is not known if a positive effect of ISO/IEC 27001 certification may become observable for medium and large-sized entities in the future, caused by a long implementation time for the standard. It may therefore be useful to conduct further research on the effect of ISO/IEC 27001 certification on technical

security performance. First, to see after a few more years if the average treatment effect will be positive also for medium and large-sized grid operators. Second, to assess if technical security measured on the inside of the entities' IT networks will give other results than this analysis based on non-intrusive, externally observable security indicators.

REFERENCES

[1] International Organization for Standardization and International Electrotechnical Commission, "Information technology — Security techniques — Information security management systems — Requirements," ISO/IEC Standard No. 27001:2013. Accessed: Sep. 29, 2022. [Online]. Available: https://www.iso.org/standard/54534.html

[2] Bundesnetzagentur, "Catalogue of IT security requirements," Accessed: Sep. 29, 2022. [Online]. Available: https://www.bundesnetzagentur.de/EN/Areas/Energy/Companies/SecurityOfSupply/ITSecurity/start.html

[3] European Union Agency for the Cooperation of Energy Regulators, "Framework Guideline on sector-specific rules for cybersecurity aspects of crossborder electricity flows," Accessed: Sep. 29, 2022. [Online]. Available: https://www.acer.europa.eu/events-and-engagement/news/acer-publishes-its-framework-guideline-establish-network-code

[4] International Organization for Standardization and International Electrotechnical Commission, "Guidelines for auditing management systems," ISO Standard No. 19011:2018. Accessed: Sep. 29, 2022. [Online]. Available: https://www.iso.org/standard/70017.html

[5] Ministry of Local Government and Regional Development, "Statlig tilsyn med kommunesektoren," NOU 2004:17. Accessed: Sep. 29, 2022. [Online]. Available: https://www.regjeringen.no/no/dokumenter/nou-2004-17/id386918/?ch=14

[6] S. C. Winter, and V. L. Nielsen, "Implementering af politik," 1st ed. Hans Reitzels Forlag, 2008.

[7] Federal Office for Information Security, "IT-grundschutz-compendium," 2021. Accessed: Sep. 29, 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4

[8] IT Governance, "Typical ISO 27001 Certification Costs." Accessed: Sep. 29, 2022. [Online]. Available: https://www.itgovernanceusa.com/iso27001-certification-costs

[9] J. Hagen and Ø. Toftegaard, "Cyber Security Requirements in the Norwegian Energy Sector," in Critical Infrastructure Protection, vol. XV, J. Staggs and S. Shenoi, Eds. Springer, Cham, 2022, pp. 3–21.

[10] Norwegian Water Resources and Energy Directorate, Unpublished.

[11] European Union Agency For Network and Information Security, "Mapping of OES security requirements to specific sectors," 2017. Accessed: Sep. 29, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/at_download/fullReport

[12] J. M. Storm, J. Hagen, and S. H. Selnes, "The Effect of Regulation and Audits on Implementation of Cybersecurity Controls in Norwegian Grid Companies," European Safety and Reliability Conference, Singapore, Research Publishing, 2022.

[13] L. B. Mohr, "Impact analysis for program evaluation," 2nd ed. SAGE Publications, 1995.

[14] E. Arntzen, "Ledelse og kvalitet i helsetjenesten," 2nd ed., vol. 1. Gyldendal, 2021.

[15] Ø. Toftegaard, J. Hagen, and B. Hämmerli, "Cybersecurity Audit: Relationships between Security Management and Technical Security," Unpublished.

[16] B. Edwards, J. Jacobs, and S. Forrest, "Risky Business: Assessing Security with External Measurements," 2019. Accessed: Aug. 16, 2022. [Online]. Available: http://arxiv.org/abs/1904.11052

[17] D. I. Jacobsen, and J. Thorsvik, "Hvordan organisasjonen fungerer," 4th ed. Fagbokforlaget, 2013.

[18] C. Hsu, T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance." 49th Hawaii International Conference on System Sciences, 2016, pp. 4842-4848.

[19] J. Hagen, The Norwegian Water Resources and Energy Directorate, 2022, Personal communication.

[20] International Organization for Standardization, "09. ISO Survey of certifications to management system standards – full results," 2021. Accessed: Nov. 13, 2022. [Online]. Available: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

[21] Forskrift om bruk av informasjons- og kommunikasjonsteknologi, FOR-2003-05-21-630, Accessed: Sep. 29, 2022. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2003-05-21-630

[22] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (EU) 2016/679. Accessed: Sep. 29, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[23] Directive concerning measures for a high common level of security of network and information systems across the Union, (EU) 2016/1148. Accessed: Sep. 29, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

[24] Gesetz über die Elektrizitäts- und Gasversorgung. Accessed: Sep. 29, 2022. [Online]. Available: https://www.gesetze-im-internet.de/enwg_2005/

[25] Gesetz über das Kreditwesen. Accessed: Oct. 1, 2022. [Online]. Available: https://www.gesetze-im-internet.de/kredwg/

[26] The Society for Worldwide Interbank Financial Telecommunications, "SWIFT Customer Security Controls Framework," Accessed: Oct. 1, 2022. [Online]. Available: https://www.swift.com/myswift/customer-security-programme-csp/security-controls

[27] European central bank, "What is TIBER-EU?," Accessed: Sep. 29, 2022. [Online]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[28] Wer zu wem, "Deutschlands firmendatenbank," Accessed: Aug. 18, 2022. [Online]. Available: https://www.wer-zu-wem.de/

[29] Proff, "Kreditt- og Markedsverktøy," Accessed: Aug. 18, 2022. [Online]. Available: https://forvalt.no/

[30] European Commission, "SME definition," Accessed: Aug. 18, 2022. [Online]. Available: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

[31] F. Tøien, J. Fagermyr, G. Treider, and H. Remvang, "IKT-sikkerhetstilstanden i kraftforsyningen," 2021. Oslo, Norwegian Water Resources and Energy Directorate, 2021.

[32] Security Scorecard, "Understand the cyber health of your ecosystem across 10 risk factor groups," Accessed: Aug. 29, 2022. [Online]. Available: https://www.greatamericaninsurancegroup.com/docs/default-source/cyber-risk/securityscorecard-10-risk-factors.pdf

[33] Black Kite, "Third party risk intelligance," Accessed: Aug. 24, 2022. [Online]. Available: https://blackkite.com/platform/

[34] Security Scorecard, "Consistent, data-driven ratings," Accessed: Aug. 24, 2022. [Online]. Available: https://securityscorecard.com/product/security-ratings

[35] Gartner, "IT Vendor Risk Management (VRM) Tools," Accessed: Aug. 22, 2022. [Online]. Available: https://www.gartner.com/reviews/market/it-vendor-risk-management

[36] P. Runeson, and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," Empirical Software Engineering, 14, 2009, pp. 131–164.

[37] Black Kite, "Technical Cyber Rating," Accessed: Aug. 15, 2022. [Online]. Available: https://blackkite.com/technical-grade/

[38] Security Scorecard, "Consistent, data-driven ratings," Accessed: Aug. 18, 2022. [Online]. Available: https://securityscorecard.com/product/security-ratings

[39] Forskrift om sikkerhet og beredskap i kraftforsyningen, FOR-2012-12-07-1157, Accessed: Sep. 29, 2022. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

[40] R. B. Cialdini, "Påvirkning - Teori og praksis," Oslo, Abstrakt forlag, 2003.