Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 225 (2023) 2781–2789

Procedia Computer Science

www.elsevier.com/locate/procedia

27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2023)

IT Governance and IT Compliance in Family Firms – the Special Case of Cyber Security

Patrick Sven Ulrich[a]*, Felix Stockert[b]

[a]*Aalen University, Beethovenstr. 1, D-73430 Aalen, Germany and University of Bamberg, Feldkirchenstr. 21, D-96405 Bamberg, Germany*
[b]*Aalen University, Beethovenstr. 1, D-73430 Aalen, Germany*

Abstract

As IT becomes more important to their business, the risk of family businesses falling victim to cyber-attacks is growing exponentially. Yet too often, cyber security is still given low priority within the company and is not embedded in the corporate strategy. Even established standards are rarely applied in companies. This is where the interaction between IT governance and IT compliance plays a central role. As stated in the established literature on IT compliance, deficits can result from ignorance of the relevant regulations, but also from rejection by employees. Particularly in the area of cyber risks, there is a presumption that inadequate dovetailing of governance and compliance opens the company to attacks. This paper discusses aspects of IT governance and IT compliance in family businesses based on an empirical survey of 184 German companies from 2019. It is shown that family businesses have fewer evaluation metrics for cyber risks and use an ISMS less often than non-family businesses.

Keywords: Family Firms; IT Governance; IT Compliance; Cyber Security; ISMS

1. Introduction

The increased competition resulting from globalization poses great economic challenges for companies. Flexibility within process structures is more important than ever for the competitiveness of companies. At the same time,

* Corresponding author: Patrick Ulrich. Tel.: +49-7361-9149022.
E-mail address: patrick.ulrich@hs-aalen.de

10.1016/j.procs.2023.10.270

digitization leads to the integration of IT in almost all processes, which makes IT an essential competitive factor. Globalization and international standardization also contribute to the fact that companies must comply with frequently changing regulations such as the Sarbanes-Oxley Act of 2002 to prevent balance sheet manipulation, which also affects the IT landscape.

As a result, the demands on corporate management are increasing, which requires a correspondingly functional and efficient organizational structure. This includes above all IT governance as a decision-making and organizational concept as well as IT compliance for the observance of standards and laws. While the goal of IT governance is to establish a framework that is ideally oriented to international standards such as COBIT or ITIL, compliance aims to fulfill the legal and other requirements of IT [2].

The interaction of IT governance and IT compliance should therefore be strongly interlinked, at least from a theoretical point of view. In business practice, however, this is often not the case, as there are institutional, process-related, and personnel coordination problems. We assume that the existence of coordination problems creates gaps that can be exploited by cyber attackers.

In this article, the problems of IT governance and IT compliance are extended by a special context: On the one hand, we focus on family businesses. Family businesses are of great importance for almost all economies of the world. However, they have not yet been extensively researched. In addition, the management of family businesses has some special characteristics, such as the adherence to strong corporate cultures, shared values and beliefs, and not as much writing down as in non-family businesses. This is already a problem when it comes to IT governance and IT compliance. However, the vulnerability of the enterprise in dealing with cyber threats is greatly increased because a single link in the corporate security cordon can lead to a breach in the enterprise systems. This has a significant impact on cyber security, and the risk for the enterprise to fall victim to an external cyber attack is growing.

This article examines the interaction between IT governance and IT compliance and the vulnerability of family businesses to cybercrime. The article is based on a theoretical analysis as well as an empirical study of a German family and non-family businesses and answers the following research question: *Does the management of cyber risks in the context of IT governance and IT compliance differ between family and non-family businesses*?

The most important contributions of this paper are:

1) We conducted the – to our knowledge – first empirical study concerning cyber security in family firms.
2) Our arguments are specific to family firms.
3) We find empirical proof that family firms handle cyber security differently than non-family firms.

The paper is organized as follows: Next, we present an overview of existing theoretical work. We focus on IT governance, IT compliance, and family firms. Then we discuss the sample, the variables, and the empirical results. Finally, we give a conclusion and a short outlook.

2. Theory

2.1 IT Governance and IT Compliance

The great importance of IT requires an appropriate organizational structure and the monitoring of existing standards and guidelines. The enterprise governance of IT or IT governance, as a function integrated into corporate governance, takes on activities "[...] to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT." [3] The units involved are the board of directors, the management and IT management [3].

IT compliance, as a core function of IT governance, is responsible for the monitoring of legal IT requirements in particular. It is mainly concerned with information security, the availability and storage of data, and data protection. The primary goal of IT compliance is to minimize cyber risks and avoid non-compliance, which has social, fi-nancial and legal consequences. [4]

There are several frameworks for the implementation and application of IT compliance, which those responsible can use for orientation. The international professional association Information Systems Audit and Control Association (ISACA) deals with IT audit, IT risk, and IT governance and developed the framework Control Objectives for Information and Related Technology (COBIT). The latest version, COBIT 2019, focuses on a more flexible

implementation of effective Enterprise Governance of Information and Technology (EGIT) and increasingly includes approaches from IT and general management literature, such as strategic alignment, balanced scorecards, or IT savviness. [5]

Unlike COBIT, IT Infrastructure Library (ITIL) does not contain any form templates or implementation rules. The standard for providing IT services is very general and therefore applicable to various industries. ITIL enables companies to be certified according to ISO 20000 and provides support through customer-specific process recommendations. [6]

Another framework is the Information Security Management System (ISMS) according to ISO 27001. The goal of an ISMS is to provide and process information to optimize business processes, achieve corporate goals and maintain the value of the company. Concerning trust, integrity, and availability, ISMS guarantees the protection of this information. The core topics are based on governance, compliance, and risk. [7]

2.2 Implementation of IT Compliance

The implementation of frameworks that support IT governance and IT compliance is very complex. When deciding on the appropriate standard, the type of company, the business area to be standardized, and the relevant characteristics of the standard play a major role. [8] According to a study by Horváth & Partners (2012), 63 percent of the participating IT managers use the ITIL standard, 37 percent of COBIT and a total of 27 percent do not use a standard. Multiple answers were possible here. [9]

The effort and complexity of the implementation are a result, among other things, of the high demand for skilled workers with the corresponding know-how. [1] Furthermore, the management and the board of directors must be supportive to motivate employees and set an example according to the principle of "tone from the top". After all, a high degree of employee acceptance is also important for efficient implementation and sustainable success. [1] Of particular importance are also regulations and standards, such as legal norms, regarding data protection or telecommunications, as well as various contracts and internal regulations. [1]

2.3 Characteristics of family firms

The definitions of family business vary widely. For a statistical survey, it is therefore particularly important to know which companies fall within the definition of family firms, otherwise, the results could be falsified. According to Shanker/Astrakhan (1996, p. 109), three definitions differ concerning the influence of the family as such: The comprehensive definition describes the family's involvement as small so that only strategic decisions are influenced. Within the middle definition, the founder or descendant runs the company and has legal control. If several generations of the family are directly involved in management positions and thus have sovereignty over the management and ownership of the company, they are included in the narrow definition. [10]

General differences between family and non-family firms often lie in the lower average amount of turnover and consequently the lower number of employees [11]. Nevertheless, family firms should not be equated with small businesses, as many large companies are also family-run [12]. Differences can also be seen in the capital structure: While the shares of non-family firms are usually spread over several shareholders, 79 percent of German family firms own all shares. Furthermore, the management and the supervisory board are mostly in the hands of the family. This is partly because they are often too small to maintain the legal form of a stock corporation, but also because they reject external management. [11]

The probably most important characteristic of a family business is the focus on maintaining so-called socio-emotional wealth (SEW) as part of the corporate strategy. Accordingly, family firms often prefer their image to their financial situation. This is characterized by a high level of identity with the company, which often carries the same name as the family itself. [13, 14]

2.4 IT Compliance and family firms: challenges to successful implementation

Due to the special characteristics of family firms and the high complexity of IT compliance, they face certain challenges. In particular, the tendency towards intuitive decision-making, which is usually less pronounced in non-family firms, formalized decision and control instruments as well as performance measurement is less used here. [15] The organizational structure also plays an important role. Since the board of directors usually takes on overlapping functions and no specialists are convened, [15] there is a lack of know-how in certain areas, which makes IT compliance concerning the regulations necessary [16]. In particular, ISO standards, such as ISO 27001, which describes the principles and requirements for ISMS, are therefore applied too rarely. [17] However, this is also related to the fact that the majority of family firms are small and medium-sized enterprises. The high costs involved, the high expenditure of time as well as insufficiently specialized and trained employees represent barriers for smaller family businesses that are difficult to overcome. [18]

The higher the family's share of the company's management, the more difficult it is to recruit qualified employees. One reason for this is that the chances of promotion are low, as the relevant positions have already been filled by the family. On the other hand, good-skilled workers are less willing to work in family firms because they may demand more decision-making power, which could conflict with the goal of the controlling family. [15]

3. Hypotheses

Family firms often have greater difficulties in implementing and operating intensive IT compliance than non-family businesses. The reasons for this are many and varied and are the driving forces behind the present empirical study. In the course of this study, four hypotheses were defined below and tested in the following chapter.

Especially the size of a company plays an important role in the question of how much importance companies attach to cyber security. The main reasons for this are excessive costs and a lack of qualified personnel. Since family firms are mostly organized as SMEs, the following hypothesis can be derived:

H1: Cybersecurity has a lower priority in family firms than in non-family firms.

Cyber security as a goal of the corporate strategy ensures a complete consideration of the risks associated with it. Furthermore, this is also firmly anchored in the organizational structures through the implementation of IT governance and IT compliance. Due to the low prioritization, cyber security in family firms is, however, also insufficiently structured from a strategic point of view.

H2: In family firms, cyber security is less often an integral part of corporate strategy than in non-family firms.

Due to the challenges of implementing and executing IT governance and IT compliance, family firms often have an imbalance between systems. As a result, the interaction between IT governance and IT compliance is inconsistent, resulting in information being lost and the extent of the risks not being properly assessed.

H3: Family Firms have generally less information and more problems identifying the value at risk of cyber threats.

The introduction of the standards, which serve as a framework for IT governance and IT compliance, also involves a great deal of effort. For family firms, which often have few employees and generate a correspondingly low turnover, time and cost expenditure as well as the required know-how are major hurdles. Therefore, the final hypothesis is as follows:

H4: Family firms use ISMS less often than non-family firms.

4. Methodology

The data collection was carried out using a standardized online questionnaire consisting of open and closed questions. A pre-test with several test persons was first conducted to verify the questionnaire. Subsequently, the actual survey was conducted in the period from October 23 to December 31, 2019. With the help of the Nexis database, the e-mail addresses of German companies were randomly selected in advance for this purpose.

In total, 14,495 companies were contacted by e-mail, of which 1,612 e-mails could not be delivered. Consequently, 12,883 companies received the link to the online survey. During the survey period, the online questionnaire was accessed 415 times, which corresponds to a participation rate of 3.22 percent. A total of 372 companies answered the questions asked, whereby 188 companies ended the survey before completion (utilization rate: 89.64 percent). Therefore, the sample size amounts to 184 companies, and the response rate to 1.43 percent.

In this context, it should be noted that individual questions may nevertheless be mentioned differently, as the partial non-response (item non-response) has not been considered in this report. The reason for this is that the questionnaire was consciously designed without specifying mandatory questions, as in some cases very topic-specific and sensitive data was requested. The data then was evaluated by using the tools Microsoft Excel and SPSS.

5. Variables

5.1 Independent Variables

The independent variable in the study is family influence. There are several operationalizations for this variable in the literature. Since the companies in the survey are primarily small and medium-sized enterprises and family businesses, which tend to answer less when questions are too complex, a single-item approach was chosen for the present study. To measure family influence, a 0/1 coded question "Is your company a family business" was used, which yields the variable FAMI-LY. Of the 184 companies in the study, 106 are family enterprises and 78 are non-family enterprises.

5.2 Dependent Variables

A different dependent variable was defined for each of the four hypotheses. For H1 the dependent variable is PRIO_CYBER. This variable describes the subjective priority of cyber risks in the enterprise. The variable was queried as a single-item variable on a five-level Likert scale with the response alternatives 1=very low to 5=very high.

For H2 the dependent variable is IN-TEGR_STRAT. The question here is whether companies integrate cybersecurity into their corporate strategy. This variable was measured as a binary 0/1 variable (no/yes).

For H3 the dependent variable is NO_VALMETH. The question of whether companies have no evaluation method for cyber risks was also measured as a binary 0/1 variable. In this respect, a 1 here means that companies have no valuation heuristic for cyber risks.

For H4 the dependent variable ISMS. The existence of an ISMS was also measured as a binary 0/1 variable.

5.3 Control Variables

As a control variable, as in other, organization-related studies, the company size was also chosen as a complexity-generating factor. The size of the enterprise - variable SIZE - was operationalized by the number of employees. The number of employees was surveyed in four classes:

- SIZE_99: enterprises with up to 99 employees (n=34);
- SIZE_100_999: enterprises with between 100 and 999 employees (n=122);
- SIZE_1000_9999: companies with between 1,000 and 9,999 employees (n=17);
- SIZE_10000: enterprises with 10,000 or more employees (n=4).

The class of up to 99 employees was chosen as the reference class.

6. Empirical Results

Various regression models were used to test the hypotheses depending on the scale level of the dependent variables. The following section first shows the correlations of the variables processed in the study.

6.1 Correlations

Table 1: Correlations

	FAMILY	99	100-999	1000-9999	10000	PRIO_CYBER	INTEGR_STRAT	NO_VALMETH	ISMS
FAMILY	1	-0.016	0.040	-0.030	-0.023	0.033	-0.121	**0.218****	**-0.204****
99		1	**-0.751****	**-0.171***	-0.080	-0.092	**-0.151***	0.016	-0.014
100-999			1	**-0.448****	**-0.209****	0.067	0.014	**0.145***	0.022
1000-9999				1	-0.048	0.014	**0.175***	**-0.189***	-0.101
10000					1	0.018	0.037	-0.141	**0.169***
PRIO_CYBER						1	**0.393****	**-0.171***	**0.309****
INTEGR_STRAT							1	**-0.473****	**0.388****
NO_VALMETH								1	**-0.405****
ISMS									1

Table 1 shows the correlations in this study. The variable FAMILY correlates positively with the absence of a valuation method and negatively with the existence of an ISMS. In the group of companies with up to 99 employees, cyber security is less integrated into the corporate strategy. Interestingly, the size effects differ in the valuation methods. The priority of Cyber Security correlates with the three other dependent variables. It does so positively with the integration into the corporate strategy and the existence of an ISMS and negatively with the absence of a cyber risk assessment method.

6.2 Test of Hypothesis 1

Table 2: Test of hypothesis 1

	Model 1			
Dependent Variable	PRIO_CYBER			
Independent Variable	ß-Coeff.	p-Value	Tolerance	VIF
FAMILY	0.032	0.667	0.998	1.002
SIZE100_999	0.103	0.233	0.746	1.340
SIZE1000_9999	0.063	0.458	0.779	1.284
SIZE10000	0.043	0.575	0.931	1.074
Model fit				
R^2	0.010			
Adjusted R^2	-0.013			
F (Model, global)	0.435			

The model is not suitable for the analysis of the suspected correlation and no significant effects are shown. Neither family influence nor the number of employees influences the priority of cyber security in companies. Overall, the median of the assessment of priority in the sample is 3.0. 67 companies in the sample see a medium, 67 a high, and 23 a very high relevance. This means that, regardless of the context factors examined, relevance is assessed as quite high. Family businesses are therefore not worse off than non-family businesses. Nevertheless, H1 is rejected

6.3 Test of Hypothesis 2

For hypothesis 2, a binary logistic regression was used. With a Nagelkerke r^2 of 0.081, this model is also not particularly well suited to test the correlation. The family shows a tendency to show a negative correlation to the integration of cyber security into corporate strategy - but this effect is not significant. The two company classes up to 9,999 employees show a stronger integration of cyber security into the corporate strategy. H2 is rejected.

Table 3: Test of hypothesis 2

	Model 2		
Dependent Variable	INTEGR_STRAT		
Independent Variable	ß-Coeff.	Sig.	
FAMILY	-0.512	0.104	
SIZE100_999	0.689	0.094	*
SIZE1000_9999	1.748	0.005	***
SIZE10000	1.117	0.298	
Constant	-0.861	0.031	
Model fit			
-2LL	233.170		
Cox and Snell R^2	0.059		
Nagelkerkes R^2	0.081		
ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics.			
* Significance at the 10% level (Wald test).			
** Significance at the 5% level (Wald test).			
*** Significance at the 1% level (Wald test).			

For hypothesis 3, a binary logistic regression was used.

Table 4: Test of hypothesis 3

	Model 3		
Dependent Variable	NO_VALMETH		
Independent Variable	ß-Coeff.	Sig.	
FAMILY	0.914	0.004	***
SIZE100_999	0.127	0.731	
SIZE1000_9999	-1.525	0.034	**
SIZE10000	-21.152	0.999	
Constant	-0.566	0.125	
Model fit			
-2LL	232.959		
Cox and Snell R^2	0.111		
Nagelkerkes R^2	0.148		
ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics.			
* Significance at the 10% level (Wald test).			
** Significance at the 5% level (Wald test).			
*** Significance at the 1% level (Wald test).			

The model shows the expected effect. At a 99% significant level, family firms more often than non-family firms state that they have no valuation logic for cyber-risks in the company. From a company size of 1,000 employees upwards, the companies then also show such metrics significantly more frequently - which was to be expected. H3 is confirmed.

6.4 Test of hypothesis 4

For hypothesis 4, a binary logistic regression was used.

Table 5: Test of hypothesis 4

	Model 4		
Dependent Variable	ISMS		
Independent Variable	ß-Coeff.	Sig.	
FAMILY	-0.980	0.006	***
SIZE100_999	0.132	0.758	
SIZE1000_9999	-0.945	0.265	
SIZE10000	2.291	0.064	*
Constant	-0.642	0.111	
Model fit			
-2LL	194.923		
Cox and Snell R^2	0.074		
Nagelkerkes R^2	0.109		
ß-coefficient describes the regression coefficient of logistic regression, and Sig. shows the probability of the Wald statistics.			
* Significance at the 10% level (Wald test).			
** Significance at the 5% level (Wald test).			
*** Significance at the 1% level (Wald test).			

The model for hypothesis 4 shows that family businesses are significantly less likely to operate an ISMS. In terms of company size, companies with 10,000 or more employees do so more often than others. H4 is thus confirmed by the model with acceptable model quality.

7. Conclusion

This article aimed to take a closer look at the interaction of IT governance and IT compliance in family businesses and to apply these findings to the specific context of cyber security. Here we have prepared what we believe to be the first empirical study on cyber security with a focus on German family businesses.

Four hypotheses were in the foreground, which were tested for their validity employing a literature analysis and statistical methods. The assessment that family businesses assign a lower significance to cyber security than non-family businesses could not be confirmed, at least from the perspective of the survey. The majority of the companies show a high level of awareness of cyber security. The second hypothesis regarding the integration of cyber security into corporate strategy could not be confirmed either. Here, no differences between family and non-family businesses are apparent.

Significant results are shown for the assessment of cyber risks and the ISMS. Family businesses have less often an evaluation metric for such risks, which greatly reduces the success of the defense and correction of the damage. An ISMS to defend against cyber attacks is also used less often in family businesses than in non-family businesses.

A closer look at the results reveals the great importance of the size of the company: The larger the company, the higher the priority of cybersecurity and the more likely it is that it will become part of the corporate strategy (see H1 and H2). The neglect of cyber security and especially IT compliance therefore mainly affects small and medium-sized family businesses.

The analysis also shows that uncovering cyber risks and assessing the value at risk in family businesses often leads to complications and takes a long time (H3). The main reason for this is the insufficient interaction between IT governance and IT compliance, which leads to regular information losses. An ISMS according to ISO 27001 is not sufficiently implemented even in family businesses (H4), so there are often no rules or methods to support the information security of the company.

Family businesses, especially the smaller ones, are therefore very vulnerable to cyber-attacks. Such an attack can take on existential proportions, as the costs, especially for SMEs, can no longer be covered. This problem is becoming increasingly important in the course of digitalization. It is therefore essential to constantly improve the interaction between IT governance and IT compliance to protect the company as much as possible from cyber threats.

7.1 Limitations

Like any other empirical study, our study is subject to some limitations: We conducted the study as a survey and single-respondent design only limited to Germany in 2019. Even though we conducted 10 accompanying expert interviews to increase validity and reliability, the low response rate and a potential non-response bias must also be mentioned as problems in addition to the design. Furthermore, we cannot make any statements with the present design about the reasons why family businesses and non-family businesses may differ in their behavior.

7.2 Future Work

Future work must penetrate deeper into the nature of family businesses and also the interactions of specific corporate culture, IT, and organizational structure. For this purpose, a qualitative follow-up study with case studies will be conducted.

References

[1] Fröhlich, Martin and Glasner, Kurt. (2007) “IT Governance – Leitfaden für eine praxisgerechte Implementierung,” Springer Gabler, Wiesbaden.

[2] PwC. (2017) “ IT governance framework”.

[3] Grembergen, Wim van. (2004) “Strategies for Information Technology Governance*”, Idea Group Publishing*, Hershey/London.

[4] Kniese, Ralf and Bülchmann. Oliver. (2015) “IT-Compliance als Teil der Corporate Governance”, Wirtschaftsinformatik & Management, Springer: 34–47.

[5] Haes, Steven de, Grembergen, Wim. Van, Joshi, Anant, Huygh, Tim. (2020) “Enterprise Governance of Information Technology. Achieving Alignment and Value in Digital Organizations”, Springer, Cham.

[6] Sahibudin, Shamsul, Sharifi Mohammed, and .Ayat, Masarat. (2008) “Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations”, *Second Asia International Conference*: 749-753.

[7] Funk, Gerhard., Hermann, Julia, Holl, Angelika, Jeliazkov, Nikolav, Knörle, Oliver, Krsic, Boban, Müller, Nico, Oetting, Jan, Rozek, Jan, Rupprich, Andrea, Sattler Tim, Schmid Michael and Schrader, Holger. (2016) “Implementierungsleitfaden ISO/IEC 27001:2013, ISACA Germany Chapter e.V., Berlin.

[8] Briscoe, J. (unknown date) “Standards zur Einführung. Anwendung im Unternehmen”, Bitkom, Berlin.

[9] Urbach, Nils and Gschwendtner, Michael- (2012) “IT-Governance in der Unternehmenspraxis” Horváth & Partners.

[10] Shanker, Melissa and Astrachan, Jospeh. (1996) “Myths and Realities: “Family firms’ Contribution to the US Economy—A Framework for Assessing Family Business Statistics”, *Family Business Review, SAGE Publications*: 107-123.

[11] Klein, Sabine. (2000) “Family Business in Germany: Significance and Structure”, *Family Business Review, SAGE Publications*: 157–181.

[12]. Litz, Reginald. (1995) “The Family Business: Toward Definitional Clarity”, *Family Business Review, SAGE Publications*: 71–81.

[13] Berrone, Pascual, Cruz, Cristina and Gomez-Mejia, Luis. (2012) “Socio-emotional Wealth in Family Firms”, *Family Business Review, SAGE Publications:* 258-279.

[14].Strankiewicz, Johannes. (2016) “Socioemotional wealth and the performance of family firms: The role of identification and transgenerational control”, University of St. Gallen, Bamberg.

[15] Hiebl, Martin, Duller, , Christine, Feldbauer-Durstmüller, Birgit, and Ulrich, Patrick. (2015) “Family Influence and Management Accounting Usage – Findings from Germany and Austria”, *Schmalenbach Business Review*, Springer: 368-404.

[16 Schäfer, Gabriele, Strolz,, Günter, Hertweck, Dieter. (2008) „IT-Compliance im Mittelstand“, Springer: 69-77.

[17] Ulber, Karl. (2016) „IT-Compliance durch Nutzungsanalyse“, Erich Schmidt Verlag, Berlin: pp. 193-240.

[18] Techconsult GmbH, IT-Sicherheit im Mittelstand. (2020) - Unwissenheit ist das größte Übel, Kassel.