Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different cultures

Dissertation with the aim of achieving a doctoral degree
at the Faculty of Mathematics, Informatics and Natural Sciences
Department of Informatics
of Universität Hamburg

Bahareh Shojaie

February 20, 2018

Gutachter:

Prof. Dr. Hannes Federrath
Prof. Dr. Dieter Gollmann

Tag der Disputation:

January 22, 2018

Abstract

In this thesis, we investigate the potential relationship between national cultural, political and economic characteristics regarding the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). ISO 27001 is the most adopted international ISMS (Information Security Management System) standard, which provides IT governance by protecting sensitive data in a structured way. Although ISO 27001 is a generic standard for all organisations and countries, some countries have yet to adopt ISO 27001 extensively. The relationship between culture (mind-set and behaviour) and the adoption of an ISMS standard such as ISO 27001 has not been investigated yet. Based on our qualitative analysis, we observe a relationship between national cultural characteristics of a country and the number of issued ISO 27001 certificates. In our quantitative analysis, we separate countries into two groups based on the average number of the total ISO 27001 certificates that were issued worldwide (2006–2014). A common comparison approach may not be helpful for investigating the relationship between the adoption of ISO 27001 and the national cultural, political and economic characteristics of several countries from different continents. For countries with more than the average number of the ISO 27001 certificates issued worldwide (2006–2014), we observe a relationship between the regulation density (regulation of credit, labour, and business), GDP (Gross Domestic Product; a monetary measure of a country's economy and economic performance that equalises the purchasing power of different currencies divided by population), and the average degree of comfortableness with uncertainty of people in a country on one side, and the adoption of ISO 27001 on the other side. For countries with less than the average number of the ISO 27001 certificates issued worldwide (2006–2014), we observe a relationship between the average degree of individualism of people in a country, the GDP, and the relation to authority and the expected level of hierarchical order of people in a country on one side, and the adoption of ISO 27001 on the other side. The correlation does not imply causality in this thesis.

Kurzfassung

Diese Arbeit untersucht die potenzielle Wechselwirkung zwischen nationalen kulturellen, politischen und wirtschaftlichen Charakteristiken, die als Gegenstand dieser Arbeit ausgewählt wurden, und der Umsetzung von ISO 27001, die wiederum anhand der durchschnittlichen Anzahl von herausgegebenen Zertifikaten (2006–2014) gemessen werden kann. ISO 27001 ist der am meisten umgesetzte internationale Standard für Managementsysteme der Informationssicherheit (ISMS, engl. Information Security Management System), der den Schutz von sensiblen Daten in einer strukturierten Art und Weise und damit IT-Governance bietet. Obwohl ISO 27001 einen für alle Organisationen und Länder allgemeingültigen und generischen Standard darstellt, müssen viele Länder ISO 27001 noch umfangreich umsetzten. Die Beziehung zwischen Kultur (Denkweise und Verhalten) und der Umsetzung eines ISMS-Standards wurde bisher noch nicht untersucht und ist Gegenstand dieser Arbeit. Basierend auf einer qualitativen Analyse können wir eine Beziehung zwischen nationalen kulturellen Charakteristiken und der Anzahl der herausgegebenen ISO 27001 Zertifikate beobachten. Darüber hinaus haben wir im Zuge unserer quantitativen Analyse basierend auf der durchschnittlichen Anzahl aller herausgegebenen ISO 27001 Zertifikate weltweit (2006–2014) Länder in zwei Gruppen eingeteilt, um die Wechselwirkung zwischen der Umsetzung von ISO 27001 und nationalen kulturellen, politischen und wirtschaftlichen Charakteristiken zu untersuchen. Ein gemeinsamer Ansatz zum Vergleich erscheint bei dieser Untersuchung verschiedener Länder auf unterschiedlichen Kontinenten nicht hilfreich. Bei Ländern mit einer überdurchschnittlichen Anzahl an herausgegebenen ISO 27001 Zertifikaten (2006–2014) beobachten wir eine Beziehung zwischen der Regulierungsdichte (Regulierung von Banken, Arbeitswelt und Gewerbe), dem Bruttoinlandsprodukt (BIP, eine monetäre Maßeinheit der Wirtschaftskraft eines Landes, die gleichzusetzen ist mit der Kaufkraft verschiedener Währungen geteilt durch die zugehörige Population) sowie dem durchschnittlichen Grad an Risikobereitschaft von Bewohnern eines Landes auf der einen Seite und der Umsetzung von ISO 27001 auf der anderen Seite. Bei Ländern mit einer unterdurchschnittlichen Anzahl an herausgegebenen ISO 27001 Zertifikaten (2006–2014) beobachten wir eine Beziehung zwischen dem durchschnittlichen Grad an Individualismus von Bewohnern eines Landes, dem BIP sowie der Beziehung zu Autorität und dem erwartetem Grad an hierarchischer Ordnung von Bewohnern eines Landes auf der einen Seite und der Umsetzung von ISO 27001 auf der anderen Seite. Die Wechselwirkungen implizieren keine Kausalität in dieser Arbeit.

Acknowledgements

I am grateful to express my sincere gratitude to Prof. Dr. Hannes Federrath for the continuous support of my Ph.D study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis significantly.

Besides my advisor, I would like to thank Prof. Dr. Dieter Gollmann, for his insightful comments and encouragement to widen my research from various perspectives.

I wish to give my heartfelt thanks to *"my angel, my heart, my entire world and my everything: Imanam"*, *"my precious: Mom"* and *"my hero: Dad."*, and I would like to dedicate this thesis to *"my best friend even before I was born: Mom"*.

Contents

List of Figures

List of Tables

Abbreviations

ASEAN	Association of South East Asian Nations
BSI	British Standards Institution
BSI	Federal Office for the Information Security
CCSC	Commercial Computer Security Centre
CISO	Chief Information Security Officer
DoD	Department of Defence
DTI	Department of Trade and Industry
DTTL	Deloitte Touche Tohmatsu Limited
EAP	East Asia and Pacific
FISMA	Federal Information Security Management Act
GDP	Gross Domestic Product
GLOBE	Global Leadership and Organisational Behaviour Effectiveness
IDV	Individualism
IEC	International Electrotechnical Commission
IMF	International Monetary Union
ISO	International Organisation of Standardisation
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ITU	International Telecommunication Fund
LSR	Least-Squares Regression
MATLAB	MATrix-LABoratory
NAMA	National Information Security Management System
NATO	North Atlantic Treaty Organisation
NCC	National Computing Centre
NCSC	National Computer Security Centre

OECD	Organisation for Economic Cooperation and Development
PDCA	Plan-Do-Ceck-Act
PDI	Power Distance Index
PPP	Purchasing-Power-Parity
RCBs	Registered Certification Bodies
RSME	Root-Mean-Square Error
ROSI	Return on Security Investment
SOA	Statement of Applicability
SCA	South and Central Asian Affairs
STOPE	Strategy, Technology, Organisation, People and Environment
TCSEC	Trusted Computer System Evaluation Criteria
Trinidad	Trinidad and Tobago
UAE	United Arab Emirates
UAI	Uncertainty Avoidance Index
UK	United Kingdom
UN	United Nations
USA	United States of America
WEIRD	Western and educated who are from industrialised, rich and democratic countries
WEO	World Economic Outlook

Chapter 1

Introduction

1.1 Introduction

An ISMS (Information Security Management System) consists of instruments and methods that management of an organisation should use in order to satisfy information security for all tasks and activities. To maintain an appropriate level of information security, a strong interaction is required between technology, organisation, and humans [HP06] to ensure protection against potential risks. A set of policies and procedures are required for managing an organisation's sensitive data. Therefore, an ISMS should include organisational structure, procedures, and resources [Boe09]. ISMS international standards are developed to provide a common approach to implement and operate an ISMS at a high-level structure with common terms and core definitions, which are coherent within a global system [BHSS14]. Besides that, international standards are strategic tools to help organisations save costs and enhance customer satisfaction [Boe08]. Therefore, the ISO (International Organisation for Standardisation)/IEC (International Electrotechnical Commission) 27001 provides a best practice approach for establishing, implementing, maintaining and continually improving an ISMS. This process is necessary for the IT security management of an organisation, which determines desired security goals for business processes. ISO 27001 is a systematic IT governance approach to meet an organisation's own information security requirements whose purpose is to keep the business afloat [FSH03] based on customer demands and legal system requirements [Can14].

TABLE 1.1: Regional share of ISO 27001 certificates (2006–2014) in percentage [Int14]

Region	**'06**	**'07**	**'08**	**'09**	**'10**	**'11**	**'12**	**'13**	**'14**
East Asia and Pacific	72	71	62	57	56	55	53	48	47
Europe	18	18	23	27	30	31	32	35	36
South and Central Asia	6	6	9	10	8	8	8	9	9
North America	1	1	2	2	2	2	2	3	3
Middle East	0.6	0.9	1	1	1	1	1	2	2
Central and South America	0.3	0.5	0.8	0.8	0.7	0.9	1	1	1
Africa	0.1	0.1	0.2	0.4	0.3	0.2	0.3	0.4	0.3

Protecting company data, sensitive information, and internal network security are possible motivations for implementing ISO 27001 [Fre07], which provides a best practice framework for identifying necessary security controls.

ISMS is a globally relevant topic, but the number of publications focusing on the ISO 27001 international standard is small [SAT12a, EUE09]. They described that adoption with real world situation and fulfilling organisational requirements are the main concerns of implementing ISO 27001. There is a lack of scholarly interest in ISO 27001 even though it is the single reference for an ISMS [FVB08]. ISO 27001 may help to improve organisational performance in fields such as legal, finance, management and operations [SG11]. The world distribution of ISO 27001 certifications in 2014 is presented in Table 1.1. The years from 2006 until 2014 are abbreviated as '06 until '14.

This thesis investigates the relationship between the adoption of ISO 27001 in terms of the average number of certificates issued (2006–2014), and the national cultural, political and economic characteristics that are selected for the purpose of this thesis (cf. 3.3.4). The relationship between culture (mind-set and behaviour) on the information security field has not been a topic of public and scientific interest [FAE14] yet, and the relationship between national cultural characteristics and the adoption of ISO 27001 still remains to be explored. Our results show a relationship between certain national characteristics on one side and higher adoption rate of ISO 27001 on the other side. The observed correlation is not indicative of a causal relationship.

The following sections explain the problem, motivation, research questions and the outline of the research.

1.2 Research Problems

IT systems are part of larger socio-technical systems, embedded in social, economic, and political structures, and users use these systems with different technical knowledge or skills for different purposes. The interactions between these diverse structures and the IT systems result in a high complexity. Organisations usually use standardisation as a means to describe the behaviour of these systems whose components interact in multiple ways. Information access and protection should be managed in changing environments and complicated situations for adopting legal system requirements, international standards, and internal policies [Rol02]. The main goal of an ISMS is to detect and prevent security breaches by security controls, such as policies [SG11]. However, a potential reason for security breaches in organisations is the inability to focus on non-technical issues such as procedures and strategies [Boe09, GAM11, AHK13]. These non-technical issues can help to reduce threats and control damage caused by security breaches [Bro06, Int13]. Traditionally, an ISMS is based on controlling employees, and policy documents are defined to inform employees about the expected behaviour [Ifi14a]. Accordingly, the main part of this thesis is based on the controls that deal with people and national cultural characteristics.

It is important to understand how peoples' mind-set or behaviour is related to the adoption of an ISMS standard as the main concern to address in this thesis. The ways employees define their attitudes toward responsibility could be related to the way they conduct their behaviour [HP11] to fit updated organisational policies and procedures [VNB93, HP11]. Besides, cultural behavioural restrictions of some Western countries are not applicable to the countries in the Far East. For example, Japanese quality control procedures are not widely adopted in the Western world [Boe09], which shows the relationship between national culture and the adoption of a definite rule, principle, or measure established by an authority.

The main cultural characteristics that could be related to adopting an ISMS standard, especially ISO 27001 are found at the national level [FVB08, Boe08, HP06, Can14, Gla09, Int14]. Thus, information security culture is related to national characteristics and the industry brand the organisation comes from, and there is a relationship between

national characteristics and the adoption rate of ISO 27001 certificates [HP06, FVB08, KS14, FVB08, BMG01].

Most organisations focus on defining effective policies based on the information security requirements [SG11]. Security policy as an accepted top-level statement with a group of rules or action plans is meant to improve information security behaviour [FCL10]. Investigating the relationship between national characteristics and employees' behaviour and mind-set could be helpful to guide employees in such a way as to match the organisational requirements as the other concern to address in this thesis. Finding the relationship between cultural characteristics and the implementation of ISO 27001 based on the cultural dimensions is not addressed adequately.

The main research problem is based on the relationship between national cultural characteristics and the implementation of ISO 27001. Therefore, this thesis analyses the correlation between an average number of ISO 27001 certification from 2006 to 2014 and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4) to address the main concerns that exist in the literature [Boe08, HP06, Dhi01, KMKRNF06, ST03, KNV04, FS09, SSA16].

The next section defines the motivation of this research.

1.3 Relevance and Motivation

According to [CJL+13], most security attacks are performed locally, and organisations should consider IT security risk treatments for internal and external attacks. Employees' mistakes were the main cause of information security breaches in 2014 [SMP14]. One of the possible reasons is assigning inadequate priority to security by senior management. The motivation for writing this thesis is the recent news about employees' security breaches [KWU12, Ben11, GLL03, ITU15, Ver14, McA14, CG16, PwC15] that has constantly intrigued us [FMS07, AS99, BS12, KS14] to investigate the adoption of ISO 27001 as a standard reference for an ISMS.

Standardisation implies uniformity; a standard reference is helpful to shape a desired organisational culture based on information security requirements. Culture implies adaption to individual circumstances that constructs people's motivation and judgment

[Ifi09]; cultural dimensions are related to organisational administration and achievements such as decision-making, work motivation, negotiation, human resource practices, as well as leadership [KMKRNF06]. For example, two branches of the social sciences, namely economics and psychology, have been considered in [Gla09] to address people's behaviour in China. Besides that, seven countries were analysed to investigate their distinct security behaviour; for example, French had the most secure behaviour, while Asian countries behaved less securely [SSC+17]. What is more, they demonstrated that self-confidence in computer security knowledge has a higher influence on security behaviour compared to the participants' actual knowledge about computer security [SSC+17] to address people's mind-set. The implementation of ISO 27001 was analysed in Indonesia based on their national information security requirements [Can14] to address national characteristics. That is why it would be useful to analyse the adoption of ISO 27001 as the success of organisations in improving the security level is related to the selected information security standards and appropriate implementation according to their requirements and features.

Although ISO 27001 is a generic standard for all types of organisations and countries, some countries have not adopted ISO 27001 extensively, which could be related to the cultural challenges that are mostly based on the end-user tasks. Understanding these cultural challenges are helpful to guide employees to conduct their behaviour as expected based on the organisational security requirements. The low adoption rate of ISO 27001 might be related to the inability of selected policies and controls in providing the expected organisational information security level [SAT12a, EUE09]. This gives some insight into the characteristics of a solution that is related to the selection, implementation, and certification of ISO 27001 based on the national cultural, political and economic fields.

Overall, investigating the potential relationship between national cultural characteristics and the adoption of ISO 27001, and the limited numbers of publications are the main motivations for this thesis.

The next section clarifies the research questions.

1.4 Research Questions

To understand the relation of culture to the information security activities, this thesis investigates the correlated national characteristics with the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). This thesis focuses on the following research questions:

1. What are possible relations between economic and political characteristics and the adoption of ISO 27001?
2. What are possible relations between the national cultural characteristics and the adoption of information security guidelines and ISO 27001?
3. How are cultural, economic and political characteristics correlated with the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014)?

1.5 Contribution

In order to answer the first research question, a literature review is conducted (cf. 1.4). The significance and main results of this research are indicated by first explaining the cultural, political and economic characteristics (cf. 3.3.4) as they provide the basis of our analysis. The political and economic characteristics are mainly based on a quantifiable measurement in comparison with cultural characteristics that are mostly descriptive, subjective or difficult to measure. Accordingly, we distinguish the first and the second research questions. The second research question is addressed with qualitative analyses (cf. 1.4), which is based on the relationship between national cultural characteristics and the adoption of ISO 27001. The third research question is addressed with our quantitative analyses (cf. 1.4) based on the characteristics that are selected for the purpose of this thesis that are classified in three fields of culture (UAI, PDI, IDV), politics (legal systems and property rights, regulation), and economy (GDP (Gross domestic product) based on PPP (purchasing-power-parity) per capita):

- **UAI**: Uncertainty Avoidance Index; the degree of comfortableness with uncertainty and the expected level of controlling the future (cf. 2.3.2),

- **PDI**: Power Distance Index; the relation to authority and the expected level of hierarchical order (cf. 2.3.2),
- **IDV**: Individualism index; self-image as "I" or "we" and the expected level of taking care of only themselves (cf. 2.3.2),
- **Legal systems and property rights**: ability of individuals to accumulate private property, secured and protected by clear laws that are enforced by the government (cf. 2.4.1),
- **Regulations**: regulations and bureaucracy to limit market entry and regulatory restraints to limit the freedom of exchange in credit, employment, and product markets (cf. 2.4.1),
- **GDP-PPP** Gross Domestic Product Purchasing Power Parity; a monetary measure of a country's economy and economic performance that equalises the purchasing power of different currencies divided by population, we refer to this characteristic as GDP-PPP (cf. 2.4.2).

Our contribution is based on analysing the correlation between the characteristics that are selected for the purpose of this thesis of two groups of countries and the adoption rate of ISO 27001, in terms of the average number of certificates issued (2006–2014). Based on our results, the information security culture of the countries of the first group with more than the average certification rate of 66 (2006–2014) is distinct from the countries of the second group with less than the average certification rate of 66. In our analyses, we observe correlations that do not imply causal relationships, and there are other factors that might have interfered with the results.

For countries with more than the average certification rate of 66 (2006–2014), we observe a relationship between the average number of ISO 27001 certification and:

- **UAI** (cf. 2.3.2),
- **Regulations** (cf. 2.4.1),
- **GDP-PPP** (cf. 2.4.2).

Given the evidence, it looks like they are related; however, there are other possible influential factors that have not been studied in this thesis (cf. 4.5). It is observed that

there is a relationship between the countries with relatively high regulations and GDP-PPP, a low UAI on one side, and higher ISO 27001 adoption rates on the other side for the countries of the first group. However, countries with less than the average certification rate of 66 (2006–2014), we observe a relationship between an average number of ISO 27001 certification and:

- **PDI** (cf. 2.3.2),
- **IDV** (cf. 2.3.2),
- **GDP-PPP** (cf. 2.4.2).

To sum up, we find a relationship between average number of ISO 27001 certification from 2006 to 2014 and the cultural, political and economic characteristics that are selected for the purpose of this thesis (cf. 3.3.4) based on two groups of countries, and we cannot draw ultimate conclusions from the results due to the factors that have not been studied (cf. 4.5).

1.6 Outline

This thesis is divided into two analysis parts: a qualitative analysis based on national cultural characteristics and a quantitative analysis based on statistical models. The first part of this thesis, qualitative analysis, is based on a literature review, ISO 27001 survey 2014 [Int14], Annex A security controls (cf. A) of ISO 27001 [Int13], and Hofstede [Hof83] cultural publications (cf. 2.3.2). In our qualitative analysis, the relationship between cultural characteristics and the adoption of ISO 27001 are investigated, and the reasons for developing and implementing national information security guidelines are analysed. In the second part, quantitative analysis, we develop a model for analysing the correlation between ISO 27001 average number of certification and the cultural, political and economic characteristics that are selected for the purpose of this thesis (cf. 3.3.4).

This thesis comprises seven chapters: introduction, fundamentals, related work, methodology, and results as well as the conclusion. The first chapter establishes the research basis, including motivation, contributions, and research questions. The second chapter,

background of the study, introduces the fundamentals of this thesis, such as an ISMS, ISO 27001 and the cultural, political and economic characteristics, while the third chapter presents the related work on the cultural characteristics and information security, especially the adoption of ISO 27001 and the relationship between the characteristics that are selected for the purpose of this thesis and the implementation of ISO 27001 is investigated. The results of this research are explained in two separated chapters. The fourth chapter presents the results of the qualitative analysis. The fifth chapter defines the research methodology of the quantitative analysis and chapter six analyses the results of the quantitative analysis. Both the fourth and sixth chapter contains a discussion and the implications on implementing ISO 27001, and the last chapter concludes this thesis.

Chapter 2

Fundamentals

2.1 Introduction

This chapter provides the fundamentals of this thesis, which is divided into four main sections. In the first section, an overview of the ISMS (Information Security Management System) structure and development process as well as the ISO 2700x family of standards are provided. The history of ISO 27001 and certification process are also covered in this section. In the second section, we explain culture, cultural characteristics, and then the cultural dimensions. Then in the third section, we describe the political and economic characteristics, which are later used in our analysis. After describing the basis of our analysis, we explain in the last section the Global Cybersecurity Index that is a measure of each nation state's level of cybersecurity development. We expand cultural, political and economic characteristics to describe how they might be related to the adoption of ISO 27001 in the next chapter.

2.2 Information Security Management System

People, governments, and organisations are all concerned about information security issues that affect economic, social, political and technical features [FCL10, ITU15, SSA16, FAE14, DF06, EE05]. An ISMS (Information Security Management System) manages an organisation's sensitive data by establishing, operating, reviewing, and improving

information security, which addresses employees' behaviour as well as data and technology. An ISMS helps organisations to establish countermeasures to information security-related vulnerabilities, which provides a secure base to grow and meet several legal expectations and information security requirements for organisations.

An ISMS consists of different processes, which begins with identifying security requirements and is continued to meet these requirements with necessary strategies and measuring results. Most security requirements come from the business an organisation is engaged in, and the other sources of security requirements could be legal, regulatory and contractual requirements as well [Bre07]. The organisation's security requirements, objectives, process as well as size, and structure influence an ISMS. To protect assets within an organisation, an ISMS provides a set of procedures and guidelines for managing resources and activities. In addition, to ensure consistent application of the security principles and policy statement [PL14], an ISMS consists of all instruments and methods the leadership should use to satisfy the information security in all tasks and activities.

The goal of an ISMS is to manage risk. In order to identify and measure organisational risk and to ensure business continuity, security policies and controls for risk mitigation are implemented. For supporting the security policy implementation, comprehensive documentation of all security processes is required. The structured management of information security as result of implementing an ISMS requires a process for creating, communicating, and maintaining policies and procedures within an organisation. Standardisation of information security management processes provides several advantages, such as reducing costs or enhanced system compatibility [Boe09].

An ISMS standard provides requirements for an ISMS, which could mitigate IT security incidents, contractual penalties or loss of reputation, such as revealing confidential customer information [Fre07].

An international standard for governing information security could improve information security methods in a competitive environment, which provides common reference points between organisations and countries. At an international level, a common shared ISMS standard could provide a consistent way of addressing information security issues between countries. Compliance with information security legislations at international level is one of the concerns of organisations in international communications, which could be addressed by an ISMS standard such as ISO 27001.

In the next section, the process of developing an ISMS is described, based on ISO 27001.

2.2.1 Processes of Developing an ISMS Based on ISO 27001

For developing an ISMS, the first step is to define the scope of the ISMS in terms of the organisational characteristics, business, its location, assets, and technology, which includes any interfaces with other systems and organisations. The scope of an ISMS may include the whole organisation or specific and identified sections of an organisation [AHK13]. It can be targeted towards a particular type of data, such as customer data, or it can be implemented in a comprehensive way that becomes part of the organisation's structure. As a part of the overall management system, an ISMS consists of interrelated or interacting elements of an organisation to establish policies, objectives, and processes to achieve objectives. To achieve organisational and ISMS objectives, an appropriate risk assessment is established based on the threats and assets within the scope of the ISMS, vulnerabilities, and impacts on an organisation. Based on the risk evaluation process, the control domains and controls for the treatment of risks are selected. The control domains, controls selected and the reasons for their selection are also documented. Then, the next stages of implementing, operating, monitoring, maintenance and improvement of the ISMS are started. ISO 27001 describes best practices for developing an ISMS as one of the standards of the ISO 2700x family, which helps organisations keep information assets secure.

ISO 27001 provides a systematic approach, which ensures the confidentiality, integrity, and availability of corporate information, applicable to all types and sizes of organisations. ISO 27001 main components are processes and policies [PL14] to help organisations safeguarding their information and physical assets in a structured manner. ISO 27001 is also the main reference standard for complying with various international laws and regulations. This compliance is based on organisational business policy, strategy, and contractual obligations. Especially, in the case of litigation or regress claims (on the grounds of inadequate information security), ISO 27001 certification could be beneficial [Int13]. For example, ISO 27001 can help management to prove an acceptable level of data protection, in case of security incidents [FVB08].

ISO 27001 provides awareness to protect against the information security vulnerabilities, which includes the requirements for continual improvement, as well as corrective and preventive action. ISO 27001 has a cycling process for developing, executing, monitoring and verifying security controls, which are flexible based on organisational information security requirements. Besides that, ISO 27001 does not mention any method for collecting, constructing and documenting the required information, which are all necessary steps for implementing this standard.

For implementing an ISMS compliant with ISO 27001, the scope of implementing ISO 27001 in an organisation and the ISMS policies are defined as a link between management and the information security activities. Afterwards, a risk assessment methodology is selected to define the rules for identifying the assets, vulnerabilities, threats, and impacts to decrease the risks that are not acceptable to the organisation. Then, a document is provided to describe the selected controls that are applicable to the organisation, the reasons for such decisions, and a description of how to implement selected controls [BHSS14]. Afterwards, the effectiveness of these controls should be measured to assess the fulfilment of objectives of the whole ISMS and each applicable control. For implementing the controls and policies, the people should be trained to be able to perform as expected [HP06]. At this stage, the ISMS policy, controls, processes, and procedures are operated, implemented and monitored based on the objectives for the controls and the measurement methodology, and then the internal audits are performed. Subsequently, the management should be informed and make decisions about the key issues related to ISMS. The most important step is management support for budget and human resource allocation because ISO 27001 is established based on responsibilities, planning, and requirements. Then, ISO 27001 requires systematic corrective and preventive actions to maintain and improve the ISMS.

The organisation should assign responsibilities for implementing information security objectives, such as internal and external staff for ISMS communication. The organisation shall determine who measures implementation and effectiveness of the ISMS and analyse the results of this evaluation afterward with clearly defined responsibilities.

Adopting ISO 27001 involves almost all employees and different sections of an organisation, and several roles are required for developing this standard. The CISO (Chief Information Security Officer) should define policies, procedures, and guidelines based

on the organisational security requirements. The CISO should ensure the security of data, applications, and data communication systems [RMC07, Bre07, BMG01]. Senior management plays an important role in motivating employees to follow policies, as compliance with the selected information security standard is one of the main concerns of senior management [MB82]. Accordingly, senior management should consider organisational culture to guide employees' behaviour in a way to match the desired information security culture [ZM13]. The management decisions for developing ISO 27001 is significant [BSKF11], such as approving selected controls and confirming essential resources.

ISO 27001 precisely mentions the involved people such as relevant external parties to communicate information security policies, and contractors to understand their responsibilities [Int13]. Selected internal auditors are also required to conduct internal audits at planned intervals to ensure objectivity and fairness of the audit process. Data operators or end users are the main executers of ISO 27001 rules and policies who have access to information and use safeguards as the first defence layer of an organisation, for example, employees, third parties or contractors [HP06]. ISO 27001 also takes stakeholders into account to ensure an adequate level of risk management process [Bre07], whose legal system and contractual requirements should be determined.

The next section introduces the history of ISO 27001 and the most important standards in ISO 2700x family of standards.

2.2.2 ISO 27001 History

The Green Books code of practice came in a green cover and therefore became known as the Green Book, which consists of evaluation criteria and certification schemes for IT security management in organisations [DTI89]. The CCSC (Commercial Computer Security Centre) of the British DTI (Department of Trade and Industry) published the User's code of practice and the Vendor's code of practice as codes of good security practice in 1989. Some sections of the Green Books shaped the BS 7799 standard for IT security [27098]. Subsequently, BS7799 was split into two parts in 1999, which covers both code of practice (BS7799-1) and specifications for certification (BS7799-2), which was revised in 1999.

The British companies and the NCC (National Computing Centre) developed the User's code of Practice for information security management in 1993. The Code of Practice for IT Security Management was the result of further revision as the British standard BS 7799:1995. Several organisations outside of the UK (United Kingdom) used the standard as a best practice guideline for the information security management. It was revised because of extensive international interests to include new technologies and processes such as E-Commerce and mobile computing in 1999.

The ISO (International Organisation for Standardisation) is an international organisation for standards from different national standard organisations [Int13]. The IEC (International Electrotechnical Commission) publishes international standards for all electrical, electronic and related technologies [Int05]. The ISO and IEC cooperated to publish the next information security standard.

The first part of BS 7799 was published as ISO/IEC 17799 in 2000 and revised again in 2005 under the name ISO/IEC 17799:2005. The result of the next revision was ISO/IEC 27002:2005. The second part of BS 7799, namely BS 7779-2, was revised in 2002 to be compatible with other management standards changes, such as ISO 9001:2000. The ISO and the IEC published ISO/IEC 27000 as a composition of different information security standards for information security management, risks and controls within an ISMS. The ISO information security standards before the ISO 2700x family of standards were ISO 13335 and the aforementioned ISO 17799.

ISO 27000 provides an overview and vocabulary, while ISO 27002, offering the code of practice for an ISMS, contains general recommendations for information security activities. In the beginning of 2007, ISO 17799 was renamed as ISO 27002, which consists of management level recommendations for IT security management. ISO 27002 is a reference for selecting commonly accepted controls in the process of implementing an ISMS, based on the specific information security risk environment of each organisation. The ISO committee finally released ISO 27001:2005 as part of the ISO 2700x family. The ISO committee published the latest revision of the standard in September 2013. Figure 2.1 shows the history of information security documents from the 1980s to the ISO 27001 update in 2013. Following the changes in the structure and content of the international standard for information security, the next section describes ISO 27001 in more details.

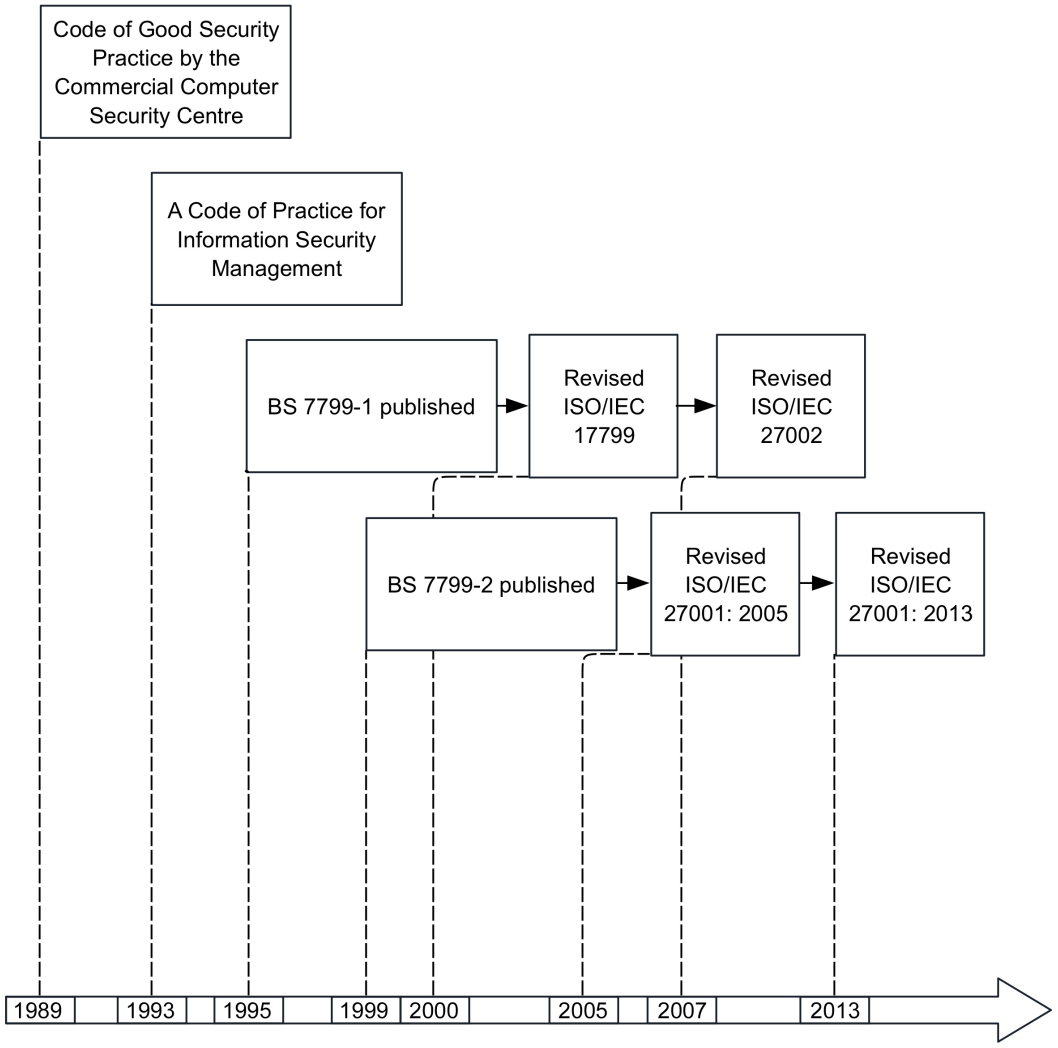

FIGURE 2.1: ISO 27001 development timeline [Int05, 27098]

2.2.3 The ISO 27001 Standard Overview

ISO 27001 is divided into two main parts. The first part is the requirements definition, while the second part is Annex A security controls. The first part defines the context of an organisation (such as scope or stakeholders' expectation), leadership (such as policy), planning (such as risk assessment) and support (resources). Besides that, the first section describes ISO 27001 evaluation measurement (such as monitoring), operation (operational planning and control) as well as an improvement (such as correction actions). The second part consists of the controls and control domains. The controls categorised under each control objective are high level and can be classified as different features, such as physical, technical or human resource.

ISO 27001:2013 Sections 1 and 2 describe the standard scope, and how the document is referenced. Section 3 explains terms and definitions. Section 4 describes the ISMS [Int05]. The information security requirements part of ISO 27001 consists of Sections 4 to 9 [Int13], which include security manuals, standards, and procedures, as well as records [MCW12]. ISO 27001 ISMS hierarchical mandatory levels provide a central point for security manuals (policy), standards, guidelines, and procedures enforcement (processes). The first managerial part could be in the form of rules and guidelines based on the security requirements; while the second practical part comprises the implemented mechanisms and countermeasures to support the execution of expected information security policies.

Annex A defines an extensive list of 114 controls, which provides a suitable solution for defining essential countermeasures in any organisation [Fre07]. Annex A controls are categorised into 14 groups, based on their common objectives, from domains A.5 (the information security policies) to A.18 (Compliance). An overview of the control domains is provided in the Appendix A of this thesis (see page 93). Most of the control domains include distinctive subdomains, which demonstrate the relevant controls in more details. The main areas of the implementation of ISO 27001 are policy, responsibilities, asset classification, personnel security, communication and access control [SLP14]. As ISO 27001 comprises two managerial and practical parts of security requirements and controls, information security activities should integrate into both fields, which guarantees practicability of information security polices to form an acceptable information security culture.

The next section clarifies the main differences between two latest versions of ISO 27001:2005 and 2013.

2.2.4 ISO 27001:2005 vs. ISO 27001:2013

ISO 27001:2013 looks structurally and fundamentally different from ISO 27001:2005. The updated standard is based on the Annex SL, which is the main reason for this notable distinction [Int13]. ISO created Annex SL to provide a universal high-level structure and common terms for all management system standards, which make it easier for organisations to be consistent with more than one management system standard. For instance, ISO 22301:2012 on business continuity, ISO 9001 (quality management

system) and ISO 27001:2013 (as mentioned) were published with conformance to Annex SL [HP11].

For the first part, the requirements for establishing, implementing, maintaining and continually improving an ISMS are defined in different sections of ISO 27001:2013. For conformity to ISO 27001:2013, Sections 4 to 10 is mandatory (cf. Table 2.1); while Annex A controls are selected based on the organisational security requirements. These requirements are defined in a way to provide a variety of choices for implementation. For example, preparing an inventory of assets is no longer a requirement for risk assessment. The titles and the contents of Sections 4 to 10 in the updated standard are different from ISO 27001:2005 (cf. Table 2.1). Every section defines a document requirement, based on the definition and specifications of each section, for example, the document requirements for Section 4 is "scope" and Section 8 is "the results of risk treatment plan". Sections 4 to 7 specify requirements for establishing an ISMS, while Sections 8 to 10 identify the implementation requirements. In ISO 27001:2013, each requirement is mentioned only one time and there are no duplicate requirements (for instance preparing a list of documents is no more required).

The updated standard is not based on the PDCA (Plan-Do-Check-Act) cycle anymore [Int13]. The PDCA is an iterative four stage management model that is used for the control and continuous improvement of processes. Therefore, related phrases and concepts are changed, such as "continual improvement" instead of PDCA. In ISO 27001:2005, the terms and definitions were mentioned in the body of the standard and the normative reference (that is deriving from this standard) is ISO 27002:2005; While ISO 27000:2013 is mentioned as a normative reference for ISO 27001:2013. Additionally, in ISO 27001:2013, ISO 31000:2009 is mentioned as a reference to determine the internal and external context of the organisation, which provides a framework for managing risk. Table 2.1 indicates the differences between the requirements sections of the two latest versions of ISO 27001 (2005 and 2013). Table 2.1 indicates the initial sections of 0: Introduction, 1: Scope, 2: Normative reference, and 3: Terms and definitions as they have not changed between the two latest versions of ISO 27001. However, the remaining sections are distinct based on the context and definitions as described so far. For the second part according to ISO 27001:2005, Annex A is a checklist to make sure all essential controls are considered and no necessary control is ignored by an organisation.

Table 2.1: ISO 27001:2005 vs. ISO 27001:2013 requirements

ISO 27001:2005	**ISO 27001:2013**
4. Information Security Management System	4. Context of the Organisation
5. Management Responsibility	5. Leadership
6. Internal ISMS Audits	6. Planning
7. Management Review	7. Support
8. ISMS Improvement	8. Operation
Annex A Control Domains & Controls	9. Performance Evaluation
Annex B OECD Principles & this International Standard	10. Improvement
Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 & this International Standard	Annex A Reference Control Domains & Controls

However, ISO 27001:2013 recommends that controls have to be selected in the risk treatment process. The risk treatment process defines the necessary controls that need to be implemented to protect an organisation from identified risks. ISO 27001:2013 is more flexible with different risk assessment methodologies [Fre07] as there is no prerequisite for identifying risk.

Besides that, the SOA (Statement of Applicability) contains the organisation's information security control domains and controls. The SOA is one of the most important documents that explains the selected controls and the reasons for including or excluding each control domain from Annex A in the scope of an ISMS. In ISO 27001:2013, the SOA emphasises more on objectives, monitoring and measuring the implementation of ISO 27001 [SG11]. Based on the ISO 27002:2013 guidelines referenced in [JM14], there is a connection between the implementation requirements of each control with other relevant controls. For example, the controls relevant to ownership of assets are supportive controls for implementing information security roles and responsibilities controls (cf. A).

For a transition to the updated version, there are some areas, which do not require any changes, such as control of documentation. Nevertheless, there are some other areas that require a rethink like objectives of the management system [HP11].

The next section describes the process of getting ISO 27001 certification as the last section of describing ISO 27001 development.

2.2.5 ISO 27001 Certification Process

ISO 27001 certification is one of the possible ways to reassure customers and clients that ISO recommendations have been followed [Boe09]. In the beginning, the adoption of ISO 27001 was among IT services and software development, and only large organisations applied for ISO 27001 certification because of high implementation complexity and certification costs [NEF08]. The number of ISO 27001:2013 certifications is steadily growing each year. For example, in December 2015, 27536 certificates were issued around the world, which increased 20% compared to 2014, based on the ISO survey 2015 [Int15]. Most of the countries with a high number of ISO 27001 certificates are among top economies in the world, for example, China, and they are interested in information security standards because of their global activities, for example, the UK or Japan. The USA, which has the biggest national economy, was ranked relatively lower compared to the top 10 countries with the highest annual growth of ISO 27001 certification. Figure 2.2 summarises the procedure of getting an ISO 27001 certificate.

Organisations have three different options for certification:

1. They can declare compliance to the standard by themselves.
2. They can ask clients to confirm their compliance with the standard.
3. An independent external auditor can verify the conformity [SW09].

The ISO introduces a list of RCBs (Registered Certification Bodies) for certification procedure as authorised certification organisations [HWL16]. These RCBs help organisations to determine the extent to which there already conforming with ISO 27001 and further actions required for successful certification, as an examination [CW08]. Afterwards, the necessary measures for ISO 27001 conformity should be defined in a preparation project. External experts are required for a certification process, for the essential level of knowledge and experience in implementing ISO 27001 policies and controls [Cal13]. Initially, the RCB reviews all the documents, such as security policy and process description. The main audit follows this preparation phase [Dis13], which consists of several steps; for instance, interviewing all responsible employees to examine their

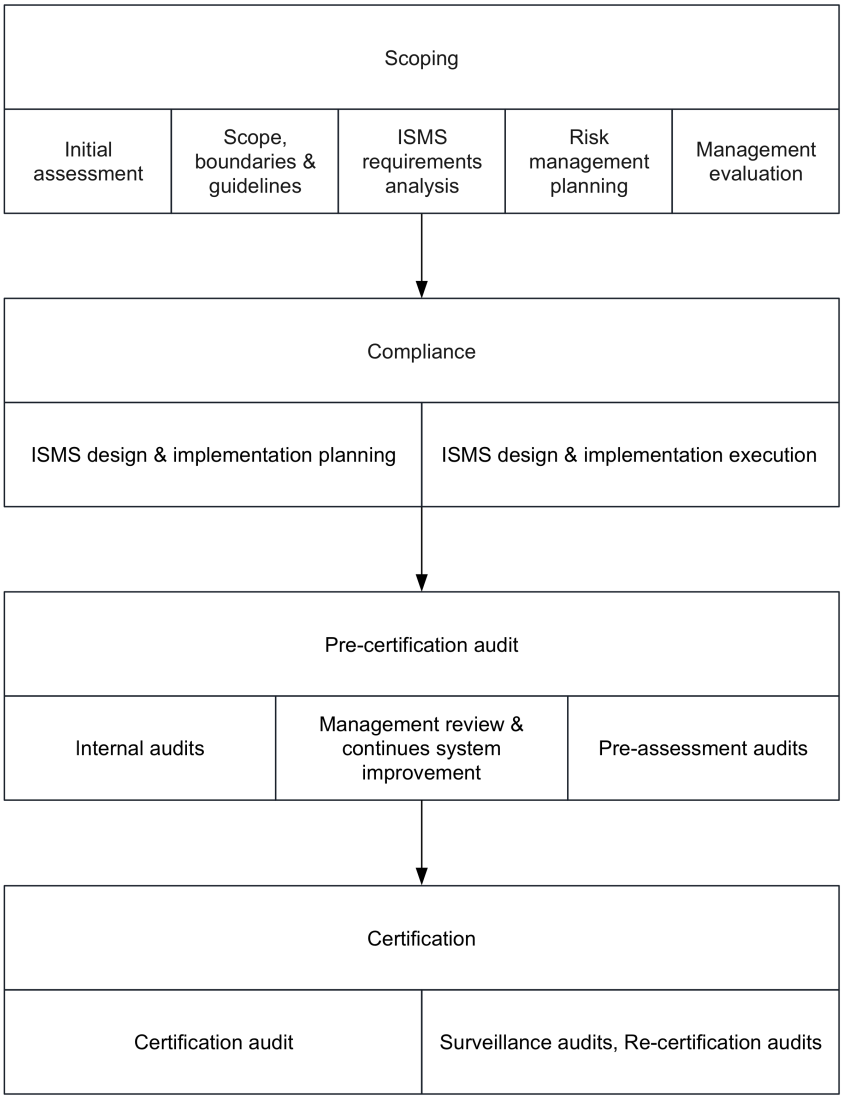

FIGURE 2.2: Getting an ISO 27001 certificate [HWL16, Cal13]

understanding of the security policy. Based on the findings of these interviews, the certification organisation generates a report describing the audit results and improvement measures before conducting the next audit.

Finally, the company receives an official certificate of the ISMS conformity with ISO 27001 requirements, in case of overall positive results. The implementation phase duration varies from a few months to some years, based on the level of the IT security management maturity in an organisation. An ISO 27001 certificate is valid for three years, and recertification mainly requires less effort than the initial certification [HWL16]. The RCBs can withdraw or suspend ISO 27001 certificates when serious deviations are observed from the requirements of ISO 27001 during a monitoring audit [HWL16]. There

are some national alternatives to RCBs, such as the German BSI (federal office for the information security) in Germany. The German BSI offers ISO 27001 certification based on the IT baseline protection guideline since 2006, which provides conformity with both ISO 27001 and an assessment of the IT security measures against the IT baseline protection catalogues.

After introducing ISMS and describing the process of developing ISO 27001, the relationship between ISO 27001 and culture is described briefly.

2.2.6 ISO 27001 and Culture

ISO 27001 provides a common framework to build a culture of security. Culture is a medium between management and employees' behaviour, which affect operation and effectiveness of their activities [SAT+11b]. An organisational culture is important for implementing ISMS [CW08] because an ISMS is implemented in the context of an organisation, and suitable choices and different methods can be used to lead organisational culture [BHSS14]. Proper methods of communicating security policies to employees [SAB07, Cal05, KMKRNF06] keep employees informed of the information security issues to have an appropriate understanding of security contribution and commitment to the ISMS. The full description of culture is provided (cf. 2.3).

The next section explains culture as the main scope of this thesis followed by the state of the art on culture, national culture, organisational culture and information security culture. Afterwards, three publications and the relevant dimensions are described.

2.3 Culture

Culture defines social attitudes and behavioural characteristic of a particular group of people or society. The research project Globe (Global Leadership and Organisational Behaviour Effectiveness) stated that culture is shared motives, values and interpretations of significant events, as the result of common experiences of members [TV10]. Culture is made up of patterns, explicit and implicit behaviour learned creating distinctive achievements [JHD+06], which are shared through generations using social learning processes of modelling and observations [KLG06]. Cultural differences reflect in different aspects

from work motivation to conflict, negotiation and human resource practices [HJHD02]. Culture as the main driver of people behaviour constructs their motivation, mind-set and their judgements [Hof84]. In this section, we introduce cultural characteristics and the literature before describing their meanings and their relation to the implementation of ISO 27001 in the next chapter.

2.3.1 Definition of Culture

National culture is broadly described as values and national behavioural patterns, which shapes people perception about risk and progress [KDHK99]. National culture comprises of a set of norms that exist within the population of a society [VNB93]. The political and educational system, media, and language lead to a shared culture in a society [GNR06]. A specific condition of social or economy may develop certain characteristics, which creates a special cultural type [VNB93]. In order to understand the reasons for some events happening in a certain period of time, the event and the motivation should be analysed separately [Hof84]. Skills, values, and opportunities affect the conversion of a motivation into an action [VNB93] because of the complicated relationship between behaviour and mind-set [Hof83]. Besides that, the way that people are thinking is different based on their culture and their patterns of thinking. Understanding these differences is important for organisations to develop their management and other practices in accordance with the national culture they are operating in, because analysing, evaluating or changing organisational culture should follow the national culture [Sch86].

Organisational culture is a system of shared assumptions, values, and beliefs, which dictates how people behave and perform their jobs in organisations [GEA07]. This culture is transferred through employees by shared practices, based on their work characteristics and job context as the group affect the employees' decisions [RMC07]. The organisational culture is applied to the whole organisation, determined and preserved by a group of people, which is hard to change [PC06]. However, organisational culture can be improved in some stages by briefing and awareness for all management levels [KKN12, CMR02, FCL10, LCMA09]. Several context-specific subcultures might exist in an organisation, although a general culture is established in an organisation [ME02]. To estimate the effects of these subcultures, a content analysis of organisational culture was conducted in four US medical centres [Hys14] to prove that subcultures are based

on the larger organisational culture that is related to organisational performance. The most effective factor in establishing organisational culture is main leaders' and founders' values [TTKG07].

Information security culture helps organisations to make security decisions. As two dimensions of information security are knowledge and behaviour, culture is the behaviour of an organisation to protect the data, knowledge and information [Übe13]. Culture also determines the social roles and guiding attitudes for responding to security threats, such as security policy [RF99], which has to be part of designing IT applications [TvSL06]. The security concerns are the same in most cases, but their importance differs in each country [SFC15]. The effects of culture on the information security were studied based on the Edgar Schein's three-layer model of culture to implement security culture in an organisation [ST03]. Kuuisto, Nyberg, and Virtanen studied the intercultural factors [KNV04] to investigate the organisational security culture in multicultural organisations. Understanding the information security culture of a local organisation is less challenging when the national and organisational cultural is the same between insiders [HJHD02] because if a user behaves in a secure manner, she/he creates a benefit for the organisation as a whole [GP07]. Zakaria stated that information security activities are related to information routines, information security norms and information security culture [Zak13]. Robbins mentioned that national culture, organisational culture and employees' performance are correlated [Rob09]. In addition to these publications, researchers [ECL07, DSM00, FFA+05, FFA+14] gave little attention to the relationship between national culture and information security in organisations, which describes the main motivation of this thesis.

As the authors of these papers may not have the same view on culture, as culture is a complicated concept to define, we have detailed what culture means in the context of this thesis. We define culture based on distinguishable widespread similarities among people within a society, which influences people behaviours and their values about right and wrong. For the purpose of this thesis, we describe culture as an ongoing learned and patterned mind-set and behaviours [Hof03]. We denote mind-set by a set of people assumptions, attitudes, and intentions of a society that result in adopting or accepting prior behaviours [Hof84]. We define behaviour as a range of actions of a group of people to act in response to a particular situation or environment [Hof83]. We describe national characteristics in the sense of nationwide measurement due to

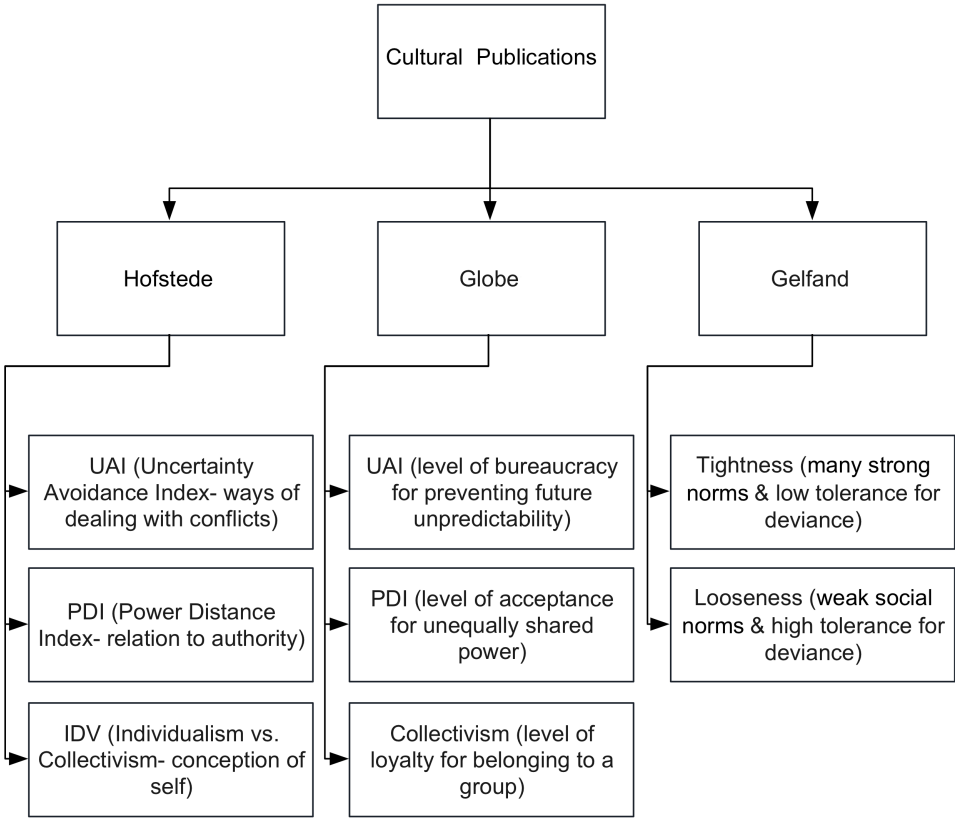

FIGURE 2.3: National cultural publications & the relevant dimensions [Hof03, JHD+06, GNR06]

common regulation that is influenced by wealth and economic power, historical background, and cultural characteristics related to existing information security requirements [Hof84, Hof83, TV10, JHD+06, KLG06]. Then, we describe the literature to specify cultural dimensions.

In order to find out the cultural related characteristics applicable to this thesis, the literature is selected for defining cultural characteristics in the field of information security. Accordingly, in this section, three publications and the relevant dimensions are analysed at the national level, which are Hofstede [Hof84, Hof83, Hof03, HHM10], Globe (Global Leadership and Organisational Behaviour Effectiveness) [JHD+06, PC06], and Gelfand [GEA07, GNR06] as presented in Figure 2.3.

Hofstede defines culture as the collective programming of the mind that distinguishes members of a group from others, who believes personality shows the uniqueness of a person; while culture shows the uniqueness of human groups [KLG06]. He explains the effects of a society's culture on the members' values and these values' relation to

behaviour. Bradley L Kirkman reviewed 180 articles and chapters that used Hofstede cultural dimensions for empirical research [KLG06]. They provide some suggestions to help researchers improve their use of Hofstede's framework in the fields of management and applied psychology [KLG06]. Hofstede is the father of defining cultural dimensions whose dimensions are shared between individuals in each country. The dimensions represent what proportion of people prefers one state of affairs to another that distinguish countries from each other. These dimensions are relative, which ranged from 0 (the lowest level) to 100 (the highest level). Hofstede's six dimensions are introduced briefly, and then the cultural, political and economic characteristics (cf. 3.3.4) are discussed in more details (cf. 2.3.2).

UAI (Uncertainty Avoidance Index) is related to the number of rules and regulations and their effectiveness to produce a desired result or the desired output [Hof83]. However, PDI (Power Distance Index) is based on a hierarchical order that shows the level of accepting and expecting unequally distribution of power among people [Hof84]. The people IDV (Individualism) level is related to the level of people's compliance with organisational requirements [VNB93]. In contrast, collectivism shows the level of integration of a group member together, which is based on undoubted loyalty and support when a conflict arises. We denote collectivism by low IDV in this thesis. The other Hofstede dimensions that are not used in this thesis are: Masculinity (the level of achievement and assertiveness), Long term orientation (the level of focus on past or future), and Indulgence (level of enjoying life and having fun) [Hof03]. Based on the literature, the relationship between cultural characteristics and the implementation of ISO 27001 are provided (cf. 3.3.1).

The Globe project investigates how cultural values are related to organisational and leadership practices [JHD+06]. Over time, organisational developers might change their behaviour and leadership style to adopt all or most members [KDHK99]. Globe investigates the national culture of middle managers to compare leadership perceptions and behaviours. Globe identified nine cultural competencies that are explained briefly.

1. Performance orientation is the degree performance improvement and excellence is encouraged.

2. Assertiveness orientation shows the level of individuals' assertiveness and aggressiveness in their social relationship.

3. Future orientation is based on individuals' engagement in future-oriented behaviours such as planning.

4. Human orientation shows the level individuals are encouraged for being fair, generous and caring to others.

5. Gender egalitarianism is the level of minimising gender role differences and gender biases.

6. Institutional collectivism shows the level of encouraging collective distribution of resources and collective action.

7. In-group collectivism is based on the level individuals express pride and loyalty to their organisations.

8. Power distance is based on the level of individuals' expectation and acceptance of unequally shared power.

9. Uncertainty avoidance shows the level of avoiding uncertainty by supporting social norms and bureaucratic practices to decrease unpredictability of future events.

The Uncertainty Avoidance (level of procedures and bureaucratic practices for preventing the future unpredictability) and Power distance (level of expectation and acceptance for unequally shared power) dimensions of Globe and Hofstede are considered to have a consistent definition based on the purpose of this thesis, which are used in the same meaning as in Hofstede [HJHD02]. The collectivism dimension of Hofstede and in-group collectivism (level of loyalty and pride for belonging to a group) of Globe have the required level of similarity for the scope of this thesis to consider as matching concepts, which is addressed as low Individualism in this thesis (cf. 2.3.2).

Gelfand's theory of tightness vs. looseness is related to the strength of social norms and monitoring in a society [GEA07]. Fixed disciplines, strict rules, integration, and uniformity are the main concerns in tight countries [GEA07]. Loose people challenge established procedures [GRN+11] and they are more flexible in changing their behaviour according to policies, and defined rules [GRN+11]. Loose employees' different interpretations about executing policies on one hand, may lead to conflicts and on the other hand, may lead to innovations [GNR06]. As the tightness score is not available for all

countries [GEA07, GRN+11], and it contributes little to our model, we eliminate this cultural characteristic in further steps.

In the following, we describe the cultural characteristics that are selected for the purpose of this thesis in more details based on the publications that discuss the relationship between culture and information security.

2.3.2 Cultural Characteristics: Uncertainty Avoidance (UAI), Power Distance (PDI), and Individualism (IDV)

The UAI is definable in both country and individual level. The countries high in UAI (such as Romania and Uruguay [HHM10]) maintain rigid codes of beliefs and behaviours by carefully planning and implementing rules, laws, and regulations to decrease the uncertainty and unpredictability of people's behaviour [KLG06]. For simple tasks, people with high UAI have more success and they mostly perform their job in such a manner as to achieve the desired result [Hof84]. For harder tasks, they have more failure and avoid the tasks that result in poor performance [Hof83]. For example, people with high UAI focus on completed tasks, solve fewer issues in case of time pressure and work better after positive feedback [Hof84]. In the countries high in UAI, it is important to have many formal and informal rules for emotional needs, and people do not feel comfortable without a structured set of rules [JHD+06]. Nevertheless, in low UAI countries (such as the Philippines and Ireland [HHM10]), people cannot cope easily with strict rules and they are more suitable for doing unclear tasks [VNB93]. The second cultural characteristic to be defined is the PDI.

The countries high in PDI (such as Malaysia and Slovakia [HHM10]) believe in centralised decision-making [Hof83]. In high PDI countries, managers do not normally consult with subordinates, and employees pay more attention to superiors and formal norms [Hof84]. Managers are possibly less cooperative and more competitive [KLG06], and they care more about the results. They are mostly influenced by prestige possessions and they need more loyal and respectful supporters [Hof84]. Besides that, they are more visible to other members of their group [VNB93]. The countries high in PDI might negatively evaluate their group members. In the countries high in PDI, if people behave positively and task-oriented, they are most likely chosen as best leaders. Leadership depends on personal characteristics and characteristics of the other members of

a group. The countries low in PDI (such as New Zealand and Iceland [HHM10]) are based on trust and they mostly consider their peers and informal norms as behaviour guidance, rather than formal obligations [Hof83]. In addition, a country low in PDI is more helpful in supporting group decision-making based on the facts. The PDI and UAI show the way organisations normally do their tasks. After analysing PDI, the third cultural characteristic to be defined is IDV.

Countries with high IDV (such as Australia and USA (United States of America) [HHM10]) resolve conflicts by using skills and training to integrate people's interests in an organisation [VNB93]. Countries with low IDV (such as Romania and Ecuador [HHM10]) look for positive and effective relationships with other persons [Hof84] to be successful in producing a desired or intended result. In these countries, managers normally learn social relationships faster as people are important for them; they have more conversations and maintain their relationship with others [Hof83]. Managers may also focus on the group relationship rather than group performance [Hof84]. They try to avoid conflicts and competitions. Moreover, in the countries with low IDV, managers, and employees work together and managers are mostly effective helpers [KLG06]. Shared responsibilities help people with low IDV to improve their performance [VNB93]. Moreover, people with low IDV mostly emphasises on following guidelines and rules in their tasks. Co-workers with different PDI and IDV may find it difficult to communicate [KLG06].

So far, we select the UAI, PDI, and IDV for the purpose of this thesis. In the following, the political and economic characteristics are introduced and described in more details. For describing political characteristics, Economic freedom of the world annual report [GLN16] and for the economic characteristic, the World economic and financial survey of World Economic Outlook (WEO) database by the IMF (International Monetary Fund) is used [Fon15].

2.4 Politics and Economy

The economic freedom is based on protecting acquired property from physical attacks with no force from fraud or theft [GLN16], according to James Gwartney and Robert Lawson. Their research was based on five areas and 42 measurements for evaluating the

level of acquired property protection and voluntary transactions engagement [GLN16]. These 42 measurements express the freedom for personal choices, open market (entrance and competing), personal security and privately owned property by clear and obligatory policies and rights. Each component has sub-components in the five areas, and the average of the sub components constructs each component rating. Then, the component areas are averaged to derive each area ranking. In 2016, 156 countries were investigated in the economic freedom research, which shows 95% of these countries have an acceptable economic freedom index. For example, Hong Kong was first ranked in the level of economic freedom, followed by Singapore, New Zealand and Switzerland [GLN16] in 2015 and 2016.

Based on Jone's research, private property security, international trend openness and a stable money system are related to economic activities promotion [HJ]. The law for protecting property and contract security possibly influence market economy [BN13], and market economy is an economic system in which economic decisions are guided. Moreover, the market economy could be improved by preventing long delays in the enforcement of contracts and property rights [Mah01]. There are several pieces of evidence that demonstrate the positive relationship between economic freedom enhancement and advanced level of GDP (Gross domestic product) [GLN16, Nys08, HJ]. Then, we introduce the literature for the economic characteristic.

The IMF (International Monetary Fund) is an organisation of 189 countries, and the WEO (World Economic Outlook) report is a survey that is usually published twice a year, which presents the analyses of global economic developments. We use the world economic and financial survey from October 2015.

The next two sections describe the political characteristics of regulation and legal systems, and economic characteristic of GDP (Gross domestic product). The relationship between ISO 27001 and these two political characteristics (cf. 3.3.2) and the economic characteristic (cf. 3.3.3) is explained in the next chapter.

2.4.1 Political Characteristics: Regulations and Legal System

The regulation is based on the level of bureaucracy to enable market entry and to limit competition [GLN16]. The regulation is an indicator of the level of restriction

of employment, product market and credit exchange. Graef discovers that some types of regulations help in reducing corruption [GM03]. Feldmann defines that the level of business regulations affects employment rate and contribution, such as price controls and administrative difficulties for establishing a new business [Fel07].

The legal system is based on public protection and property rights, as one of the important economic freedom and public rights [GLN16], which indicates if people can use, exchange or give their property freely when they do not violate others' rights. Mahoney expresses that countries with legal systems and common laws have developed financial markets [Mah01]. Berggren declares that trust increases with legal system structure and property rights security [BN13]. We denote legal system and property rights by legal system in this thesis. In this thesis, we describe the political characteristics in terms of regulation and legal system.

After describing political characteristics of legal system, and regulation, the next section explains the GDP and the selected GDP type.

2.4.2 Economic Characteristic: Gross domestic product (GDP)

The GDP is based on the fiscal costs of all final services and goods in a period of time. It is one of the major assessments of a country's economy [OS11]. The constant-price GDP measures a country's goods value and services in relation to a base year based on the annual values of all services and goods. The constant-price GDP is not influenced by money value changes, which is an indicator for measuring a country's growth rate compared to the previous year [Fon15]. The constant-price GDP per capita is based on volume changes of goods and services, which is calculated by dividing constant-price GDP by total population [Fon15] to the base year.

PPPs (Purchasing-Power-Parity) equalise the purchasing power of different currencies by eliminating the differences in price levels between countries, which present the ratio of the prices of the same good or service in different countries. PPP is based on the values of a set of different amounts of different goods and possibly services in each country, which serves to monitor the state of an economy. PPP is used to monitor the amount of money needed to buy all the items of different goods and possibly services a typical consumer will likely need over time. In order to add the population size, the GDP-PPP

per capita is used, which is an appropriate indicator for comparing data internationally. The PPP indicator is suitable for comparing countries' living standard, considering the relative living costs and inflation rate [Fon15]. The GDP-PPP per capita is calculated by dividing the fiscal PPP value of a country's final good and services by the average population. According to the OECD (Organisation for Economic Co-operation and Development), in order to provide a global economic overview of countries' domestic economy, GDP-PPP is used to assign weights to countries to determine their economic performance. According to [BRH16], the World Economic Outlook report of the IMF is a commonly referenced statistic to measure the relative economic strengths of 189 member nations. We use the economic characteristic of Gross domestic product based on purchasing-power-parity (PPP) per capita GDP (dollars). We denote Gross domestic product based on purchasing-power-parity (PPP) per capita GDP by GDP-PPP in the following. In this thesis, we describe the economic characteristic in terms of GDP-PPP.

The next section introduces Global Cybersecurity Index.

2.5 Global Cybersecurity Index

Global Cybersecurity Index [ITU15] is a profile about cybersecurity development of a country based on five measures of:

1. Legal,
2. Technical,
3. Organisation,
4. Capacity building,
5. Cooperation.

These five measures are mainly based on political, economic and social features [ITU15], which are explained in the following. The law enforcement, justice, technology developers, intra-state cooperation institutes, educational and private sectors are all involved to evaluate the Global Cybersecurity Index [ITU15]. For calculating the Global Cybersecurity Index, each sub group has three possible comprehensive levels of activity. The total

level of readiness point evaluated based on the number of subgroups of each indicator. The five measures are introduced in more details, which cover widespread information security concepts and activities. For example, the legal, technical, and capacity building measures are based on standards as well as certifications to assess the level of the information protection of studied countries.

1. Legal measure can help nations with integrated and uniform regulatory basis as a response mechanism to breaches, which covers regulation and compliance (data protection and certification), as well as criminal legislation (unauthorised access) [ITU15].

2. Technical measure is based on the number of national institutions and frameworks to detect and respond to threats, such as computer emergency response team (response and management), standards (government approved or recommended international framework), and certification (government approved or recommended framework for certification and accreditation of national professionals for implementing international standards) [ITU15].

3. Organisation measure applies procedures for implementing and measuring national initiatives uniformly in a country, based on policy (minimum recovery time and damage), governance roadmap (legal system and cultural challenges for reporting, collaboration and management of incidents), responsible agency (committee or consultant for organisational structure), and national benchmarking (best practices to measure cybersecurity development) [ITU15].

4. Capacity building measure is a supportive measurement for the mentioned measures, based on education, training, research, and development that involve socio-economic and political features [ITU15]. It consists of standardisation development (technology maturity level and new standards), manpower development (widespread public campaigns for safe behaviour), professional certification (number of certified professionals for international certification programs), and agency certification (number of certified agencies for international certification standards) [ITU15].

5. Cooperation measure focuses on communication and sharing attack scenarios and best practices for enhancing the level of cybersecurity, based on partnership and information sharing networks [ITU15]. It consists of intra-state cooperation (official

TABLE 2.2: Global overview of Global Cybersecurity Index [ITU15]

Region	Legal	Technical	Organisational	CB	Cooperation
Africa	0.31	0.13	0.17	0.11	0.16
Americas	0.44	0.24	0.24	0.25	0.20
Asia pacific	0.41	0.30	0.30	0.27	0.25
Europe	0.79	0.42	0.45	0.37	0.34

national partnership for globally sharing cybersecurity assets), intra-agency cooperation (official national partnership within the public sector for sharing cybersecurity assets), public-private partnerships, and international cooperation (recognised cooperation in international platforms and forums).

We summarise the results of this publication findings after introducing these five measures.

Broadly speaking, Europe had the highest Global Cybersecurity Index, and the highest level of legal measure that is based on response mechanisms and recovery to information security breaches [ITU15]. This high level could be the result of the EU (European Union) legislation on cybersecurity, and the overall strategic framework of the EU initiatives on cybersecurity, which propose additional measures on cybersecurity standards and certification. However, Africa had the lowest Global Cybersecurity Index, and the lowest level of capacity building measure that is based on supportive information security activities, such as certification development. Table 2.2 presents the measures of the Global Cybersecurity Index. We denote Capacity building with CB. The Americas focused on the legal measure, which includes the continents of North and South America. To emphasise, most of the countries focused on the legal measure; however, capacity building measure received the lowest attention in 2014. These findings indicate that the response mechanism, such as legal, regulations, and compliance were developed adequately to address bureaucratic measures for managing security. On the other hand, the supportive information security activities require more attention, such as education and manpower development (insiders' safe behaviour), as well as certified professionals and certified agencies for international certification standards.

The Global Cybersecurity Index does not measure the number of security incidents or damages from security incidents, but security management, such as rules and regulations,

as well as reporting structures. The ITU (International Telecommunication Union) describes this index as a multi-stakeholder initiative to measure the commitment of countries to cybersecurity [ITU15], based on different features of managerial, technical, and international collaboration.

In the next chapter, we describe the related work to shape the relationship between the implementation of ISO 27001 and the cultural, political and economic characteristics that have been described in this section.

Chapter 3

Literature Review and Cultural, Political and Economic Characteristics

3.1 Introduction

This chapter starts by briefly stating which fields of work are related to this research, followed by separate sections on related work in each of the fields. In the first section, we describe the related work on ISO 27001 and cultural characteristics followed by the literature about information security and Hofstede cultural dimensions. In the second section, based on the cultural, political and economic characteristics that are introduced in Chapter 2, we investigate the potential relationship between those characteristics and the adoption of ISO 27001. Then, we provide an overview of all those characteristics that are used in our quantitative analyses.

3.2 Related Work on Information Security and Culture

IT management specialists analysed different characteristics of people (such as age, gender, and culture (mind-set and behaviour)) in executing information security activities [LGJ10] because people are the main planners, executors and decision makers of developing any standard from the beginning phase. Among these studied characteristics, culture is defined as the main criterion regarding information security standards adoption [PC11, HP11, Übe13, RF99]. The national culture for protecting important assets

could be related to the decisions of selecting an ISMS standard, such as ISO 27001 [FVB08]. Accordingly, various social characteristics are analysed in cultural, political and economic fields, which form the basis of our analysis to answer the first research question (cf. 1.4). As the combination of culture and information security has not been considered in the available publications [FAE14, SSC+17, KMKRNF06, PC11, Übe13], the following sections describe the main cultural drivers of implementing ISO 27001.

Accordingly, we investigate related works on culture dealing with information security and the adoption of ISO 27001, followed by the Hofstede cultural dimensions.

3.2.1 ISO 27001 and Cultural Characteristics

The literature is selected based on the number of citations for defining cultural characteristics, which is focused particularly on the adoption of ISO 27001. The logical flow of presenting these publications is in terms of time. This section describes existing literature on the relations of culture to information security and ISO 27001 to show how our work differs from these existing publications.

One year after the publication of ISO 27001:2005, Calder et al. suggested that large organisations should create a single ISMS with a single business culture [CW06]. Although a clear definition of culture was not provided, they pointed out that the management should trust employees to enhance employees' commitment to maintaining information security. For example, the policy for acceptable use of email and Internet or documenting policies, procedures and processes should reflect organisational culture. They stated that organisations should implement a reporting system for employees to report security events.

Broderick stated that security compliance culture fosters information security culture among employees [Bro06] to follow up on [FA98], which was based on rewards to demonstrate that desirable behaviours are recognised for creating a security compliance culture. Broderick described when a security compliance culture is established; compliance with an ISMS standard is a business process that users follow. He suggested having several internal audits to encourage adoption of a security culture because audits make employees realise that they will be assessed on compliance [Bro06]. However, this was the view

of ten years ago, and supposedly experience has shown that it does not work particularly well. For example, Meng Chow Kang described several examples where such a compliance culture does not necessarily improve security [Kan13].

In addition to organisational efforts in shaping the desired level of information security culture, national culture might be related to fulfilling information security requirements. This could be related to the practicability of established security countermeasures, which provides fewer opportunities for employees' commitment [ECL07, RMC07]. For example, organisations are suggested to embed the information security culture with their information security practice to influence employees' actions and behaviours [LCMA09]. Besides that, listening to employees' feedback and reports is helpful to guide employees to the expected security behaviour based on the established policies [FCL10]. Organisations are suggested to communicate security policies with employees, for example by clarifying the reasons for establishing policies, and there should be processes for monitoring the effects of policies, from both positive and negative aspects.

Besides that, Brenner shows that ISO 27001 helps foster a strong culture where strong values are promoted for protection of client and business information [Bre07]. They followed up on [KMKRNF06] who conducted a research to describe the relationship between cultural values and performance as well as learning motivation. In 2007, STOPE (Strategy, Technology, Organisation, People and Environment) was introduced [SAB07], which was later used for evaluating and continuously improving an ISMS, based on ISO 27001 [SMAT12]. They followed up on [ALK94] to describe the effects of environment on adopting ISO 27001. Alison Anderson and Dennis Longley developed a security model for information security officers, which considers information system environment, information systems, and information system assets in their analysis [ALK94]. They selected the environment of an information processing system because risks are transmitted through that environment, which is related to the system and the assets that are stored, processed or communicated by that system. They introduced environment as one of the related factors in establishing a secure system.

It is known [Ash08] that several nontechnical issues are related to the implementation of ISO 27001. Information security requirements could be related to the cultural characteristics, which are different between organisations and countries. Ashenden indicated that individuals in organisations are influenced by the identity of their job as well as

their personal and social identity (unique attitudes, beliefs, and perceptions) that they bring with them to work. Her research focused on management and organisational behaviour based on the required skills to change organisational culture, the identity of the information security manager and effective communication with end users. Organisational culture is based on assumptions that individuals will use as guidance when facing situations in the organisation that they have not experienced before. The organisational culture is shaped based on the observable behaviour of individuals, what they say and do and core values, such as the followed rituals and routines and the told stories [Ash08]. She considered the main challenge is to manage the mix of the organisational, social and personal elements of individual identity to ensure the optimum structure, business processes and relationships for organisational objectives. Ashenden suggested information security managers should develop their skills in different areas, such as communication skills. She focused on the importance of organisational culture rather than national culture for implementing an ISMS standard such as ISO 27001.

Although these publications mostly focused on organisational culture, Schmidt et al. explained that national culture affects employees and management perceptions as well as privacy-related issues. For example, they described that countries had different perceptions of relevant computer security threats [SJA+08]. However, this was the result of ten years ago and might not be still true today. The results of studying contextual factors such as national transparency levels and ethical behaviour of organisations indicated positive associations with some information security threats and controls [Ifi14b]. Individuals may view issues based on their environments preconditioned of different countries [Ifi14b]. For example, countries with less transparency may have little or no need for compliance with organisational security and privacy policies, which has an indirect relationship with their organisations risk and information security threats. In addition, Ifinedo suggested managers establishing information systems security policies and practices based on regional differences [Ifi14b]. There might be a relationship between a national culture and an organisational culture as the psychological development of individuals [Hof84] guide their daily behaviours.

Parkin et al. stated that external standards should be customised based on the organisational culture and employees' requirements [PvMC09]. As vulnerabilities are mostly based on a potential pattern of employees' behaviour in comparison to the technical configuration, employees' capabilities and organisational culture should be considered

[PvMC09]. They addressed some controls as behaviour control, for example deploying a password-authentication system might be challenging for employees who are encouraged to have a culture of trust. They mentioned that behavioural foundation includes ethical, temporal, mind-set, capability and cultural types, and they described that different cultural practices might exist across geographic or social boundaries.

Veiga et al. addressed culture as a narrow security-centric concept, which was considered as a helpful way to understand the relationship between culture and ISO 27001 [DVE10]. Accordingly, the culture was defined as the behaviour of an organisation to protect data, information, and knowledge. The term cultural change was mentioned as the main challenge for receiving ISO 27001 certification, which requires employees' acceptance and ownership across the organisation to overcome this challenge, especially in smaller companies [SG11].

Alan Gillies' approach is based on a maturity model to develop processes for making organisations mature enough to achieve ISO 27001 certification [SG11]. His model is based on motivating employees, as he stated that a cultural change is required within the organisation to shift processes from strategic commitment into implementation. These processes are required to achieve organisational goals, such as collecting monitoring data for identifying employees' non-compliances with the process.

To find out the challenges of implementing ISO 27001 in Saudi Arabia's organisations, interviews were conducted and employees' resistance to change was known as primary or a secondary obstacle [ASAK11]. When they asked if there is a relationship between Saudi Arabia's culture and the implementation of ISO 27001 process, more than 50% of the organisations said that Saudi Arabia's culture was not a factor; while 25% stated that their culture was not a major challenge, and the rest mentioned that their culture was a major obstacle for implementing ISO 27001 process. The results of their study indicated that employees' attitudes were one of the main drivers of achieving ISO 27001 goals compared to national culture. Although they questioned the effects of national culture on the implementation of ISO 27001, they did not describe the definition of culture and attitude in their research, and the justifications of their interviewees' response.

Susanto et al. investigated the relationship between Annex A controls of ISO 27001 and culture to analyse the implementation of ISO 27001 more specifically [SAT+11b]. Their results indicated that there is a relationship between culture and the Annex A controls

relevant to Information Security Incident Management and Business Continuity Management [SAT+11b]. They proposed a framework to assist stakeholders in assessing the level of their ISO27001 compliance readiness [SAT12b], which consists of six layers of an organisation, stakeholder, tools and technology, policy, culture, and knowledge. They defined organisational culture as the values and behaviours that contribute to the social and psychological environment of an organisation, based on an organisation's past and current assumptions [SAT12b]. They followed on [SG11] to show that organisational change could be related to organisational culture because employees should adapt to new security controls and policies [SAT12a]. The results of mapping the ISO27001 information security standard by six layers of their framework indicated that security plans should carefully look at the people, policy and the technology in order for achieving organisational goals [SA12]. To follow up on [FA98] and [Bro06], organisations are suggested having a reward enforcement system based on the organisational moral standards and values [CRW12] to reduce the employees' non-compliances with the process. They stated that organisations' information security efforts might be threatened by employees' negligence and insider breaches [CRW12].

Researches followed on previous works in respect to the role of people and change process for implementing ISO 27001. For example, Calder et al. suggested organisations should ensure a cultural fit between the organisational desires and certification bodies for getting ISO 27001 certificates [CW12]. They also stated that cultural environment should be considered for establishing information classification policies. Organisations should assign members to a team in an organisation tasked with working towards ISO 27001 certification. For this team, it is important to select people who are able to represent the needs and concerns of key parts of an organisation, because the implementation of ISO 27001 may require a change process with a cultural impact on people and the organisation. However, general statements were mentioned about culture and a concrete definition for measuring culture was not explained.

Selamat et al. investigated the relationship between information security activities and information security culture in an organisational setting of the banking industry in Nigeria [SB14]. They explained culture as a system of values and norms that influence society, organisations and political systems, which could be described as motivation to the employee to be loyal to security practices. They suggested establishing the culture of compliance with security measures would improve organisational performance, which

improves operational activities by reducing costs and increasing profitability. They mentioned that developed countries mostly establish information security culture through information security activities compared to developing countries, such as Nigeria.

One year after the publication of ISO 27001:2013, Flores et al. mentioned that knowledge sharing indicates management approach toward information security governance mechanisms, and those governance mechanisms are used to form employees' information security behaviour and mind-set. Accordingly, national characteristics, the variety of the implementation of ISO 27001 approaches, and information security requirements are related to management decisions and prioritisation [FAE14].

Besides that, AlHogail proposed a framework based on the STOPE (Strategy, Technology, Organisation, People, and Environment) [SAB07] to develop an information security culture in organisations, which impacts employees' perceptions and security behaviour. His framework is based on four domains of human preparedness, responsibility, management, and society and regulations [AlH15] to protect from information security threats by insiders. He surveyed experts to provide their views and feedback to validate the framework structure. To follow up on [SAT+11b], the implementation of ISO 27001 challenges were investigated with respect to the Annex A controls to show the importance of clear definitions of people roles.

Feltus et al. developed a responsibility model and analysed the responsibility elements in the Annex A controls of ISO 27001, such as accountability and commitment [FK17]. They also proposed some improvement perspectives for implementing ISO 27001 such as clarifying the description of top management's responsibility or the definition of rights and capabilities needed for each responsibility.

Tsao indicated that the differences and conflicts between organisations employees' information security management acceptance would be related to the information security policy and the organisation coordination systems [Tsa17]. Based on the results of the interviews, there is a relationship between information security management acceptance and organisation conflicts in user's view. King used linear regression as the statistical method to indicate a positive linear relationship between effective IT governance and ISO 27001/27002 [Kin17]. He stated that corporate leadership should become accountable and embrace IT governance awareness as part of organisational culture. He examined if there is a linear relationship between IT governance and ISO 27001/27002, based on

SMEs located within the Continental USA (Alaska and Hawaii). Armeanu et al. used regression models to analyse the relationship between following ISO management system standards, such as ISO 27001 and 21 European Union member states' levels of economic confidence [AVG17].

To sum up, securing information system resources and assessing organisational readiness was the main focus of these publications toward implementation of ISO 27001. The results of conducted literature review show the relationship between employees' information security culture as well as adequate information security knowledge and the implementation of ISO 27001. Most of the publications did not introduce a measurement for evaluating organisational culture and researchers investigated the approaches for selecting and implementing appropriate information security controls. Cultural characteristics should be considered in the early stages of establishing ISO 27001 because employees are involved in executing ISO 27001 policies and procedures, based on the job requirements [CW08, FVB08, Cal06]. Although most of these publications described the relationship between organisational culture and ISO 27001, this thesis focuses on the relationship between national characteristics and the implementation of ISO 27001. Based on our knowledge, there is no related work in analysing the correlation between the adoption of ISO 27001 in terms of an average number of certification, and the search keywords of the discussed characteristics. The relationship between national characteristics in such fields of cultural, political and economic have not been addressed yet. Among the studied literature, there was a single publication that was the closet research to this thesis, which is described in the following.

3.2.2 Information Security and Hofstede Cultural Characteristics

Ifinedo investigated the effects of national culture on information security threats and controls in global financial services institutions based on the 2012 DTTL (Deloitte Touche Tohmatsu Limited) survey [Ifi14a]. The results of multiple regression analysis indicated that UAI and IDV are correlated with the assessment of information threats and controls related to acquisition and implementation of security tools, such as identity access management and cloud computing. His results demonstrated that national cultural norms are correlated with respondents' experiences with privacy breaches and

TABLE 3.1: Research with national culture and information system security [Ifi14a]

Dependent variable	Moderating variable
Behavioural intention of security technologies	UAI, PDI, IDV
Information systems misuse	UAI, PDI, IDV
Effectiveness of information system security implementation	UAI, IDV
Information security management in organisations	UAI, PDI, IDV

assessment of information security budget, as national culture influence individuals and organisations.

In the following, Ifinedo's research is summarised based on the relationship between information system security as a dependent variable and national culture as a moderating variable [Ifi14a] as Table 3.1 resents: These findings indicated that the most dominant cultural characteristics are based on Hofstede's cultural dimensions of UAI, PDI and IDV [Ifi14a].

Next, we investigate the possible relationship between the implementation of ISO 27001 and characteristics that are selected for the purpose of this thesis, such as national culture (cf. 2.3.2), politics (cf. 2.4.1) and the economy (cf. 2.4.2).

3.3 Cultural, Political and Economic Characteristics

In this section, we write about how the cultural (cf. 2.3.2), political (cf. 2.4.1) and economic (cf. 2.4.2) characteristics may be relevant to the adoption rate of ISO 27001, in terms of the average number of certificates issued (2006–2014). First, we investigate the potential relationship between the Hofstede cultural dimensions and the implementation of ISO 27001 to initiate our research contribution. Next, the relationships between ISO 27001 and the political as well as economic characteristics are described. The last section presents an overview of the characteristics that are selected for the purpose of this thesis, which serve as an input to our model for our quantitative analysis.

3.3.1 ISO 27001 and Hofstede Cultural Characteristics

Several publications pointed out the relationship between UAI, PDI, and IDV dimensions and shaping the organisational culture, the employees' behaviour and management decisions [VNB93, JHD+06, Hof03, HHM10]. Information security publications [DVE10, Ifi14a, ME02] have mainly discussed the impacts of one cultural publication on information security activities. For example, the impact of Chinese culture on the outsourcing market was analysed using Hofstede cultural dimensions [Gla09]. Glaser suggested security managers should understand human behaviour in addition to political and economic systems to improve system regulation [Gla09].

Based on the literature and the possible relationship between the cultural characteristics and the adoption of ISO 27001, Hofstede's publication is selected for further analysis whose framework explains national cultural differences. In the context of this thesis, culture is the national characteristics of a society that is defined based on the three dimensions of Hofstede to show the differences of individual behaviour in various cultural groups. The Hofstede dimensions that we pick for this thesis are [Hof03]:

- **UAI**: how to make sure what must be done is really done (cf. 2.3.2),
- **PDI**: who decides what (cf. 2.3.2),
- **IDV vs. Collectivism**: self-image as "I" or "we" vs. the degree people are integrated into groups in a society (cf. 2.3.2).

At the country level, we have investigated the potential relationship between these dimensions and the controls relevant to people in Annex A, such as A.6.1.1 (Information security roles and responsibilities) [SFS14, SFS15, SFS16a, SFS16b] that are described in more detail in the qualitative analysis. For example, there might be a relationship between the people with high UAI and the controls relevant to establishing rules, regulations and policies, for example A.5.1.2 (Review of the policies for information security). Comparatively, there might be a relationship between the people with high PDI and the controls relevant to management contribution, such as A.5.1.1 (Policies for information security). There might be a relationship between the people with high IDV and the

way roles and responsibilities are defined, like the levels of details, generality or overlapping, such as A.6.1.2 (Segregation of duties) and A.6.1.1 (information security roles and responsibilities).

We extend our characteristics to economic and political characteristics because the level of national wealth, the governance of a country, and political relations between countries [HJ, GOG05, GLL03, FVB08, GM03, BN13] might be related to the adoption rate of ISO 27001 [AL09, And01, KH14, AHK13].

3.3.2 ISO 27001 and Regulations and Legal System

To date, there are requirements for compliance with several international and national information security business, legal, contractual and regulatory requirements as results of extensive international communications and contracts, which requires structured and organised strategies [Fre07]. One of the motivations for ISO 27001 certification is to comply with the core requirements of information related regulations as well as the required laws and contractual obligations [Boe09, HP06, Can14, SZK08, Boe08]. When a government allocates adequate resources in different forms of policies and regulations, then citizens can pursue their own economic interests [GLN16]. Horst's findings [Fel07] described that level of regulations and bureaucracy to limit market entry is related to the level of economic growth. Armeanu et al. investigated 21 EU (European Union) member states to reflect perceptions of the government's ability to formulate and apply sound policies and regulations by following ISO management system standards, such as ISO 27001 [AVG17]. In this section, we investigate the possible relationship between legal systems and regulations (cf. 2.4.1) and information security management activities and the implementation of ISO 27001.

The legal system is based on public rights [GLN16], which might have a relationship with some of the security controls of ISO 27001 defined in the Annex A (cf. A), such as A.18.1.2 (Intellectual property rights) or A.18.1.3 (Protection of records). The security of property rights and effective law enforcement have an influence on the level of successful financial market operation for the contracts [GLN16], which could have a relationship with some of the controls of the Annex A , such as A.7.1.1 (Screening) or A.5 (Information security policies). Nystrom stated that legal system structure, property rights security and credit regulations support the capacity and willingness to develop,

organise and manage a business [Nys08], which might be related to some controls, such as A.18.1.4 (Privacy and protection of personally identifiable information) or the controls relevant to compliance and contracts, such as A.18 (Compliance) or A.14.1.2 (Securing application services on public networks).

To sum up, legal systems and regulations are potential political characteristics, which might be related to the motivation for ISO 27001 certification. For example, economic growth and development could have a relationship with the level of international trading that demands an acceptable assurance of the information security level, which might be satisfied by implementing ISO 27001.

3.3.3 ISO 27001 and GDP (Gross domestic product)

Publications have investigated the relationship between national economy and the adoption rate of ISO 27001 [Bre14, OOQ10, KKN12, JKW11, EVS00, CMR04, BVS00, FVB08]. For example, Armeanu et al. examined the correlation between following ISO management system standards and economic sentiment indicator for the EU member states from 2005 to 2014, which reflects and represents judgments and attitudes of producers and consumers about economic activity [AVG17]. They used regression models to show a positive relationship between following ISO standards, such as ISO 27001 and the economic sentiment indicator [AVG17].

For the economic characteristic, we select the GDP (Gross Domestic Product) to measure economic performance of a country [Fon15]. Based on the results of comparing different types of GDPs and the studied literature, the GDP-PPP (Purchasing Power Parity) (cf. 2.4.2) is selected to compare different countries' market exchange rate, which is GDP converted to international dollars using PPP rates and divided by total population [Fon15]. There might be a relationship between economic performance of a country and the implementation of the security controls of the Annex A relevant to maintenance, such as A.17 (Information security aspects of business continuity management) or A.16 (Information security incident management).

We denote those cultural, political and economic characteristics by characteristics that are selected for the purpose of this thesis in the following.

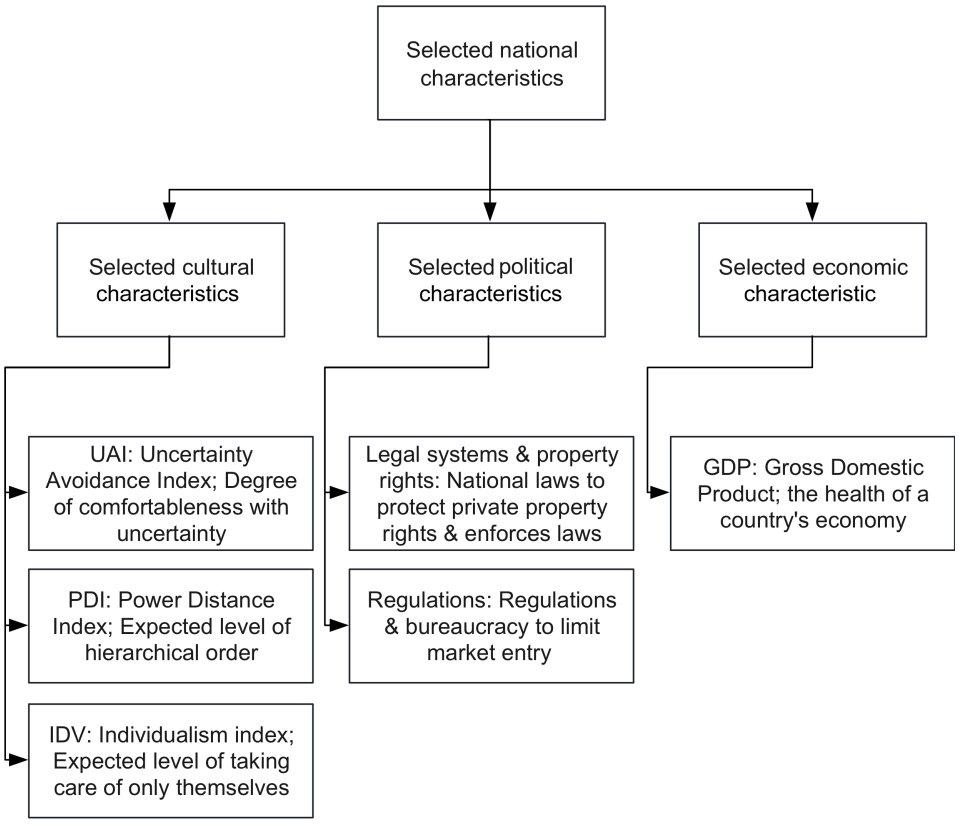

FIGURE 3.1: Cultural, political and economic characteristics that are selected for the purpose of this thesis

3.3.4 The Selected Characteristics for the Purpose of This Thesis

In this section, we provide an overview of the characteristics that are selected for the purpose of this thesis, which might have a relationship with the adoption of ISO 27001, which are cultural (UAI, PDI, IDV) (cf. 2.3.2), political (legal systems and property rights, regulation) (cf. 2.4.1), and economic (GDP-PPP) (cf. 2.4.2) characteristics as Figure 3.1 presents. Cultural characteristics are comparably more stable and only gradually change in the long-term [Übe13, VNB93, Gar04, VNvS05, KDHK99, Ifi09, GRN+11, Sch94, SS95]; while the economic and political characteristics are more likely to reform over time [GLN16, GM03, Fel07, Mah01, BN13, Nys08, HJ, OS11].

Note that in Figure 2.3, three cultural publications and the relevant dimensions are analysed at the national level, and in Figure 3.1 we present the cultural characteristics, which are selected for the purpose of this thesis. We analyse the correlation between the cultural, economic and political characteristics and a number of ISO 27001 certificates in our quantitative analysis.

After describing the characteristics that are selected for the purpose of this thesis, we describe the results of our qualitative analysis.

Chapter 4

Qualitative Analysis

4.1 Introduction

For our qualitative analysis, we conduct a literature review and we investigate Annex A controls of ISO 27001 to answer the second research question (cf. 1.4). The results of the qualitative analysis are based on the relationship between the national cultural characteristics that are selected for the purpose of this thesis, and the implementation of ISO 27001. First, the relationship between ISO 27001 Annex A controls and the national cultural characteristics are analysed. Then, the adoption rate of ISO 27001 is analysed in different countries to investigate possible reasons for the number of issued ISO 27001 certificates. The next section describes the motivation for developing national information security guidelines and the possible relationship with the adoption rate of ISO 27001. Next, we state possible alternative factors that can explain our empirical observations that have not been studied in this thesis. Then, the results of our qualitative analysis are summarised as a basis for further research.

4.2 Annex A controls of ISO 27001

One of the research contributions is to identify and discuss the issues that might be related to the implementation of ISO 27001 based on the national cultural characteristics. We describe national characteristics as characteristic of a particular nation as a whole, which is influenced by wealth and economic power, historical background, and cultural characteristics related to existing information security requirements [Hof84, Hof83, TV10, JHD+06, KLG06]. There might be a relationship between cultural distinctiveness and the adoption of ISO 27001. In the following, Annex A controls of ISO 27001:2013 (cf. A) are investigated based on a high-level classification.

4.2.1 High-Level Classification

We classify Annex A controls to a high-level classification to investigate the main focus of each control. For example, management's perceptions are possibly related to the definition of formal procedures such as policies, and employees' attitudes may be related to execution and design phases of the controls. Accordingly, Annex A controls are classified into three general groups of detection, prevention, and reaction.

Most of the control domains defined in Annex A are related to all these three general groups. Annex A controls are mostly based on the prevention concept, which covers more than two-thirds of the total number of controls, such as A.10 (Cryptography). The controls A.14 (System acquisition, development, and maintenance), and A.16 (Information security incident management) are mostly based on the reaction concept, which focuses on maintenance activity in the process of developing ISO 27001. Moreover, the control A.17 (Business continuity management) particularly focuses on the reaction concept. The controls A.11 (Physical and environmental security) and A.12 (Operations security) are mainly based on the detection concept.

The cultural characteristics could also be related to each group of our high-level classification; for example, there might be a relationship between the countries with high UAI (cf. 2.3.2) and the controls that are based on the prevention concept. The goal of most of the controls is to eliminate future uncertainty by establishing policies, guidelines, and procedures to control employees' behaviour. Accordingly, we investigate the

relationship between the Annex A controls and the cultural characteristics of UAI, PDI, and IDV (cf. 2.3.2), based on Hofstede as the adopted literature at a national level [JHD+06, TV10, VNB93, KLG06].

4.2.2 The National Cultural Characteristics Selected

We expect a relationship between the implementation of ISO 27001 and the national cultural characteristics that are selected for the purpose of this thesis. The cultural distinctiveness is one of the potential factors that might be related to the number of issued ISO 27001 certificates, which could prevent or hinder employees from cooperating with established policies and procedures. Accordingly, Annex A controls are analysed to come up with the aim of the controls based on the cultural characteristics selected.

There are requirements that have to be met so that a control can be implemented. Based on the focus of each control in a control domain, we investigate the controls that are based on the People category, such as A.5.1.1 (Policies for information security) or A.6.1.1 (Information security roles and responsibilities). For example, there might be a relationship between the countries with high PDI and the controls relevant to management decision-making and interaction with employees, as well as the controls relevant to defining and communicating policies, such as A.7.2.1 (Management responsibilities). In countries with high PDI, not involving and consulting with employees is more tolerable, and communicating with management mostly requires a formal procedure [KLG06]. In high PDI countries, employees constantly seek for management's confirmation about their duties [Hof03]. In general, employees are not expected to contradict management in high PDI countries [Hof83] and it is more likely that rules are followed strictly.

There could be a relationship between countries with high IDV and the level of details of policies and employees' segregation of duties. The people with high IDV may have more security concerns and they may be more precise about defining guidelines and rules, for example, access control polices. However, the people with low IDV may have fewer security concerns about internal unauthorised access that can be related to some of the controls, such as A.9.2.2 (User access provisioning). The countries with high levels of UAI and IDV may define more restrictions and limitations for employees committing breaches, by forcing harder penalties compared to the countries with low IDV [VNB93].

Annex A control domains may not have the same weight in every organisation and every country. It is important to prepare an appropriate environment for guiding employees to conduct their behaviour according to the policies and procedures, such as access control policy. Development stages of ISO 27001 are possibly related to the cultural characteristics of the people planning or maintaining this standard. There could be a relationship between the selected cultural characteristics of UAI, PDI, and IDV on one side, and adoption of some controls on the other side, for example, the A.7 (Human resource security) controls, such as A.7.2.2 (Information security awareness, education and training). There might be a relationship between selection and execution of some controls such as A.5 (Information security policies) and the cultural characteristics selected, which are called cultural controls in this thesis.

However, the cultural characteristics selected might not be related to the controls that mainly address technical issues, such as A.10 (Cryptography) or A.14 (System acquisition, development, and maintenance). The control A.17 (Business continuity management) might not be related to the cultural characteristics of UAI, PDI, and IDV, which are called technical controls in this thesis. The cultural controls, such as policies, might not be updated or maintained regularly, compared to technical controls [Ash08, Ifi14a, HP06].

To sum up, people mind-set and behaviour has a long-term influence and cannot be changed in a short period of time. Accordingly, a pre-phase plan is recommended before commencing the first phase of ISO 27001 development for analysing the current organisational culture. Such a pre-phase plan could be useful for estimating an organisation's readiness for adopting ISO 27001 because cultural characteristics are considered early on. However, there could be other factors that might be related to the adoption rate of ISO 27001 that have not been measured in this thesis. The motivation for the further research is based on the fact that the country's cultural characteristics might have a relationship with the adoption and development phases of ISO 27001.

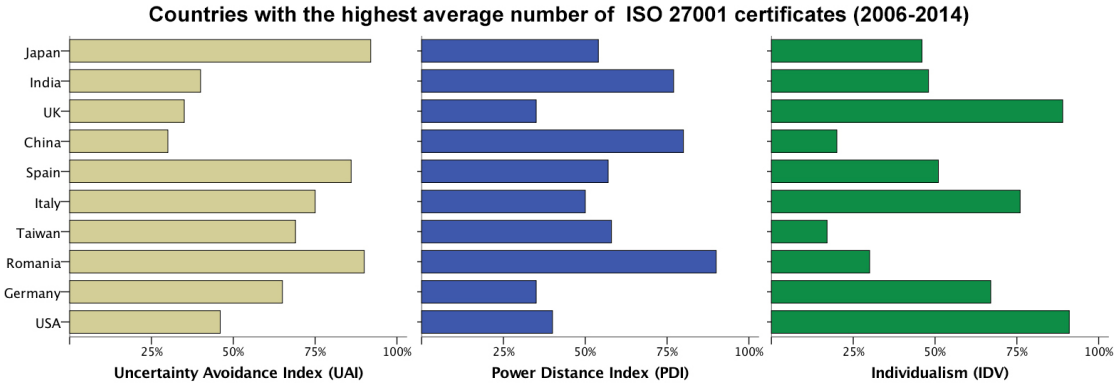

FIGURE 4.1: High adoption rate of ISO 27001 & cultural characteristics selected [Int14, Hof03]

4.3 Spectrum of Adoption Rate of ISO 27001 in Different Countries

To measure the adoption rate of ISO 27001, the average number of ISO 27001 certification is calculated from 2006 to 2014 [Int14]. After describing the cultural characteristics of the countries with the highest adoption rate of ISO 27001, the countries with the lowest adoption rate are investigated. For both groups, we investigate the relationship between those countries and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4).

4.3.1 Countries with the Highest Average Number of Certification

Figure 4.1 shows the relationship between the cultural characteristics selected (cf. 2.3.2) and the average number of ISO 27001 certification from 2006 to 2014 [Int14].

The higher values of these cultural characteristics indicate that these countries are relatively stronger in these cultural dimensions. Most of these countries have reasonably high levels of UAI and IDV with comparably low levels of PDI. There is an empirical relationship between the countries with relatively high UAI and IDV, but low PDI on one side, and higher average number of ISO 27001 certification on the other side from 2006 to 2014. The highest average number of ISO 27001 certification belonged to Japan as one of the most important economies with a relatively high UAI and PDI.

TABLE 4.1: High adoption rate of ISO 27001 & characteristics that are selected for the purpose of this thesis

Country	Ave. Cert	UAI	PDI	IDV	LS	Reg	NI	GCI
Japan	7150.17	92	54	46	7.78	7.24	✓	0.70
UK	1881.33	35	35	89	8.59	7.49	✓	0.70
India	1818.00	40	77	48	5.87	6.23	✓	0.70
China	934.50	30	80	20	5.36	6.96	✓	0.44
Italy	696.17	75	50	76	5.72	6.82	-	0.55
Romania	767.00	90	90	30	6.23	7.23	-	0.47
Taiwan	885.33	69	58	17	6.62	7.38	-	0.50
Spain	721.83	86	57	51	6.56	6.85	-	0.58
USA	574.00	46	40	91	7.07	8.16	✓	0.82
Germany	579.67	65	35	67	8.03	6.72	✓	0.70
Czech Rep.	358.33	74	57	58	6.99	8.01	-	0.50
Poland	301.00	93	68	60	6.77	7.33	✓	0.52
Rep. of Korea	238.67	85	60	18	6.14	6.91	-	0.70
Hungary	237.67	82	46	80	6.31	7.27	-	0.67
Netherlands	253.00	53	38	80	9.10	7.56	-	0.67
Bulgaria	222.83	85	70	30	4.91	7.44	-	0.44
Turkey	170.33	85	66	37	4.40	5.93	-	0.64
Australia	126.67	51	36	90	8.63	7.86	✓	0.76
Israel	159.67	81	13	54	6.71	7.29	-	0.67
Malaysia	147.50	36	100	26	7.28	8.48	-	0.76
Hong Kong	112.83	29	68	25	7.87	8.85	✓	0.61
Slovakia	143.50	51	100	52	5.46	7.13	✓	0.61
Switzerland	89.83	58	34	68	8.66	7.82	-	0.35
UAE	109.83	80	90	25	7.68	6.31	✓	0.35
Thailand	111.33	64	64	20	4.74	6.61	-	0.41
Mexico	79.83	82	81	30	4.16	6.65	-	0.32
Singapore	72.83	8	74	20	8.03	8.32	✓	0.67
France	103.17	86	68	71	7.67	6.83	✓	0.58
Brazil	67.50	76	69	38	4.74	4.88	✓	0.70
Austria	65.67	70	11	55	8.39	6.58	✓	0.67

Next, we extend our analysis to more countries based on the ISO survey 2015. We investigate the relationship between countries with high average number of ISO 27001 certification from 2010 to 2015 and the characteristics that are selected for the purpose of this thesis as Table 4.1 presents. We denote the average number of ISO 27001 certification with Ave. Cert, Legal System with LS, Regulations with Reg, the existence of national information security guidelines with NI, and Global Cybersecurity Index with GCI. The top countries listed in Table 4.1 are mostly the main manufacturers and the biggest economies with distinct information security requirements [HHN10b, Jon10, HHN10a].

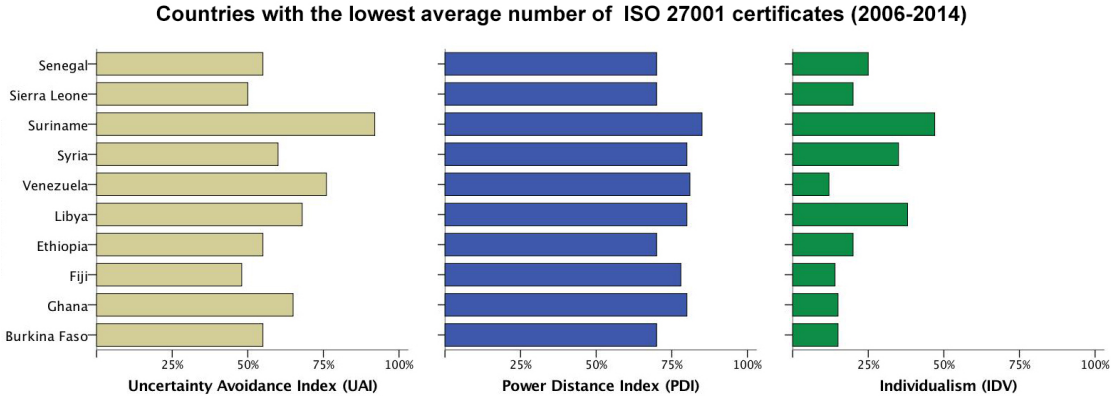

FIGURE 4.2: Low adoption rate of ISO 27001 & cultural characteristics selected [Int14, Hof03]

Most of these countries have reasonably high levels of UAI, PDI and IDV as well as comparably high property rights and regulations. Half of these countries have national information security guidelines.

Then, we describe the relationship between the Global Cybersecurity Index and the number of issued ISO 27001 certificates. The Global Cybersecurity Index is a comprehensive profile for covering several countries' national characteristics of political, economic and social characteristics based on the five measurements such as legal, technical and cooperation. We investigate the relationship between the top countries with the highest level of Global Cybersecurity Index and the adoption of ISO 27001 in Appendix B. Our results indicate that ISO 27001 certification has a moderate positive relationship with Global Cybersecurity Index (cf. 2.5), which acts as a multi-stakeholder initiative to measure the commitment/preparedness of countries to cybersecurity [ITU15].

We now investigate the countries with the lowest average number of ISO 27001 certification.

4.3.2 Countries with the Lowest Average Number of Certification

Figure 4.2 displays the cultural characteristics of the countries with the average number of certification of almost one from 2006 until 2014 based on the cultural characteristics selected (cf. 2.3.2).

Most of these countries have relatively high levels of UAI and PDI as well as low IDV (cf. 2.3.2). The combination of these cultural characteristics might be related to lower

numbers of ISO 27001 certificates. However, there might be other influential factors that we have not studied in this thesis.

In countries with high PDI, managers may not consult with employees during the process of developing policies [Hof84]. They might not ask for employees' opinions or execution experiences, in order to deal with organisational security concerns [Hof83]. In order to increase practicability of established policies and procedures, assigning a responsible group is necessary for taking feedbacks in short and interactive meetings [KKN12, UB13, SMP14, PS10]. Training and awareness programs could be a formal process of educating employees about computer security, corporate policies and procedures for working with IT. Employees' security awareness training and education [PC11, CDMS08, Gar04, EUE09, ST05, FCL10] may be helpful especially for these countries to guide employees to conduct their behaviour as expected and to adapt to established policies and procedures [SAT12b, HWL16, CW08, Cal13, Dis13, Gar04, EUE09, SA12]. Besides that, legal system and social sanctions for employees' non-compliance [FFA+14, TvSL06, Sch14, SFC15] could be related to practicability of ISO 27001 policies [AS13, AS99]. However, if employees have the fear of losing their job and the consequences of non-compliance, they would be committed to following the policies even when they feel that it is counterproductive [SMP14, PS10].

Then, we investigate the countries who had less than ten certificates of ISO 27001 in 2014, as can be seen in Table 4.2. These countries mostly had low average of ISO 27001 certificates from 2006 to 2015. We denote ISO 27001 certification in 2014 with Cert, Legal System with LS, Regulations with Reg and Global Cybersecurity Index with GCI. Comparing to the studied top countries (cf. Table 4.1) with the highest number of issued ISO 27001 certificates in 2014, the main difference is based on the levels of IDV, and GDP-PPP. However, the difference between these two groups of countries' UAI is relatively low. We observe a relationship that does not imply causality. Then, we discuss possible reasons for this low adoption rate.

According to Ivan Flechais, a particular style of information security management may not be acceptable and fitting in all countries [FCvS+10, FS09, FSH03], which could be one of the possible reasons for ISO 27001 low adoption. He also identified that the ISO 27000 family of standards and similar documents are essentially of English-speaking origin and are inherently based on their governance structures. Accordingly,

Table 4.2: Countries with a drop in the number of issued ISO 27001 certificates in 2014 & characteristics that are selected for the purpose of this thesis

Country	Cert	UAI	PDI	IDV	LS	Reg	GDP-PPP	GCI
Ukraine	9	95	92	25	4.57	6.87	8680.83	0.35
Albania	8	70	90	20	5.21	6.34	11390.71	0.20
Ecuador	7	67	78	8	3.46	6.31	11302.68	0.35
Luxembourg	7	70	40	60	9.04	7.38	97638.71	0.47
Malta	7	96	56	59	8.35	7.16	33197.52	0.35
Morocco	5	68	70	46	7.50	5.82	7813.38	0.55
Kenya	4	50	70	25	5.02	7.09	3098.61	0.41
Tanzania	3	50	70	25	6.59	7.24	2741.69	0.20
Dominican Rep.	3	45	65	30	4.40	6.68	14014.41	0.11
Estonia	3	60	40	60	7.39	7.55	27879.72	0.70
Guatemala	3	99	95	6	4.36	6.77	7549.75	0.20
Jordan	2	65	70	30	6.17	7.00	11970.54	0.20
El Salvador	1	94	66	19	4.13	7.50	8059.80	0.20
Lebanon	1	50	75	40	4.38	6.17	18051.81	0.08
Mozambique	1	44	85	15	4.07	5.81	1178.27	0.58
New Zealand	1	49	22	79	9.07	8.20	35305.27	0.73
Trinidad	1	55	47	16	5.46	6.74	32170.23	0.20
Venezuela	1	76	81	12	1.18	4.00	17759.40	0.20

translating the document into a foreign language could possibly influence comprehension of the requirements that have to be met for implementing ISO 27001 because of different interpretations and cultural differences.

To sum up, the motivation for adopting ISO 27001 might be related to national characteristics, such as historical background, economy, and global activities. Our results empirically show that there is a relationship between the countries' levels of IDV and GDP-PPP and the adoption of ISO 27001 in 2014.

We follow up on previous works by analysing the relationship between national information security guidelines and the selection as well as implementation of ISO 27001.

4.4 National Information Security Guidelines

Cultural differences may be related to several types of national information security guidelines, and studying similarities and differences between these guidelines guides us to investigate the possible related characteristics with the adoption of ISO 27001.

This section analyses national information security guidelines, and classifies them based on common characteristics, such as national economy and global activities. Next, the reasons for implementing and selecting national information security guidelines are described to investigate the information security requirements that are not possibly fulfilled by implementing ISO 27001. Then, these countries' average number of ISO 27001 certification and their social characteristics are described with some examples.

4.4.1 The Implementation of ISO 27001

The average number of ISO 27001 certification of the developed countries with national information security guidelines was higher than the developing countries studied from 2006 until 2014 [Int14]. For example, the average number of certification of Rwanda, Uganda, Malawi and Azerbaijan was comparatively lower than Japan, the UK, India, China, the USA and Germany from 2006 until 2014 [Int14]. Most of these countries with a high number of issued ISO 27001 certificates [Int14] have a strong national economy level (such as China or Japan), and they mostly adopt both ISO 27001 and national information security guidelines. Then, possible motivations for developing a national information security guideline are described.

One of the possible reasons for creating a national information security guideline is to address specific national or industrial information security requirements. The developing countries' motivation for their national information security guideline might be to establish the basic information security knowledge and awareness for related security risks. For example, the Uganda's government published the national information security guideline for improving information security awareness and establishing an information security culture. The second reason could be the time of establishing the international information security standard. The other possible reasons might be ISO 27001 generic ISMS requirements, which addresses every organisation regardless of their system's properties, business and finance in every country.

The cultural characteristics of the countries with national information security guidelines are described as the next step, based on and the cultural characteristics selected (cf. 2.3.2).

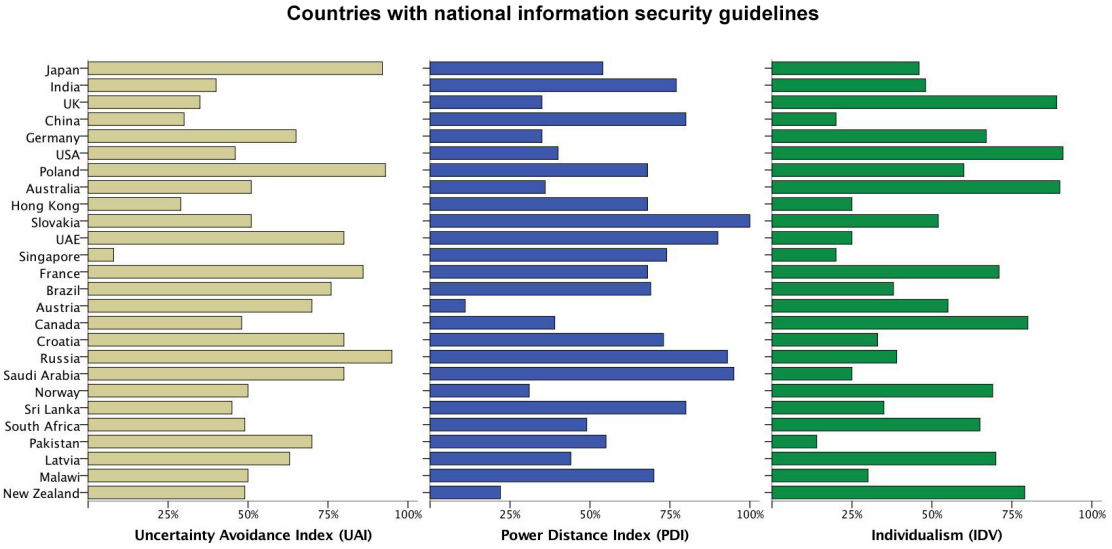

FIGURE 4.3: National information security guidelines & cultural characteristics selected [Hof03]

4.4.2 Cultural Characteristics

Figure 4.3 shows that most of these countries have relatively high levels of UAI and PDI. There might be a relationship between the countries with high levels of UAI, PDI and IDV on one side, and adoption of both ISO 27001 and national information security guidelines on the other side. The cultural characteristics of some of the studied countries are not available (such as Rwanda), which is one of the limitations of this thesis.

To sum up, ISO 2001 adoption could be related to several national characteristics such as historical background, governmental regulations and population [Boe08, SAT12a, FVB08, NEF08, SAT12b]. There might be a relationship between the adoption rate of ISO 27001 in these countries and the national socio-economic background and cultural characteristics. The countries with national information security guidelines may not select ISO 27001 as a single point of reference for an ISMS, because of the language or generality of ISO 27001.

4.5 Alternative Factors

In the qualitative analysis, we investigate the relationship between the adoption of ISO 27001 and the cultural characteristics. However, the potentially influential factors are

not limited to cultural characteristics. The most important alternative factors that can be related to the number of issued ISO 27001 certificates are listed in the following [FVB08, Can14, Fre07, Boe09, SAT12a, HWL16]:

- Security breaches in the organisation,
- Difficult economic situation for the organisation and/or its environment,
- Competitors achieving certification,
- Lack of qualified security experts,
- Resistance to change from employees,
- Management not being aware of the need for security,
- Employees not complying with security measures,
- Lack of qualified security experts,
- Local regulations that require certification,
- Contracts requiring the organisation to be certified.

4.6 Conclusion of Qualitative Analysis

In the qualitative analysis, we investigated the ISO 27001 survey 2014 [Int14] and the national cultural characteristics of UAI, PDI and IDV (cf. 2.3.2) to build a relationship between the adoption of ISO 27001 and the cultural characteristics that are selected for the purpose of this thesis. Assessing organisation's readiness as a pre-phase plan, especially for the cultural controls (cf. 4.2.2) can help in the implementation of ISO 27001, based on the organisational information security requirements and employees' cultural characteristics. The results of conducted literature review show the relationship between employees' adequate security awareness as well as knowledge [BHSS14, SAT12a, HP06, Cal06, SCHH09, FG02, CMR02, Sip00, KBS13, PC11, CDMS08] and the adoption rate of ISO 27001. To sum up, there might be a relationship between the adoption of ISO 27001 on one side, and several global and national characteristics on the other side, for example, financial crisis of recent years, governmental regulation and information security well-known events, such as privacy breaches.

The following chapters discuss the methodology and results of the quantitative analysis as the main focus of this thesis.

Chapter 5

Methodology of Quantitative Analysis

5.1 Introduction

The initial hypothesis to be tested is based on the relationship between the adoption of ISO 27001 in terms of the average number of certificates issued (2006–2014) and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4). Theories used to formulate the hypothesis included Hofstede [Hof84]. Our hypothesis is that the cultural, political and economic characteristics selected (cf. 3.3.4) have a relationship with the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). In this section, we describe methods used to answer the third research question (cf. 1.4). We present the process of developing the quantitative analysis part of this research, including the basis of the statistical models, as well as basic assumptions and fundamentals. Afterwards, we describe the methods and functions in more details to results of our qualitative research with our quantitative analysis.

5.2 Statistical Fundamentals for Statistical Models

When the independent selected variables are correlated (for example cultural dimensions of Hofstede), then extending the number of independent variables decreases the impact of each independent variable separately that may result in misleading results. Therefore, we select each variable from a category (for example culture, politics and economy) so

that the characteristics that are selected for the purpose of this thesis may be individually significant. Each selected predictor in our model may provide enough information because we select the potential national characteristics that might have a relationship with the adoption of ISO 27001. We eliminate some of the dependent variables such as cultural features, when they are correlated with each other, and knowledge of one necessarily covers the knowledge of the others [DK92], such as power distance dimensions of Hofstede and Globe.

The variables are mainly quantitative, which were initially presented with arithmetic operations in some cases in our qualitative analysis, such as an average number of ISO 27001 certification. All of the quantitative variables are discrete, with a finite number of possibilities, for example, score of Global Cybersecurity Index, cultural or economic characteristics. Some levels of the measurements are ratios, such as regulations (cf. 3.3.4). Some variables are intervals, implying that zero does not mean that the parameter does not have any value, such as GDP-PPP (cf. 2.4.2) or cultural characteristics (cf. 2.3.2). Some variables have an extensive range, such as a number of issued ISO 27001 certificates, or the GDP-PPP. This indicates the wide distribution of our data; for example, the UK with ISO 27001 certificates: 2253, IDV: 89% (relatively high), and Global Cybersecurity Index: 0.706, compared to Venezuela with ISO 27001 certificate: 1, IDV: 12% (relatively low), and Global Cybersecurity Index: 0.205.

Table 5.1 indicates the top 10 countries with the highest number of issued ISO 27001 certificates in 2014, with different values of UAI, PDI, IDV, legal, regulation, GDP-PPP and Global Cybersecurity Index.

It is necessary to examine where the bulk of the values lie and the range of the values to make the variables more condensed; for example, a number of issued ISO 27001 certificates ranges from 634 to 7171, or IDV from 20 to 91. Our data show high dispersion as Table 5.1 presents, so we group countries with at least one certificate in 2014 based on the certain ranges for a number of issued ISO 27001 certificates to approximately mitigate the effects of this dispersion at the beginning. For example, we define a range for a number of issued ISO 27001 certificates (for instance 0-10), instead of absolute numbers for developing our dataset. For analysing the correlation between the adoption of ISO 27001 and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4), we select the regression analysis model.

TABLE 5.1: Top 10 countries of number of issued ISO 27001 certificates

Country	Cert	UAI	PDI	IDV	LS	Reg	GDP-PPP	GCI
Japan	7171	92	54	46	7.78	7.24	37,518.75	0.70
UK	2253	35	35	89	8.59	7.49	39,826.06	0.70
India	2168	40	77	48	5.87	6.23	5,808.43	0.70
China	1210	30	80	20	5.36	6.96	13,224.00	0.44
Italy	969	75	50	76	5.72	6.82	35,131.05	0.55
Romania	893	90	90	30	6.23	7.23	19,743.54	0.47
Taiwan	781	69	58	17	6.62	7.38	46,035.83	0.50
Spain	698	86	57	51	6.56	6.85	33,835.01	0.58
USA	654	46	40	91	7.07	8.16	54,369.83	0.82
Germany	634	65	35	67	8.03	6.72	46215.70	0.70

Regression analysis is a statistical technique for investigating and modelling the relationship between the dependent (or response) and the independent (or predictor) variables [BLB08]. The response variable is the focus of a question in a study, and a predictor variable explains changes in the response variable that might affect the response variable. This method is applicable to find the relationship between an average number of ISO 27001 certification as the response variable and the selected predictor variables (cf. 3.3.4). Then, we explain the reasons why regression analysis is more appropriate compared to clustering as one of the possible methods for our analysis.

Clustering might be applicable provided that the data and parameters required for clustering are available and accessible for grouping a set of data points in such a way that data points in the same group of a cluster are more similar than those in other groups in order to segregate groups with similar traits and assign them into clusters. Such data for different counties are hardly accessible. Clustering based on one parameter could be misleading, such as population. The similarity among data points is subjective, which can impact our results [XW05]. Cluster analysis maximises in-group homogeneity; while regression analysis seeks to determine which independent variable plays the biggest role in distinguishing between groups on a dependent variable.

Regression analysis will help us to answer a question such as which variables (cf. 3.3.4) have the strongest correlation with the number of issued ISO 27001 certificates, which is more applicable to analyse the dataset. We assume that the characteristics that are selected for the purpose of this thesis have the same meaning across countries and that they are measured in the same way. We also assume that the measurement and

the underlying relationships are the same in all countries, and regression analysis is an applicable method. Regression analysis has several requirements to meet.

To use a linear regression method, the relationship between the independent and dependent variables should be linear. The linear regression analysis requires all variables to be normally distributed [DSP66]. Normal distribution and equal variance between response and predictor variables should be satisfied. For accepting a regression analysis output, we have to address these main points. First, the residual mean is always approximately zero. Next, the residual variance is almost constant and the residual distribution is normal for every x value.

Our model uses multiple regression analysis, as the number of predictor variables is more than one. Our model is only based on national characteristics, and the organisational culture is not included in the quantitative analysis. We analyse how dependent variable y: ISO 27001 certification is explained in terms of independent variables of x: the national characteristics that are selected for the purpose of this thesis (cf. 3.3.4), given as:

$$y = B_0 + B_1X_1 + B_2X_2 + e \tag{5.1}$$

In multiple regression, y, x and e are column vectors of observed values, regression parameters, and random errors. Each value of the y column matrix corresponds with observations of the x matrix, and both matrices have the same row number. B_0 is the y-intercept, and B_1 to B_6 evaluates changes in y, based on x_1 to x_6 (cf. 3.3.4). The input to the regression model is a x matrix with each row defining a data point for each country, and each column representing a feature for the variables selected for the purpose of this thesis. For instance, x_2 is the PDI (cf. 2.3.2), and x_6 is the GDP-PPP (cf. 2.4.2).

After describing the fundamentals, we explain the forward selection method as the main part of this analysis. The results of the statistical models are described in the next chapter.

5.3 Basic Assumptions and Definitions

We choose a forward selection for entering inputs based on the predictor variable in the regression analysis. In this method, predictor variables are entered into the regression model based on the criteria for accepting or removing observed predictor variable [BLB08]. The forward selection method adds predictors sequentially for assessing a predictors' significance to shape a satisfactory model [CH15]. The complete regression model includes all the predictor variables; while the reduced model leaves out one predictor variable in each step. The forward selection is formulated as follows:

$$[b, bint, r, rint, stats] = regress(y, x) \tag{5.2}$$

Values of b are called regression coefficients, for example in our model b_1 is the UAI (cf. 2.3.2), and b_6 is the GDP-PPP (cf. 2.4.2). r shows residual as the difference between the observed data of the dependent variable y and the fitted values, which is used to discover model assumption failures. The residual is the distance between observed and predicted response values [DSP66], which shows whether the LSR (Least-Squares Regression) is an appropriate model [MPV15]. *bint* and *rint* are the possible intervals for regression coefficients and each residual. The default value of *bint* (confidence interval for x) and *rint* (confidence interval for residuals r) is 0.05 for a confidence level of 95% [DK92]. In our forward selection method, we set a confidence level of 95%. Then, we introduce the stats variable as the main part of this regression function.

The stats structure includes additional statistics, which comprises of R^2 value, F-statistic, p-value, and the estimated error variance [KVAZ07]. The response variability explained by the model is called the adjusted R^2. R^2 value measures how close the data are to the fitted regression line, F-statistic indicates if the model fits the data better than the mean and a group of variables is jointly significant, and p-value indicates if the model is significant. R^2 coefficient of determination is a statistical measure of how well the regression line approximates the real data points. F-statistic is the test statistic used for assessing the statistical significance of the model, which tests for a significant linear regression relationship between the response variable and the predictor variables. p-value is the probability for a given statistical model when the hypothesis of no relationship between the response variable and the predictor variables is true. p-value is

calculated based on the assumptions that the difference in the sample is caused entirely by random chance. The error variance is the variance of the error variable and the error is the difference between predicted and observed value. Then, we describe these variables in more details.

The correlation coefficient is a number that quantifies a type of correlation and dependence (statistical relationships) between two or more values, which is a measure of the strength (positive or negative) and direction of the linear relationship between predictor and response variables. The Pearson correlation coefficient is always between -1 and 1. Values that are not equal to zero show a strong relationship and direct when it is positive (reverse when it is negative). The correlation coefficient returns a matrix based on the input matrix x with observations as rows, and variables as columns, or between 2 columns matrixes of x and y. We apply the correlation coefficient to measure the strength of the linear relationship between our variables, for example, a number of issued ISO 27001 certificates and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4). The coefficient of determination is the square of coefficient of correlation.

R^2 as the coefficient of determination measures how well observed outcomes are represented by the model. R^2 shows how close the data are to the fitted regression line, for example, 0% indicates that the model explains none of the variability of the response data. When R^2 is a large number, it does not mean causality, as a strong correlation does not necessarily mean a causal relationship. There are four possibilities in this case [KVAZ07]:

- **Causal link**: when we are not sure x causes y or y causes x,
- **Hidden cause**: when there is a hidden factor that creates the correlation,
- **Confounding factor**: when a hidden factor and x both cause y,
- **Coincidence**: by chance correlation.

R^2 changes are the key factor for choosing predictors, based on the significant predictor strength after entering the model. Furthermore, R^2 value ranges between 0 and 1, which is used to find the best predictor variables. When R^2 value is close to 1, it means a strong

relationship between x and y. The higher R^2 value leads us to explain response variables variation more accurately.

F-statistics is used to measure data variability of the model from the random error, and to compare these two values. F-statistic is also used to test the hypothesis that all regression coefficients are zero, and the p-value is associated with the F-statistic. In correlation syntax, the p-value is used to test the hypothesis of no correlation between two variables [BLB08]. The smallest p-value demonstrates stronger evidence for supporting the initial hypothesises. If the p-value is smaller than 0.05, then the correlation is not zero.

The error of prediction is called residuals, and the error variance is called RSME (Root-Mean-Square Error) [BLB08]. If the exclusion of an observation causes the prediction to change by a large value, then it is an influential observation [MPV15, DSP66]. For interpreting the results, the influential observations should be examined as their inclusion may change the results. In statistics, excluding an influential observation from the dataset considerably change the result of the calculation. Eliminating this influential point has a noticeable effect on the parameter estimation, in regression analysis.

After introducing the tools and functions of our statistical models, we focus on the last section of adopting this tool to match the objectives of our research.

5.4 Tools and Statistics of Our Model

The stepwise forward selection is an interactive method for predicting y based on the predictors' subset of matrix x columns, by including or excluding predictors into or out of the model. The aim of the stepwise forward selection is to build a model that accurately predict the response [KVAZ07]. This function chooses and adds the candidates, which suggest the best correlation with the response. This method also helps to find the outliers that affect the quality of the overall result as an outlier is an observation that does not fit the rest of the data [BLB08]. This method begins with selecting the variables that minimise the deviation from the mean value, until adding more data does not decrease the mean value deviation. This method builds a linear model at each step of an iteration. As a result, the output of this method shows the final chosen data. The data selection stops when the new candidate does not considerably reduce the prediction error. For

analysing the accuracy of our data to find the suitable model, we use the MATLAB (MATrix LABoratory) computer program. In this section, we describe the forward selection method, the functions and the variables for interpreting their meaning in our forward selection method.

The first value R^2 of the stats shows the coverage percentage of the model for the variability of observations. If F-statistic is significant, then it means the excluded variable in the reduced model contributes in predicting the value of criterion variable. Accordingly, the overall regression F-statistic and the associated probability of significance are also computed to add the most significant data (the largest F-statistic or smallest p-value) and remove the least significant data until no data remains [DSP66]. The combination of a high F-statistic value and low amount of p-value indicates that it is unlikely that all regression coefficients are zero [DK92]. Regarding the correlation coefficient, every p-value is the probability of finding a large correlation based on the observed data. The low value of an error variance of stats indicates the low level of variability between regression function and the variable. After explaining the stats variables, we discuss forward selection functions, which builds up the bases of our statistical models. The forward selection method consists of several functions that we present in this section.

The main part of the forward selection method is the *SFS* function. The inputs to the *SFS* function are predictors (x), target (y), and p-value. The *SFS* function adds the significant predictors in the model that predicts the response variable more accurately together with the old variables until the new variables do not change the prediction error. The stepwise forward selection forms the target vector as an output based on the variables. The target is the same size as x, and the correlation coefficient of each element of x is calculated with y. After calculating R^2 of all elements, the max R^2 value is calculated and replaces the old ones.

The other function that builds up this forward selection method is *SFLIN*. The inputs of *SFLIN* are x and y, which calculates the weight vector. The minimum error is stored in a temp variable to find the fitting new model. After that, the p-value of the new model is calculated and the significance is calculated with the F-statistic. The most significant data is selected based on the overall regression F-statistic and the associated significance of R^2 values. The gained p-value is substituted with the smallest initial

p-value, and the residual of the model terms is compared with the chosen term to build the final model.

To sum up, we conduct our research based on the countries with available information about a number of issued ISO 27001 certificates and the characteristics that are selected for the purpose of this thesis based on the forward selection method in the context of linear regression.

Chapter 6

Results of Quantitative Analysis

6.1 Introduction

In this section, we firstly present a brief overview of how we create our dataset before establishing our research process and describing the results. Secondly, we investigate the countries with more than the average number of the ISO 27001 certificates issued worldwide (2006–2014), followed by the statistical models to investigate the relationship between the cultural, political and economic characteristics that are selected for the purpose of this thesis and the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). Similarly, we analyse the relationship between the adoption of ISO 27001 and the cultural, political and economic characteristics selected for the countries with less than the average number of the ISO 27001 certificates issued worldwide (2006–2014), followed by the discussion section that reflects on the results and the limitations. For both groups, we describe the number of issued ISO 27001 certificates in 2014 as well. Then, we analyse Germany and Iran to illustrate our results using two culturally different countries.

6.2 Dataset Preparation

In this section, we describe the establishment of our dataset. In total, 83 countries have been analysed to investigate the relationship between the average number of ISO 27001 certification and the characteristics that are selected for the purpose of this thesis. In

this section, first we provide an overview of our dataset based on the general criteria for records to be excluded, and then we describe how we classify our dataset into two groups.

6.2.1 Overall Evaluation of our Dataset

In order to take into account the possible relations of the population and urban population with the number of issued ISO 27001 certificates, we give weight to the number of issued ISO 27001 certificates in 2014 per population and per urban population in Appendix C. Based on the results, the low populated countries placed on the top of our list, such as Iceland with 31 certificates in 2014 as the first country with the highest number of issued ISO 27001 certificates-per urban population. Most of the top countries with the highest number of issued ISO 27001 certificates-per urban population does not have relatively high numbers of ISO 27001 certificates in 2014, such as Bahrain, Latvia, Luxembourg, Malta as well as Trinidad (Trinidad and Tobago). Accordingly, assigning weight to the number of certificates based on one factor is not applicable. In this section, we describe the relationship between a number of issued ISO 27001 certificates and possible influential factors before selecting an average number of ISO 27001 certification for our statistical models.

Comparing absolute numbers of ISO 27001 certificates is not conclusive, as these countries' differences should be considered, such as size. Accordingly, we normalise the number of issued ISO 27001 certificates in 2014 by the GDP-PPP and population in the Appendix D to restrict the range of values in the dataset and to eliminate the effects of certain factors.

A number of issued ISO 27001 certificates could also be related to the number of successful attacks per country. Therefore, we calculate the correlation coefficient between a number of issued ISO 27001 certificates in 2014 [Int14] and the average total cost of a data breach [Ins17] for limited numbers of countries to find out whether there is a relationship between implementing ISO 27001 and the average costs of data breaches for organisations in these countries in Appendix E.

Figure 6.1 displays an overview of the top countries of our initial dataset based on the number of issued ISO 27001 certificates in 2014.

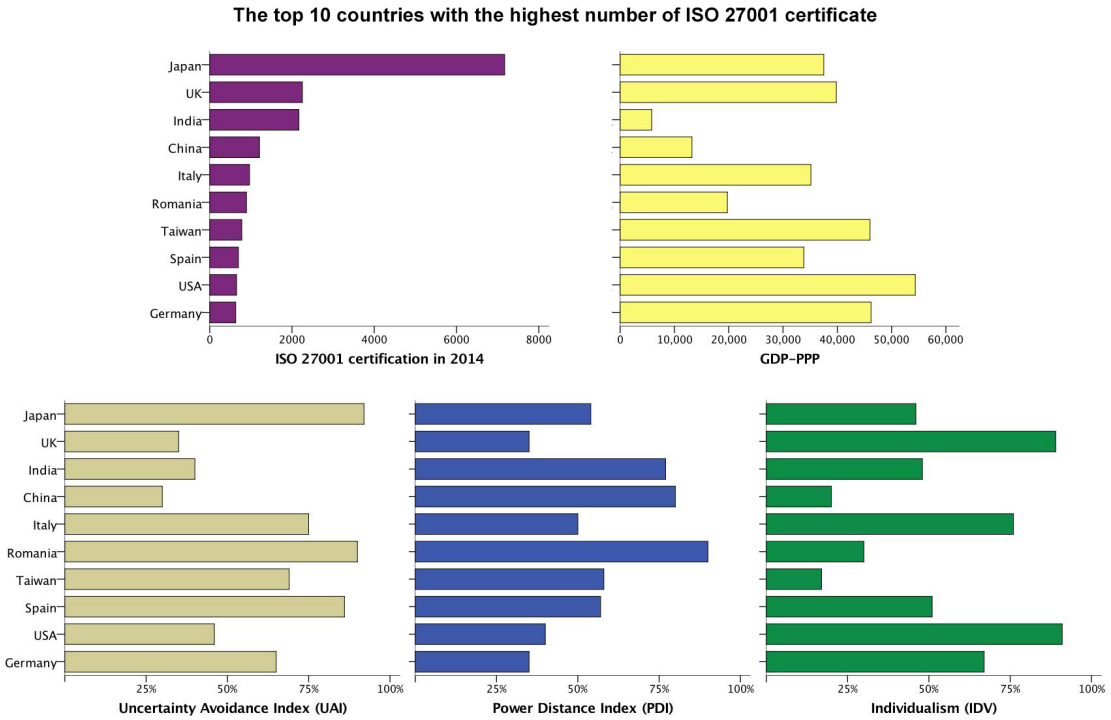

FIGURE 6.1: Overview of the top 10 countries with at least 1 certificate in 2014 & the characteristics selected [Int14]

We have to narrow down our research based on the available information about the cultural characteristics of the UAI, PDI and IDV after collecting data about an average number of ISO 27001 certification issued from 2006 to 2014. For example, the countries with average certification of less than one [Int14] are eliminated, e.g. Gabon, Fiji, Somalia, and Yemen. Most of these countries have few numbers of certificates during these 9 years and no certificate in 2014. In further steps, Iraq is also excluded because of unavailable data about legal systems and regulation. Japan is an observation point that is distant from other observations in our sample, which could be the result of an unusual event or factor that was missed during the study. Japan's number of issued ISO 27001 certificates is 31.34% of the total number of issued ISO 27001 certificates in 2014, and the average of Japan's certificates is around half of the total average number of ISO 27001 certification from 2006 to 2015. We eliminate Japan from our final analysis as an outlier [RH11] because Japan's number of issued ISO 27001 certificates deviates markedly from other countries of our dataset as Figure 6.2 displays.

To sum up, the general criteria for records to be excluded from our analysis are countries with unavailable data of the characteristics that are selected for the purpose of this thesis,

the countries with average certification of less than one, as well as Japan.

6.2.2 Classifying our Dataset into Two Groups

One of the leading publications that distinguish the mind-set and behaviour of different countries are based on the WEIRD (Western and educated who are from industrialised, rich, and democratic countries) theory [HHN10b]. Henrich et al. demonstrated that most of the assumptions about human thinking and behaviour are not applicable to all countries, which characterise only 12% of the world's population that are distinct in analytical reasoning and economic decisions [HHN10a]. Generalising these assumptions may lead to false claims about the main drivers of human behaviour [Jon10]. Besides that, WEIRD countries may have distinct cultural characteristics and requirements from the rest of countries [HHN10a]. In our qualitative analysis, we observe distinct information security culture for the top countries with the highest number of issued ISO 27001 certificates, which can match the samples of WEIRD countries. The cultural characteristics and information security requirements are largely distinguishable between developed European countries in comparison with the countries struggling with internal conflicts, such as Uganda. Wealthy countries and big manufacturers' risk management, information security activities, culture and economy differ from those countries with budget constraints and financial crises.

Accordingly, a common comparison approach may not be helpful for investigating the relationship between the adoption of ISO 27001 and the cultural, political and economic characteristics selected for several countries from different continents with distinct information security requirements. As our data is ranked based on the average number of ISO 27001 certification, the motivation for implementing ISO 27001 might be distinct between the countries with more than 1000 certificates (such as India or UK), and the rest with fewer than 10 certificates (such as Albania or Kenya). As the citizens of WEIRD countries must cope with the demanding information security culture, these countries' number of issued ISO 27001 certificates and the adoption rate of ISO 27001 is comparably high. Accordingly, we classify our dataset into two groups based on the average number of ISO 27001 certification from 2006 to 2014 (excluding Japan), which is 65.41.

Then, we describe the first group with more than the average certification rate of 66 (2006–2014), followed by the results of the quantitative analysis of the second group.

6.3 First Group

The first group consists of 23 countries with the highest average number of ISO 27001 certification from India as the 1st ranked country to the UAE (United Arab Emirates) as 23rd ranked country. More than two-thirds of ISO 27001 certificates in 2014 belong to the top 23 countries. In this section, we describe the adoption rate of ISO 27001, followed by statistical models and discussion.

6.3.1 Average Number of ISO 27001 Certification

As Figure 6.2 shows the UK and India have almost the same average number of issued ISO 27001 certificates viz. more than 1000 certificates. From China to Germany, countries have an average number of 834 certificates in 2014. The rest of the countries from the Netherlands to the UAE have 247 certificates on average in 2014. The average certification of this group is more than 66 from 2006 to 2014. To make the captions self-contained, we include the cut-off point that we have used as criterion based on the number of issued ISO 27001 certificates in 2014.

Most of the countries of the first group are leading manufacturers with a strong economy, which is directed by their extensive international communication. The number of ISO 27001 certification has increased for these countries yearly [Int14]. These countries' stable systems may support international standards based on the extensive international communication [SAT12a, FVB08], which demands an acceptable level of data protection [Boe09, HP06] or consistency with applicable regulatory or legal requirements [SAT12a, NEF08].

Then, we explain the relationship between the first group's average number of ISO 27001 certification and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4).

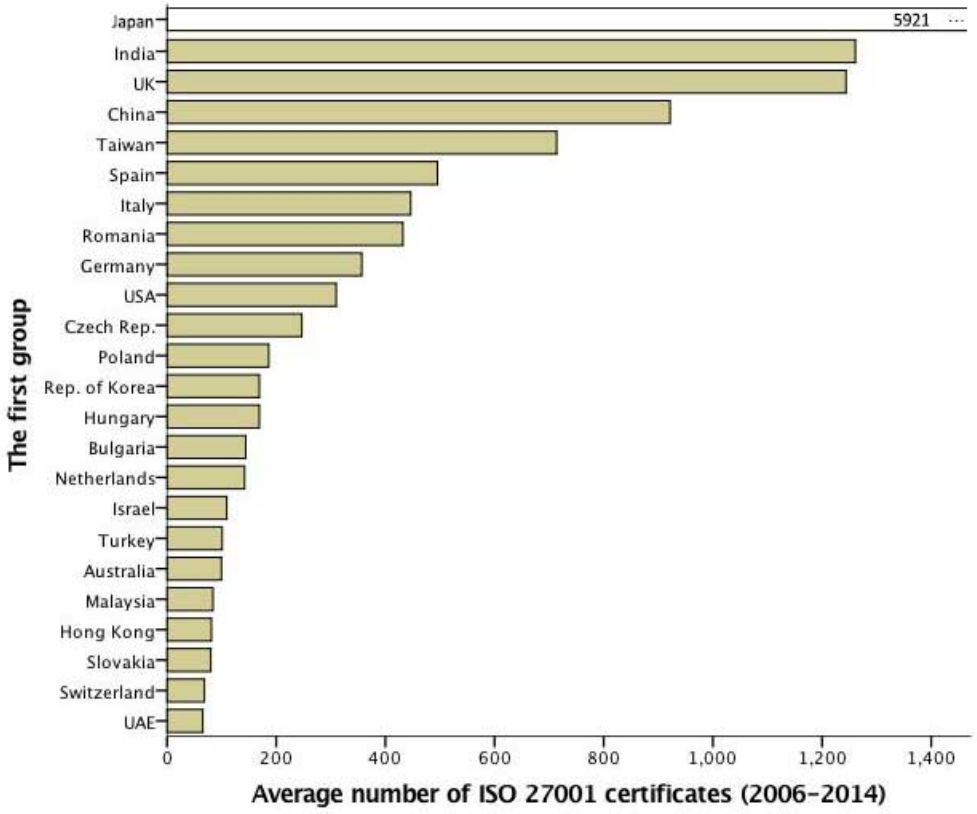

FIGURE 6.2: The countries with more than the average certification rate of 66 (2006–2014) [Int14]

6.3.2 Statistical Models

The results of the statistics of the regression analysis of the first group is: R^2 value: 0.5016, F-statistic: 3.4213, p-value: 0.0255, and an estimate of the error variance: 0.2357. The R^2 value indicates that the model accounts for over 50% of the variability in the observations, which equals the square of the Pearson correlation coefficient between the observed and modelled data values of the dependent variable: the adoption of ISO 27001. The F-statistic of almost 4 and the p-value of 0.02 demonstrates it is unlikely that all of the regression coefficients are zero. The error variance of 0.2 indicates that there is a small random variability between the variable and the regression function.

The results indicate that the the adoption rate of ISO 27001 is correlated with the 1^{st}, 5^{th}, and 6^{th} variables, which are UAI (cf. 2.3.2), regulations (cf. 2.4.1) and GDP-PPP

(cf. 2.4.2) with the R value of 0.7082. The signs of the variables' regression coefficients (UAI, regulations, and GDP-PPP) show a positive or negative association of these predictors with the adoption rate of ISO 27001. The results of the regression analysis demonstrate the positive correlations of regulations and GDP-PPP with the adoption rate of ISO 27001. The UAI is correlated with the adoption rate of ISO 27001 negatively.

To sum up, there is a relationship between countries with relatively high regulations and GDP-PPP, a bit low UAI on one side, and higher ISO 27001 adoption on the other side for the first group. We measure the correlation that does not imply causality, and there might be hidden root factors that explain our results, such as similar size or region.

Then, we discuss the first group's characteristics that are selected for the purpose of this thesis that is correlated with the average number of ISO 27001 certification: UAI, regulations, and GDP-PPP.

6.3.3 Statistical Models and the Characteristics Selected

Most of these countries have reasonably high levels of the cultural characteristics of UAI, PDI, and IDV, as Figure 6.3 displays.

The UAI is based on the level of formulating different types of rules, regulations, laws, and controls to reduce the uncertainty of future, which could be related to the practicability of established policies. Clarifying the main objectives of security rules and policies are helpful for these types of cultures. Besides that, it is important to address daily and routine behaviours with an adequate number of policies and to reduce unnecessary details. For example, Poland, Spain, and Romania have relatively high values of UAI. Then, we explain the first group level of regulations.

Regulations are based on the level of bureaucratic procedures and market entry strategies, which may be related to poor security decisions to bypass challenging policies. These countries mostly have a relatively high level of regulations (such as Hong Kong and Malaysia) as can be seen in Figure 6.4. These countries are mostly supported by an adequate level of administrative procedures to enter market freely and to guarantee property rights. Then, we explain these countries level of GDP-PPP.

Most of the countries in the first group are among the top economies as Figure 6.5 presents. The GDP-PPP is based on the size of a country's economy that may be related

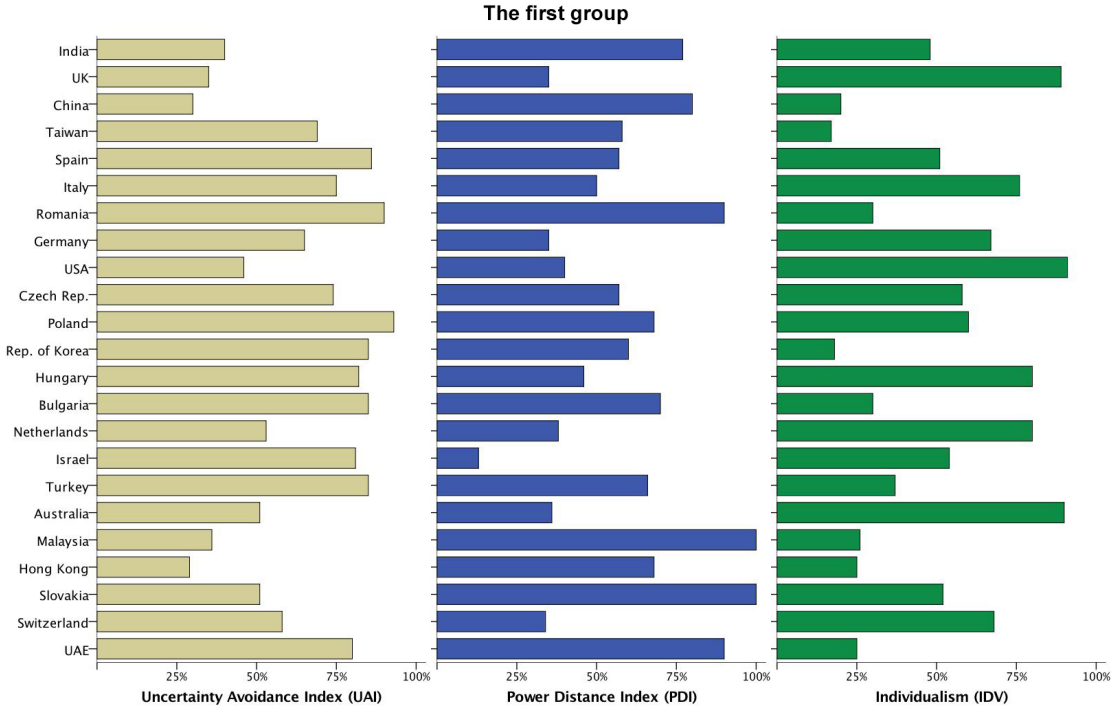

FIGURE 6.3: The countries with more than the average certification rate of 66 (2006–2014) & the cultural characteristics selected [Hof03]

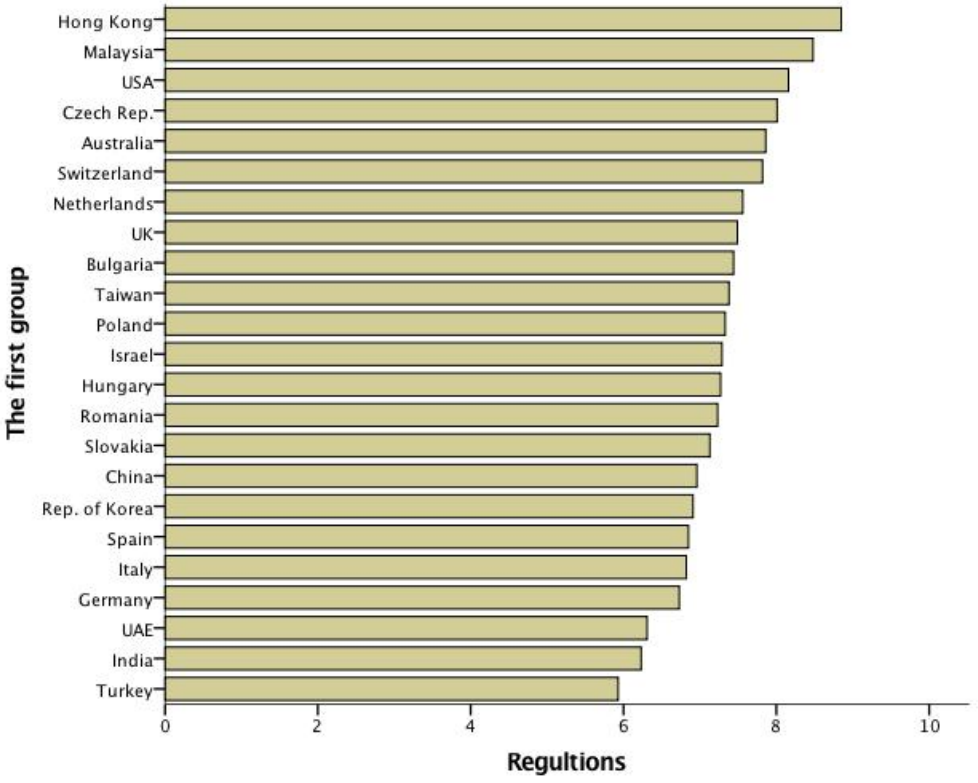

FIGURE 6.4: The countries with more than the average certification rate of 66 (2006–2014) & the political characteristics selected [GLN16]

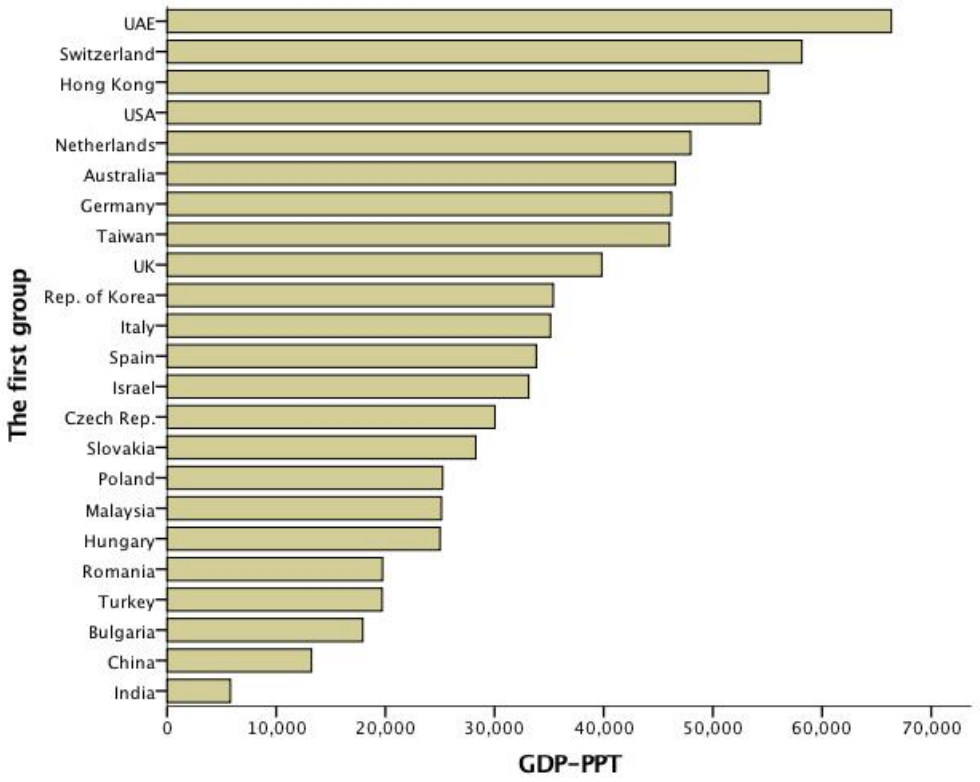

FIGURE 6.5: The countries with more than the average certification rate of 66 (2006–2014) & the economic characteristics selected [Fon15]

to high industrial growth rate, a stable currency, and investments on security mechanisms. Financial constraints could be related to the selection and the implementation of security mechanisms among the number of proposed security mechanisms. Most of the countries in the first group as large and fast-growing economies may focus on several types of information security activities, but not necessarily implement ISO 27001. For example, the USA, Netherlands, and Australia have relatively high levels of GDP-PPP in 2014 [Fon15].

As the cultural characteristics are comparably more stable and only gradually change in the long-term, the economic (cf. 2.4.2) and political characteristics (cf. 2.4.1) are more likely to reform over time. For example, China's GDP-PPP (cf. 2.4.2) score increased from 9215.4 USD (2010) to 14189.52 USD (2015) [Fon15], or Turkey's GDP-PPP score grew from 16193.13 USD (2010) to 20276.9 USD (2015) [Fon15]. Czech Republic's regulation score ranged from 4.4 (1990) to 8.01 (2014), or Poland's regulation score extended from 2.06 (1980) to 7.33 (2014) [GLN16].

Then, we state the limitations and discuss possible motivations for the adoption of ISO 27001 that have not been considered in the characteristics that are selected for the purpose of this thesis.

6.3.4 Discussion

We consider history as one of the influential factors that have not been studied in this thesis, which deals with the growth of a particular country. History and culture are both inter-related, and culture can be defined as a subset of history. The first group includes the former Warsaw Pact countries, such as Romania, Bulgaria, Poland, Hungary, Czech Republic, and Slovakia. The number of issued ISO 27001 certificates might not match the economic importance of those countries. These EU countries and companies in these countries have an incentive to proactively adhere to international norms to extend their collaboration opportunities with markets they had little access to until the dissolution of the Warsaw Pact. Western European countries do not have the same incentive. Then, we state the other limitations of this research.

The USA is the prime mover in the IT sector. The UK is the origin of ISO 27001, which is one of the main reasons that it comes on top of our list. The UK and India have relatively high numbers of ISO 27001 certificates, which could be related to their language. The same language with ISO 27001 could reduce misunderstanding and misinterpretations of translation. India and China have a high population, which can be related to the number of issued certificates. One of the characteristics that most of these countries have in common is a strong economy, which might influence our results.

Around 67% of first groups' countries have privacy policy legislations, such as the UK, India, Germany, and France, and half of these countries have anti-terrorist legislations such as China, and Turkey. The EU also adopted a directive for the security of information networks and systems for member countries to be equipped and prepared to respond to incidents, by having a national competent authority, which possibly impacts our findings.

Besides that, our results are possibly influenced by selecting the average number of certificates as the criterion for splitting the dataset into two parts, and the existence of a mix of diverse countries in each group. Most of the countries with a high average

number of ISO 27001 certification from 2006 to 2014 are in East Asia and the Pacific [Int14]. These countries are known for having a high level of order, discipline, and a system of behaviour, such as Japan.

Then, we explain the second group' adoption rate of ISO 27001, which comprises more than two-thirds of our dataset.

6.4 Second Group

The second group starts from Thailand ranked as 24^{th} to Honduras as 83^{rd} country based on the average number of ISO 27001 certification from 2006 to 2014. In this section, we explain the adoption rate of ISO 27001, and then we describe the relationship between the average number of issued ISO 27001 certificates and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4). For each section, we discuss the differences between the first and the second group.

6.4.1 Average Number of ISO 27001 Certification

This group is a mix of different countries from different continents such as Canada, Thailand, and El Salvador, and it is unlikely that they would be driven by common motivations for implementing ISO 27001 as can be seen in Figure 6.6. The second group's countries have less than the average certification rate of 66 from 2006 to 2014.

Around 30% of these countries have fewer than 10 certificates in 2014, and some of these countries struggle with poverty and internal conflicts such as Trinidad. The population standard deviation of the second group is 40.15 and the mean value is 40.65; while the population standard deviation of the first group is 591.91 and the mean value is 629.76 in 2014. These countries have a high spectrum of nationalities, political characteristics, geographic distribution and distinct levels of information security requirements. The number of ISO 27001 certifications of the second group could be related to the size of economy and population. For example, in the second group, there are countries with highly developed economies but relatively small population, such as Singapore, Austria, Norway or Sweden. The Singaporean government has a fifty-year plan that may be related to their decisions to information security activities.

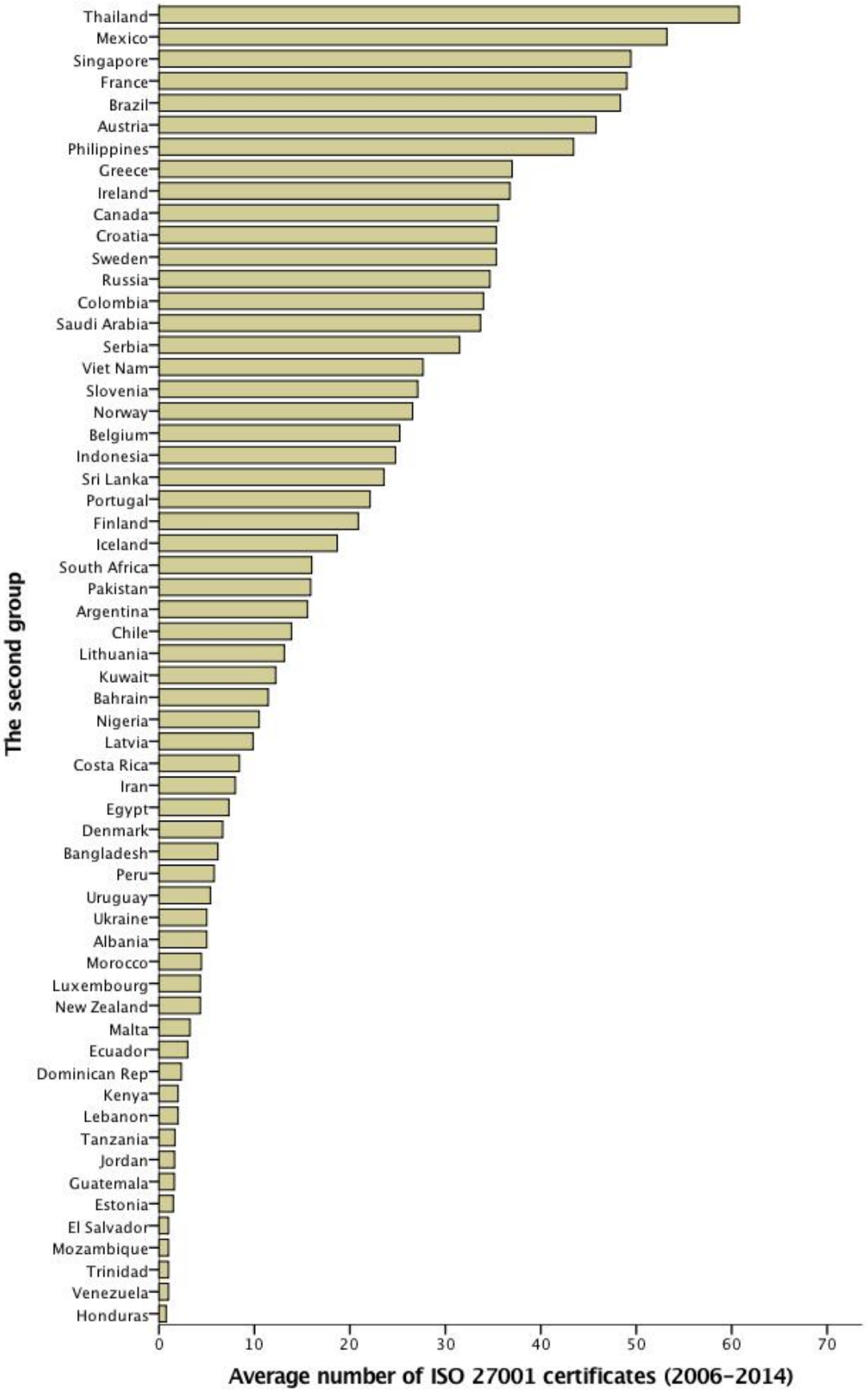

FIGURE 6.6: The countries with less than the average certification rate of 66 (2006–2014) [Int14]

Then, we analyse the relationship between the characteristics that are selected for the purpose of this thesis and the average number of ISO 27001 certifications of the second group.

6.4.2 Statistical Models

The results of the second group regression analysis is: R^2 value: 0.3087, F-statistic: 6.3648, p-value: 0.0003, and an estimate of the error variance: 0.1947. The R^2 value shows that this model accounts for over almost 30% of the variability in our observation of the second group. The F-statistic of almost 6.4 and the p-value of 0.0003 indicate that it is unlikely that all of the regression coefficients are zero. The error variance of 0.19 indicates that variability between our variables and the regression function is a small random number.

The second group's average number of ISO 27001 is correlated with the 6^{th}, 2^{nd}, and 3^{rd} variables of GDP-PPP (cf. 2.4.2), PDI (cf. 2.3.2) and IDV (cf. 2.3.2) with the R-value of 0.555. IDV and GDP-PPP are positively, and PDI is correlated negatively with the second group's average number of ISO 27001 certification. In both groups, GDP-PPP is positively correlated with the adoption rate of ISO 27001; while the cultural characteristic of UAI and PDI are negatively correlated with the average number of ISO 27001 certifications in the first and second group. The results show that two out of three predictors are cultural characteristics. To sum up, the results demonstrate that there is a relationship between the countries of the second group with a reasonably high IDV and GDP-PPP, a bit low PDI on one side, and higher ISO 27001 adoption on the other side. The observed correlation does not imply causality.

Then, we describe the second group's characteristics that are selected for the purpose of this thesis that is correlated with the average number of ISO 27001 certification: PDI, IDV, and regulations.

6.4.3 Statistical Models and the Characteristics Selected

Figure 6.7 presents that most of the second group' countries have relatively high levels of UAI (such as Serbia, Malta, and Uruguay) and PDI (such as Saudi Arabia and Bahrain).

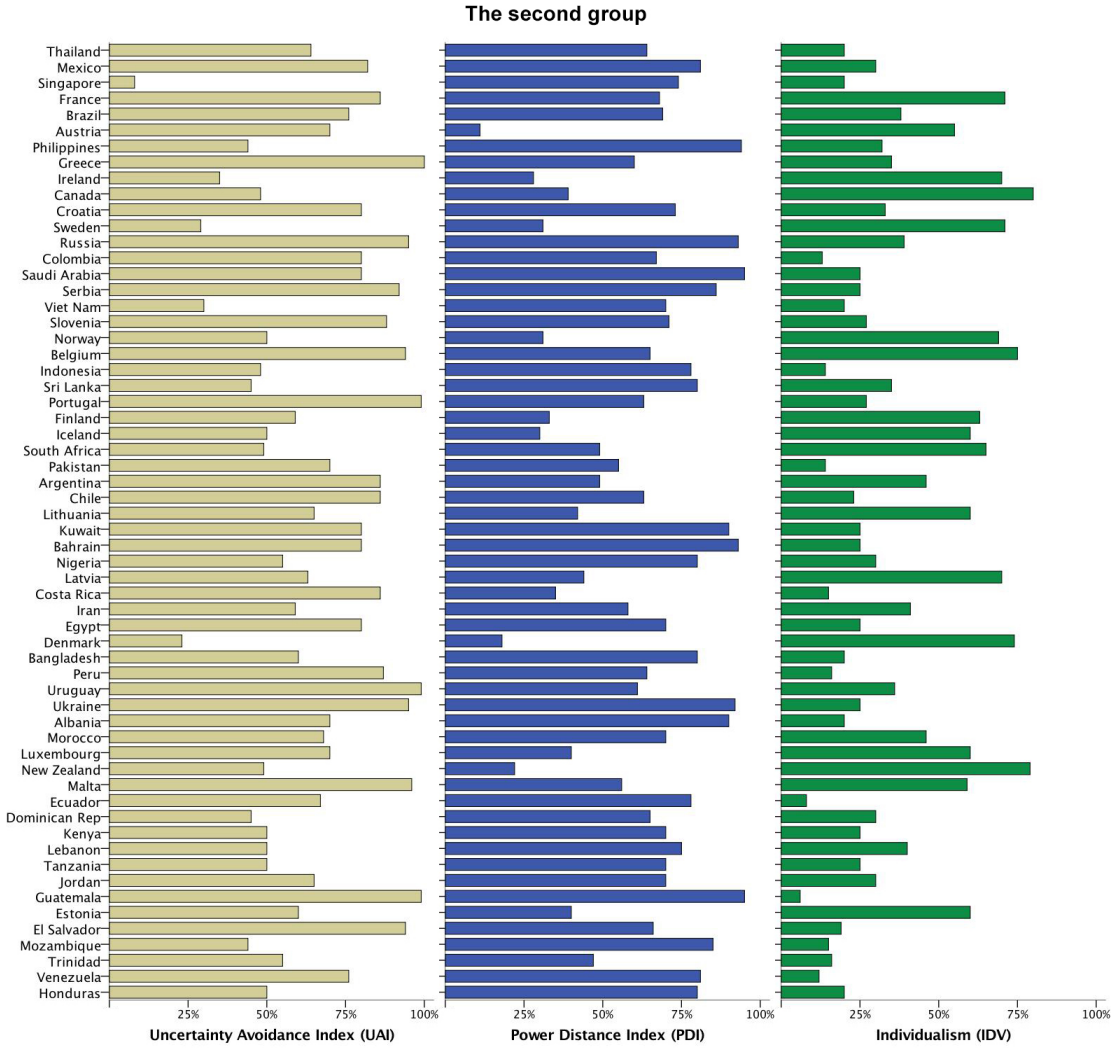

FIGURE 6.7: The countries with less than the average certification rate of 66 (2006–2014) & the cultural characteristics selected [Hof03]

Most of the countries in the second group have a relatively low IDV (such as Costa Rica, Guatemala, and Ecuador).

Figure 6.8 presents the second group's GDP-PPP (cf. 2.4.2), which shows the GDP on a purchasing power parity (PPP) basis divided by population in 2014 and is expressed in USD (US Dollar).

The PPP indicates that the exchange rate between two currencies is equal to the ratio of the currencies' respective purchasing power. The PPP exchange rates might be helpful for making comparisons between countries because they change modestly from year to year. However, the PPP exchange rate calculation is controversial because it is relatively difficult to find a comparable relatively fixed set of consumer products and services

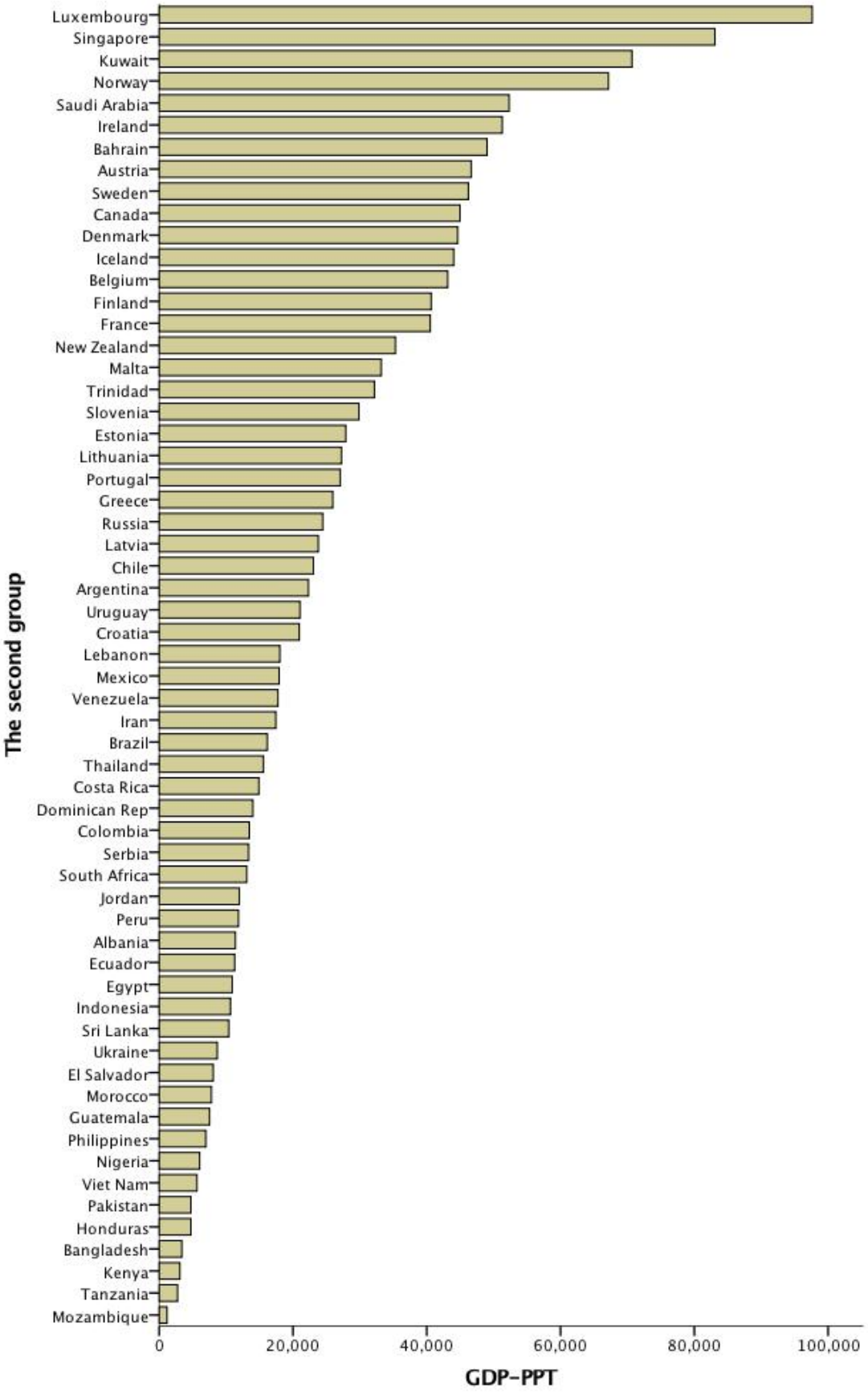

FIGURE 6.8: The countries with less than the average certification rate of 66 (2006–2014) & the economic characteristics selected [Fon15]

valued on an annual basis to compare purchasing power across countries. The small countries that dominate the top ten all have small populations compared to the world's top economies, such as the USA, China, or Germany.

Some of the second group's countries have relatively high levels of GDP-PPP (such as Luxembourg, Singapore, and Kuwait), while some countries have relatively low levels of GDP-PPP (such as Mozambique, Tanzania, and Kenya). All Northern hemisphere countries have highly advanced economies, and very good social security systems, which do not have too large population. A mixture of very diverse countries into the same group possibly influences our results.

Then, we discuss the results, and we state the limitations of this research, based on the influential factors that have not been considered, such as population and area.

6.4.4 Discussion

Possible influential factors that have not been studied in this thesis are considered to be population and a countries' land area, which is the aggregate of all land within international boundaries, excluding water area. The smaller European countries in this group have a number of issued ISO 27001 certificates proportional to their size compared to the European countries in the first group. This would suggest that in this case the number of certificates could be explained by size, rather than by cultural differences. For example, Iceland with population: around 330 thousand and GDP-PPP: 44029.39 USD, placed above Pakistan with population: around 190 million and GDP-PPP: 4749.08 USD. In this case, almost similar average numbers can be explained by economic differences. One of the factors that could influence these observations is the level of sanctions against one country, which result in economically or politically isolation from the global community.

Then, we interpret our results followed by one sample from each group. We select Germany from the first group and Iran from the second group to analyse these countries' information security culture.

TABLE 6.1: Germany vs. Iran the characteristics that are selected for the purpose of this thesis

Country	Cert	UAI	PDI	IDV	LS	Reg	GDP-PPP	GCI
Germany	634	65	35	67	8.034	6.72	46215.70	0.70
Iran	23	59	58	41	6.2292	5.8128	17442.52	0.29

6.5 Case Study: Germany vs. Iran

We select Germany as one of the leading industrial countries with a national information security approach making use of IT Baseline Protection (in German: IT-Grundschutz) from the first group. Then, we select Iran from the second group whose political conditions limited international communication due to sanctions in recent years, and an institute called NAMA [ITC] responsible for ISO 27001 certification. In this section, we compare these two countries' adoption rate of ISO 27001 and the characteristics that are selected for the purpose of this thesis to provide an overview of their social characteristics.

We present the characteristics that are selected for the purpose of this thesis of Germany and Iran in Table 6.1. We denote ISO 27001 certification with Cert, Legal System with LS, Regulations with Reg, and Global Cybersecurity Index with GCI. Germany is among the top ten countries based on the number of issued ISO 27001 certificates in 2014 that ranked globally 10^{th}. Iran is in the middle of the second group that ranked globally 56^{th} based on ISO 27001 certification in 2014.

Both countries are high in UAI, and the results of our quantitative analysis demonstrate that UAI is negatively correlated with the adoption of ISO 27001 in the first group. There might be a relationship between relatively high regulations and GDP-PPP, a bit low PDI on one side, and the adoption of ISO 27001 on the other side in Germany. Iran has a relatively higher PDI compared to Germany, which is negatively correlated with the adoption of ISO 27001 in the second group.

Table 6.2 presents these countries' scores based on the measures of Global Cybersecurity Index. We denote Capacity building with CB.

TABLE 6.2: Germany vs. Iran Global Cybersecurity Index [ITU15]

Country	Legal	Technical	Organisational	CB	Cooperation
Germany	1	1	0.62	0.62	0.50
Iran	0.50	0.33	0.50	0.12	0.12

Germany is ranked first on the legal and technical measures of the Global Cybersecurity Index in 2014 [ITU15]. For example, regulations and compliance, as well as technical standards and certification are supported in Germany comprehensively. The cooperation measure is relatively low for all countries as well as Germany. For example, intra-state and international cooperation is not supported in Germany comprehensively. The legal and organisational measures of the Global Cybersecurity Index are moderately supported in Iran [ITU15]. For example, regulation, compliance, and national benchmarking are supported in Iran in 2014. Iran does not seem to focus on the cooperation measure of the Global Cybersecurity Index in 2014. For example, professional certification and public sector partnership might not be supported in Iran comprehensively [ITU15]. Then, we provide some recommendations to develop an ISMS standard based on the ISO 27001 in Iran.

When organisations agree with ISO 27001 and get certified, it is important to follow up on living a security culture and commit to ISO 27001 policies and procedures in a substantial way. It is necessary to establish adequate numbers of information security policies, and communicate information security policies and procedures on a regular basis for every employee to understand each policy, and how they relate to them. Bureaucratic and complex procedures as well as process of decision-making could be challenges of executing ISO 27001 security controls in a country with high level of PDI, such as in Iran.

6.6 Conclusion of Quantitative Analysis

To take into account for the differences between the countries of our dataset, we identified groups of countries based on the average number of ISO 27001 certification from 2006 to 2014. Based on the results of our regression analysis, there is a relationship between high regulations and GDP-PPP, as well as low UAI on one side, and higher adoption

of ISO 27001 on the other side for the countries in the first group. However, there is a relationship between the countries of the second group with high IDV and GDP-PPP as well as low PDI on the one side, and higher adoption of ISO 27001 on the other side. The observed correlation does not imply causality. Whether the observed correlation is indicative of a causal relationship requires further investigations that are left to future work.

This research has several limitations. It is possible that several factors influence our statistics, especially the accurate number of issued ISO 27001 certificates in each country. For instance, the NAMA (National Information Security Management System) institute in Iran as national reference organisation for the ISMS is responsible for ISO 27001 certification [ITC]. The NAMA statistics about ISO 27001 is different from ISO 27001 survey 2014 [Int14] and NAMA might present the actual numbers. Besides that, there could be a relationship between the number of issued ISO 27001 certificates and a specific condition at both national and international scale, such as the global financial crisis in 2008.

Forward selection method has drawbacks, for example, each addition of a new candidate may reduce the significance of the already included candidates. Forward selection does not guarantee the best model containing a particular subset of the predictors. Looking at all possible models may not be applicable to the model could be affected by variance. One of the limitations of these methods is based on a small sample size, which might increase the probability of fitting the randomness and obtaining a spurious model. In addition, outliers can have a large impact on stepwise methods.

Our results are possibly influenced by the references that are selected for the characteristics that are selected for the purpose of this thesis, as in any statistical analysis; some sampling and estimation errors are to be expected.

Chapter 7

Conclusion

ISO 27001 is an international ISMS (Information Security Management System) standard comprising policies and procedures for systematically managing information assets. Data and systems could be protected with ISO 27001 security mechanisms to minimise risk and ensure business continuity based on the organisational security requirements. Although ISO 27001 requirements are intended to be generic, there are some countries that have not adopted ISO 27001 extensively. Recent studies have shown the importance of culture (behaviour and mind-set) on information security activities, which have not focused specifically on the implementation of ISO 27001. In this thesis, we have analysed both qualitative and quantitative data to address the relationship between the adoption of ISO 27001 and the characteristics that are selected for the purpose of this thesis (cf. 3.3.4).

We described three cultural characteristics of UAI, PDI, and IDV (cf. 2.3.2) that are selected for the purpose of this thesis, which indicate the level of inconvenience with future uncertainty, power distribution, and interdependence to a society, based on Hofstede's publications on culture. Two political characteristics of legal systems and regulations (cf. 2.4.1) are based on the level of support for legal ownership of individual property, and efficiency of established business regulations for national and international trading. The economic indicator of GDP-PPP (cf. 2.4.2) indicates national economic performance based on the exchange rates between currencies.

In the qualitative analysis, we investigated Annex A controls of ISO 27001 (cf. A) to find the relationship between the national culture and the implementation of ISO 27001.

We also described the relationship between the cultural characteristics selected and the average number of ISO 27001 certification issued from 2006 to 2014. Then, we investigated the relationship between national information security guidelines and the adoption of ISO 27001. The qualitative analyses indicate that there is a relationship between cultural characteristics and the implementation of ISO 27001.

Our contribution is to demonstrate the correlated national characteristics with the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). To address different national characteristics, we classify our dataset into two groups of 23 countries and 60 countries based on the average number of ISO 27001 certification from 2006 to 2014. The relationship between the characteristics that are selected for the purpose of this thesis and the adoption of ISO 27001 of the first group with more than the average certification rate of 66 is distinct compared to the second group with less than the average certification rate of 66. The observed correlation does not imply causality in this research as there could be other influential factors that have not been studied (cf. 4.5).

The results of our quantitative analysis indicate that there is a relationship between relatively high regulations (cf. 2.4.1) and GDP-PPP (cf. 2.4.2), a bit low UAI (cf. 2.3.2) on one side, and higher ISO 27001 adoption rates on the other side for the countries of the first group. However, there is a relationship between relatively high IDV (cf. 2.3.2) and GDP-PPP (cf. 2.4.2), a bit low PDI (cf. 2.3.2) on one side, and higher ISO 27001 adoption rates on the other side for the countries of the second group. In both groups, the GDP-PPP is positively correlated with the adoption of ISO 27001.

This thesis paves the way for future research and improves knowledge about correlated characteristics, which may extend the cultural characteristics for evaluating the adoption of ISO 27001. Our work can be extended in the future to investigate a distinct measurement for information security standards that we have left out due to time constraints. We suggest that analysing influential organisational characteristics and the possible measurements needed for evaluating ISMS standard implementation would be worthwhile to follow up in future work.

Appendix A

Annex A Controls

An overview of the control domains are provided in the following [Int13]:

A.5 Information security policies

A.5.1 Management direction for information security

A.5.1.1 Policies for information security

A.5.1.2 Review of the policies for information security

A.6 Organisation of information security

A.6.1 Internal organisation

A.6.1.1 Information security roles and responsibilities

A.6.1.2 Segregation of duties

A.6.1.3 Contact with authorities

A.6.1.4 Contact with special interest groups

A.6.1.5 Information security in project management

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy

A.6.2.2 Teleworking

A.7 Human resource security

A.7.1 Prior to employment

A.7.1.1 Screening

A.7.1.2 Terms and conditions of employment

A.7.2 During employment

A.7.2.1 Management responsibilities

A.12.1.4 Separation of development, testing & operational environments

A.12.2 Protection from malware

A.12.2.1 Controls against malware

A.12.3 Backup

A.12.3.1 Information backup

A.12.4 Logging and monitoring

A.12.4.1 Event logging

A.12.4.2 Protection of log information

A.12.4.3 Administrator and operator logs

A.12.4.4 Clock synchronisation

A.12.5 Control of operational software

A.12.5.1 Installation of software on operational systems

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities

A.12.6.2 Restrictions on software installation

A.12.7 Information systems audit considerations

A.12.7.1 Information systems audit controls

A.13 Communications security

A.13.1 Network security management

A.13.1.1 Network controls

A.13.1.2 Security of network services

A.13.1.3 Segregation in networks

A.13.2 Information transfer

A.13.2.1 Information transfer policies & procedures

A.13.2.2 Agreements on information transfer

A.13.2.3 Electronic messaging

A.13.2.4 Confidentiality or nondisclosure agreements

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

A.14.1.1 Information security requirements analysis & specification

A.14.1.2 Securing application services on public networks

A.14.1.3 Protecting application services transactions

A.14.2 Security in development and support processes

A.14.2.1 Secure development policy

A.14.2.2 System change control procedures

A.14.2.3 Technical review of applications after operating platform changes

A.14.2.4 Restrictions on changes to software packages

A.14.2.5 Secure system engineering principles

A.14.2.6 Secure development environment

A.14.2.7 Outsourced development

A.14.2.8 System security testing

A.14.2.9 System acceptance testing

A.14.3 Test data

A.14.3.1 Protection of test data

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

A.15.1.1 Information security policy for supplier relationships

A.15.1.2 Addressing security within supplier agreements

A.15.1.3 Information and communication technology supply chain

A.15.2 Supplier service delivery management

A.15.2.1 Monitoring and review of supplier services

A.15.2.2 Managing changes to supplier services

A.16 Information security incident management

A.16.1 Management of information security incidents & improvements

A.16.1.1 Responsibilities and procedures

A.16.1.2 Reporting information security events

A.16.1.3 Reporting information security weaknesses

A.16.1.4 Assessment of and decision on information security events

A.16.1.5 Response to information security incidents

A.16.1.6 Learning from information security incidents

A.16.1.7 Collection of evidence

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

A.17.1.1 Planning information security continuity

A.17.1.2 Implementing information security continuity

A.17.1.3 Verify, review and evaluate information security continuity

A.17.2 Redundancies

A.17.2.1 Availability of information processing facilities

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

A.18.1.1 Applicable legislation identification & contractual requirements

A.18.1.2 Intellectual property rights

A.18.1.3 Protection of records

A.18.1.4 Privacy and protection of personally identifiable information

A.18.1.5 Regulation of cryptographic controls

A.18.2 Information security reviews

A.18.2.1 Independent review of information security

A.18.2.2 Compliance with security policies and standards

A.18.2.3 Technical compliance review

Appendix B

Countries with the Highest Levels of Global Cybersecurity Index

The relationship between the countries with high Global Cybersecurity Index and the cultural characteristics selected cf. 2.3.2) can be seen in Table B.1. Some of theses countries have no available data on the cultural characteristics (such as Oman and Qatar) (cf. 2.3.2), and we have to eliminate them. We denote average number of ISO 27001 certificates with Av.Cert from 2006 to 2014, and the ISO 27001 certification in in 2014 with Cert, Global Cybersecurity Index with GCI, Global rank with Rank. Most of these top countries have relatively high numbers of ISO 27001 certificates in 2014 and they also have high average number of ISO 27001 certificates from 2006 to 2014. These top countries are also ranked high in cultural characteristics of UAI, PDI, and IDV. The USA had the highest Global Cybersecurity Index in 2014, followed by Canada and Australia.

TABLE B.1: Countries with high levels of Global Cybersecurity Index & the cultural characteristics selected [ITU15, Hof03]

Country	**Av.cert**	**Cert**	**UAI**	**PDI**	**IDV**	**GCI**	**Rank**
USA	574.00	654	46	40	91	0.82	1
Canada	60.67	66	48	39	80	0.79	2
Australia	126.67	157	51	36	90	0.76	3
Malaysia	147.50	232	36	100	26	0.76	3
New Zealand	5.83	1	49	22	79	0.73	4
Norway	36.17	70	50	31	69	0.73	4
Brazil	67.50	85	76	69	38	0.70	5
Estonia	1.83	3	60	40	60	0.70	5
Germany	597.67	634	65	35	67	0.70	5
India	1818.00	2168	40	77	48	0.70	5
Japan	7150.17	7171	92	54	46	0.70	5
Rep. of Korea	238.67	288	85	60	18	0.70	5
UK	1881.33	2253	35	35	89	0.70	5
Austria	65.67	87	70	11	55	0.67	6
Hungary	237.67	295	82	46	80	0.67	6
Israel	159.67	201	81	13	54	0.67	6
Netherlands	253.00	335	53	38	80	0.67	6
Singapore	72.83	84	8	74	20	0.67	6
Latvia	15.00	24	63	44	70	0.64	7
Sweden	42.33	45	29	31	71	0.64	7
Turkey	170.33	224	85	66	37	0.64	7
Hong Kong	112.83	125	29	68	25	0.61	8
Finland	31.17	33	59	33	63	0.61	8
Uruguay	9.67	11	99	61	36	0.61	8
Colombia	61.83	78	80	67	13	0.58	9
Denmark	11.33	13	23	18	74	0.58	9
Egypt	10.00	11	80	70	25	0.58	9
France	103.17	155	86	68	71	0.58	9
Spain	721.83	698	86	57	51	0.58	9
Italy	696.17	969	75	50	76	0.55	10

Appendix C

Number of ISO 27001 Certificates per Population and Urban Population

We give weight to the number of ISO 27001 the number of our initial dataset per population and urban population as Table C.1 presents. Our initial dataset includes Japan. We denote countries' urban population with Urban-Pop, assigned weights to population with Per-Pop, and assigned weights to urban population with Per-Urban-Pop. Assigning weight to the number of ISO 27001 based on one related variable could be misleading as the low populated countries that are mostly considered as small countries by area mostly place on top of this list, although they have few numbers of ISO 27001 certificates.

TABLE C.1: ISO 27001 certificates per population & urban population

Country	Urban-Pop	Per-Urban-Pop	Per-Pop
Japan	120043900	9.03	15.13
UK	52463320	6.49	9.37
India	414080000	0.79	0.45
China	785664000	0.23	0.24
Italy	42978530	3.41	4.28
Romania	12178800	11.09	12.06
Taiwan	17825000	6.62	9.12
Spain	38351400	2.75	4.01
USA	261570600	0.38	0.55
Germany	62516560	1.53	2.10
Netherlands	15216740	3.33	5.34
Bulgaria	5374656	9.28	12.27
Poland	22806000	2.06	2.19
Hungary	7138640	6.25	8.04

Country	Urban-Pop	Per-Urban-Pop	Per-Pop
Rep. of Korea	41310500	1.05	1.52
Czech Rep.	7876440	5.30	7.04
Malaysia	22732960	1.54	2.06
Turkey	54845360	0.62	0.78
Israel	7304024	4.16	6.57
Slovakia	2915422	8.40	8.03
Australia	20644800	1.15	1.80
France	53196660	0.44	0.63
Thailand	34894200	0.62	0.56
Switzerland	5961592	3.32	4.30
UAE	8082261	2.45	3.88
Ireland	2950263	6.71	7.62
Hong Kong	7242000	2.61	4.64
Serbia	4242945	3.60	3.81
Croatia	2530086	5.74	6.09
Mexico	96006600	0.15	0.20
VietNam	30666740	0.46	0.28
Austria	5637720	2.33	2.74
Brazil	170507000	0.08	0.11
Singapore	5470000	2.32	4.13
Colombia	37467360	0.31	0.44
Saudi Arabia	23823720	0.46	0.63
Norway	4042819	2.62	3.66
Canada	28822940	0.35	0.50
Greece	8712000	1.08	1.53
Indonesia	136223400	0.07	0.07
Slovenia	1028938	8.52	7.56
Portugal	6884800	1.21	1.42
Philippines	44244200	0.16	0.13
Sweden	8197740	0.83	1.25
Russia	105261600	0.06	0.08
Belgium	10761600	0.60	1.03
Sri Lanka	3987840	1.25	0.43
Finland	4555308	1.10	1.62
Iceland	313593	14.95	25.47
Pakistan	70675500	0.06	0.04
Bahrain	1154304	3.41	5.23
Lithuania	2058264	1.84	2.29
Chile	6427650	0.56	0.37
Latvia	1395800	2.60	3.23
Argentina	37908360	0.09	0.14
Iran	57552940	0.06	0.08
South Africa	34331100	0.10	0.11
Costa Rica	3815916	0.87	1.24
Kuwait	3339506	0.81	1.28
Nigeria	84367000	0.03	0.02
Bangladesh	54993000	0.04	0.03

Country	Urban-Pop	Per-Urban-Pop	Per-Pop
Denmark	4931982	0.40	0.62
Peru	23970780	0.08	0.10
Uruguay	3249000	0.51	0.86
Egypt	35805900	0.05	0.03
Ukraine	31598460	0.04	0.05
Albania	1857627	0.65	0.74
Ecuador	10080600	0.10	0.12
Luxembourg	473156	2.24	3.38
Malta	419314	2.52	4.40
Morocco	20317440	0.04	0.04
Kenya	11873160	0.05	0.02
Tanzania	15982380	0.03	0.02
Dominican Rep.	8317590	0.05	0.08
Estonia	867900	0.52	0.61
Guatemala	8119200	0.06	0.05
Jordan	7337897	0.04	0.06
El Salvador	4428105	0.03	0.04
Lebanon	4140617	0.04	0.05
Mozambique	8326260	0.02	0.01
New Zealand	3923700	0.04	0.06
Trinidad	111028	1.36	0.20
Venezuela	27204900	0.01	0.01

Appendix D

The Normalised Values Number of ISO 27001 Certificates by GDP-PPP and Population

We normalise the number of ISO 27001 certificates of our dataset by the GDP-PPP and population as Table D.1 presents. We denote countries' area with Area, Gross domestic product based on purchasing-power-parity (PPP) per capita GDP with GDP-PPP, population (million) with Pop, normalise by GDP-PPP with Norm-GDP, normalise by population with Norm-Pop.

TABLE D.1: ISO 27001 certificates normalised by GDP-PPP & population

Country	Area	GDP-PPP	Pop	Norm-GDP	Norm-Pop
UK	243610	39826.06	64.61	97638.71	1364.00
India	3287263	5808.43	1294.00	93997.46	1312.53
China	9572900	13224.00	1364.00	52963.41	732.42
Italy	301230	35131.05	60.79	42640.65	586.49
Romania	238391	19743.54	19.90	39385.34	540.47
Taiwan	35980	46035.83	23.43	34588.04	472.65
Spain	504781	33835.01	46.77	31032.90	422.39
USA	9525067	54369.83	318.60	29148.24	395.74
Germany	357021	46215.71	80.98	28291.58	383.63
Netherlands	41526	47959.90	16.87	15484.50	202.58
Bulgaria	110910	17925.79	7.224	15270.34	199.55
Poland	312685	25247.21	38.01	14413.68	187.44
Hungary	93030	25019.03	9.86	13771.18	178.36
Rep. of Korea	98480	35379.02	50.75	13471.35	174.12
Czech Rep.	78867	30046.76	10.53	12957.36	166.85
Malaysia	329750	25145.35	30.23	11072.70	140.21

Country	Area	GDP-PPP	Pop	Norm-GDP	Norm-Pop
Turkey	780580	19698.30	77.03	10730.04	135.36
Israel	26990	33135.69	8.216	9744.88	121.43
Slovakia	48845	28278.81	5.42	8074.39	97.82
Australia	7692024	46550.05	23.46	7860.22	94.79
France	675417	40537.54	66.33	7774.56	93.58
Thailand	514000	15578.56	68.42	7260.56	86.31
Switzerland	41210	58148.75	8.19	6746.56	79.05
UAE	82880	66346.63	9.07	6746.56	79.05
Ireland	71273	51283.75	4.62	6746.56	79.05
Hong Kong	1092	55096.96	7.24	6489.57	75.41
Serbia	88361	13378.02	7.13	5461.57	60.88
Croatia	56542	20947.34	4.24	5247.41	57.85
Mexico	1964375	17950.01	124.20	5161.74	56.64
VietNam	329560	5655.79	90.73	5161.74	56.64
Austria	83858	46640.27	8.54	4861.91	52.40
Brazil	8515767	16155.34	204.20	4776.25	51.19
Singapore	692.7	83065.59	5.47	4733.41	50.59
Colombia	1197411	13479.70	47.79	4476.41	46.95
Saudi Arabia	2149690	52310.95	30.78	4219.42	43.32
Norway	324220	67165.70	5.14	4133.75	42.11
Canada	9984670	44967.27	35.54	3962.42	39.69
Greece	131940	25953.58	10.89	3791.09	37.26
Indonesia	1904556	10651.34	255.10	3791.09	37.26
Slovenia	20253	29866.54	2.06	3619.75	34.84
Portugal	88267	27068.89	10.40	3491.25	33.03
Philippines	300000	6973.67	100.10	3148.59	28.18
Sweden	449964	46219.39	9.70	3062.92	26.97
Russia	17098246	24448.67	143.80	2977.26	25.76
Belgium	32545	43139.15	11.21	2977.26	25.76
Sri Lanka	65611	10410.21	20.77	2548.93	19.70
Finland	337030	40660.71	5.46	2548.93	19.70
Iceland	103000	44029.39	0.33	2463.26	18.49
Pakistan	803940	4749.08	185.50	2334.76	16.68
Bahrain	665	49020.17	1.34	2249.10	15.47
Lithuania	65201	27258.88	2.93	2206.26	14.86
Chile	756950	23056.96	17.61	2163.43	14.25
Latvia	64589	23793.48	1.99	2163.43	14.25
Argentina	2780400	22301.68	42.98	2120.60	13.65
Iran	1648000	17442.52	78.41	2120.60	13.65
South Africa	1219912	13093.90	54.15	2077.76	13.04
Costa Rica	51100	14919.11	4.76	2077.76	13.04
Kuwait	17820	70685.70	3.78	1906.43	10.62
Nigeria	923768	6053.53	176.50	1820.77	9.41
Bangladesh	147570	3390.79	159.40	1777.93	8.80
Denmark	43098	44625.32	5.64	1692.27	7.59
Peru	1285220	11859.99	30.97	1649.43	6.99
Uruguay	176220	21054.99	3.42	1606.60	6.38

Country	Area	GDP-PPP	Pop	Norm-GDP	Norm-Pop
Egypt	1001450	10918.00	91.81	1606.60	6.38
Ukraine	603628	8680.83	45.27	1520.93	5.17
Albania	28748	11390.71	2.89	1478.10	4.57
Ecuador	283560	11302.68	15.90	1435.27	3.96
Luxembourg	2586	97638.71	0.56	1435.27	3.96
Malta	316	33197.52	0.43	1435.27	3.96
Morocco	446550	7813.38	34.32	1349.60	2.75
Kenya	580367	3098.61	46.02	1306.77	2.14
Tanzania	945087	2741.69	52.23	1263.94	1.54
Dominican Rep.	48730	14014.41	10.41	1263.94	1.54
Estonia	45339	27879.72	1.32	1263.94	1.54
Guatemala	108890	7549.76	15.92	1263.94	1.54
Jordan	92300	11970.54	8.81	1221.10	0.93
El Salvador	21040	8059.80	6.28	1178.27	0.33
Lebanon	10452	18051.81	5.60	1178.27	0.33
Mozambique	801590	1178.27	27.21	1178.27	0.33
New Zealand	269190	35305.27	4.51	1178.27	0.33
Trinidad	5128	32170.23	1.35	1178.27	0.33
Venezuela	912050	17759.40	30.74	1178.27	0.33

Appendix E

Number of ISO 27001 Certificates and the Average Total Cost of a Data Breach

ISO 27001 as a compliance-based security approach uses the measurement as number of boxes ticked on a checklist. For example, the UK has mainly applied compliance-based approaches for business until 2015 [Int14, SSA16, EVS00], which are based on best practices and state of the art practices [HP11]. However, an active debate is based on the concern if compliance-based approach helps to enhance the security level in practice [NMSR14, TBOM14, SG11, BHSS14, SAT11a, KKN12, Poj06] as compliance is a legal or regulatory requirement. According to Meng-Chow Kang, compliance deals with information security requirements, which are mainly based on the past experiences [Kan96, Kan13] and might not be suitable for approaching new breaches [Par98]. Focusing on the past could prevent organisations from analysing and considering threats of unknown breaches, as they may perceive current security controls sufficient to approach all breaches [Par03].

There are several ways to choose security controls, which are mostly selected from Annex A of ISO 27001 [HP06, Cal13, Bre07, Boe09, SAT12a, Ifi09, YAAB11]. In the literature [Can14, HWL16, Dis13, Cal05, NEF08], most researchers have focused on a specific organisation that has already implemented ISO 27001, which is normally a medium-sized organisation. It is difficult to select ISO 27001 security controls by means of statistics [ITU15, KWU12, Ben11], such as organisational potential risks or IT failures [Dis13, Bre07]. It is not easy to estimate accurate losses before implementing security controls [Bre07, PwC15, BMG01], or to make an exact trade-off between

security and cost-benefits of established security controls due to extensive and various information security requirements. One of the possible measurements is the level of protection from cybersecurity attacks. There are several publications addressing the information protection level of countries. Most of these publications are limited to particular countries and information security breaches, in a specific time period [GLL03, CG16, Ver16, Ben11, GOG05]. Accordingly, we summarise the results of the cybersecurity attacks since 2006, focusing on insiders as the main executers of organisational rules and responsibilities.

Studying several publications of information protection indicate the inconsistent researches, considering the investigated countries and time interval. The results of studying several cybersecurity publications indicate that the external threats decreased; while insiders accidentally or deliberately cause more security breaches as time passes [KWU12, Ben11, Ver14, McA14]. Most of the insiders' breaches follow a basic pattern, for example insiders misused their privileged access right to do their normal tasks [SAT12a]. Most of the time, there was more than one cause of security breaches, such as unauthorised hardware and email misuse or data manipulation [McA14]. In 2013, the main sources of incidents were disabling or bypassing controls [Ver14] or misusing gained information for their company or competitors' benefits [Ver14]. Most of the time, end users and developers were the main source of mistakes [McA14]. In 2014, most of the attacks were based on soft intellectual properties (such as processes and organisational knowledge) compared to hard intellectual properties (such as financial documents) [Ver14, McA14]. Accordingly, it is important to establish internal rules such as law enforcement or legal system charges for malicious employees.

The countries' properties are possibly related to types of attacks, such as wealth, economy and national resources [ITU15], for example countries' economy could influence security investment, security investments strategies and allocated annual security budget [SAT12a]. Most of the targeted countries were ranked with high number of ISO 27001 certification. For example, the USA was among the top list of cyber attacks in 2013 and 2014, possibly because of high population and internet users as one the main target of technical support frauds [Ver14]. Accordingly, organisations may implement ISO 27001 to communicate their efforts for worldwide collaborations about common security threats and possible countermeasure.

Based on analyses of different cybersecurity literature [Ver16, PwC15, McA14, Ver14, ITU15, SAT12a], those publication covered few numbers of countries. Therefore, we perform a correlation analysis between numbers of ISO 27001 certificates [Int14] and the average total cost of a data breach [Ins17] for a limited number of countries. The average total cost of a data breach from 2014 to 2017 included all breaches in which an individual's name, a medical record or a financial record or debit card was potentially put at risk, based on malicious or criminal attack, system problem or human error [Ins17]. This survey did not include data breaches of more than approximately 100,000 compromised records to represent global organisations costs when protected information was lost or stolen. These statistics were provided for limited numbers of countries:

- The USA,
- UK,
- Germany,
- Australia,
- France,
- Brazil,
- Italy,
- India,
- Canada,
- South Africa,
- The Middle East (including the United Arab Emirates (UAE) and Saudi Arabia),
- ASEAN region (including Singapore, Indonesia, the Philippines and Malaysia).

Table E.1 presents the number of ISO 27001 certificates and the average total cost of a data breach, which was measured in USD (millions). We denote the ISO 27001 certification in in 2014 with cert.

Considering these 26 countries, there is a weak negative linear relationship between the number of ISO 27001 and the average total cost of a data breach. This weak relationship could be related to the fact that accurately identifying security threats and

vulnerabilities might not be possible for all organisations during risk management of ISO 27001 [BMG01, Bre07]. As the risk management process is based on previous models of attack, it may not be applicable for the future. Moreover, Ketil Stölen's experience about risk management indicates that it is seldom possible to provide exact numbers [BHSS14]. Different assumptions might impact selected security controls [KH14, KMS12], for example the skills of information security staff to evaluate risks realistically and perceptions of decision-makers about protection such as reputation and insurance [RF99, VNB93, Gar04, KH14, BS12]. The number of countries and the type of attack are limited that influences the strength of relationship between these two variables.

Table E.1: ISO 27001 certificates & average total cost of a data breach

Countries	**Cert**	**Average cost of a data breach**
USA	654	6.69
Germany	634	4.58
Canada	66	4.56
France	155	4.19
Egypt	11	4.12
Iran	23	4.12
Israel	201	4.12
Jordan	2	4.12
Kuwait	18	4.12
Lebanon	1	4.12
Turkey	224	4.12
UAE	131	4.12
Saudi Arabia	72	4.12
Bahrain	26	4.12
UK	2253	3.55
Australia	157	2.39
Thailand	143	2.29
Vietnam	94	2.29
Singapore	84	2.29
Indonesia	62	2.29
Philippines	47	2.29
Malaysia	232	2.29
Italy	969	2.87
South Africa	22	2.2
Brazil	85	1.7
India	2168	1.53

Bibliography

[27098] BS7799-2:1998: Information security management, specification for information security management system. In *British Standards Institute BSI*, 1998.

[AHK13] Abbass Asosheh, Parvaneh Hajinazari, and Hourieh Khodkari. A practical implementation of ISMS. In *2013 7th International Conference on E-Commerce in Developing Countries: with Focus on E-Security (ECDC)*, pages 1–17. IEEE, 2013.

[AL09] Spyros Arvanitis and Euripidis N Loukis. Information and communication technologies, human capital, workplace organization and labour productivity: A comparative study based on firm-level data for Greece and Switzerland. *Information Economics and Policy*, 21:43–61, 2009.

[AlH15] Areej AlHogail. Design and validation of information security culture framework. *Computers in human behavior*, 49:567–575, 2015.

[ALK94] Alison Anderson, Dennis Longley, and Lam For Kwok. Security modelling for organisations. In *Proceedings of the second ACM Conference on Computer and Communications Security*, pages 241–250. ACM, 1994.

[And01] Ross Anderson. Why information security is hard-an economic perspective. In *17th proceedings on Annual Computer Security Applications Conference (ACSAC)*, pages 358–365. IEEE, 2001.

[AS99] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42:40–46, 1999.

[AS13] Debi Ashenden and Angela Sasse. CISOs and organisational culture: Their own worst enemy? *Computers and Security*, 39:396–405, 2013.

[ASAK11] Belal AbuSaad, Fahad A Saeed, Khaled Alghathbar, and Bilal Khan. Implementation of ISO 27001 in Saudi Arabia-obstacles, motivations, outcomes, and lessons learned. 2011.

[Ash08] Debi Ashenden. Information security management: A human challenge? *Information Security Technical Report*, 13:195–201, 2008.

[AVG17] Stefan Daniel Armeanu, Georgeta Vintila, and Stefan Cristian Gherghina. A cross-country empirical study towards the impact of following iso management system standards on Euro-area economic confidence. *AMFITEATRU Economic*, 19:144, 2017.

[Ben11] Terry Benzel. The science of Cyber security experimentation: the DETER project. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 137–148. ACM, 2011.

[BHSS14] Kristian Beckers, Maritta Heisel, Bjornar Solhaug, and Ketil Stölen. ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. In *Engineering Secure Future Internet Services and Systems*, pages 315–344. Springer, 2014.

[BLB08] F Guillaume Blanchet, Pierre Legendre, and Daniel Borcard. Forward selection of explanatory variables. *Ecology*, 89:2623–2632, 2008.

[BMG01] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 Workshop on New Security Paradigms*, pages 97–104. ACM, 2001.

[BN13] Niclas Berggren and Therese Nilsson. Does economic freedom foster tolerance? *Kyklos*, 66:177–207, 2013.

[Boe08] Wolfgang Boehmer. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In *Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'08)*, pages 224–231. IEEE, 2008.

[Boe09] Wolfgang Boehmer. Cost-benefit trade-off analysis of an ISMS based on ISO 27001. In *Availability, Reliability and Security (ARES), 2009*, pages 392–399. IEEE, 2009.

[Bre07] Joel Brenner. ISO 27001: Risk management and compliance. *Risk Management*, 54:24, 2007.

[Bre14] Jakub Breier. Security evaluation model based on the score of security mechanisms. *Information Sciences and Technologies*, 6:19, 2014.

[BRH16] Tod Beardsley, Bob Rudis, and Jon Hart. National exposure index inferring internet security posture by country through port scanning. 2016.

[Bro06] J Stuart Broderick. ISMS, security standards and security regulations. *Information Security Technical Report*, 11:26–31, 2006.

[BS12] Steffen Bartsch and M Angela Sasse. Guiding decisions on authorization policies: a participatory approach to decision support. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pages 1502–1507. ACM, 2012.

[BSKF11] Kristian Beckers, Holger Schmidt, Jan-Christoph Kuster, and Stephan Fassbender. Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In *2011 Sixth International Conference on Availability, Reliability and Security (ARES)*, pages 327–333. IEEE, 2011.

[BVS00] Lynette Barnard and Rossouw Von Solms. A formalized approach to the effective selection and evaluation of information security controls. *Computers and Security*, 19:185–194, 2000.

[Cal05] Alan Calder. Nine steps to success: an ISO 27001 implementation overview. In *IT Governance Publishing*, 2005.

[Cal06] Alan Calder. Information security based on ISO 27001/ISO 1779: A management guide. In *Van Haren Publishing*, 2006.

[Cal13] Alan Calder. ISO 27001/ISO 27002: A pocket guide. In *IT Governance Publishing*, 2013.

[Can14] Candiwan Candiwan. Analysis of ISO 27001 implementation for enterprises and SMEs in Indonesia. In *International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS)*, pages 50–58. The Society of Digital Information and Wireless Communication, 2014.

[CDMS08] Charlie C Chen, B Dawn Medlin, and RS Shaw. A cross-cultural investigation of situational information security awareness programs. *Information Management and Computer Security*, 16:360–376, 2008.

[CG16] CyberEdge-Group. 2016 Cyberthreat defense report. In *Cyber Defense Review (CDR)*, 2016.

[CH15] Samprit Chatterjee and Ali S. Hadi. Regression analysis by example. In *John Wiley and Sons*, 2015.

[CJL+13] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. Future directions for behavioral information security research. *Computers and Security*, 32:90–101, 2013.

[CMR02] PA Chia, SB Maynard, and AB Ruighaver. Understanding organizational security culture. *Proceedings of Pacific Asia Conference on Information Systems (PACIS)*, 2002.

[CMR04] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. A model for evaluating IT security investments. *Communications of the ACM*, 47:87–92, 2004.

[CRW12] Yan Chen, K Ramamurthy, and Kuang-Wei Wen. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29:157–188, 2012.

[CW06] Alan Calder and Steve Watkins. International IT governance: an executive guide to ISO 17799/ISO 27001. In *Kogan Page Publishers*, 2006.

[CW08] Alan Calder and Steve Watkins. *IT governance: A manager's guide to data security and ISO 27001/ISO 27002.* Kogan Page Ltd., 4^{th} edition, 2008.

[CW12] Alan Calder and Steve Watkins. It governance: an international guide to data security and ISO 27001/ISO 27002. In *Kogan Page Publishers*, 2012.

[DF06] Neil F Doherty and Heather Fulford. Aligning the information security policy with the strategic information systems plan. *Computers and Security*, 25:55–63, 2006.

[Dhi01] Gurpreet Dhillon. Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security*, 20:165–172, 2001.

[Dis13] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for information security management. 2013.

[DK92] Shelley Derksen and HJ Keselman. Backward, forward and stepwise automated subset selection algorithms: Frequency of obtaining authentic and noise variables. *British Journal of Mathematical and Statistical Psychology*, 45:265–282, 1992.

[DSM00] James R Detert, Roger G Schroeder, and John J Mauriel. A framework for linking culture and improvement initiatives in organizations. *Academy of Management Review*, 25:850–863, 2000.

[DSP66] Norman Richard Draper, Harry Smith, and Elizabeth Pownell. Applied regression analysis. In *John Wiley and Sons*, 1966.

[DTI89] Department of Trade and Industry DTI. Users' Code of Practice (Green Book). 1989.

[DVE10] A Da Veiga and Jan Hp Eloff. A framework and assessment instrument for information security culture. *Computers and Security*, 29:196–207, 2010.

[ECL07] Shuchih Ernest Chang and Chin-Shien Lin. Exploring organizational culture for information security management. *Industrial Management and Data Systems*, 107:438–458, 2007.

[EE05] Jan HP Eloff and Mariki M Eloff. Information security architecture. *Computer Fraud and Security*, 2005:10–16, 2005.

[EUE09] Mete Eminaugaouglu, Erdem Ucar, and Saban Eren. The positive outcomes of information security awareness training in companies-a case study. *Information Security Technical Report*, 14:223–229, 2009.

[EVS00] Mariki M. Eloff and Sebastiaan H Von Solms. Information security management: An approach to combine process certification and product evaluation. *Computers and Security*, 19:698–709, 2000.

[FA98] Robert J Fisher and David Ackerman. The effects of recognition and group need on volunteerism: A social norm perspective. *Journal of Consumer Research*, 25:262–275, 1998.

[FAE14] Waldo Rocha Flores, Egil Antonsen, and Mathias Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers and Security*, 43:90–110, 2014.

[FCL10] Steven M Furnell, Nathan Clarke, and David Lacey. Understanding and transforming organizational security culture. *Information Management and Computer Security*, 18:4–13, 2010.

[FCvS+10] Steven M Furnell, Nathan Clarke, Rossouw von Solms, Shamal Faily, and Ivan Flechais. Designing and aligning E-science security culture with design. *Information Management and Computer Security*, 18:339–349, 2010.

[Fel07] Horst Feldmann. Economic freedom and unemployment around the world. *Southern Economic Journal*, pages 158–176, 2007.

[FFA+05] Ronald Fischer, Maria Cristina Ferreira, Eveline Maria Leal Assmar, Paul Redford, and Charles Harb. Organizational behaviour across cultures theoretical and methodological issues for developing multi-level frameworks involving culture. *International Journal of Cross Cultural Management*, 5:27–48, 2005.

[FFA+14] Ronald Fischer, Maria Cristina Ferreira, Eveline Maria Leal Assmar, Gulfidan Baris, Gunes Berberoglu, Figen Dalyan, Corbin C Wong, Arif Hassan, Katja Hanke, and Diana Boer. Organizational practices across cultures: An exploration in six cultural contexts. *International Journal of Cross Cultural Management*, 14:105–125, 2014.

[FG02] SM Furnell and M Gennatou. A prototype tool for information security awareness and training. *Logistics Information Management*, 15:352–357, 2002.

[FK17] Christophe Feltus and Djamel Khadraoui. Strengthening the management of ubiquitous internet by refining ISO/IEC 27001 implementation using a generic responsibility model. 2017.

[FMS07] Ivan Flechais, Cecilia Mascolo, and M Angela Sasse. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1:12–26, 2007.

[Fon15] International-Monetary-Fund Fondo. World economic and financial surveys: World economic outlook database. In *Fondo Monetario Internacional Washington, DC*, 2015.

[Fre07] Edward H Freeman. Holistic information security: ISO 27001 and due care. *Information Systems Security*, 16:291–294, 2007.

[FS09] Ivan Flechais and M Angela Sasse. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in E-science. *International Journal of Human-Computer Studies*, 67:281–296, 2009.

[FSH03] Ivan Flechais, M Angela Sasse, and Stephen Hailes. Bringing security home: A process for developing secure and usable systems. In *Proceedings of the 2003 Workshop on New Security Paradigms*, pages 49–57. ACM, 2003.

[FVB08] Vladislav V Fomin, Henk J. Vries, and Yves Barlette. ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption. In *Proceedings of the third Europe an conference on Management of Technology (EuroMOT)*. ResearchGate GmbH, 2008.

[GAM11] M Ahmadzadeh Ghasemabadi, M Gorji Ashtiani, and F Mohammadipour. PMBOK five process plan for ISMS project implementation considering cost optimization for a time constraint: A case study. In *2011 2nd IEEE International Conference on Emergency Management and Management Sciences (ICEMMS)*, pages 788–791. IEEE, 2011.

[Gar04] Ad Chris Garrett. Developing a security-awareness culture-improving security decision making. In *Citeseer*, 2004.

[GEA07] Michele J Gelfand, Miriam Erez, and Zeynep Aycan. Cross-cultural organizational behavior. *Annual Review of Psychology*, 58:479–514, 2007.

[Gla09] Timo Glaser. Culture and information security-outsourcing IT services in China. In *Technical University of Berlin*, 2009.

[GLL03] Lawrence A Gordon, Martin P Loeb, and William Lucyshyn. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22:461–485, 2003.

[GLN16] James Gwartney, Robert Lawson, and Seth Norton. Economic freedom of the world 2016 annual report. In *Fraser Institute*, 2016.

[GM03] Peter Graeff and Guido Mehlkop. The impact of economic freedom on corruption: different patterns for rich and poor countries. *Europe an Journal of Political Economy*, 19:605–620, 2003.

[GNR06] Michele J Gelfand, Lisa H Nishii, and Jana L Raver. On the nature and importance of cultural tightness-looseness. *Journal of Applied Psychology*, 91:1225, 2006.

[GOG05] Esther Gal-Or and Anindya Ghose. The economic incentives for sharing security information. *Information Systems Research*, 16:186–208, 2005.

[GP07] Timo Glaser and Frank Pallas. Information security and knowledge management: solutions through analogies? In *Technical University of Berlin*, 2007.

[GRN+11] Michele J Gelfand, Jana L Raver, Lisa Nishii, Lisa M Leslie, Janetta Lun, Beng Chong Lim, Lili Duan, Assaf Almaliach, Soon Ang, and Jakobina Arnadottir. Differences between tight and loose cultures: A 33-nation study. *Science*, 332:1100–1104, 2011.

[HHM10] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov. Cultures and organizations: software of the mind. In *McGraw-Hill*, 2010.

[HHN10a] Joseph Henrich, Steven J Heine, and Ara Norenzayan. Beyond WEIRD: Towards a broad-based behavioral science. *Behavioral and Brain Sciences*, 33:111–135, 2010.

[HHN10b] Joseph Henrich, Steven J Heine, and Ara Norenzayan. Most people are not WEIRD. *Nature*, 466:29–29, 2010.

[HJ] Robert E Hall and Charles I Jones. Levels of economic activity across countries. https://ssrn.com/abstract=80211. Accessed: 2017-08-24.

[HJHD02] Robert House, Mansour Javidan, Paul Hanges, and Peter Dorfman. Understanding cultures and implicit leadership theories across the GLOBE: an introduction to project GLOBE. *Journal of World Business*, 37:3–10, 2002.

[Hof83] Geert Hofstede. National cultures in four dimensions: A research-based theory of cultural differences among nations. *International Studies of Management and Organization*, 13:46–74, 1983.

[Hof84] Geert Hofstede. Cultural dimensions in management and planning. *Asia Pacific Journal of Management*, 1:81–99, 1984.

[Hof03] Geert Hofstede. Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. In *SAGE Publications*, 2003.

[HP06] Ted Humphreys and Angelika Plate. Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001. In *British Standards Institution BSI*, 2006.

[HP11] Keith M Heston and William Phifer. The multiple quality models paradox: how much best practice is just enough? *Journal of Software Maintenance and Evolution: Research and Practice*, 23:517–531, 2011.

[HWL16] Carol Hsu, Tawei Wang, and Ang Lu. The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 4842–4848. IEEE, 2016.

[Hys14] Sylvia J Hysong. The role of organizational culture on a subculture of feedback. In *Proceedings on ATLAS.ti User Conference 2013 : Fostering Dialog on Qualitative Methods*, 2014.

[Ifi09] Princely Ifinedo. Information technology security management concerns in global financial services institutions: is national culture a differentiator? *Information Management and Computer Security*, 17:372–387, 2009.

[Ifi14a] Princely Ifinedo. The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, 12:75, 2014.

[Ifi14b] Princely Ifinedo. Relationships between relevant contextual influences and information security threats and controls in global financial services industry. *Journal of Computing and Information Technology (CIT)*, 21:235–246, 2014.

[Ins17] Ponemon Institute. 2017 cost of data breach study: Global overview. In *IBM Security*, 2017.

[Int05] International Organisation of Standardisation/International Electro Technical Commission ISO/IEC. ISO/IEC 27001:2005 -information technology -security techniques -information security management systems -requirements. 2005.

[Int13] International Organisation of Standardisation/International Electro Technical Commission ISO/IEC. ISO/IEC 27001:2013 -information technology -security techniques -information security management systems -requirements. 2013.

[Int14] International Organisation of Standardisation ISO. ISO survey 27001: 2014. 2014.

[Int15] International Organisation of Standardisation ISO. ISO survey 27001: 2015. 2015.

[ITC] ITC.IR (Information Technology and Communications in Iran). Nama (National Information Security Management System) institute in iran. http://nama.ito.gov.ir. Accessed: 2017-08-24.

[ITU15] International-Telecommunication-Union ITU. Global Cyber security index and Cyber wellness profiles. In *International Telecommunication Union, Telecommunication Development Bureau, Switzerland, 2015*, 2015.

[JHD+06] Mansour Javidan, Robert J House, Peter W Dorfman, Paul J Hanges, and Mary Sully De Luque. Conceptualizing and measuring cultures and their consequences: a comparative review of GLOBE's and Hofstede's approaches. *Journal of International Business Studies*, 37:897–914, 2006.

[JKW11] Heasuk Jo, Seungjoo Kim, and Dongho Won. Advanced information security management evaluation system. *Transactions on Internet and Information Systems (TIIS)*, 5:1192–1213, 2011.

[JM14] Maritta Heisel Wouter Joosen and Javier Lopez Fabio Martinelli. Engineering Secure Future Internet Services and Systems. In *Springer*, 2014.

[Jon10] Dan Jones. A WEIRD view of human nature skews psychologists' studies. *Science*, 328:1627–1627, 2010.

[Kan96] Meng-Chow Kang. Network security-have you installed a firewall or fireplace? In *IT Security in Banking Conference*, 1996.

[Kan13] Meng-Chow Kang. Responsive security: Be ready to be secure. In *CRC Press*, 2013.

[KBS13] Iacovos Kirlappos, Adam Beautement, and M Angela Sasse. Comply or die is dead: Long live security-aware principal agents. In *International Conference on Financial Cryptography and Data Security*, pages 70–82. Springer, 2013.

[KDHK99] Paul L Koopman, Deanne N Den Hartog, and Edvard Konrad. National culture and leadership profiles in Europe : Some results from the GLOBE study. *Europe an Journal of Work and Organizational Psychology*, 8:503–520, 1999.

[KH14] Ritsuko Kawasaki and Takeshi Hiromatsu. Proposal of a model supporting decision-making on information security risk treatment. *International Journal of Economics and Management Engineering*, 1, 2014.

[Kin17] Kenneth E King. Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management. In *Capella University*, 2017.

[KKN12] Mehdi Kazemi, Hamid Khajouei, and Hashem Nasrabadi. Evaluation of information security management system success factors: Case study of municipal organization. *African Journal of Business Management*, 6:4982, 2012.

[KLG06] Bradley L Kirkman, Kevin B Lowe, and Cristina B Gibson. A quarter century of culture's consequences: A review of empirical research incorporating Hofstede's cultural values framework. *Journal of International Business Studies*, 37:285–320, 2006.

[KMKRNF06] Kenneth J Knapp, Thomas E Marshall, R Kelly Rainer, and F Nelson Ford. Information security: management's effect on culture and policy. *Information Management and Computer Security*, 14:24–36, 2006.

[KMS12] Kat Krol, Matthew Moroz, and M Angela Sasse. Don't work. can't work? why it's time to rethink security warnings. In *2012 7^{th} International Conference on Risk and Security of Internet and Systems (CRiSIS)*, pages 1–8. IEEE, 2012.

[KNV04] Rauno Kuusisto, Kaj Nyberg, and Teemupekka Virtanen. Unite security culture. In *Proceedings of 3^{rd} Europe an Conference on Information Warfare and Security, Royal Holloway University of London*, pages 221–229. Citeseer, 2004.

[KS14] Iacovos Kirlappos and M Angela Sasse. What usable security really means: Trusting and engaging users. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 69–78. Springer, 2014.

[KVAZ07] Jafar A Khan, Stefan Van Aelst, and Ruben H Zamar. Building a robust linear model with forward selection and stepwise procedures. *Computational Statistics and Data Analysis*, 52:239–248, 2007.

[KWU12] Seung Hyun Kim, Qiu-Hong Wang, and Johannes B Ullrich. A comparative study of Cyberattacks. *Communications of the ACM*, 55:66–73, 2012.

[LCMA09] Joo S Lim, Shanton Chang, Sean Maynard, and Atif Ahmad. Exploring the relationship between organizational culture and information security culture. In *Australian Information Security Management Conference*, page 12. Edith Cowan University, 2009.

[LGJ10] S Looso, M Goeken, and W Johannsen. Comparison and integration of IT governance frameworks to support IT management. *Quality Management for IT Services: Perspectives on Business and Process Performance: Perspectives on Business and Process Performance*, page 90, 2010.

[Mah01] Paul G Mahoney. The common law and economic growth: Hayek might be right. *The Journal of Legal Studies*, 30:503–525, 2001.

[MB82] David C McClelland and Richard E Boyatzis. Leadership motive pattern and long-term success in management. *Journal of Applied Psychology*, 67:737, 1982.

[McA14] McAfee. Net losses: Estimating the global cost of Cybercrime. In *Centre for Strategic and International Studies*, 2014.

[MCW12] Maranda McBride, Lemuria Carter, and Merrill Warkentin. One size doesn't fit all: Cybersecurity training should be customized. 2012.

[ME02] Adele Martins and Jan Elofe. Information security culture. In *Security in the Information Society*, pages 203–214. Springer, 2002.

[MPV15] Douglas C Montgomery, Elizabeth A Peck, and G Geoffrey Vining. Introduction to linear regression analysis. In *John Wiley and Sons*, 2015.

[NEF08] Thomas Neubauer, Andreas Ekelhart, and Stefan Fenz. Interactive selection of ISO 27001 controls under multiple objectives. In *International*

Information Security Conference of International Federation for Information Processing (IFIP), pages 477–492. Springer, 2008.

[NMSR14] Merry Nancylia, Eddy K Mudjtabar, Sarwono Sutikno, and Yusep Rosmansyah. The measurement design of information security management system. In *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pages 1–5. IEEE, 2014.

[Nys08] Kristina Nystrom. The institutions of economic freedom and entrepreneurship: evidence from panel data. *Public Choice*, 136:269–282, 2008.

[OOQ10] Angel R Otero, Carlos E Otero, and Abrar Qureshi. A multi-criteria evaluation of information security controls using boolean features. *International Journal of etwprk Security and its Application*, 2, 2010.

[OS11] Lars Osberg and Andrew Sharpe. Moving from a GDP-based to a well-being based metric of economic performance and social progress: results from the index of economic well-being for OECD countries, 1980-2009. 2011.

[Par98] Donn B Parker. Fighting computer crime: A new framework for protecting information. In *John Wiley and Sons*, 1998.

[Par03] Donn B Parker. Motivating the workforce to support security objectives. *Risk Management Society Publishing*, 2003.

[PC06] Mark F Peterson and Stephanie L Castro. Measurement metrics at aggregate levels of analysis: Implications for organization culture research and the GLOBE project. *The Leadership Quarterly*, 17:506–521, 2006.

[PC11] Celia Paulsen and Tony Coulson. Beyond awareness: using business intelligence to create a culture of information security. *Communications of the IIMA*, 11, 2011.

[PL14] Sanghyun Park and Kyungho Lee. Advanced approach to information security management system model for industrial control system. *The Scientific World Journal*, 2014.

[Poj06] Robert B Pojasek. Is your integrated management system really integrated? *Environmental Quality Management*, 16:89–97, 2006.

[PS10] Petri Puhakainen and Mikko Siponen. Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, pages 757–778, 2010.

[PvMC09] Simon E Parkin, Aad van Moorsel, and Robert Coles. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2nd International Conference on Security of Information and Networks*, pages 46–55. ACM, 2009.

[PwC15] Price-Waterhouse-Coopers PwC. Managing Cyber risks in an interconnected world: Key findings from the global state of information security survey. In *Department for Business, Innovation and Skills*, 2015.

[RF99] Chris Robertson and Paul A Fadil. Ethical decision making in multinational organizations: A culture-based model. *Journal of Business Ethics*, 19:385–392, 1999.

[RH11] Peter J Rousseeuw and Mia Hubert. Robust statistics for outlier detection. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 1:73–79, 2011.

[RMC07] Anthonie B Ruighaver, Sean B Maynard, and Shanton Chang. Organisational security culture: Extending the end-user perspective. *Computers and Security*, 26:56–62, 2007.

[Rob09] Stephen P Robbins. Organizational behavior. In *Pearson Education*, 2009.

[Rol02] Jean-Pierre Rolland. The cross-cultural generalizability of the five-factor model of personality. In *Five-Factor Model of Personality Across Cultures*, pages 7–28. Springer, 2002.

[SA12] Heru Susanto and Mohammad Nabil Almunawar. Information security awareness within business environment: An IT review. In *Cornell University Library, PhD Colloquium 2012*, 2012.

[SAB07] Mohammad Saad Saleh, Abdullah Alrabiah, and Saad Haj Bakry. Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach. *International Journal of Network Management*, 17:85–97, 2007.

[SAT11a] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. Information security management system standards: A comparative study of the Big Five. *International Journal of Electrical Computer Sciences (IJECSIJENS)*, 11:23–29, 2011.

[SAT+11b] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, Mehmet Aksoy, and Wahyudin P Syam. Integrated solution modeling software: a new paradigm on information security review and assessment. *International Journal of Science and Advanced Technology*, 2011.

[SAT12a] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology (IJET)*, 2, 2012.

[SAT12b] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement. In *arXiv Research Articles*, 2012.

[SB14] Mohamad Hisyam Selamat and Dorcas Adebola Babatunde. Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. *International Journal of Business and Management*, 9:33, 2014.

[Sch86] Edgar H Schein. What you need to know about organizational culture. *Training and Development Journal*, 1986.

[Sch94] Shalom H Schwartz. Are there universal aspects in the structure and contents of human values? *Journal of Social Issues*, 50:19–45, 1994.

[Sch14] Shalom H Schwartz. Rethinking the concept and measurement of societal culture in light of empirical findings. *Journal of Cross-Cultural Psychology*, 45:5–13, 2014.

[SCHH09] Ruey Shiang Shaw, Charlie C Chen, Albert L Harris, and Hui-Jou Huang. The impact of information richness on information security awareness training effectiveness. *Computers and Education*, 52:92–100, 2009.

[SFC15] Emad Sherif, Steven Furnell, and Nathan Clarke. An identification of variables influencing the establishment of information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 436–448. Springer, 2015.

[SFS14] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In *2014 Ninth International Conference on Availability, Reliability and Security (ARES)*, pages 259–264. IEEE, 2014.

[SFS15] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. The effects of cultural dimensions on the development of an ISMS based on the ISO 27001. In *2015 tenth International Conference on Availability, Reliability and Security (ARES)*, pages 159–167. IEEE, 2015.

[SFS16a] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. The effects of national culture on the implementation of ism standards based on the ISO 27001. In *ATINER's Conference*, 2016.

[SFS16b] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. Getting the full benefits of the ISO 27001 to develop an ISMS based on organisations' InfoSec culture. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, 2016.

[SG11] Madhav Sinha and Alan Gillies. Improving the quality of information security management systems with ISO 27000. *The TQM Journal*, 23:367–376, 2011.

[Sip00] Mikko T Siponen. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8:31–41, 2000.

[SJA+08] Mark B Schmidt, Allen C Johnston, Kirk P Arnett, Jim Q Chen, and Suicheng Li. A cross-cultural comparison of US and Chinese computer

security awareness. *Journal of Global Information Management*, 16:91, 2008.

[SLP14] Ivan Sedinic, Zrinka Lovric, and Tamara Perusic. Customer and user education as a tool to increase security level. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1441–1445. IEEE, 2014.

[SMAT12] Heru Susanto, Fahad Bin Muhaya, Mohammad Nabil Almunawar, and Yong Chee Tuan. Refinement of strategy and technology domains STOPE view on ISO 27001. In *arXiv Research Articles*, 2012.

[SMP14] Mikko Siponen, M Adam Mahmood, and Seppo Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51:217–224, 2014.

[SS95] Shalom H Schwartz and Lilach Sagiv. Identifying culture-specifics in the content and structure of values. *Journal of Cross-Cultural Psychology*, 26:92–116, 1995.

[SSA16] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36:215–225, 2016.

[SSC+17] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 2202–2214. ACM, 2017.

[ST03] Thomas Schlienger and Stephanie Teufel. Information security culture-from analysis to change. *South African Computer Journal*, 2003:46–52, 2003.

[ST05] Thomas Schlienger and Stephanie Teufel. Tool supported management of information security culture. In *International Information Security Conference of International Federation for Information Processing (IFIP)*, pages 65–77. Springer, 2005.

[SW09] Mikko Siponen and Robert Willison. Information security management standards: Problems and solutions. *Information and Management*, 46:267–270, 2009.

[SZK08] Mario Spremic, Zlatan Zmirak, and Krunoslav Kraljevic. IT and business process performance management: Case study of ITIL implementation in finance service industry. In *30th International Conference on Information Technology Interfaces (ITI)*, pages 243–250. IEEE, 2008.

[TBOM14] Anel Tanovic, Asmir Butkovic, Fahrudin Orucevic, and Nikos Mastorakis. The importance of introducing information security management systems for service providers. In *World Scientific and Engineering Academy and Society (WSEAS)*, 2014.

[Tsa17] Yu-Jen Tsao. The effect of information security management system in hospitals on the maturity of information security. 2017.

[TTKG07] Aggeliki Tsohou, Marianthi Theoharidou, Spyros Kokolakis, and Dimitris Gritzalis. Addressing cultural dissimilarity in the information security management outsourcing relationship. In *International Conference on Trust, Privacy and Security in Digital Business*, pages 24–33, 2007.

[TV10] Rosalie L Tung and Alain Verbeke. Beyond Hofstede and GLOBE: Improving the quality of cross-cultural research. *Journal of International Business Studies*, 41:1259–1274, 2010.

[TvSL06] Kerry-Lynn Thomson, Rossouw von Solms, and Lynette Louw. Cultivating an organizational information security culture. *Computer Fraud and Security*, 2006:7–11, 2006.

[UB13] Jorg Uffen and Michael H Breitner. Management of technical security measures: an empirical examination of personality traits and behavioral intentions. In *2013 46th Hawaii International Conference on System Sciences (HICSS)*, pages 4551–4560. IEEE, 2013.

[Übe13] Sven Übelacker. Security-aware organisational cultures as a starting point for mitigating socio-technical risks. In *Hamburg University of Technology (TUHH)*, 2013.

[Ver14] Verizon. 2014 data breach investigations report. In *Verizon Enterprise Solutions*, 2014.

[Ver16] Verizon. 2016 data breach investigations report. In *Verizon Enterprise Solutions*, 2016.

[VNB93] Scott J Vitell, Saviour L Nwachukwu, and James H Barnes. The effects of culture on ethical decision-making: An application of Hofstede's typology. *Journal of Business Ethics*, 12:753–760, 1993.

[VNvS05] Johan Van Niekerk and Rossouw von Solms. A holistic framework for the fostering of an information security sub-culture in organizations. In *Information Security South Africa (ISSA)*, pages 1–13. Nelson Mandela Metropolitan University, 2005.

[XW05] Rui Xu and Donald Wunsch. Survey of clustering algorithms. *IEEE Transactions on Neural Networks*, 16:645–678, 2005.

[YAAB11] Ebru Yeniman Yildirim, Gizem Akalp, Serpil Aytac, and Nuran Bayram. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31:360–365, 2011.

[Zak13] Omar Zakaria. Information security culture: A human firewall approach. In *LAP LAMBERT Academic Publishing*, 2013.

[ZM13] Muhamad Khairulnizam Zaini and Mohamad Noorman Masrek. Conceptualizing the relationships between information security management practices and organizational agility. In *2013 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pages 269–273. IEEE, 2013.

List of Publications That Resulted from the Dissertation Project

The publications that resulted from the dissertation project are the following:

1. Bahareh Shojaie, Hannes Federrath, and Iman Saberi. Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In 2014 9^{th} International Conference on Availability, Reliability and Security (ARES), pages 259-264. 2014.

2. Bahareh Shojaie, Hannes Federrath, and Iman Saberi. The effects of cultural dimensions on the development of an ISMS based on the ISO 27001. In 2015 10^{th} International Conference on Availability, Reliability and Security (ARES), pages 159-167. 2015.

3. Bahareh Shojaie, Hannes Federrath, and Iman Saberi. The effects of national culture on the implementation of ISM standards based on the ISO 27001. In ATINER's Conference, 2016.

4. Bahareh Shojaie, Hannes Federrath, and Iman Saberi. Getting the full benefits of the ISO 27001 to develop an ISMS based on organisations' InfoSec culture. In Proceedings of the 10^{th} International Symposium on Human Aspects of Information Security & Assurance (HAISA). 2016.

For all four papers I am the main contributor.

In the first paper, Prof. Federrath gave me some hints and ideas to enhancing the contribution, which compares ISO 27001 in version 2005 and the updated 2013 standard. I classified the ISO controls into five categories, and did all empirical work. I. Saberi helped on the figures and did some proof reading.

In the second paper, we looked closely to the impacts of cultural characteristics on different phases of developing ISO 27001, based on three levels (country, organisational, and personal), which is especially helpful for Small and Medium Enterprises (SMEs), based on the Prof. Federrath's comments. The results are mainly based on a literature review (done by myself). I. Saberi helped again on the figures and did some proof reading.

In the third paper, we present the most applicable cultural dimensions with respect to the ISO 27001 to point out new ways of enhancing this standard long-term performance. Prof. Federrath and I. Saberi commented on my ideas.

In the fourth paper, based on the literature review, personal interviews and limited results of the preliminary survey, our study found three distinguished cultural behaviours the most applicable cultural characteristics to the ISO 27001 efficiency. All studies, interviews and the literature review were done by myself, with support by I. Saberi. Prof. Federrath gave some hints and comments on the study methodology.

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich, Bahareh Shojaie, die vorliegende Dissertation selbst verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Ort, Datum	Unterschrift