2018

"Development and Importance of Management Systems According to ISO for IT Organizations and the Resulting Demand for Consulting Services. An Analysis Between USA and Germany."

Lara Scholtze
Long Island University, Lara.Scholtze@my.liu.edu

”Development and Importance of Management Systems According to ISO for IT Organizations and the Resulting Demand for Consulting Services. An Analysis Between USA and Germany.”

An Honors Program Thesis

By

Lara Scholtze

Spring, 2018

Department of Management

_____

Principal Advisor:
Professor Edward G. Verlander

_____

Reader:
Courtney Tricarichi

Abstract

This research analyzes the demand of two international standards, ISO 27001 (Information Security) and ISO 20000-1 (IT Service Management), and the resulting impact on the demand for ISO consulting. Due to rising security breaches with increased media coverage, the public and the government is starting to recognize the importance of protecting critical data. Implementing an Information Security Management System enables companies to sufficiently safeguard their information in the long-term and adhere to governmental regulations. Companies seek to implement an IT Service Management System in order to implement best practices in their organization and enable themselves to compete in the market on a global basis. ISO 27001 and ISO 20000-1 enable a company to operate in more successful ways by reducing the cost of operations and reducing the risk of severe damages to a company's reputation in case of any cyberattacks.

The standards are complex in nature and most companies do not have enough internal resources to implement the standards on their own. Also, the introduction of an Information Security Management System requires adoption by the *entire* organization and not just single departments. The scope of such a system requires deepener knowledge of the standards in order to successfully implement the management system and for the company to benefit from its long-term effectiveness.

Thus, the demand for the implementation of ISO 27001 and ISO 20000-1 result in an increased demand for the services of ISO consulting firms.

Table of Contents

1. Introduction

1.1 Purpose of this research

In this paper, we will examine two standardized management systems written by the International Organization for Standardization (ISO) that center their focus on two areas in particular: 1) the structure, and 2) the processes used in the IT department of businesses. Our interest is to understand the drivers of demand and how this demand for businesses to implement those two standards affects the demand for ISO consulting and the respective client industry.

We will begin with the context for ISO by looking at the consulting industry in general, how consulting is defined, the current state of the consulting industry, as well as the future trends of the consulting industry. This will enable us to accurately draw conclusions about the demand for ISO consulting in regards to the two international standards. In order to create a better understanding of those two international standards, based on best practices of the clients relevant industry, we will identify the definition of management systems, the need for management systems, and why they are important for businesses success. After we have established this context, we will clarify the purposes of the International Organization for Standardization and the two international standards, ISO 27001 and ISO 20000-1, we hypothesize areas central for driving ISO consulting demand.

Since this research focuses on trends in ISO demand in the United States and Germany, we will further examine the different factors in those two countries that are leading forces in the demand for the two international standards. We will also include in the research and analysis the efforts in Japan and India, since both of those countries display the highest adoption rates of the two standards.

In addition to reviewing the research literature of ISO development and trends, we will also present findings of interviews of users of ISO standards. The interviews represent both, consulting practices and end-user experiences. The research is intended to validate or nullify the hypothesis regarding the drivers of ISO consulting demand.

1.2 Hypothesis to be tested

The hypothesis we will test is that the demand for ISO consulting is rising due to the increasing demand of the two international standards ISO 27001 and ISO 20000-1. The demand is a result of businesses needing to meet the demands of their customers, which, in turn, want to 1) improve their operations, and 2) comply with government regulations. To meet these needs, ISO consulting firms must be “ISO certified”. This has created a new, secondary consulting service focused on helping other consulting firms to prepare to be certified. Our hypothesis is that this system from certifiers, to consultants, to business users, is a powerful stimulant to ISO consulting demand.

1.3 Implications

As business grows more and more dependent on sustainable functioning IT systems, preventing the failure and breakdowns of such IT systems is increasingly critical for business success. As a result, business end-users intensify their demands for IT departments and service providers to verify through an external certification that their IT is organized in a sustainable and secure manner, using best practices in their operations, such as ISO. Therefore, more companies seek to become certified in ISO 27001 (Information Security) and ISO 20000-1 (IT service management). Our research will examine how the process of

becoming certified to one of those standards is really complex in nature leading to rising demand for IT consulting services.

2. Consulting Industry

2.1 Definition of consultants and consulting

Consulting is a means for a company to adapt their business to the speed, intensity, direction and complexity of change and adjust to the global business environment where their business model not only got extended but also uprooted (Verlander, 2012, p.xvi). Companies invest time and money in consultants to find out how to conduct business at a lower cost to keep quality high but overall cost of business processes low. “Consultants offer advice based on education, expertise, and judgment formed over many years of experience. The advice is normally directed toward some kind of solution that the patient or client wants and needs, and the solution itself is the “deliverable” (Verlander, 2012, p.16). Therefore, the job of a consultant is to develop solutions that drive change in client organizations and that enables them to be FBBC by being effective and efficient as possible. Consulting requires giving advice to clients who then make a choice about the solutions presented. Consultants become surrogate managers for clients. A surrogate manager is simply someone to whom a manager refers his or her responsibilities, because “they both use fact-based, rational decision making in their work, supported by analytical techniques and systematic project management procedures” (Verlander, 2012, p.11).

As a consultant, it is not enough to just simply have expertise in a field or possess the consulting techniques, a consultant also needs to understand the affective side of consulting. In doing their work, it is extremely important that consultants not only possess technical skills, but also interpersonal skills and skills in using various methods and procedures. Interpersonal skills include the elements of the affective side of consulting, which means

being able to speak well, listen carefully, present ones ideas clearly and influence the clients thinking. A lack of trust from the client has the potential of creating barriers to getting the job done. These “relationship management” interpersonal skills are important in environments where the consulting is highly technical, such as in ISO consulting. In such environments the affective side of management is often neglected as the technical work is over emphasized.

Moreover, consultants need to be able to take on different roles depending on the wants and needs of the individual clients. There is the expert role, which requires the consultant to act out his superiority based on his expertise and completely take over the project without any interference of the client, the pair-of-hands role, which requires the consultant to apply specialized knowledge to implement action plans towards the achievement of a goal that has been pre-defined by the manager and the manager remains in full control of the project, and the collaborative role, which requires the consultant to collaborate together with the client and draw from his expertise of the organization whereas the consultant will apply his expertise about the specific problem (Block, 2011).

Lastly, there are two kinds of consultants that need to be differentiated, internal consultants and external consultants. An internal consultant means that the consultant is permanently embedded in an organization and will only have as many clients as the organization has managers. As a result, an internal consultant has a direct boss and since consulting drives change, the workings of the politics of the organization often put in a more delicate position than an external consultant. This often occurs when dealing with resistance to change inside an organization. Therefore, internal consultants often face many constraints, because they may feel reluctant to state reality and give honest feedback. As a result, it is difficult for an internal consultant to find the right balance between cautious behavior (with feedback) and ignoring the constraints all together. An external consultant, on the other hand, does not face this kind of challenge, as he or she is not permanently imbedded in the

organization and therefore feels freer to give his honest feedback and the ability to question many aspects of the clients operations and management. This may be another subtle driver of ISO consulting demand.

Overall, consultants often encounter people within an organization that are reluctant to change their way of doing things and oppose newly introduced solutions by a consultant. Therefore, consultants need to be able to know how to deal with such resistance to change by involving the people responsible for changing the organization to make it FBBC. Building trust, therefore, is a critical element for the relationship between the consultant and the client in order to develop a long-term relationship with deepened focus of involvement over time. Clients rely on the integrity of the analysis and recommendations given by the consultant and expect to be given the best advice.

In sum, “consultants solve problems created by the powerful forces of change in an organization’s environment, and in doing so, they themselves create change” (Verlander, 2012, p.xxi). There are three areas of consulting, where the consultant needs to be able to take on a different role based on what the client is expecting of him or her. The consultant needs to be able to take on the expert role, pair-of-hands role, or collaborative role. In order to be successful in each of those roles, the consultant needs to possess certain technical skills, interpersonal skills, and knowledge of the methods and procedures of consulting. Moreover, a consultant needs to be aware of the different relationships in IT and the prevalent politics that might create barriers for a consultant to implement change. Therefore, it is important for a consultant to know how to deal with those relationships and how to handle change in order to overcome those barriers. Since implementing an international standards always required change within an organization, it is important for consultants to possess those skills in order to be effective and efficient in doing so. As all organizational change of any kind is done by people and most of them try to resist change for political reasons, ideological reasons and

emotional reasons, there are many human aspects to change and change management required when implementing international standards. Only a consultant who can meet all of the requirements listed above will be successful in driving change and implementing solutions for their clients.

2.2 Overview of the Industry.

The competitive environment of companies is constantly changing due to rapid changes in competition, demand, technology, and regulations. Companies may not be always able to keep up with those changes on their own, which requires them to either hire an internal consultant or an external consulting company that help them implement required changes. As a result, the consulting industry is linked to the overall economic conditions that directly demand companies to adapt to what is going on in their immediate environment.

Since overall economic conditions are directly linked to the profitability of the consulting industry, consulting firms faced decreasing business demand during the financial crisis in 2009. Consulting companies started to shift their focus towards emerging economies in order to find a solution to their decreasing profit margins and a market share. However, they had been facing major resistance by small, local firms in those emerging economies, which lead the big consulting companies to turn towards their traditional markets again and expand in those areas.

Today, companies who are operating in increasingly complex and volatile business environments are changing their structure to be more agile in order to better adapt and be more flexible to their rapid changing environment in their respective industry. The financial services sector, as well as the telecommunication, media and entertainment, and high tech industries are among the industries that perceive their environment to be most unstable. This aligns with the fact that the financial industry as well as the telecommunications and high tech

industries are the ones that have the highest amounts of ISO 27001 certifications (ISO, 2017). Since those companies operate in unstable environments, they are looking to the international standard set by ISO to give them some sense of security and stability that would otherwise not exist. This volatility stimulates companies to seek consulting expertise.

Overall, the scope of consulting depends on the level of advice that needs to be given and the size of the business problem that needs to be solved. Consulting is a continuous process where developing a client-focused mind set is the key to success, as it helps to establish a long-term, deepened client-customer relationship. In the consulting industry, most of the business that a consultant receives comes from already existing clients. Purba and Delaney (2003) refer to this phenomenon as the eternal 80-20 rule, where 80 percent of future projects will come from 20 percent of their already existing client base (Purba & Delaney, 2003). Essentially this means that a consultant should always remain in good standing with their past clients, as well as their circle of references, as those contact points can help them find out more about upcoming opportunities that they might want to take advantage of. This is also called the client reservoir that the consultant should try to build and access.

However, a consultant should never stop looking for new projects once current projects have been completed, and should be continuous advertising. Those efforts should never fall under the mark of 10% of a consultant's time (Purba & Delaney, 2003). This is so important, because clients do not just wait for the consultant to be free. Their needs are ongoing and consultants must continuously try to fill their pipeline of new business. This involves sending out proposals on the projects that are of future interest. This "book of business" helps consultants to estimate future people, money and time required. Keeping this important fact in mind, already characterizes a possible driver of demand for consulting in accordance to the ISO 27001 (Information security management system) and ISO 20000-1 (IT service management system) published by ISO. The demand is not only driven by the clients

themselves, but also by the consultants, who continuously advertise their services to potential new clients. This essentially increases the awareness of the clients about the service that the consultant is offering, thus being a possible source of the driver of the demand.

Another driver of demand for consulting services, according to, for example, the problem-solving process by McKinsey, is the *Business Need* of a client that begins the entire problem-solving process that the consultant then will be hired to work on (Ahlbäck, Fahrbach, Murarka, & Salo, 2017). Without a need of the client, there are no solutions that need to be analyzed and implemented by a consultant. Those business needs by the client can have many different sources. They may have a competitive need, as they want to be able to compete with their competitor and adapt to changing environment or an organizational need, where they have to address barriers to the performance of the organization as a whole. Furthermore, clients can have financial needs, such as optimizing the structure of their financial functions to improve their contributions to the business, or operational needs, which require the company to adjust their internal processes as operations must be updated due to the changing environments requiring companies to be agile. Therefore, there are many drivers of demand requiring consulting expertise and all those needs act as drivers of the potential demand for ISO consulting.

2.3 Business Processes

Business Processes are defined as “a succession of actions undertaken to bring about some desired result. A series of gradual changes moving towards some particular end; a forward movement; progression” (Verlander, 2012, p.38). This means that a business process is a chain of activities aimed to deliver a higher quality output based on a measurable input. Every process is a set of activities that follows a sequential order and needs a trigger that

prompts the chain of activities. Such a trigger can be defined as an “Incident” in the form of an end-user calling the IT Service Desk because of a disruption of the application.

The activities are conducted by roles, which are defined in each process. Roles are independent organizational units with their own resources that are assigned individual activities, responsibilities, competencies or entire processes. A person or an organizational unit can be assigned to more than one role (TÜV Süd, 2015a).

In many organizations, business processes are not properly documented and employees do not entirely know the exact nature of the process they need to complete, which results in inconsistencies and omissions. Therefore, it is crucial for an organization to keep track of their business processes, make sure that they are properly documented and communicated, and put a continuous effort into making sure that they are up to date.

A standardized, structured, and documented process secures a sustainable and efficient creation of value and the possibility to measure and continuously improve the process. In the age of digitalization, many reoccurring steps in a process can be automated, which creates the possibility for automated continual quality improvement of those automated activities. As a result, only standardized processes can be supported by IT solutions.

Automation of business Processes have increasingly become important over the past decades, since they become crucial to a business’s success in the globalized world. Due to globalization, companies have to adapt more readily to changes in their environment, which in turn means that they have to constantly adapt their business processes. Changes in the organization are inseparable from changes in the business processes. Also, since companies achieve a better position to compete due to implementing more efficient and cost-effective business processes, they must continuously improve their processes.

Business process are supported by IT systems which are mapped out on specific IT solutions. With such IT solutions, the standardization of an activity can be codified in IT

systems in order to automate and efficiently produce those steps and minimize cost. Functioning, secured, available, performance oriented IT systems that support crucial business processes are an operational necessity which makes it inevitable for the IT department to align with best practices within the scope of the implementation of IT specific management systems, especially compliance with ISO 270001 and ISO 20000-1. On the basis of such supporting IT systems, regular key performance indicator (KPI) reports are generated which constitute an important foundation for the identification of improvement potential that can be used within the scope of quality management for a continual improvement process.

Business process engineering is an important element of business process improvement in order to enable a company to efficiently and effectively design, layout, analyze, improve, optimize and document the basic condition of their operational activities. If business processes are not properly engineered, then costs may rise for the company due to quality problems in the practical implementation of such processes (Schönthaler, Vossen, Oberweis, & Karle, 2010).

Continuous improvement of business processes play a key role in international competition and need special consideration upon implementation of such standards in the organization. Therefore, implementing an ISO standard enables that the business processes need to be changed in an organization to improve a company's competitiveness. Especially for ISO 20000-1, which is primarily made up of the Information Technology Infrastructure Library, which requires designing new business processes that support a certain quality of service for IT Service Management. ISO 20000-1 specifies the necessary minimum requirements for processes that need to be defined, implemented and improved on a continual basis in order to provide IT Services in a predefined quality, and how it is managed. Since companies might not have the skill and expertise of business process engineering among their

employees, they will hire consultants to redesign their business processes, specifically tailored to their needs or the international standards that they want to implement.

2.4 Trends in the Consulting Industry

There are six emerging trends that the consulting industry currently encounters, which are homogeneity, modularization, importance of scale, consolidation of the industry, few government regulations and the ease of entry.

One of the emerging trends in the consulting industry is the increasing homogeneity in service offerings, which means that the range of services that consulting companies provide to their clients are becoming very similar (Parakala, 2016).

The purchasing behavior of the clients is changing as well, as they are becoming increasingly selective and modular in their demands as opposed to large traditional outsourced deals.

Furthermore, the importance of scale and brand name of a consulting company is decreasing, as more and more companies are willing to contract with small startups and medium enterprises, in order to find innovative solutions such firms may provide. This stimulates the growth of small consulting companies that fill in the gap with their flexibility which large companies cannot provide.

Since the entry barriers to open up a business in the consulting industry are so low, it makes the industry fragmented with a lot of small business competing against each other. As a result, smaller companies engage into market consolidation in order to overcome the incurred growth challenges.

The ISO consulting industry is a fragmented one with a lot of small companies competing to offer their ISO expertise to their clients as well. There are few government regulations of the industry in, for example, Germany, which means that a consulting company does not have to register their involvement in ISO consulting. As a result, the entry barrier

into this kind of consulting is essentially low, which increasingly enables start-up companies and smaller consulting companies to engage in this type of consulting (LS_10/12/2017).

2.5 IT Industry Trends.

"The explosion of "computer-to-computer" communication in the twenty-first century is triggering a growth phase for IT consultants (Johnston, 2002). Just as the consulting industry in general is undergoing significant change, the IT consulting industry in particular, continues to evolve new areas of practice as well as itself being a significant driver of change for client companies. The work of IT consulting firms includes (Business.com, 2018):

- "Providing advice and expertise on the use of computers, telecommunications equipment, and distribution networks that store, retrieve, transmit, and manipulate data to effectively achieve business objectives, and assessing operational efficiency and capacity of your IT environment
- Planning, designing, testing, implementing, and managing IT technologies on behalf of a business
- Developing and supporting change management activities to transition users to new technologies and procedures
- Writing technical and user documentation
- Purchasing hardware and software systems on behalf of a business
- Providing and monitoring network security
- Training and supporting employees and customers in the use of IT technologies
- Staffing technical job functions on a temporary contract basis"

Trends in client applications include cloud computing, big data, and outsourcing (Business.com, 2018; Ibisworld, (2018):

Cloud Computing. The big attraction of cloud computing -- where your software and data are housed off-premises and accessed via a Web portal -- is that it's generally less expensive. Moreover, software updates are usually relatively painless, eliminating costly and time-consuming installations, reducing the need for IT consultants. But, as more companies move their data to the cloud, more IT consultants are needed to get them there. It's not just the need to migrate to new technology in the cloud, it's also the need to sure legacy systems work in the cloud.

Thoran Rodrigues, writing in *Tech Republic*, about the new role of IT in a cloud-based world, says: 'In our new world, IT must shift its perspective from owner to custodian. While it is still very important for IT departments to take a proactive approach in learning about and presenting new technologies and solutions to users, the most important side of the updated IT department will be its ability to act as a custodian of multiple technologies and systems. Instead of worrying about purchasing the technology and building out the infrastructure where it will run, it will have to work to ensure that all systems are interoperable and can work together, and that the service providers have long-term visions that are compatible with the direction that the company is heading.'

Big Data. Organizations have increased the amount of data they gather by orders of magnitude in recent years. To make use of all this data, companies needs to sift it. IT consultants can help parse this data into useful and manageable reports.

In *InformationWeek*, writer Jeff Bertolucci quotes David McJannet, vice president of marketing for Hortonworks. "Big data isn't this nebulous thing," he said "Very pragmatically, it's about building net-new analytic applications based on new types of data that (an organization) wasn't previously tracking."

It could make sense for your business to hire outside consultants for this (big data) specialized IT task.

Outsourcing. It is generally easier and less expensive to have your IT needs handled by outside consultants, rather than developing the expertise in-house, particularly given the ever-changing dynamic of IT technologies and requisite competencies to manage them.

One of the advantages of outsourcing IT, according to an article by Colette L. Meehan in the *Houston Chronicle* online, is that "outsourcing allows management to defer the details to a specialized company. Removing the details permits management to focus on the larger issues within the organization."

According to BusinessWire (2018) global trends in IT consulting firms (such as the big five companies Accenture, Deloitte, IBM, Hewlett Packard, and CGI Group) include:

- Adoption of environment-friendly technology
- Growing preference for remote working environments
- Increase in service offshoring
- Increase in market consolidation
- Rise in use of cloud-based IT infrastructure

In the US, growth of IT consulting in general between 2011 and 2017 has been 2.1% (IBIS*World,* 2018). While these trends do not reference ISO IT consulting in particular, they do suggest that the nature of ISO consulting practice is likely to be directly effected by them. To the extent that ISO IT consulting firms adjust to and take advantage of the trends, growth in this area is likely to be consistent with the growth of the management consulting industry in general. Growth in the management consulting industry was 7.7% in 2015 (Greentarget, 2016) and is projected to be 2.4% between 2016 and 2021 (IbisWorld, 2016)

3. Management Systems

Management systems are a tool for management to control its operations to reach organizational goals. Every organization must clearly define their vision, mission and goals (Verlander, 2012). A company is made up of many different departments that then work towards fulfilling the organizational goal. In order to accomplish a clearly defined direction, organizational goals have to be properly communicated to the entire company and it has to be ensured that every employee, no matter their position, know what the company is trying to accomplish. Organizational goals are, therefore, crucial to a company's success, as they give purpose to everyone's work and everyone knows what they are working towards. As a result, companies need management systems to communicate, track performance, adjust, and achieve their goals.

Since one of a company's major goals is to generate profit, they have to operate as effectively and efficiently as possible. The more effective the company is able to structure their operations, the more money they will be able to generate in the end. Hence, management systems support a company in reaching their organizational goals in a structured and process-oriented manner enabling a company to save costs and produce profits.

There are many different management systems in a company. For example, there are planning systems, supervising systems, sales and production operations systems, financial control systems, human resource systems, IT systems, customer relation systems, supply chain systems, and compliance systems.

Companies need such management systems, especially when they operate in a highly competitive and fragmented industry. Every company needs to define their competitive advantage that sets themselves apart from all the other companies that operate within the same industry and offer the same services or products. Their success can be easily threatened by others and companies need to look for a way to differentiate themselves. Obtaining

certification for an industry-relevant international standard can be a way of creating differentiation. If a company becomes certified to a specific standard, they signal to their customers that they comply with their requirements as well as possible government regulations.

Additionally, companies enhance their ability to instill the best possible quality in their products, services and operations by instituting best practices that have been recognized by their industry. Furthermore, companies who choose to improve their management system relevant to their operations, obtain enhanced ability to grow their organization, increase their customer reach, provide higher levels of satisfaction with their product and service, as well as increase revenue streams. As a result, obtaining an ISO certification enables the company to communicate to their customers, suppliers and competitors that they have successfully implemented such management systems, which may give them a competitive advantage over their competitors.

Moreover, complying with an international standard enhances bigger companies who heavily rely on international operations to market themselves in a more and more globalized world. By validating the implementation of a management standard through an external third party accredited certification body, companies gain the opportunity to signal to their customers all over the world, that the products and services they offer all adhere to the same set of operations and quality as in the rest of the world. As a result, customers can be certain that the product and services they are buying are consistent to the product and services that other customers are buying from this company regardless of the country they are in.

Every management system follows a specific goal and is characterized through a series of components including policies, goals, steps, roles, responsibilities, processes, resources, communication, and risks. (LS_10/12/2017). One of those components is that every management system comprises a policy that describes the goal of the management system as

well as contains instructions by management for the organization about the rules and regulations that have to be followed within the management system. Moreover, management systems are organized by defining roles and responsibilities, as well as consisting of processes and process supported by software applications with the goal to standardize and automate those processes, document the individual business incidents, as well as provide information about the quality and quantity of those processes (Reports). In order for a management system to function properly, further resources have to be made available, such as financial resources, human resources, facilities and additional resources that are necessary in reaching the goal of a management system.

Furthermore, all management systems have to be documented and those documents have to be communicated to all stakeholders that are involved in the management system, such as upper management, departmental employees, and end-users. External stakeholders would include governmental agencies, certifying agencies, and suppliers that interface with the management system. Those documents have to be available and store in a filing structure that everyone can access and use. Further components of a management system are quality assurance and a continuous improvement process in accordance with the ISO standard 9001. Continuous improvement processes have internal and external audits to examine the level of achieved quality and maturity of the management system, as well as to 1) identify potential areas for improvement, 2) prioritize them and 3) implement them in a targeted and structured manner. Lastly, a structured risk management process has to be established as an essential component of management systems. The goal of risk management is to identify relevant risks which then have to be evaluated by conducting a risk analysis. Risk management then has to make sure that the identified risks are properly monitored and that appropriate measures are in place to prevent those risks from developing.

3.1 History of Management Systems

The emergence of management systems goes a long way back in history, all the way to 1798. During this time, mass production had been on the rise and people faced severe challenges to fulfill previously agreed arrangements in terms of the quantity and quality of their delivered products. The first person in the United States to come up with a set of best practices in order to enhance his ability to face those challenges was Eli Whitney, starting the trend of the development of rules and regulations that resembled management systems that we have in place today. Eli Whitney entered into a contract with the federal government of the United States agreeing to build 10,000 muskets with interchangeable parts in order to obtain the possibility to re-use the parts of a broken musket to produce a new one. The main challenge that Whitney faced was properly handling change management, as he faced difficulties to eradicate defects even though improvements were suggested. He further struggled to implement changes when it came to processes and document control. As a result, Whitney started to develop a set of rules and procedures that would allow him to better control and handle much needed changes. One of the rules and procedures he came up with in 1798 is still present in today's management systems. Rather than fixing an individual problem, he introduced the idea to find the root cause of re-occurring incidents and that a change had to be made throughout an entire organization, which involved updating the process used, updating previously approved documents and redistributing them to the entire organization for recommunication (Ames, Blake, Caurso, & Heinle, 2011).

When Henry Ford started to mass produce cars in 1913, management systems had increased in detail and scope. Management systems now included assessing the capabilities of potential employees before hiring them, establishing a set of requirements that suppliers had to meet, as well as taking the impact of multiple business areas into consideration for a product design and outcome of a products quality. However, the real major changes that

elevated management systems to the next level did not occur until World War II. WWII called for intensified demands of the production processes due to the increased scope of the quantity needed to fight a war. During that time, military organizations found that suppliers whose top management vigorously participated in controlling the operations yielded the best result in quantity and quality. As a result, top management was recognized as an important factor in developing and improving management systems, especially with regards to periodic review of processes, keeping track of accountability and responsibility, complying with policies and regulations, as well as enhancing communication internally and externally. Furthermore, the demand for transparency was generated during WWII, as the military organizations needed to be able to trust in the results of their suppliers to comply with the agreed terms of a contract. Therefore, they demanded documented procedures and instructions from which they could assess the reliability of the chosen supplier. Since then, transparency has been playing an important role in the implementation of management systems (Ames, Blake, Caurso, & Heinle, 2011).

3.2 Standardization of Management Systems

An implication of improving management systems is that organizations have been working on standardizing management systems in order to enhance their ability to improve operations, manage risk and promote stakeholder confidence. Standardized management systems enable employees and partner corporations to work jointly and across departments as well as company organizational boundaries on projects and processes in a collaborative way, make mass production possible, simplify production processes and reduce production costs. Businesses that adopt such standardized management systems generally enhance their customer service, increase their overall performance, more readily acquire new customers while keeping existing clients and save costs. Companies turn to external sources for the

implementation of such standardized management systems, in order to ensure that they resort to their industry relevant best practices that have been developed by experts and constitute a proven business model. One such external source is the International Organization for Standardization.

The International Organization for Standardization (ISO) is one of the organizations that develops and publishes International Standards on the basis of their research of best practices. Companies can then get certified on ISO standards in order to have an external verification that proves that they are improving their business practices and operations, as well as, where needed, to prove their compliance to industry standards and/ or government regulations.

3.3 ISO Definition of a Management System

ISO defines a management system as “the way in which an organization manages the inter-related parts of business in order to achieve its objective” (ISO, 2018). Consequently, management systems can be of different complexity depending on the size of a company, their objectives, and the scope of the area a company wants to implement a management system for. As a result, a smaller business might want to make sure that their management and organizational goal are clearly defined, while bigger companies often operate in highly regulated industries that require them to produce comprehensive documentation on their processes and operations in order to be in compliance with legal regulations (ISO, 2018).

3.4 Benefits of Management Systems

The management system standards written by ISO help enhance the performance of organizations by laying out a repeatable set of steps that are implemented to reach their defined goals, to establish an organizational culture that participates in continuous

improvement of operations and processes through upper management leadership, and commitment displayed throughout the entire organization. As a result, companies enable themselves to more efficiently allocate their resources and use the potential that is already existing in the company.

Furthermore, ISO standards not only enhance a private business' competitiveness, but also provide many benefits to the government. ISO standards are a pool of knowledge from experts on those particular subjects from all over the world that governments can use to when developing public policies. Not only do ISO standards back those public policies with crucial information from experts, but they also help to reduce and potentially remove barriers to world trade. The goal to remove trade barriers is essential for governments in the globalized world that we live in today, as it enhances their competitiveness on the global market, in comparison to other countries that do not comply with ISO standards. Complying with an ISO standard means that the same specifications are implemented for operations in different countries, which ensures consistency of vital components of goods and services such as "quality, ecology, safety, economy, reliability, compatibility, efficiency and effectiveness." Overall, ISO standards are starting to take up a much bigger part in a countries economic growth. For example, in England, where ISO originated from, ISO standards have contributed $8.2 billion annual growth to their GDP, as of September 2016, and in Canada, ISO standards have infused over $91 billion into their economy since 1981 (Antaris Consulting, 2016).

3.5 The International Organization for Standardization

ISO was founded in 1946 in England, when the International Federation of the National Standardizing Associations and the United Nations Standard Coordinating Committee decided to merge together. Together they formed ISO and started their operations for the first time in February 1947. When ISO started, 25 countries were involved in ISO with

the shared goal of establishing an organization that was capable to “facilitate the international coordination and unification of industrial standards”. Today, more than 150 countries are represented in ISO with a total number of 21,835 international standards publications, covering most industries from technology and manufacturing, to food safety and agriculture (ISO Quality Services Ltd., 2018).

Besides publishing International Standards, ISO develops Technical Specifications, Publicly Available Specifications, International Workshop Agreements and ISO Guides. A Technical Standard has the potential to eventually become an International Standard, but there is no agreement yet reached due to the fact that it is still under development. The purpose of a Technical Standards is for companies and experts to use the standards and provide feedback to ISO, so that it can be conclusively developed and transformed into an International Standard. A Publicly Available Specification is generated on the basis of a market problem that demands an immediate response from experts or external organizations. Just as a Technical Standards, Publicly Available Specifications are a means to gather feedback from the users in order to transform Publicly Available Specifications into an International Standard at the end of six years (or it will be withdrawn). Lastly, ISO Guides give advice to standards writers and national standards bodies on how to incorporate specific requirements while drafting standards, as well as issues regarding standardization principles. Overall, the aim of ISO is targeted towards creating International Standards which are publicly recognized by organizations and the industries in which they apply.

Companies that are looking to become certified on one of the standards that are published by ISO, need to hire an external accreditation body that certifies they have achieved the standard. ISO itself does issue any certifications and companies need to turn to companies like TÜV Süd, TÜV Nord, DAkks and DQS GmbH in Germany, or NSF International Strategic Registration, BSI Assurance UK Limited and SRI Quality System Registrar in the

United States to receive their certification. Those companies have to be accredited by national members of the International Accreditation Forum (IAF). In every country, the IAF has located national accreditation bodies that supervise those local accreditation bodies allowing them to offer the service of certification of international standards to companies.

According to ISO, certification is not a requirement for companies. Upper Management can choose to align their operations according to a standard and implement it into their operational culture, but not get officially certified. In those cases, companies cannot use the seal that a company obtained upon certification (that serves as proof to clients and suppliers that the company complies with the standard), and cannot market themselves as ISO compliant. Many companies see the benefit of aligning their operations according to a specific standard, but will only become certified once it is demanded by their customers or due to governmental regulations. Since the government is increasingly trying to regulate specific infrastructure in critical industries (e.g. in Germany) requiring them to adopt certain international standards, more companies are looking to actually become certified on the standards they adopt. This is, therefore, a driver for demand for companies can only proof to the government that they are in compliance with the regulations if they are certified on the standard by an external accreditation body (ISO, 2018).

3.6 ISO 9001 and ISO 14001

Two of the most popular international standards of ISO is 1) the quality systems management standard, ISO 9001, and 2) the environmental management system standard, ISO 14001. Those two standards account for 1,462,303 certifications in the entire world in 2014, which makes them the most important standards (Antaris Consulting, 2016). In 1996, ISO 14001 was the outcome of a General Agreement on Tariffs and Trade negotiations in Uruguay and the Rio Summit on the Environment. The international standard applies to companies in

countries that wish to ensure compliance with environmental laws and regulations, as well as a company's own written environmental policies. The standard enhances a company's ability to assess environmental impacts and mitigate the risks of environmental impacts. Since the standard was first introduced in 1996, over 300,000 companies obtained certification on ISO 14001 in 171 countries Antaris Consulting, 2016).

The need for quality assurance originated in the defense industry and quickly expanded to other industries, especially to manufacturing companies. The first quality management standard was written in England and carried the name BS 5750. This quality management standard took a different approach to manufacturing, as it did not concentrate its efforts on what was being produced, but **how** the manufacturing process was designed and how it should be managed in order to ensure an efficient and effective outcome in quality. In 1987, ISO became aware of the standard and took it over, naming it ISO 9001. Since then, ISO has consistently worked on publicizing this standard in many different variations that would be applicable to the various types of business in many different industries.

Overall, the main purpose of a quality management system is to achieve its previously outlined quality objectives and goals that have been either imposed by the company or by the government. An ISO quality management system helps to align the operations of a company with imposed regulations and requirements as well as customer demands while continuously enhancing its effectiveness and efficiency. The main purpose of an ISO quality management system is to "improve processes, reduce waste, lower costs, facilitate and identify training opportunities, engage staff, and set organization-wide direction" (ASQ, 2018b).

Quality Management Systems originated during the Industrial Revolution in the United Kingdom, United States, and Japan. The origins of quality management can be traced to Japan. Since the 1980's, Japan has been a leader in the development of quality management systems, due, in part, to the work of the American consultant W. Edwards Deming, who

introduced quality management in Japan and was subsequently used in the United States. It became increasingly important to implement best practices in order to ensure the best outcome of their products while increasing quantity and improving the way people would work together to produce a product (Izadi, Kashef, & Stadt, 1996).

3.7 ISO and Information Technology Trends

There are several important IT trends. 1) Since Information Technology (IT) plays such an important role in today's business and has become a crucial factor for success, there are many management systems that IT creates for a business, as well as management systems that support the IT department itself. 2) Systems used in the IT department itself give it the ability to achieve its organizational goals and secure its operations. IT has become business-critical in our globalized world. 3) Companies that service a wider range of users and operations would fail if there were IT system breakdowns or data breaches. 4) More and more businesses start expanding into the field of data analytics and big data, as well as digitization of business functions. All of those business trends increase the risk of information security incidents. Many businesses are not equipped to prevent attacks from highly motivated and skilled cybercriminals. The possibility of cyber-attacks to gain access to classified or secure data has become more likely, with the advancement of technology. According to the breach level index, only in 4 percent of data breaches could the stolen data not be used due to encryption being used. There are 58 records stolen every second, 3,479 every minute, 208,719 every hour, and 5,009,252 records every day (Gemalto, 2018). According to the National Institute of Standards and Technology, businesses have to pay around $400B in damage per year on a global basis resulting from operation shutdowns due to cyber-attacks (NIST, n.d.). Companies in the United States encounter the highest average cost per capita of data breaches

of $225, and an average total organization cost of $7.35 million (Ponemon Institute LLC, 2017).

When looking at the data breaches occurred in 2017 on a global level on Table 1, four out of the first six most severe data breaches where encountered in the United States of which three incidents where accidental losses of the data. There was no data breach listed in Germany under the first hundred most severe data breaches (Gemalto, 2018).

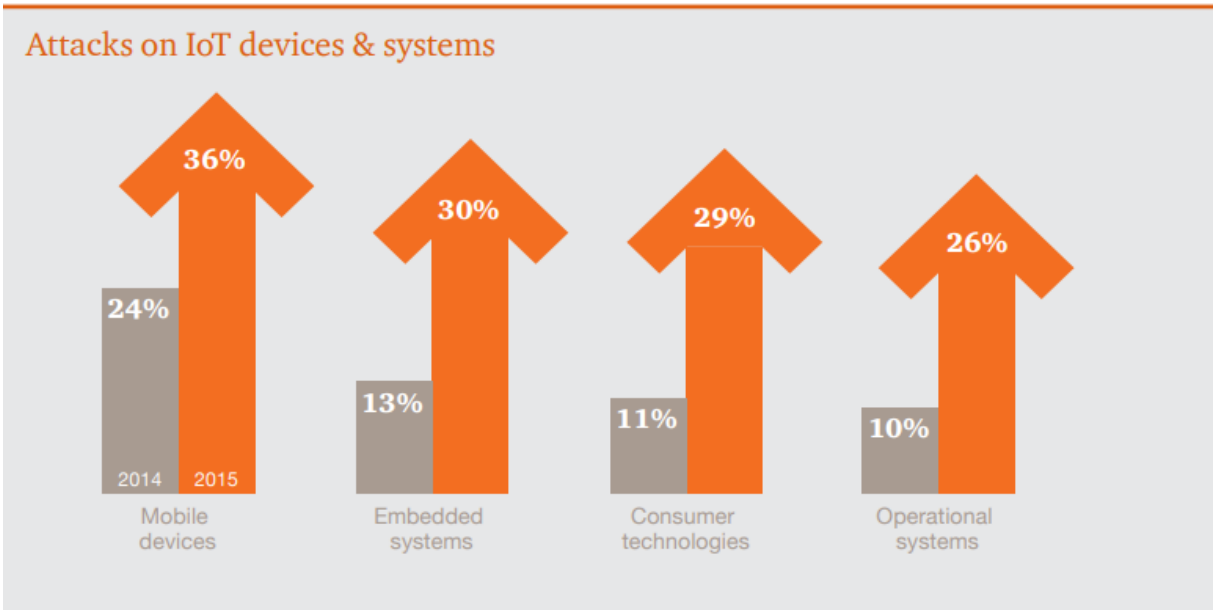
Table 1.

Rank	Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
1	Equifax	147,900,000	07/15/17	Identity Theft	Malicious Outsider	United States	Financial	10.0
2	Reliance Jio	120,000,000	07/10/17	Account Access	Malicious Outsider	India	Technology	10.0
3	Motor Vehicles Department in Kerala	200,000,000	05/01/17	Nuisance	Malicious Outsider	India	Government	9.9
4	River City Media	1,340,000,000	03/06/17	Nuisance	Accidental Loss	United States	Other	9.8
5	Deep Root Analytics/ Republican National Committee	198,000,000	06/13/17	Identity Theft	Accidental Loss	United States	Government	9.6
6	Alteryx	123,000,000	12/19/17	Identity Theft	Accidental Loss	United States	Technology	9.4

(Source: Gemalto, 2018)

Moreover, there has been a recognized increase of detected information security incidents of 38 percent in the year 2016, according to a PwC survey (PwC, 2016). Table 2 shows the results of a Security Survey conducted by PwC of more than 10,000 participants from over 127 countries. The table illustrates the rising numbers of cyber security attacks that companies experience, and highlights the need in company IT departments to enhance their management systems. In other words, IT departments need to implement ISO standards in their departments aimed at preventing cyber-attacks.

Table 2.

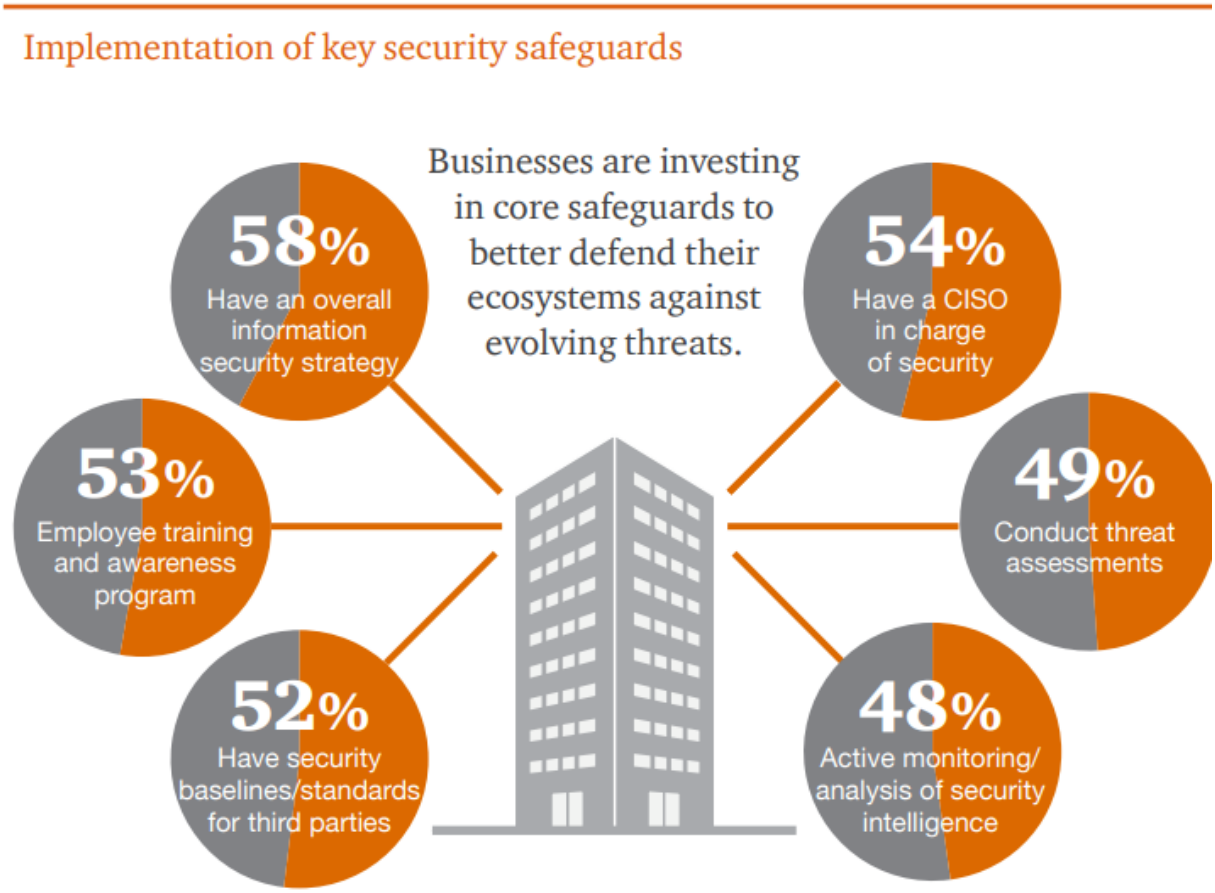


(Source: PwC, 2016)

It is in the hands of upper management to find long-term solutions that will help to arm their IT departments in a sustainable way, against the prevailing risk of cyber-attacks. “Many executives are declaring cyber as the risk that will define our generation,” said Dennis Chesley, Global Risk Consulting Leader for PwC (PwC, 2016).

Moreover, the willingness of companies to invest into sustainable security solutions that stabilize their IT department and decrease their probability of data breaches, shows a rising trend, as upper management is starting to recognize the benefits they gain from implementing ISO related procedures. The PwC survey indicates that over 50 percent of the respondents have increasingly shifted their focus in this direction. Table 3 shows the range of investments companies are making in cyber security. The data illustrates areas of growth in ISO-related requirements and thus are important sources of growth for ISO consultants.

Table 3.



(Source: PwC, 2016)

The IT department deploys IT systems that are essential in supporting every day operations, and enables a company to provide quality services and products for their customers. The PwC Survey strongly indicates the importance of improving IT security management systems and the IT service management system (PwC, 2016). Both management systems are areas of consulting practices.

3.8 ISO 20000-1

The international standard ISO 20000-1 is a service management system standard. The standard has been updated twice by ISO with the most current version published in 2011. The ISO 20000 family consists of five published documents that include ISO/IEC 20000-1 (service management system requirements), ISO/IEC 20000-2 (Guidance on the application

of service management systems), ISO/IEC 20000-3 (Guidance on scope definition and application of ISO/IEC 20000-1, ISO/IEC 20000-4 (Process reference model), and ISO/IEC 20000-5 (Exemplary implementation plan). ISO 20000-1 describes normative requirements that are mandatory for a business to implement in order to obtain certification on the standard. The other four documents in the ISO 20000 family are supporting documents that are intended to help a business looking to become certified to implement a service management system into their organizational structure. A company cannot obtain certification on any of those supporting documents (ISO, 2011a).

The service management system is aimed towards building an organization that is specifically structured to support the goals of the management systems that are implemented. In order to accomplish this, processes have to be adopted in the organization that are defined in the standard, resources have to be allocated to specifically support the goals of the processes, and the implemented management system has to be continually analyzed and updated. Processes and technology have to be maintained in written documents, filed away according to the requirements of the standard, and employees working with those processes and technologies need to be able to access those documents. Once a year, the upper management has to conduct a management review in which they control that the implemented management system works as designed by looking at the KPI's, reviews and audits previously conducted throughout the year.

ISO 20000-1 is the first part to the International Standard on IT Service Management which entails measurable standards of quality for IT Service Management. The document specifies the necessary minimum requirements for processes that need to be defined, implemented and improved on a continual basis in order to provide IT Services in a predefined quality and to be able to better manage it. ISO 20000 is geared to the process definitions of the IT Infrastructure Library (ITIL).

Part 1 contains the formal specifications of the standard that an Organization needs to document, abide by, guarantee and verify in order to obtain certification. These are mandatory instructions regarding general requirements to service management system, planning and implementation of service managements, service level management, service reporting, availability and service continuity management, incident management, problem management etc (ISO, 2011a).

The goal of Part 1 is to ensure IT Services on a defined quality level with a process oriented life cycle.

ISO 20000-2 is the second part to the International Standard on IT Service Management which builds upon Part One of the standard, giving further guidance and explanations of how to actually implement a service management system in your organization. It takes the standard from the first part and further elaborates on it by giving examples and suggestions to give a better understanding on how to meet the requirements from Part One. For example, ISO 20000-1 says that an organization needs to have a service management plan and ISO 20000-2 describes exactly what the service management plan should entail (ISO, 2011b).

An organization cannot obtain certification on Part Two, as it only gives guidance and no hard facts that a company actually has to meet.

ISO 20000-3 is the third part to the International Standard on IT Service Management which supplements part two of the standard that gives further guidance and explanations of how to actually implement a service management system in an organization. This part assists in the establishment of the scope of the SMS and prepares the organizations for a conformity assessment. By and large, this documents consists of scenarios that cover commonly found and practical service provider circumstances to help establish if ISO 20000-1 is applicable to a service provider's circumstance (ISO, 2012).

This document defines to whom ISO 20000-1 may be applicable, to what extent the organization has to fulfill the requirements in ISO 20000-1 internally, what requirements can be fulfilled by an external organization, how it should be proceeded, and who is accountable in each scenario. An organization should be entirely clear on what its scope is, because services that they provide, but are not included in the scope, do not need to fulfill the requirements of ISO 20000-1.

The third part of ISO 20000 has an informative character, which means it does not list any requirements that need to be fulfilled by an organization when becoming certified on ISO 20000-1. However, this document is a supporting document of ISO 20000-1 that is especially useful for consultants and assessors when helping a company to implement a SMS (ISO, 2012).

ISO 20000-4 is the fourth part to the International Standard on IT Service Management which connects the requirements from ISO 20000-1 with ISO 15504-1 that outlines how to facilitate the development of a process assessment model, as one is described in ISO 20000-1 (ISO, 2010).

Part Four consists of the various processes that need to be implemented in an organization by name, context, purpose, outcomes, and requirements traceability for each one, in order to meet the requirements that are necessary in order to become certified and listed in ISO 20000-1. The lists of the processes needed in order to be able to implement ISO 20000-1 further helps consultant to identify the areas in an organization that need to be enhanced (ISO, 2010).

ISO 20000-5 is the fifth part to the International Standard on IT Service Management which provides a generic, three-phased plan of how an organization could go about implementing the requirements of ISO 20000-1. It outlines the benefits of a phased

implementation of the requirements of ISO 20000-1, such as more efficient risk management and cost allocations (ISO, 2013a).

Part Five is a technical report that gives one hypothetical example of what processes and requirements need to be implemented in a specific phase. However, organizations cannot just take this as standard as a default setting as they have to adapt it to the individual needs of their organization and scope. This document can be helpful when wanting to implement ISO 20000-1, but should not be provided as a primary document to be looked at when doing so. However, it is a good document to reference, in case an organization is not entirely sure on how to go about planning to implement the standard and therefore gives guidance.

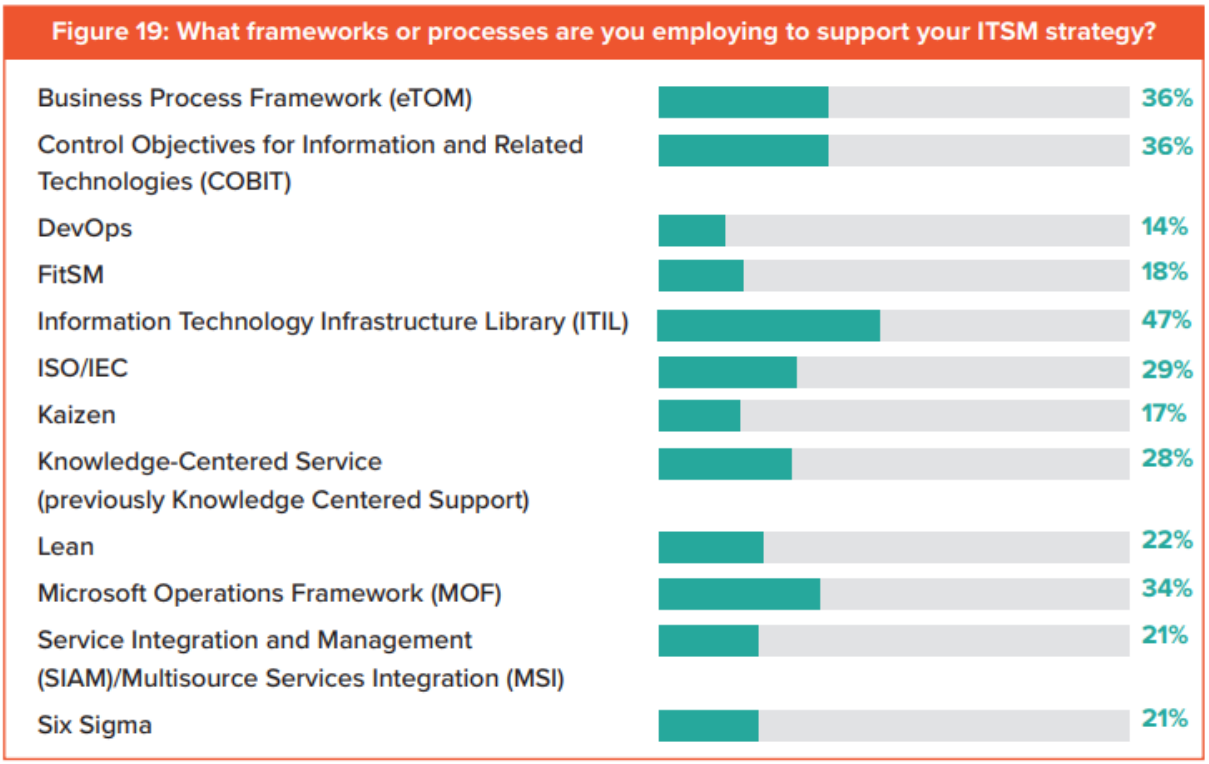
3.9 ITIL and the ISO 20000 Framework

The ISO 20000 Framework is directly based on the foundation of the Information Technology Infrastructure Library (ITIL) framework. ITIL is a set of best practices that describes the detailed practices for IT service management that are necessary in order to align IT services offered by an organization with their particular business needs. As described by Jäntti & Cater-Steel, “thousands of IT service provider organizations world-wide are improving their traditional customer support processes based on IT management frameworks. The main reason for the change is that IT customers are increasingly focused on the purchase of services that support their business processes rather than separate software products” (Jäntti & Cater-Steel, p. 192, 2017).

As business executives see the need to enhance their IT services, the demand for ISO standards has risen, along with new frameworks. Besides ITIL, other ITSM frameworks include Control Objectives for Information and related Technology (COBIT) and Business Process Framework (eTOM). Table 4 shows results of a recent study conducted by Forbes

Insight (2017) indicates that the ITIL framework is the most widely-used framework with the highest rate of adoption.

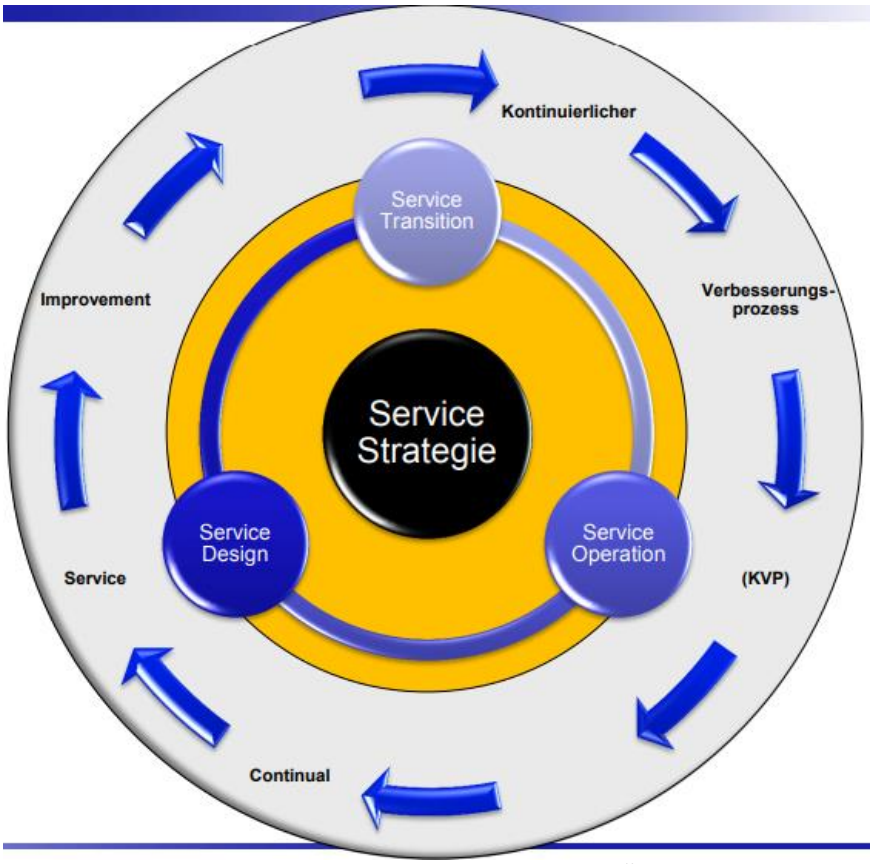
Table 4.



(Source: Forbes Insight, 2017)

The ITIL framework was developed in the United Kingdom in the 1980s, where the Office of Government Commerce commissioned the Central Communications and Telecommunications Agency (CCTA) to manage the production of ITIL due to a series of important public sector IT projects that failed. ITIL originally consisted of more than 30 books and has been revised three times. As depicted in Figure 1, the latest version published in 2011 consists of five metaprocesses that describe the ITIL service lifecycle; 1) Service Strategy, 2) Service Design, 3) Service Transition, 4) Service Operation, and 5) Continual Service Improvement.

Figure 1.

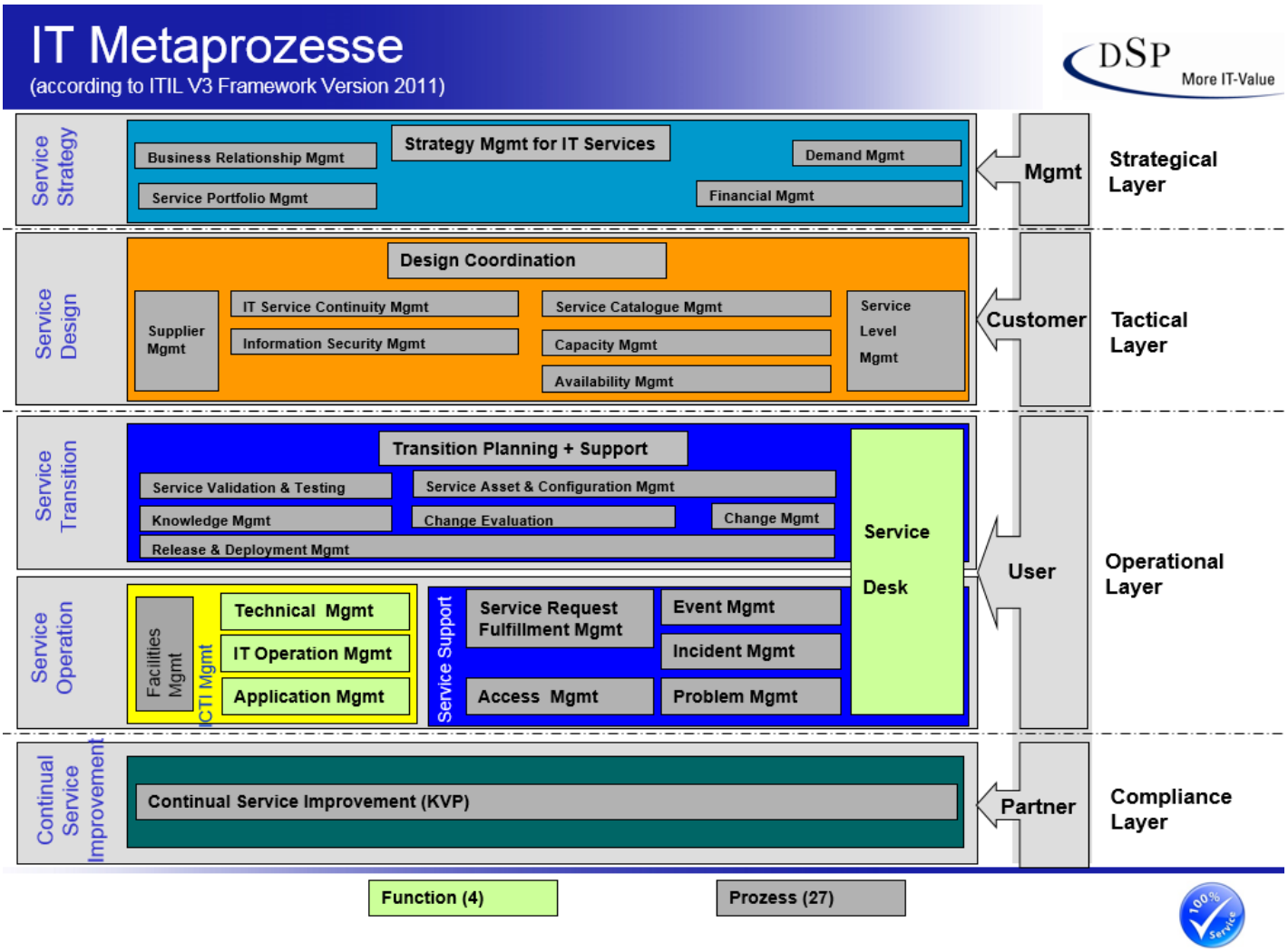


(Source: TÜV Süd, 2015a)

ISO first published the standard ISO/IEC 20000 in 2005 that formalized the ITIL processes and included certification requirements of the management system. Those certification requirements include documentation, reviews, and external audits.

Table 5 depicts the ITIL framework with the five metaprocesses and the micro processes of each core process (TÜV Süd, 2015a). The metaprocesses can be found on the left hand side of table 5, with the corresponding micro processes depicted to the right of each metaprocess.

Table 5.



(Source: TÜV Süd, 2015a)

The framework includes twenty-seven processes and four functions. All of the processes depicted are measurable in order to track their performance.

Benefits of implementing ITIL include

- gaining knowledge about the type, scope and quality of provided services,
- transparency of performance and quality,
- used and needed IT competencies and resources,
- known cost of IT services,
- defined processes preventing duplication of effort,
- known security holes lower risk,

- satisfied clients, user and employees.

To understand the complexity of ISO and the likely increased demand for ISO consulting, the following sections describe this complexity as a set of five metaprocesses and their corresponding micro processes. The following overview provides a general perspective on the standard and the reader is encouraged to explore each of the standards in more detail; but that detail is beyond the scope of this paper.

3.11.1 Metaprocess One: Service Strategy

The first metaprocess makes up the core of the IT Service lifecycle described in the third version of ITIL that is designed to enhance a company's ability to think and act in a strategic manner. The ultimate goal is to convert a company's IT service management from an organizational capacity to a strategic asset by developing a strategic plan that ensures matching customer needs with business needs and retaining customer loyalty trough effectively managing the time and money invested into developing a particular service (TÜV Süd, 2015b).

In the service strategy process, current market conditions are analyzed in order to find out if they are capable of meeting the business needs of an organization. The result of this stage will be a strategic approach for IT service management where the customer needs are being identified, the organization obtains the ability to respond to changing market conditions, and a maximum return is ensured on their investment of IT services per customer needs.

A key principle of the service strategy stage is the definition of the service value to a customer and the business. In order to assess the value creation, the person coming up with the strategy has to measure the added value to the business requirement, as well as keeping in mind that the value is ultimately defined by the customer and that his definition of the service value can change over time.

Another issue addressed in this phase of the ITIL lifecycle is the governance of the services being provided. Governance is the only overlapping department that connects IT with the rest of the organization. Therefore, governance is meant to build a consistent approach to manage processes on all organizational levels by defining clear strategies and requirements, as well as boundaries for the scope of action. Governance includes the definition of rolls and responsibilities, overseeing the correct compliance of strategies, requirements and processes, as well as activities to solve issues that have been identified. Many ITSM strategies are not successful, because a company tries to build new structures and processes instead of working with the governance structure already in place.

The processes in this phase include 1) service portfolio management, 2) demand management, 3) financial management, and 4) business relationship management.

Service portfolio management. One of the processes included in the service strategy phase is service portfolio management. The purpose of service portfolio management is for the service provider to find the right composition of services being offered in order to enable the company to reach its business objectives with the right IT investments. The goal of this process is to assess earnings and risk of the services in order to enable them to make the right decision on what services should be offered. It is important to continuously manage the service portfolio to evaluate if the services offered still support the overall strategy, to react to changes in the environment, and to track the investments into the services to find out which service should be retained or deactivated. The scope of the service portfolio management is all services that a company intends to offer, currently offers and the services that have been deactivated.

Demand management. The next process is demand management, where the customer need is being analyzed. Demand management tries to understand what service the customer is asking for, what they will demand in the future, and how they can influence the demand of

their customers towards specific services. Demand management works closely together with capacity management in order to ensure that the company is able to provide enough capacity for the demand encountered. One aspect of this process is to identify and analyze patterns of business activity that will better help to assess the demand of the services offered to the clients.

Financial management. Financial management is another important process of this stage. A company needs to calculate what it needs invest to create, develop and render a service. Part of this process is to develop a business case, which is a 'decision and planning tool' designed to predict possible consequences of business actions. A business case describes the foundation for an economic justification for high extensive expenditures.

Business relationship management. Lastly, the business relationship management process is created to foster and ensure an ongoing business relationship between the service provider and the customer on the basis of the extensive knowledge gained from the demand management process. Business relationship management is important to track customer satisfaction, formulate business requirements, and to mediate and escalate actions in times of conflicts between the service provider and the customer (TÜV Süd, 2015b).

3.11.2 Metaprocess Two: Service Design

The second metaprocess in the ITIL lifecycle service design is aimed at creating IT services in alignment with current processes and requirements in order to put the service strategy plan into practice and facilitate the introduction of services. The service design phase is also designed to ensure that the performance of services, customer satisfaction and economic efficiency is guaranteed when new services are being introduced to the service portfolio, or old services are being deactivated (TÜV Süd, 2015c).

In the stage of service design, it is really important to follow a holistic approach in order to ensure consistency and integration among all activities and processes across the entire IT. Only if a holistic approach is being followed can business relevant, consistent functionality and quality be reached. This means that if one single design element has to be changed or adopted, all other elements have to be considered as well.

The output of the service design stage is a service design package for every new service, major changes on a service, and deactivation of a service, as well as changes to a service design package itself. This service design package is then transferred to the service transition stage that will then implement the requirements of the service design package.

The processes in this phase include 1) design coordination, 2) service catalogue management, 3) service level management, 4) supplier management, 5) availability management, 6) capacity management, 7) IT service continuity management, and 8) information security management.

Design coordination. The design coordination process is the overlying guide in this stage, as it ensures that the goals of this stage are being met. For this purpose, one single coordination and management unit will be responsible for all activities and processes that are delivered during this phase.

Service catalogue management. The service catalogue management process serves as the single source of information about all operational services, as well as all services being developed for operations. The service catalogue management is required to ensure that all data contained in the service catalogue is exact and consistent, as well as accessible for all authorized persons. The scope of this process includes definition of services and service packages, development and maintenance of service descriptions, as well as the interfaces and dependencies between all services and supporting services in the service catalogue.

Service level management. The service level management process is another important part of the service design stage. It is designed to ensure that all current and planned IT services are rendered according to agreed-upon goals between the service provider and the customer. The output of this process includes the documentation of a service level agreement, operational level agreement and underpinning contracts. The goal of the process is to measure and oversee all defined, documented, agreed-upon service levels in the contracts, as well as issuing reports on the findings. Based on the reports, service level management needs to identify improvement possibilities, proactively prevent service disruptions, and improve service quality.

Supplier management process. Another process included in the service design stage is the supplier management process. Since a business most often cannot provide all aspects needed in order to offer the best service possible itself, it needs to engage in a supplier relationship. The purpose of the supplier management process is to reach an optimal cost-benefit ratio by using suppliers that provide the best quality for the IT services offered. This process ensures that all contracts and agreements with suppliers support business requirements and that all suppliers adhere to their contractual responsibilities.

Availability management. The availability management is another process in the service design stage. Availability management ensures that the level of availability of all IT services fulfills the agreed upon availability requirements, or rather the service level goals, in a cost-effective and timely manner. This includes

- the development and maintenance of a current and relevant availability plan,
- consultation and specification of guidelines for all availability aspects,
- aid to the diagnosis of incidents and problems that concern the availability,
- evaluation of the effect of all changes on the availability plan,

- ensuring the implementation of all proactive measures to improve the availability of services within the financial budget.

Important aspects of the availability management are reliability, maintainability, serviceability and vital business factors.

Capacity management. Capacity management ensures that IT services and the IT infrastructure adheres to the agreed upon requirements of capacity and performance in an economic and timely manner. This process includes the same aspects as the process of the availability management with regards to the capacity management. The capacity management process should be the first contact point for all issues regarding the connection between the performance and capacity of IT services. As part of this, the capacity management has to oversee the patterns of business activity, as well as the exertion of influence on the demand in accordance with the financial management for IT services and the demand management. Sub-processes of this process are the business capacity management, the service capacity management and the component capacity management.

IT service continuity management. The IT service continuity management process is also part of the service design stage. The purpose of the IT service continuity management process is the support of the superordinate business continuity management process. IT service continuity management has to ensure that risks with the potential to severely hinder the performance of IT services are properly managed so that the service provider always has the ability to meet at least the agreed upon service goals in relation to business continuity. Part of this process is the development of a business impact analysis that quantifies the effects of a failure of a service on business.

Information security management. The last process included in the metaprocess service design is the information security management process. The purpose of this process is to protect information of an organization, to ensure it is confidential, available, has integrity,

and is accountable. The goal is to secure the interests of people, systems and communication facilities of potential harm from data leaks. We will consider this process more in depth when looking at the international standard ISO 27001 for IT information security, because of the intersection between ISO 20000-1 and ISO 27001 (TÜV Süd, 2015c).

3.11.3 Metaprocess Three: Service Transition

The purpose of the third phase of ITIL processes is to ensure that new, modified or discontinued services operate exactly as planned and documented in the previous two books, Service Strategy and Service Design. In order to do so, necessary resources and capacities have to be available to support the transition and a stable framework has to be in place to evaluate the service capabilities and risk profiles before deploying a new or modified service. Furthermore, efficient and repeatable mechanisms have to be allocated to build, test and deploy services and releases (TÜV Süd, 2015d).

Service Transition. Processes in this phase are important for organizations to consider, as it brings a higher number of successfully implemented changes, less delays through unexpected conflicts or dependencies, increases in trust that new or modified services are in accordance with the specifications, and ensures maintainability and economic efficiency.

The processes in this phase include 1) the transition planning and support process, 2) change management process, 3) service asset and configuration management process, 4) release and deployment management process, and 5) the knowledge management process.

Service transition and support. The service transition planning and support process encompasses the entire planning for the service transition phase and to coordinate necessary resources. This includes the establishment of new or modified services in supported environments within the predicted costs, quality and time, the coordination of all major

changes or new services through all transition processes, determination of priorities in cases of resource conflicts in the transition phase, and plan the budget and resources needed to fulfill all future requirements of the transition phase.

Change management. The change management process navigates the life cycle of all changes in order to enable changes to be deployed under minimal disruption of other IT services. This includes recording and evaluating all changes and that authorized changes are prioritized, planed, tested, implemented, documented and reviewed in a controlled manner. Change is defined as an addition, modification or removal of an element that has a potential impact on IT services. The scope includes all changes of processes, tools, measured quantities, documentation, as well as services and configuration items.

Service asset and configuration management. The service asset and configuration management process ensures that all assets necessary for service delivery are controlled in an appropriate manner and that the available information regarding those assets is exact and reliable. The scope of this process entails the management of the entire life cycle of all configuration items. Configuration items are classified as service assets that need to be managed in order to deliver a service.

Release and deployment management. The release and deployment management process plans, terminates and controls the building, testing, and deployment of releases, as well as provides new functionalities according to business requirements, and secures the integrity of already existing services. This includes the construction and testing of release packages, as well as ensuring that those release packages are able to be followed, installed, tested, confirmed and/or uninstalled or withdrawn. The scope of this process includes all processes, systems, and functions needed to build, test and deploy a release in its live environment, the establishment of services indicated in service design, and the formal transfer of the service to its service operation function.

Knowledge management. The knowledge management process consists of the exchange of ideas, experiences and information that are accessible at the right time and at the right place, in order to facilitate well-informed decisions. This includes the enhancement of the quality of decision making of management by ensuring that reliable and secure knowledge and information is accessible (TÜV Süd, 2015d).

3.11.4 Metaprocess Four: Service Operation

The fourth phase of ITIL encompasses the coordination and performance of activities and processes that are necessary for the provision and management of agreed services. This includes to uphold trust in IT through efficient and effective provision and support of agreed services and to minimize the impact of service disruptions on routine activities. The processes included in this phase are important to follow as they help to reduce the duration and frequency of service disruptions, as well as provide fast and effective access to standard services (TÜV Süd, 2015e).

The processes in this phase include 1) event management, 2) incident management, 3) request fulfilment, 4) problem management, 5) access management, as well as the functions 1) service desk, 2) technical management, 3) application management, and 4) IT Operations Management.

Event management. The event management process manages the entire life cycle of events including activities to detect events, to logically classify them, and to determine appropriate measures to be taken. The event management process is relevant for all aspects of service management that have to be controlled and can be automated. An event is defined as a status change that is important for managing configuration items or IT services, and is generally detected through notifications generated by IT services, configuration items, or monitoring tools.

Incident management. The incident management process aims to restore normal service operation as quickly as possible and minimize negative effects on business operations. In order to do so, the process ensures that standardized methods and procedures are implemented to efficiently and quickly react to incidents, analyze, and document ongoing operations and report occurring incidents. Incidents include all events that have the potential to lead to a disruption of a service.

Request fulfillment. The request fulfillment process is designed to manage the life cycle of all service requests. The process aims to obtain user and client satisfaction by efficiently handle all service requests in a professional manner, to provide information for users and clients regarding the availability of services and the procedure to retrieve the services, and to provide a communication channel for users and clients.

Problem management. The problem management process manages the life cycle of all problems from the detection, analysis and documentation of problems all the way to the solution of problems. A problem is defined as the source of one or more incidents. The goal of this process is to prevent re-occurring incidents and minimize the impact of inevitable incidents.

Access management. The access management process authorizes users to use a service or a group of services. The process aims to efficiently react to requests to access a service and generally takes place within the IT operations management or service desk.

Service Desk. The service desk is the single point of contact for users and is therefore the link between services offered and the clients. The service desk usually manages incidents and service requests, and aims to restore normal service operations as quickly as possible.

Technical management. The technical management process defines how to manage the technical knowledge of the IT infrastructure and provides the resources to support the life cycle of the business operations in the organization.

Application management. The application management defines the technical knowledge of all applications and provides the resources to support the life cycle of the business operations in the organization.

Operations management. IT operations management is responsible for the daily operational activities of an organization. The IT operations management process is split into two functions: 1) the IT operations control and 2) the facilities management. The IT operations control oversees the performance and monitoring of all operational activities and events. The facilities management is responsible for managing the physical IT environment (e.g. computer center, computer rooms, cooling installation) (TÜV Süd, 2015e).

3.11.5 Metaprocess Five: Continual Service Operation

The last phase of ITIL processes aim to adjust IT services to the ever changing business conditions and environment by identifying and implementing improvement possibilities for IT services. In doing so, organizations continually identify room for improvement and ensure that their services meet the best service quality possible and that they are continually in accordance with the business requirements. These processes also lead to a gradual improvement in economic efficiency and cost reduction. This requires monitoring and reporting all life cycles of all the existing phases and processes (TÜV Süd, 2015f).

The basic concept underlying this phase is the Deming Cycle of plan, do, check, act (Deming, 1986). This means that a snapshot of the current business environment will be taken and serves as a reference point for all further actions taken. After that, critical success factors and key performance indicator have to be identified in order to establish measured quantities by which all further data will be measured against. After the collection of data, the information gathered will be analyzed in an attempt to find certain trends, the fulfilment of goals, or areas for improvement. Based on the analysis of the data and findings, an action plan

will be developed that will support the implementation of improvement measures. After the improvement measures have been implemented, the cycle will start again with taking a snapshot of the new business environment (TÜV Süd, 2015f).

3.10 ISO 27001 Information Security Management

The international standard of IT security management systems is called ISO 27001 and the last version was published by ISO in 2013. This international standard is part of the ISO/IEC 27000 family of standards and includes ISO/IEC 270001, ISO/IEC 270002, ISO/IEC 27003, ISO/IEC 270004, ISO/IEC 270005, ISO/IEC 270006, ISO/IEC 270007 and ISO/IEC TR 27008 (ISO, 2013b).

ISO 27000-1 is the normative part to the International Standard on Information security. The document specifies the requirements for the establishment, implementation and continual improvement of a documented information security management system. Furthermore, the standard entails the requirements to assess, prioritize and take actions in regard to information security risks of an organization. Annex A of ISO 27001 contains technical and organizational measures that are mandatory to implement if the company wants to obtain certification on the standard. Additionally, there are sub-standards for the individual industries that need special clarification. For example the energy or health industry.

According to ISO, management systems compliant with ISO 27000-1 have the goal to protect information of an organization so that it is confidential, available, has integrity and is accountable. The document outlines the general requirements to achieve this goal through policies, documentation, organization, document control and management reviews.

ISO 27002 is a guideline for companies to help to implement the compulsory controls listed in Annex A in ISO 27001. ISO 27003 entails a general guideline to implement the information security management system, ISO 27004 is a guideline to help define and

measure the KPIs of an organization, ISO 27005 is principally involved in risk management (classify and protect assets in need of protection, analyze the risk of those assets, calculate probability of occurrence, implement measure to mitigate risk), and ISO 27007 is a guideline for audits that help to identify if the right processes are implemented and managed accordingly while identifying potential for improvement.

An organization can only become certified by an external accreditation body on the first part of the standard. The sub-standards for specific industries have to be implemented as well, as they differ in requirements in Annex A (depending on what industry the company operates in). The guidelines are a deepened source of information supporting ISO 27001 when companies are seeking to implement this standard.

According to the ISMS, the whole company is affected by the standard, but since information data is mostly processed by the IT, it is essential that the IT department is part of the scope when implementing the standard. The scope further entails the data that the organization classifies as worthy of protection. On top of that, data that the law protects has to be part of the standard as well, which is covered in Annex A under compliance with laws.

Attached to ISO 27001 is Annex A, that specifically outlines control objectives and controls that need are compulsory for an organization to adhere to, if they want to successfully protect the data included in the scope of the information security management system and become certified on the standard. Annex A describes a catalogue of measures that start with Annex A.5. In the first four chapters of Annex A (A.1 – A.4), the general requirements for the management system are being listed. From A.5 on, every measure listed entails a control objective with the corresponding controls that a company needs to be in compliance with.

The controls listed in this catalogue of measures in Annex A include the implementation of a security policy that needs to be reviewed at least once a year in A5. This

security policy is defined by the organization and needs to include the scope, as well as a guideline for the scope. Furthermore, a security organization needs to established with an information security officer, a person responsible for business critical assets/ services/ incidents/ and change management, as described in A6. This security organization needs to be properly documented and contact information has to be communicated to authorities and special interest groups.

A.7 lists the control objectives in regards to employment. It states that an employee in prospect has to be properly screened and security relevant restriction clauses have to be implemented in their contracts. When the employee has been employed, he has to be provided with training in accordance to the policy guidelines on information security to ensure that he will be able to properly execute them. If the contract with that employee is terminated, A.7 states that it has to be ensured that the employee adheres to specific security guidelines even after employment.

A.8 is concerned with the organizations definition of assets and the establishment and maintenance of an asset inventory. Each asset has to be allocated to an owner, who can be a single person or a part of the organization (e.g. a department). An asset owner is responsible for the maintenance, application, and security of that asset. Furthermore, A.8 states that a schema has to be developed to classify information according to the value of that information, government regulations, sensibility, and criticality. Once an information has been classified, it has to be labeled and stored accordingly. Highly classified information is under control of the ISMS.

The control objectives of A.9 are concerned with the management of user access and responsibility. This includes the registration of users, allocation of passwords, and the limitation of access to system functions and program sources.

A.10 deals with key management and cryptographic measures. This includes the methods used to encrypt information that is included in the scope, the management of those methods, as well as the management of physical keys used to store information and security sectors.

A.11 makes it mandatory for organizations to establish security sectors to secure areas with information processing systems. Also areas that contain data or information not stored in information processing systems (e.g. medical records in the cellar of hospitals) have to be included in security sectors. This includes the establishment of physical access controls, protection of working areas, and physical protection against external risks (e.g. fire, water, earthquake, explosions, and civil disturbances). Moreover, operating equipment has to be properly secured (including outside the company's locations), protected against failures of utility services, and protected against interception by third parties (telecommunication).

A.12 is concerned with the operating processes and responsibilities. The control of A.12 is to have clearly defined processes for the operation of information processing institutions and systems, change management, capacity management, and differentiation between development, test, and life environment. It also includes the protection against malware and the promotion of threat awareness of users in this context. Data backup is another important topic in A.12, as it demands the development and tests of continual backup files of information, software and system configuration. A.12 further includes the surveillance of system usage, monitoring of software in the operations, handling of technical vulnerabilities, and auditing of information systems.

A.13 deals with the principles and procedures to securely exchange information, meet agreements on the exchange of information, protect information that is exchanged via electrical data services, and the confidentiality and secrecy agreements.

A.14 establishes principles to securely develop software and systems, procedures for change control, user tests after modifications of operating systems, limitations of software modifications, principles for the development of secure systems, monitoring of outsourced development, protection and management of test data, as well as the specifications for information security requirements.

A.15 deals with information security regarding contracted suppliers. A guideline has to be established for the relationship with suppliers that covers topics such as access to information and systems, processing and communication of information, security requirements for the supply of services or product components, and handling of security risks. It further states that services provided by suppliers have to be properly monitored and audited, and procedures have to be established that deal with the handling of modifications in accordance with the supply of services of those suppliers.

A.16 specifically outlines how security incidents have to be handled and improvement measures have to be implemented as a result of each security incident. Clear responsibilities and processes have to be established, information security incidents have to be reported (as well as security vulnerabilities in systems and services) and classified, and an appropriate reaction has to be introduced in accordance with pre-defined processes.

A.17 is concerned with the preservation of information security, which includes the business continuity management and the effectiveness of continuity plans concerned with information security.

A.18 outlines the liability to be in compliance with government regulations and contractual agreements, such as ownership rights, recording activity, data protection, and usage of cryptography. Moreover, there have to be regular independent reviews of the implementation of the information security management, the conformity of information security guidelines and relevant standards, and the technical conformity (ISO, 2013b).

3.12 Connection between ISO 27001 and ISO 20000-1

ISO 20000-1 contains the two processes 1) Information Security Management and 2) IT Service Business Continuity Management. Both of those processes draw upon ISO 27001, which supports those two processes of ISO 20000-1 and requires further implementation of more detailed processes to secure data and business continuity (Federal Office for Information Technology Security Germany, 2005).

ISO 20000-1 is tailored towards the IT department of organizations, whereas ISO 27001 includes the entire organization in its scope. ISO 20000-1 entails parts of ISO 27001 and refers on those occasions to ISO 27001. Where ISO 20000-1 focuses on the IT service management and only touches on information security, ISO 27001 is much narrow and only includes the processes specifically tailored on information security. When implementing ISO 27001, it should be paid close attention to the already existing processes in the IT department and ISO 27001 should be built on the basis of those processes, rather than creating a parallel world of processes that step into competition with those already existing processes. In order for an organization to become ready to be certified in the IT department for ISO 27001, the IT department has to be structured according to Annex A of ISO 20000-1.

Joint core processes that both of the standards entail are

- Asset management and CMDB
- Event management
- Incident management
- Change management
- Access management
- Availability management
- Capacity management
- Security management

- Business continuity management
- Supplier management

Similar processes included in both standards that exhibit some intersections and differences in the specific implementation of the processes in the organization include the following:

- Risk analysis
- Resource management
- Roles and responsibilities
- Supplier management
- Knowledge management
- Information security management
- Service continuity management

Therefore, a high ITIL degree of maturity in the IT department is a good starting point for implementing information security management in IT departments (Federal Office for Information Technology Security Germany, 2005).

4. Situation in Germany

4.1 General

On the 24th of July in 2015, the Federal Office for Information Security passed a bill, the IT Security Law (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 2015) in Germany requiring default providers (supplier in critical infrastructures) and companies that exceed legally determined threshold values to implement information security management systems. Prior to this bill, the German government had a law in place that demanded companies to adopt an organization-wide risk management system that should ideally include the IT department as well. However, many companies did not follow the demands to take into account the IT department in the practical implementation of those risk

management systems. With the introduction of the IT security law in 2015, the government now made it mandatory for companies to implement an information security management system according to ISO 27001 in all IT departments.

There are no laws in place that would require companies to adopt ISO 20000-1. However, the IT service management system according to ISO 20000-1 offers an ideal foundation to support the information security management system (required by law). A company that has already implemented an IT service management system meets many of the requirements for their IT department that they would need to implement for the IT security management system according to ISO 27001. Since the core processes incident management, change management, service request management, problem management are already contained in an IT service management system, the implementation of the processes according to ISO 27001 often only require an extension of the processes already in place through the IT service management system (Federal Office for Information Technology Security Germany, 2005).

4.2 IT Security Law

This Federal Office for Information Security bill got passed in Germany on the 24th of July in 2015. Section 8 of the bill requires default providers in the sectors of energy, information security and telecommunications, transport and traffic, health, water, nutrition as well as finance and insurance to implement information security management systems. The law requires companies to adhere to a minimum level of IT security, to prove verification through security audits, and to implement and maintain procedures to report significant IT security incidents to the Federal Office for Information Security (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 2015).

The threshold values in order to determine which companies' falls under the IT security law vary depending on the industry the company operates in. In general, the threshold value requires all companies (operating in one of the industry mentioned earlier) that supply 500,000 citizens or more to be in compliance with the bill. This makes a total of 700 companies in Germany. For some industries, the 500,000-rule could not be used as a measure. Therefore, the government published an attachment to the German Federal IT-Security Law that specifically outlines the certain threshold values for each industry.

The document brings forward specifically designed formulas that are followed by grids that restate the particular threshold values that companies can use as reference. For example, the document defines that companies operating in agricultural food production need to implement those requirements when exceeding 334,000 tons of food per year or 274.5 million liter per year (Federal Ministry of the Interior Germany, 2015).

Additionally, there are many companies that do not fall under the IT security law directly and are therefore not required to implement an IT security information management system by law, but have to comply with the requirements in an indirect way. Part of the IT information security management system is that the company has to require all of its suppliers to adopt an IT information security management system as well, because only then can they guarantee that their data are secure. As a result, many more than the original 700 companies that directly fall under the IT security law have to implement an IT information security management system, which by implication, creates an enormous demand for consulting expertise in Germany.

The bill requires companies to secure their data in IT departments in order to prevent incidents in relation to data confidentiality, availability, integrity and accountability and that they can guarantee the confidentiality, availability, integrity and accountability of their information technology system. The IT information security system according to ISO 27001

meets all those demands that are set by the government in the bill. However, upon setting the scope for the information security management system, the critical infrastructure of an organization has to be part of it. If the scope is not set accordingly, the company will not meet the requirements of the bill. Therefore, this is a potential driver for the demand of ISO consulting, as companies might seek to bring in an external expert on information security management systems to ensure that they will be in compliance with governmental requirements when setting up the scope.

Organizations, to which this bill applies, have to be in compliance with ISO 27001 two years after it got enacted. The government decided that the companies have to present their certificate of compliance of the standard by the 31st of January in 2018. After they have initially done so, they have to report back to the Federal Office of Information Security every two years and provide further audits or certification as proof that they are able to continuously meet the requirements of the bill. Organizations who are not able to be in compliance with the bill due to methods implemented that only meet the requirements in part, not in the right way, not at all or not at the due date have to pay a penalty charge of up to 100,000€ every time the Federal Office of Information Security demands proof of compliance (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 2015).

5. Situation in the United States

5.1 General

The government of the United States has passed a number of laws on the federal level in an attempt to make data more secure. The purpose of those cyber security regulations is to make it mandatory for companies to equip themselves against possible cyber-attacks aimed at stealing intellectual property or confidential information. The majority of the cyber security regulations are created by Executive Branch directives and legislations from Congress.

"The US has also led the way for the world not only on establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect personal data from consumers, employees and other individuals" (Raul, 2014, p. 269). However, cyber security regulations are mainly directed at specific industries and there is no single federal privacy law. There are many regulations on the state level that require federal banking, health-care and communicative agencies to implement safeguards against cyber-attacks and report data breaches.

The three main federal regulations include the Health Insurance Portability and Accountability Act (HIPPA) of 1996, the Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act) and the Homeland Security Act of 2002 (including the Federal Information Security Management Act). Those three federal regulations require healthcare organizations, financial institutions and federal agencies to secure their information and data. However, the scope of those regulations are not clearly stated and only require a "reasonable" level of security. The Federal Information Security Management Act requires federal agencies to develop mandatory policies and guidelines on information security, but does not make it mandatory for any private entity (Appknox, n.d.).

5.2 Baldrige Award and Deming Prize (Total Quality Management)

Modern efforts in the United States to introduce changes in business practices and improvements in business processes can be traced back to the work of Edwards Deming and Malcolm Baldridge. US Secretary of Commerce Malcolm Baldridge launched the Malcolm Baldrige National Quality Award in 1987. The award is managed by the U.S. Commerce Department's National Institute of Standards and Technology (ASQ, 2018a). Baldridge, together

with Deming and the US Department of Navy, helped to initiate the Total Quality Management movement (Houston & Dockstader, 1997).

Total quality management recognizes that it is not the product or service that should be looked at but the interconnection of functions across an entire organization in order to promote customer satisfaction by continually improving operations, management processes and products.

Japan was the first country to initiate TQM by introducing the Deming Award and has received world-wide recognition that open up many markets internationally for their products. The Deming Prize was established in 1951by Dr. W. Edwards Deming and is used in Japan as a tool to spread the knowledge of a proven and established method for continuous improvement that leads to success. It awards companies that continuously apply Company-wide quality control through statistical quality control techniques (Izadi, & Kashef, & Stadt, 1996).

The United States has been reluctant at first to implement TQM, but has been forced to do so in 1987, as their products lacked quality and productivity which resulted in a weak position to compete globally. The criteria of the Baldrige Award help companies to assess strategic improvement, enhance planning for continuous improvement and increase customer satisfaction. The award only applies to American companies, but the criteria are used by foreign companies to internally assess their organization (Izadi, & Kashef, & Stadt, 1996).

ISO 9000 focuses on continuous quality improvement and was the European answer to the Baldrige Award and Deming Prize. The objective of the standard is to promote operating efficiency and productivity while reducing costs world-wide. The intention of the standard is to stimulate trade by providing assurance to a third-party that the organization can meet specifications and perform the negotiated standard (Izadi, & Kashef, & Stadt, 1996).

5.3 Framework for Improving Critical Infrastructure Cybersecurity

The United States government recognizes the importance of the protection of crucial information as cybersecurity, especially for the growing role of organizations in critical infrastructures on national security. As a result, the National Institute of Standards and Technology (NIST) has published a framework that guides those organizations in critical infrastructures in order to assess its risk tolerance and the possible measures that can be implemented in order to reduce the risk of cyber threats. The framework has been established in collaboration with the government and the private sectors of the industries in those critical infrastructures. However, the framework is a *voluntary* implementation and does not place additional requirements on businesses. The framework establishes defined roles, responsibilities, policies and processes in order to enhance and ensure the safety, security, business confidentiality, privacy and civil liberties of the information possessed by an organization. Everyone can participate in the framework (NIST, 2014).

The framework acknowledges the importance of the integrity of information security in the United States. The document references globally recognized standards for cybersecurity, such as ISO 27001.

As a result of the NIST framework and the Presidents Executive Order (13636) the demand for consulting of ISO 27001 may increase as companies seek to comply with the framework. Even though this is a voluntary framework, companies in critical infrastructure industries should be aware of the existence of this framework and how they can benefit from the implementation of ISO 27001. This is a possible opening of a driver of demand in the United States that can be stimulated by the consulting companies themselves (NIST, 2014).

6. Situation in India

6.1 General

The Indian government put data regulation and protection policies in place, in order to prevent data breaches from cybercrime and make information technology more secure. The handling of personal data is regulated by the Indian Information Technology (IT) Act 2000. In addition, certain industries have imposed additional data protection obligations such as banking, telecommunication and medical practices (Mathias & Naqeeb, 2017).

For private organizations, the Act does not require the implementation of a particular security standard, but they suggest the implementation of ISO 27001. However, the banking industry has regulations in place that specifically demands that all banks to follow ISO 27001. Also, the Indian securities exchange regulations require stock exchanges, depositories and clearing corporations to follow ISO 27001 as well. This regulation has been prescribed by the Reserve Bank of India outlining guidelines on information security, electronic banking, technology risk management and cyber frauds (Mathias & Naqeeb, 2017).

6.2 Drivers of Demand of ISO 27001

One of the drivers to implement ISO 27001 in India is the need to keep their information technology secure in order to prevent hackers from obtaining crucial data that would lead to the destruction of the company. Such damages can be in form of severe damage to a company's reputation or incurring financial fines, if their security systems are insufficient.

Moreover, globalization is another source that drives the demand for ISO 27001 in India. India is a major hub for big international corporations that are looking to outsource their IT departments to IT provider in India. Those companies insist on security certification in order to ensure that the companies they are outsourcing to meet the standards from their

respective country. As a result, many Indian companies are looking to become ISO 27001 certified in order to be able to compete on the international market (IT Governance Ltd., 2011).

Furthermore, the ISO 27001 standards gets particularly supported by the government in India. The Indian Department of Information Technology in the Ministry of Communication made a statement in April 2011 declaring that companies who have implement ISO 27001 complied with all security practices and regulations that need to be implemented by law (IT Governance Ltd., 2011).

As a result, the government plays an important role in India as a major driver in the growth of adopting ISO 27001. ISO 27001 not only allows Indian companies to compare themselves on an international level and companies outside India to assess their compliance, but it also gives companies the reassurance that they comply with all governmental regulations and that no fines will be imposed on them (IT Governance Ltd., 2011).

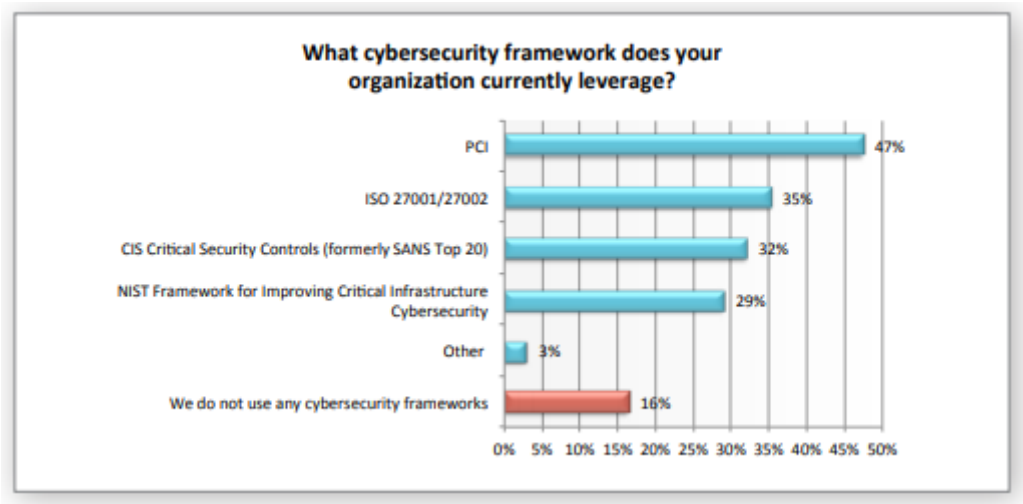
Since India is one of the countries with the highest rate of adoption of ISO 27001 in the world (ISO, 2017) the drivers of the demand in India (mentioned above) give us crucial inside behind the motivation of a company's willingness to comply with ISO 27001. We can reasonably infer from this, that the demand to implement ISO 27001 is directly linked to governmental regulations, since the government is a major driving force behind the demand in India.

7. Adoption Rates of the Various Frameworks

There are many different frameworks that help companies to make their data more secure. Those frameworks include ISO 27001, CIS Critical Security Controls, NIST Framework for Improving Critical Infrastructure Cybersecurity, and Payment Card Industry Data Security Council Standard (PCI). According to a Survey of 338 IT and security

professionals in the United States, 84 percent of the respondents have implemented one of the security frameworks listed above (Dimensional Research, 2016). The framework that is most frequently adopted is PCI, which is a framework for retail companies that is dependent on credit card transactions. ISO is the second most implemented framework, as it is best known on an international basis. ISO is followed by the NIST framework (Dimensional Research, 2016).

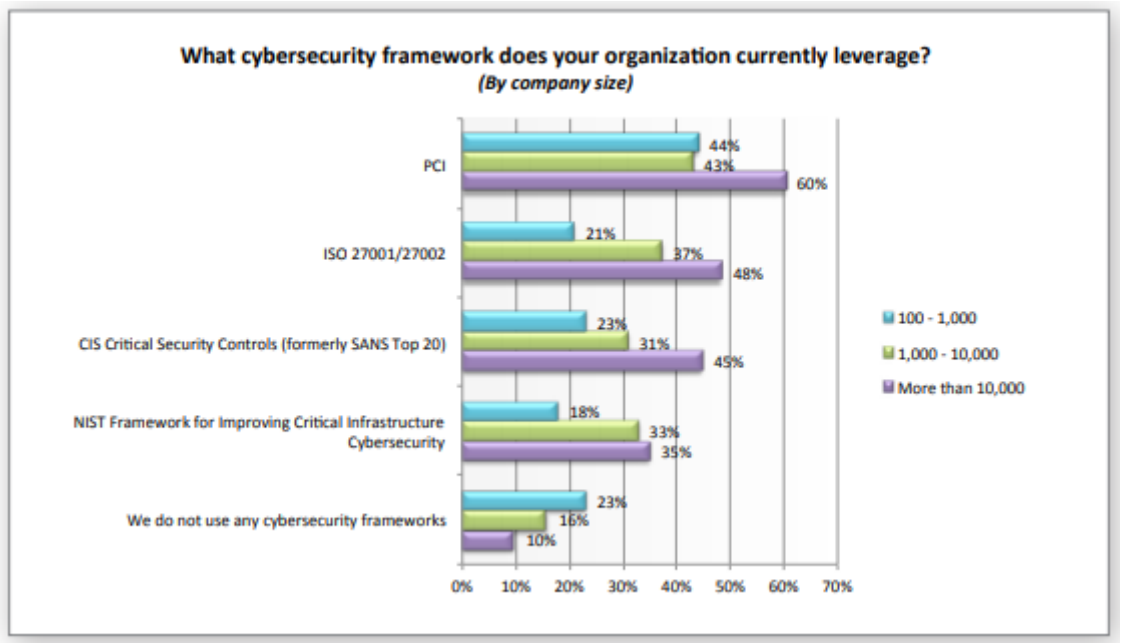
Table 6.



(Source: Dimensional Research, 2016)

The survey further shows that not only big corporations have implemented security frameworks (90 percent), but that also smaller companies increasingly focus on adopting measures that help make their data more secure (77 percent).

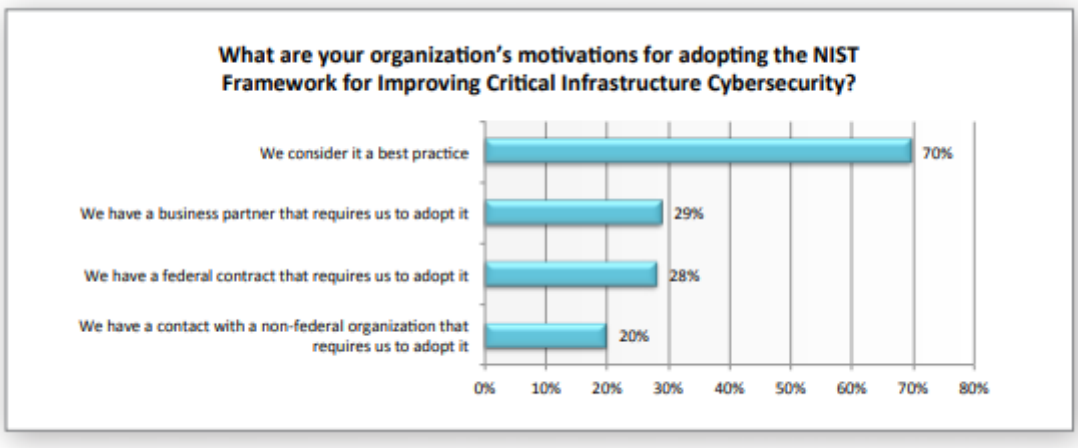
Table 7.



(Source: Dimensional Research, 2016)

Moreover, the survey assessed the various needs of companies to implement those frameworks in their organizations. The majority of respondents adopted a security framework, because it was considered best practice, followed by business partners and federal contracts that require those companies to have security frameworks in place (Dimensional Research, 2016).

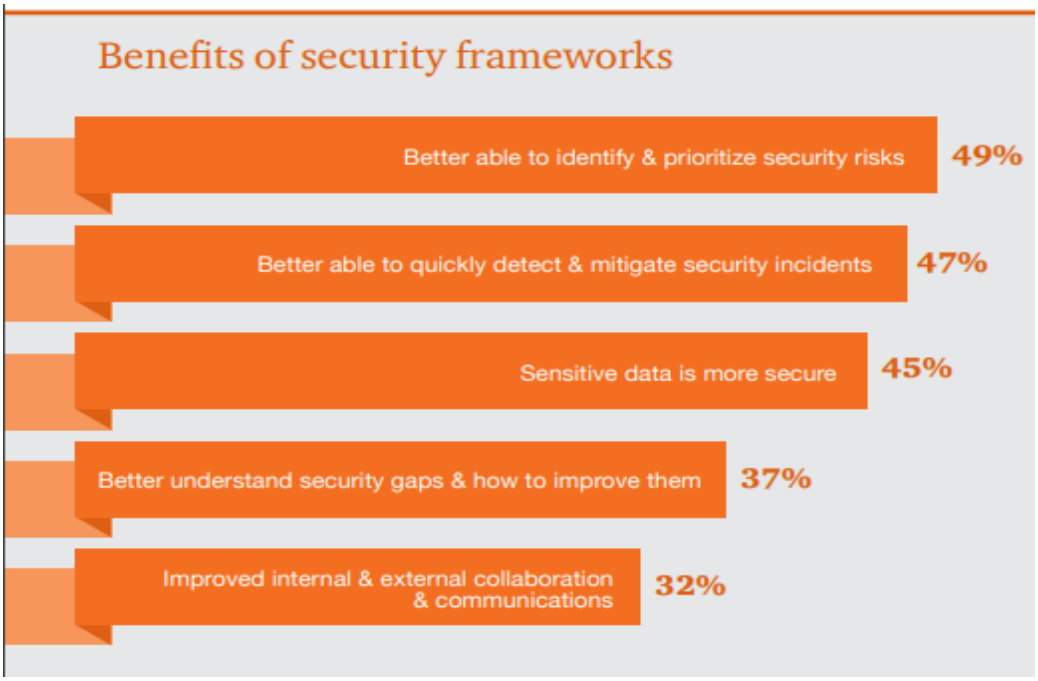
Table 8.



(Source: Dimensional Research, 2016)

Respondents from another survey on risk-based cybersecurity frameworks conducted by PwC claim to have adopted a framework as it enhances their ability to identify and prioritize security risks, detect and mitigate security incidents, secure sensitive data, understand and improve security gaps, and improve internal and external collaboration and communication (PwC, 2016).

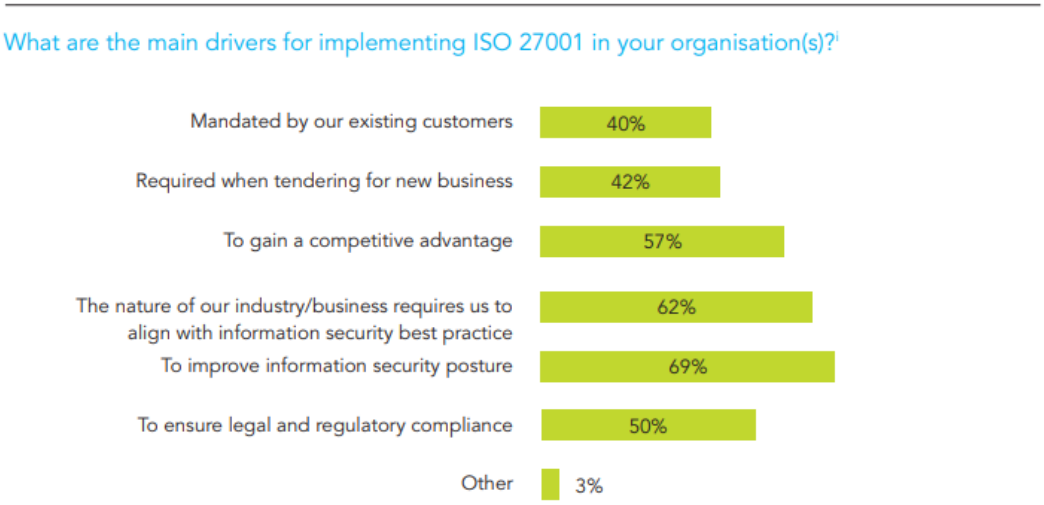
Table 9.



(Source: PwC, 2016)

According to the ISO 27001 Global Report, companies who have adopted ISO 27001 list the following reasons behind obtaining certification on the standard.

Table 10.



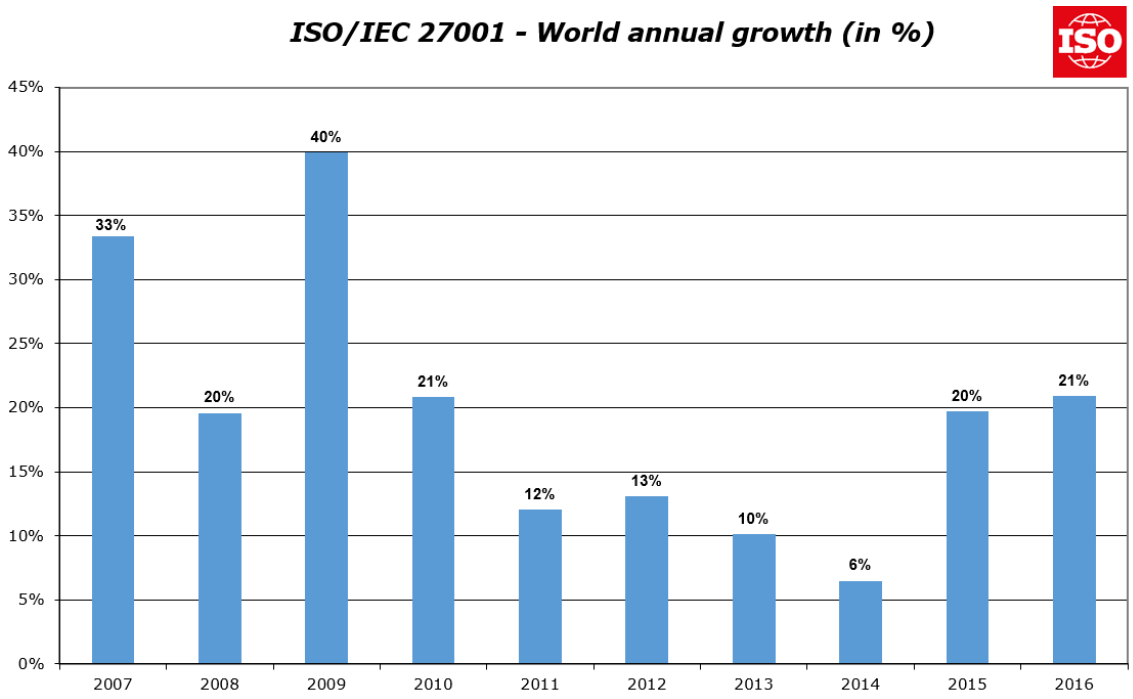
(Source: IT Governance Ltd., 2015)

7.1 The ISO Survey

ISO conducts an annual study where they publish the amount of certificates issued to companies that have implemented management systems according to one of their international standards. The ISO survey is comprised of Excel files that cover surveys from every year since the specific standard had been introduced. The survey only considers those certifications that have been issues by certification bodies accredited by national members of the International Accreditation Forum.

When looking at the survey results for ISO 27001, there were 5,797 certificates issued in 2006 and 33,290 certificates issued in 2016. This shows that overall, the adoption rate of ISO 27001 has been continuously growing since the standard was first introduced. The standard experienced the highest amount of growth of 40 percent in 2009. After that the annual growth steadily decreased until 2014 with a low of 6 percent. In 2015 and 2016 the amount of certifications issued in those years rose again to 20 and 21 percent. Unfortunately, the ISO survey for 2017 has not been released yet (ISO, 2017).

Table 11.



(Source: ISO, 2017)

Furthermore, the survey identifies the top five industries that have obtained the highest amount of certifications. For ISO 27001, the by far leading industrial sector is Information Technology with 6,578 certificates, and financial intermediation, real estate, renting is listed on number 5 with 250 certificates issued.

Table 12.

Top five industrial sectors for ISO/IEC 27001 certificates 2016		
1	Information technology	6578
2	Other Services	1432
3	Transport, storage and communication	401
4	Electrical and optical equipment	311
5	Financial intermediation, real estate, renting	250

(Source: ISO, 2017)

If we look at the per country numbers, we can see that the top six leading countries are China, India, Japan, Germany, United Kingdom and United States. Japan ranks first with a total of 8,945 certificates, then the United Kingdom (3,367 certificates), India (2,902

certificates), China (2,618), Germany (1,338 certificates), and then the Unites States (1,115 certificates).

When looking at the survey results for ISO 20000-1, a total of 2,778 certificates were issued in 2015 and a total of 4,537 certificates were issued in 2016. There are no data available for the previous years since the standard was first published in 2015. As a result, the standard has experienced a growth rate of 63 percent over the course of those two years. ISO relates the strong growth for ISO 20000-1 to the fact that is it a relatively new standard to the market.

The top five industries identified for ISO 20000-1 are almost in accordance with the top five industries of ISO 27001. The information technology sector is listed second place with a total number of 876 certificates issued.

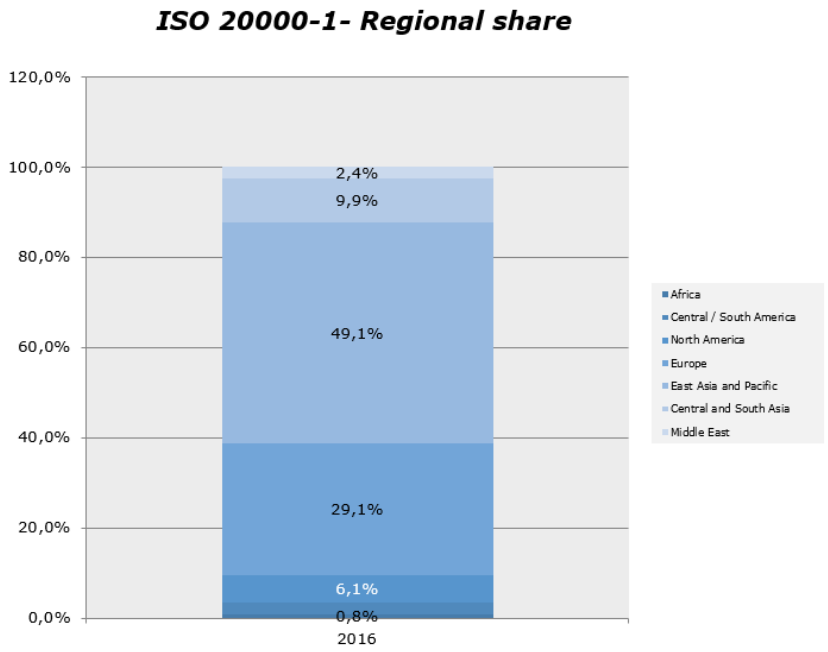
Table 13.

Top five industrial sectors for ISO 20000-1 certificates 2016			
1	Machinery and equipment		3180
2	Information technology		876
3	Other Services		47
4	Electrical and optical equipment		45
5	Health and social work		44

(Source: ISO, 2017)

The top 6 countries for the implementation rate of ISO 20000-1 are China, India, Japan, Germany, United Kingdom and the United States. China has by far the most certificates with a total of 1,666, then India (442), Japan (285), United Kingdom (217), United States (175), and then Germany (104). As a result, East Asia and Pacific make up 49.1 percent of the regional share and Europe 29.1 percent.

Table 14.



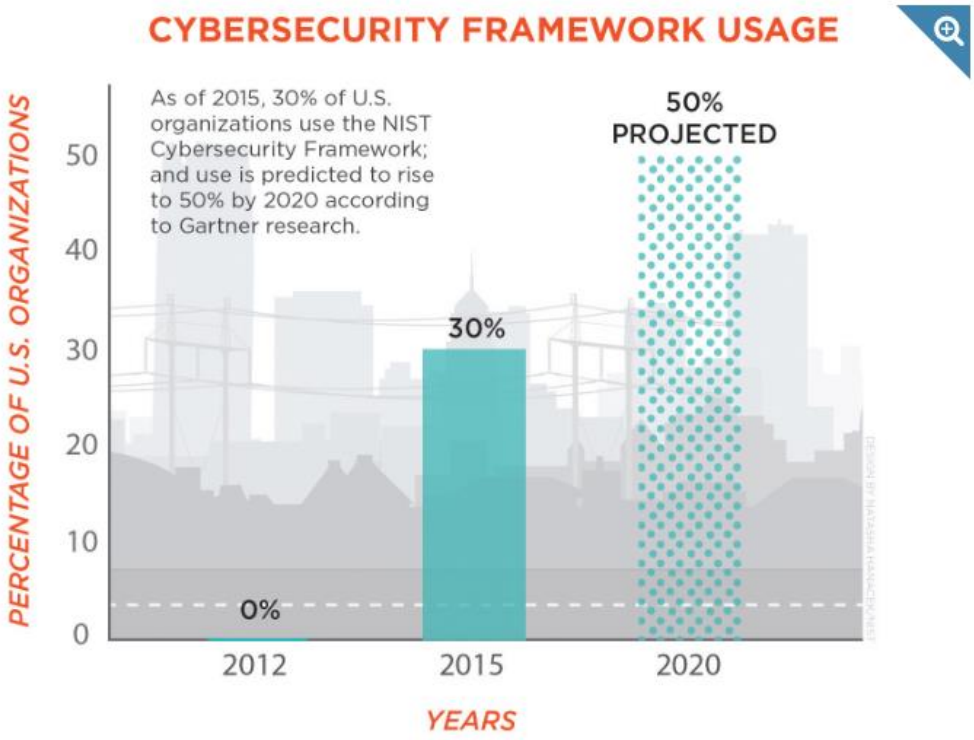
(Source: ISO, 2017)

7.2 NIST Framework for Improving Critical Infrastructure Cybersecurity

The NIST Framework for Improving Critical Infrastructure Cybersecurity is one of the frameworks that has emerged as de facto standard together with the ISO 27001 framework in the finance industry (FSSCC, 2017). According to a survey conducted by PwC (PwC, 2016), 91 percent of more than 10,000 respondents of IT and security practices have adopted a risk-based cybersecurity framework of which ISO 27001 and the NIST Framework for Improving Critical Infrastructure Cybersecurity were adopted most often.

According to the research institute Gartner, the NIST Framework for Improving Critical Infrastructure Cybersecurity is used by 30 percent of all companies in the United States. By 2020, Gartner projects the adoption rate of the framework to be 50 percent of all companies. The companies that have already adopted the framework currently operate in 16 different critical infrastructure industries and in more than 20 states (NIST, n.d.).

Table 15.



(Source: NIST, n.d.)

8. The Interviews

The interviews conducted for this research have confirmed that most companies seek external help when implementing ISO 27001 and ISO 20000-1. The implementation of those management systems in an organization is an undertaking that takes on average two to three years. This indicates the complexity of the standards and that extensive knowledge is essential in order to successfully implement the management systems. If a company would choose to implement the standard by itself, the project is likely to take even longer which would correlate with increased cost and perhaps jeopardize the long-term gains.

In general, companies rely on the experience of external consultants who have an end-to-end understanding of the standard and how the management system should be best implemented, in order to meet all demands and requirements. This ensures that a company

will obtain the external certification, which in turn will help the company with their competitive edge.

According to the Chief Executive Office of DSP IT Service GmbH (DSP), companies experience increase pressure to align their IT with best practices and operate their IT in a professional way, as the dependency of the operational business of IT increases. Furthermore, DSP's clients hire them to implement ISO 27001 in order to proactively take measures against gaps in their security systems. The clients indicate that the people working in their IT departments are very technical, which makes it hard for them to understand business processes and their client's business structure. As a result, they need an external consultant to implement the ISO standards for them.

PricewaterhouseCoopers in Germany confirmed in our interview that their (PwC's) clients hire them for their consulting expertise in the area of ISO 27001, as the clients do not have enough internal resources to conduct such major projects by themselves. Due to digitalization of business operations, the demand on IT has been increasing tremendously. This often results in shortages in capacity and resources in PwC's client IT departments, which makes them unable to implement ISO 27001 on their own.

Another company, Stadtwerke Schwäbisch Hall, falling under the German IT security law, hired external consultants to implement ISO 27001 and ISO 20000-1. They also indicated that they hire external consultants due to their lack of knowledge on the standards and the lack of resources to complete such projects on their own.

All of the companies interviewed said that certification on ISO 27001 is mandatory in order to be able to compete in the market. Even though they did not all fall under the IT security law, these consulting companies said they need the ISO certification to even be considered by prospective clients in response to their requests for proposals. All the companies indicated that in every request for proposal that they obtain, the client directly asks

for the company's certification on ISO 27001. If the company cannot provide their client with such a certification, they are unable to take part in the bidding. As a result, the companies have indicated that one hundred percent of their clients ask for their certification on the standard ISO 27001.

In addition, DSP IT Service GmbH uses ISO 20000-1 as the foundation to build upon when implanting ISO 27001. It is easier for a company to obtain certification on ISO 27001, when they already have aligned their IT to best practices and have reached a certain level of process maturity. DSP also indicated that companies need to: 1) automate recurring business activities to reduce cost, by ensuring service around the clock, faster service of better quality, and freeing up support capacities that can be used otherwise; 2) professionalize their IT; and 3) be able to better market themselves as the drivers of demand for ISO 20000-1. Since not all clients directly demand certification on that standard, many companies do not seek to obtain certification, but simply align their IT with best practices.

DSP IT Service GmbH also indicated that the demand for their consulting services for ISO 27001 has increased by fifty percent since the introduction of the IT security law, and PwC indicated that the demand for their consulting expertise has increased by twenty percent.

DSP IT Service GmbH and Exxeta GmbH (an IT consulting company) both indicated that they expect to see an increased demand for their consulting expertise in the future. According to those two companies, there will be an increased trend due to the fact that governments will become more aware of the role they play in information security, increased awareness of the public in cases of security breaches, increasing costs and damages in cases of security breaches, and that information security is an integral part of an information security management system.

9. CONCLUSION

In conclusion, this study confirms our hypothesis that the demand for ISO consulting is rising due to the increasing demand of the two international standards, ISO 27001 and ISO 20000-1. We have found that there are a number of different factors that drive the demand for the implementation of ISO 27001 and ISO 20000-1 and thus the services of ISO consulting firms. Those factors include a company's need to implement best practices in their organization, adherence to government regulations, being able to compete in the market on a global basis, as well as implementing a security framework that sufficiently protects their information. ISO 27001 and ISO 20000-1 enable a company to operate in more successful ways by reducing the cost of operations and reducing the risk of severe damages to a company's reputation in case of any cyberattacks.

Moreover, the demand in Germany is currently driven by the new IT security law that companies have to adhere to by January 31st in 2018. The IT security law demands companies implement ISO 27001 and promotes the implementation of ISO 20000-1 by using the synergy effects between those two standards. Thus, the next ISO Survey conducted in 2018 should depict a major increase in the adoption rates of ISO 27001.

In the United States, there are no governmental regulations that mandate a company in the private sector to implement security frameworks. By examining the ISO Survey, we can see that the adoption rates of ISO 27001 are lower in the United States (ISO, 2017). This is due to the fact that many companies in the United States adopt the NIST Framework that stands in direct competition with ISO 27001. However, the NIST Framework references ISO 27001 in many parts.

India has by far one of the highest adoption rates of ISO 27001, where the government is a major driver behind the adoption of ISO 27001. This reinforces the fact that the government plays an important role in promoting companies to adopt safety measures to

secure valuable assets. The lack of governmental regulations in the United States is, therefore, a possible source and explanation for the fact that the adoption rates of ISO 27001 are rather low in comparison to other countries.

The standards are complex in nature and most companies do not have enough internal resources to implement the standards on their own. Also, the introduction of an Information Security Management System requires adoption by the *entire* organization and not just single departments. The scope of such a system requires deepener knowledge of the standards in order to successfully implement the management system and for the company to benefit from its long-term effectiveness.

Reflecting the complexity of ISO and the broader issue of professional development in ISO consulting firms: "… organizations shouldn't shy away from investing in professional staff training and calling upon external experts in order to complete the project successfully within the timeframe they have set." (IT Governance Ltd., 2015).

10. ADDENDUM

Questionnaire used for companies receiving ISO consulting services:

- Do you have to adhere to the requirements of the new IT security Law?
    - If yes:
        - Did you already implement/ work in implementing the security management system according to ISO 27001?
        - How did you approach implementing it?
            - Did you implement ISO 27001 yourself, or did you need external help in the form of a consultant/ will you need external help?
                - In which form did you need external help?
            - Did you introduce ITIL based processes in your IT?
        - Who certified/ will certify you?
            - Contact information from your certifier?
        - Did you already exploit the synergy effects between the standards ISO 20000-1 and ISO 27001?
            - If not:
                - Are you aware of the Synergy effects between those two standards?
                - Are you planning to implement ISO 20000-1, or do you deem this step as not relevant for your organization?
    - If not:
        - Are you familiar with the standard ISO 27001?
        - Do you think it would be useful for BMW Bank to implement this standard?
            - What are your reasons for implementing ISO 27001?
                - Clients demand the certification? (Ex. Requirement to continue or pick up a contract, tender requirements…)
                - Self-motivation for professionalization
                - Different reason
        - Are you using a different standard?
            - If yes: which one?
        - Did you encounter security incidents in the past?
            - Did you examine the incident in a structured manner and could you identify the damage?
                - Which system did you follow?
                - Did you develop concrete measured based on the incidents to prevent future similar incidents?
- Are you familiar with the standard ISO 20000-1?
    - Are you certified on this standard/ are you planning to get certified on it?
        - If yes: Why did you get certified on this standard/ why did you implement it?
            - How would you classify the importance of the ITSM in your operation?
                - High (IT – and general management are informed on a regular basis)
                - Medium (IT management is informed)
                - Low (IT service manager takes care of it)
                - Not at all, if someone escalates, we will take care of it
            - How would you evaluate the satisfaction of your clients?
                - Are there IT user surveys?
                - Did you define a complaint management process?
        - If not: Why not?
            - How many IT workplaces/users do you oversee?
            - Are your operations process-oriented? (COBIT, MOF, ITIL, different Process Framework)
            - How is your service desk structured?

        - Do you have a dedicated service desk?
        - Service Desk as Single Point of Contact
        - No, everyone operates the telephone
    - Do you open and maintain a ticket for every new request for IT?
        - Do you categorize your tickets and handle them accordingly? (Incidents, Request for Change, Service Request, Problems)
    - Do you use ITSM tools?
        - Service catalogue
        - Ticketing system
        - Asset & Configuration Mgmt System
        - License Mgmt System
        - Software Mgmt System
        - Mobile Device Mgmt System
        - Identity & Access Mgmt Systems
    - Do you automate recurrent IT business incidents?
        - (exp.: reset passwords, Onboarding, Offboarding, User Rights Administration & Mgmt, Client Software Mgmt,…)
    - Do you have a meaningful ITSM/ SLA-reporting?
        - Daily reports
        - Monthly reports
        - none
        - Are the reports used for Quality management?
    - Do you have a continual improvement process with a service improvement plan (o.ä.)
- Do you have clients that specifically ask for an ISO 27001 or ISO 20000-1 certificate?
    - How would you assess the trend for consulting for ISO 20000-1 and ISO 27001?
    - Is it possible for you tell me the percentage increase of clients that demand the ISO 27001 certificate from you since the introduction of the new IT security law?
    - Did clients already asked of you to be ISO 27001 certified before the introduction of the new IT Security Law?
    - Can you refer me to someone else that can give me insight in their approach to implementing ISO 27001?
- Do you know further contact persons, also someone who is certified on the standards ISO 20000-1?

Questionnaire used for ISO consulting companies:

- Does your company offer consulting services on ISO 27001?
    - Since when do you offer the service?
    - What was your motivation behind entering that market?
    - Are you certified on ISO 27001 yourself?
        - What was your motivation behind obtaining certification? Do clients explicitly ask for that certification?
        - Did you use external consultants to obtain certification or did you implement the standard yourself?
    - Why do clients hire you for the service? What is their motivation?
        - What are the main motives of your clients wanting to implement ISO 27001?
        - What are the main motives of your clients to hire you as an external consultant?
    - How many more clients are asking for your external expertise on ISO 27001 since the introduction of the IT Security Law? (in percentage)
- Does your company offer consulting services on ISO 20000-1?
    - Since when do you offer the service?
    - What was your motivation behind entering that market?
    - Are you certified on ISO 20000-1 yourself?
        - What was your motivation behind obtaining certification? Do clients explicitly ask for that certification?

        - Did you use external consultants to obtain certification or did you implement the standard yourself?
    - Why do clients hire you for the service? What is their motivation?
        - What are the main motives of your clients wanting to implement ISO 20000-1?
        - What are the main motives of your clients to hire you as an external consultant?
- In comparison to ISO 27001, how many clients require your service on ISO 20000-1?
- Clients that require your service for ISO 20000-1, do they also hire you for ISO 27001?
    - Do you alert your clients on the existing synergy effects between ISO 27001 and ISO 20000-1?
- What is the percentage share of clients directly asking for your ISO 27001/ ISO 20000-1 certificate?
- How would you evaluate the trend in ISO consulting on ISO 27001/ ISO 20000-1?

11. Bibliography

Ahlbäck, K., Fahrbach, C., Murarka, M., & Salo, O. (2017). *How to create an agile organization*. McKinsey & Company.

Ames, M., Blake, R., Caurso, M. J., & Heinle, P. (2011). *Why Management System Standards Add Value, Part 1*. Retrieved from https://www.qualitydigest.com/inside/quality-insider-column/why-management-system-standards-add-value-part-1.html#.

Antaris Consulting. (2016). *The History of ISO Standards*. Retrieved from https://antarisconsulting.wordpress.com/2016/09/14/the-history-of-iso-standards/.

Appknox. (n.d.). *A Glance at the United States Cyber Security Laws*. Retrieved from https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/.

ASQ. (2018a). *Malcom Baldrige National Quality Award*. Retrieved from http://asq.org/learn-about-quality/malcolm-baldrige-award/overview/overview.html

ASQ. (2018b). *What is a Quality Management System (QMS)?—ISO 9001 & Other Quality Management Systems.* Retrieved from http://asq.org/learn-about-quality/quality-management-system/.

Block, P. (2011). *Flawless Consulting: A Guide to Getting Your Expertise Used*. San Francisco, Ca: Pfeiffer.

Business.com., (2018). *Trends in IT Consulting*. Retrieved from https://www.business.com/articles/trends-in-it-consulting/.

BusinessWire, (2016). *Top 5 Emerging Trends Impacting the Global IT Consulting Services Market until 2020*. Retrieved from https://www.businesswire.com/news/home/20161020005073/en/Top-5-Emerging-Trends-Impacting-Global-Consulting

Deming, E., (1986) *Out of the Crisis.* MIT Press. *ISBN 0-911379-01-0. OCLC 13126265*

Dimensional Research (2016). *Trends in Security Framework Adoption: A Survey of IT and Security Professionals.* Doi:https://static.tenable.com/marketing/tenable-csf-report.pdf.

Federal Office for Information Technology Security Germany. (2005). *ITIL und Informationssicherheit* (pp.1-32). Berlin: HiSolutions AG.

Federal Ministry of the Interior Germany. (2015). Verodnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).

Forbes Insight (2017). *The State of IT Service Management, 2017.* Retrieved from http://www.bmc.com/content/dam/bmc/migration/pdf/Delivering-Value-to-Today%27s-Digital-Enterprise-FINAL.pdf.

FSSCC. (2017). *Financial Services Sector Specific Cybersecurity "Profile".* NIST Cybersecurity Workshop. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf.

Gemalto (2018).*The Breach Level Index*. Retrieved from https://breachlevelindex.com/data-breach-database.

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. (2015). *IT Sicherheitsgesetz*. Teil I Nr. 31 Bundesgesetzblatt 1324-1331 (enacted).

Greentarget.com (2016). *2017 Management Consulting Outlook*. Retrieved from http://greentarget.com/wp-content/uploads/2017/03/Management-Consulting-Outlook-2017-Final.pdf.

Houston, A. & Dockstader, S. L. (1997), *Total Quality Leadership: A Primer (PDF)*, Washington, D.C.: United States Navy, pp. 10–11, OCLC 38886868, 97-02, retrieved 2013-10-19

IbisWorld (2016) *"Management Consulting Industry Report". ibisworld.com.*

Ibis*World*, (2017). *IT Consulting - US Market Research Report*. Retrieved from https://www.ibisworld.com/industry-trends/market-research-reports/professional-

scientific-technical-services/professional-scientific-technical-services/it-consulting.html.

ISO. (2010). *Information technology – Service management – Part4: Process reference model* [PDF].ISO.

ISO. (2011a). *Information technology – Service management – Part1: Service management system requirements* [PDF].ISO.

ISO. (2011b). *Information technology – Service management – Part2: Guidance on the application of service management systems* [PDF].ISO.

ISO. (2012). *Information technology – Service management – Part3: Guidance on scope definition and applicability of ISO/IEC 20000-1* [PDF].ISO.

ISO. (2013a). *Information technology – Service management – Part5: Exemplar implementation plan for ISO/IEC 20000-1* [PDF].ISO.

ISO. (2013b). *Information technology – Security techniques – Information security management systems – Requirements* [PDF]. ISO.

ISO. (2017). *ISO Survey*. Retrieved from www.iso.orf/the-iso-survey.html and http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. (2018). *Management System Standards*. Retrieved from https://www.iso.org/management-system-standards.html.

ISO Quality Services Ltd. (2018). *What is ISO*. Retrieved from https://www.isoqsltd.com/about-us/what-is-iso/.

IT Governance Ltd. (2011). *Information Security in India: A new approach to ISO 27001*. Retrieved from https://www.itgovernance.co.uk/blog/information-security-in-india-a-new-approach-to-iso-27001/.

IT Governance Ltd. (2015). *ISO 27001 Global Report*. Retrieved from http://www.consultia.co/wp-content/uploads/2015/05/ISO27001-Global-Report-2015.pdf.

Izadi,M., Kashef, A. E., & Stadt, R. W. (1996). *Quality in Higher Education: Lessons Learned from the Baldrige Award, Deming Prize, and ISO 9000 Registration.* Journal of Industrial Teacher Education, 33, 2nd ser. Retrieved from http://scholar.lib.vt.edu/ejournals/JITE/v33n2/izadi.html

Jäntti, M., & Cater-Steel, A. (2017). *Proactive Management of IT Operations to Improve IT Services.* Journal of Information Systems and Technology Management: JISTEM, 14(2), 191-218. http://0-dx.doi.org.liucat.lib.liu.edu/10.4301/S1807-17752017000200004 Retrieved from http://0-search.proquest.com.liucat.lib.liu.edu/docview/1944207856?accountid=12142

Johnson, M. W., Hately, A., Miller, B. A., & Orr, R. (2007). *Evolving standards for IT service management.* IBM Systems Journal, *46*(3), 583-597. Retrieved from http://0-search.proquest.com.liucat.lib.liu.edu/docview/222431491?accountid=12142.

Johnston, S. J. (2013) Harvard Business Review, March 2003; *The Future of IT Consulting*. Retrieved from https://hbswk.hbs.edu/item/the-future-of-it-consulting.

Keel, A. J., Orr, M. A., Hernandez, R. R., Patrocinio, E. A., & Bouchard, J. (2007). *From a technology-oriented to a service-oriented approach to IT Management*. IBM Systems Journal, 46(3), 549-564. Retrieved from http://0-search.proquest.com.liucat.lib.liu.edu/docview/222436140?accountid=12142.

LS_10/12/2017. CEO Interview of DSP IT Service GmbH.

Mathias, S. & Naqeeb, A. K. (2017). *Data Security and Cybercrime in India*. Retrieved from https://www.lexology.com/library/detail.aspx?g=e7b6cb3b-f534-45ba-b1fb-86d7ed39e558.

Mesquida, A. (2014, August 07). *Integrating IT service management requirements into the organizational management system*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0920548914000786.

Naden, C (2017). *Blockchain technology set to grow further with International Standards in Pipelin*e. ISO. Retrieved from https://www.iso.org/news/Ref2188.htm.

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

NIST. (n.d.). *NIST Impacts: Cybersecurity*. Retrieved from https://www.nist.gov/industry-impacts/cybersecurity.

Parakala, K. (2016). *Top 15 Strategic Trends for Consulting and IT Services firms in 2016.* Retrieved from www.linkedin.com/pulse/top-15-strategic-trends-consulting-services-firms-2016-kumar-parakala/.

Ponemon Institute LLC (2017). *2017 Cost of Data Breach Study*. Sponsored by IBM Security. Retrieved from https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

Purba, S., & Delaney, B. (2003). *The Client Account Pipeline and the Decision-Making Process*. In IT Consulting in Tough Times: 12 Keys to a Thriving Practice. Dreamtech press.

PwC. (2016). *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security*. Retrieved from https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf.

Rasiel, E. M., & Friga, P. N. (2002). *The McKinsey Mind: Understanding and Implementing the Problem-solving Tools and Management Techniques of the World's Top Strategic Consulting Firm.* McGraw Hill.

Raul, A. C. (2014). *The Privacy, Data Protection and Cybersecurity Law Review.* Retrieved from https://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf

Schönthaler, F., Vossen, G., Oberweis, A., & Karle, T. (2010). *Business Processes for Business Communities*. Springer. doi10.1007/978-3-642-24791-0.

TÜV Süd. (2015a). *ITIL Einführung Foliensatz.* Approved Training Documents from DSP IT Service GmbH.

TÜV Süd. (2015b). *IT Strategy.* Approved Training Documents from DSP IT Service GmbH.

TÜV Süd. (2015c). *Service Design.* Approved Training Documents from DSP IT Service GmbH.

TÜV Süd. (2015d).*Service Transition.* Approved Training Documents from DSP IT Service GmbH.

TÜV Süd. (2015e). *Service Operation.* Approved Training Documents from DSP IT Service GmbH.

TÜV Süd. (2015f). *Continual Service Improvement.* Approved Training Documents from DSP IT Service GmbH.

Verlander, E.G. (2012). *The Practice of Professional Consulting* (1st ed.). San Francisco, CA, Pfeiffer.

Wood, P. (2017). *Key Trends in 2017 for the Consulting Industry*. Retrieved from www.infodesk.com/consulting-industry/key-trends-in-2017-for-the-consulting-industry.