A Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics.

Cybersecurity Regulations in the water sector

Level of cybersecurity maturity in the Portuguese water sector

Samuel Darius Kührer

Work project carried out under the supervision of:

Professor Paulo Faroleiro

February 4th, 2022

Cybersecurity Regulations in the water sector

Level of cybersecurity maturity in the Portuguese water sector

ABSTRACT

Cyber-attacks are a massive threat for public organizations in the water sector. Protecting sensitive data and securing plants or technological assets are on the top priority list of governments worldwide. To advance this critical field of research, this study examined the Portuguese water sector's cybersecurity maturity based on the cybersecurity maturity assessment framework (CMAF). The outcome of this study highlights the unformalized level of maturity and the lack of cybersecurity measures implemented in the Portuguese water sector. Limiting factors and interdependencies between different cybersecurity focus areas are identified, providing recommendations for the water utility and other critical sectors.

Keywords:

Cybersecurity, Water sector, CMA Framework, EU Regulations, Governance of Enterprise IT, Cybersecurity Strategy, Operational Technology, Information Technology

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

TABLE OF CONTENTS

1. INTRODUCTION

Cybersecurity issues hold power to become one of the most critical challenges of our future. Cyberattacks and cybercrime emerged as an integral threat, ranked as one of the most important law enforcement procedures in the United States (US). However, additionally, to the challenges these attacks entail for the private and business life in general, in the past decade, it is mainly the crucial infrastructures such as water supply and energy production that have come under scrutiny (Clark et al. 2017). The US Department of Homeland Security even considered the water utility sector as one of the main targets for cyber-attacks (The White House - Office of the Press Secretary 2013) in the US in 2013. Since then, it has become a matter of national security to protect the sector from cybercrime and any correlated threats.

Water systems integrate physical and computational capabilities and are thus considered a type of cyber-physical system. Traditionally, security was ensured by limited access control. In the past years, however, water utilities incorporated advanced technologies into their operations, exponentially increasing the risk for cyber threats. Particularly with the emergence and adoption of the Internet of Things (IoT), water utility providers became highly interconnected but, on the downside, faced new, more complex security challenges (Tuptuk et al. 2021). This digital transformation made even the best practice cybersecurity control measures and systems vulnerable. Simultaneously to this increase in dependence on automated processes and information technology systems, attackers have more powerful tools and methods at their disposal increasingly. Based on these developments, it is inevitable to ensure an adequate definition, implementation, and control of cybersecurity measures and processes, minimizing external and internal threats (Clark et al. 2017).

In order to secure cybersecurity more holistically, the European Commission proposed an Information Security directive in 2016, the so-called NIS directive. One central part of this initiative aims at the national supervision of critical sectors, including the water sector (Drivas

et al. 2020). Therefore, all EU countries, including Portugal, need to comply with the defined EU security requirements on a comprehensive level. The state of art literature on cybersecurity that would be needed to assess these adequate measures is, however, quite in its infancy. This is partly because cybersecurity is still a very new topic, and cyber risks have not yet been extensively explored (Kullik 2014). Nevertheless, cybersecurity ensures the unrestricted operation of IT systems. In this respect, it aims to counteract security gaps in IT systems and ward off cyber-attacks and is thus a fundamental component of a functioning supply process. Despite extensive research into protecting organizations against cyber-attacks, the many security breaches and incidents in the past have shown that cybersecurity challenges remain a severe problem (de Bruijn and Janssen 2017). Moreover, in comparison to other utilities, cybersecurity research in the water sector has not received much attention in the past. Particularly in Europe, the topic is merely addressed in this sector (Tuptuk et al. 2021).

In order to close this literature gap and to advance cybersecurity research in Europe, this research aims at assessing the cybersecurity maturity level in the Portuguese water sector. For this purpose, two research questions are defined: *RQI: What is the level of cybersecurity maturity in the Portuguese water sector? RQ2: What are factors limiting the cybersecurity maturity in this sector?* The following research objectives accompany the two research questions: (1) To explore the most mature focus areas in the Portuguese water sector; (2) To identify similarities and differences of cybersecurity maturity levels between the different players in the Portuguese water sector; (3) To assess dependencies between different focus areas of cybersecurity in the Portuguese water sector.

By answering the research questions, this study provides an overview of specific focus areas impacting the overall cybersecurity maturity level of the Portuguese water sector. These findings can assist players in this sector in assessing their weaknesses and in identifying measures to increase their cybersecurity maturity level. The developed model can serve as a blueprint for the

water sector, but an assessment based on the dependencies could also show which factors are highly relevant in other sectors. Thereby, the key findings of this research contribute to research and practice, providing an outlook for future research.

2. LITERATURE REVIEW

2.1 Cybersecurity

2.1.1 What is Cybersecurity?

Cybersecurity has been a highly present subject in academic research, yet there is no standard definition established up to date. Prior definitions are mostly highly variable, subjective, or context-bound. For the purpose of this paper, however, cybersecurity is defined as the combination of people, policies, processes, and technologies that an organization uses to protect its cyber resources and cyber-space-related systems (Craigen et al. 2014) from advanced persistent threats. On a general level, cybersecurity ensures user privacy and ensures "system availability, integrity, authenticity, confidentiality, and non-repudiation" (International Telecommunication Union 2008, p. 6).

IT security refers to the protection and the combating of network system threats both from so-called external cyberattacks or unauthorized access (Federal Ministry of the Interior and Community 2021). Further, cybersecurity can be further classified into the sub-areas of Information Technology (IT) security, Internet of Things (IoT) security, information security, and Operational Technology (OT) security (Gartner Information Technology Glossary 2021a). More generally, IT describes the entire scope of technologies for information processing. This incorporates software, hardware, communication technologies, and related services. In terms of general definition, IT does not include embedded technologies that do not generate data for corporate use (Gartner Information Technology Glossary 2021a). IT is playing an important role for governments. On the one hand, IT is used to make political decisions, and on the other

hand, IT ensures a primary supply of today's systems, especially because the fundamental systems mainly run automatically nowadays (Margetts 2012).

Next, IoT aims at merging the digital and the real world. It is defined as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner Information Technology Glossary 2021b). With more data being shared among manifold parties, security risks increase exponentially with IoT. In this cyber-physical world, resources are scarce, leading to an impracticality of traditional security mechanisms such as firewalls or anti-virus software (Fraunhofer Institute for Integrated Circuits IIS 2021). Hence, advanced, digitized security measures are crucial to secure enterprises from this additional risk.

Finally, OT is defined as a combination of software and hardware, which is used to identify and monitor changes as well as control and change industrial equipment, processes, and events (Gartner Information Technology Glossary 2021c). However, there are some common OT limitations for operational technologies regarding security controls. The main issue comes with controlling the access to those systems or system capabilities because OT platforms fail to provide enforcement options for access control. Also, several of these platforms do not support data storage of security-related events, which may be necessary to detect potential security breaches. Further limitations are shown in the following Appx. 1.

2.1.2 Cybersecurity Governance

On a general level, governance aims at providing strategic direction, mitigating risks, and allocating resources responsibly. It comprises a set of liabilities and practices typically exercised by the leading members of an enterprise. Since most risks and resources of a company are department-specific and thus require specific expertise, enterprise governance is usually structured by domain, such as IT, finance, or information security (Bodeau et al. 2010).

Cybersecurity Governance (CsG) ensures that the generally accepted enterprise governance controls are constantly adapted, supplemented, and used in the presence of advanced persistent threats in cyberspace (Evans and Smith 2019). An enterprise's CsG structure ensures that investment decisions, alignment with other domains of enterprise risk management, and the coordination of related managerial decisions are made consistently in a transparent manner (Bodeau et al. 2010). Traditionally CsG was handled as a technology issue. Cybersecurity was addressed by designing solutions to mitigate a specific risk. Hence, technological security systems such as automatic detection of intruders and firewalls are usually established, yet actual companywide CsG policies or processes are either not defined or defined but neglected (Nigro 2020). According to the CMMI Institute and ISACA, the most critical aspect of reaching a sufficient maturity stage in cybersecurity is making CsG an enterprise-wide risk management issue addressed and supported by the executive level (ISACA 2020).

2.1.3 Cybersecurity Management

Cybersecurity Management (CsM) involves an enterprise's capability to secure and protect information resources from internal and external threats. It comprises recommended strategies and control instances such as processes, procedures, software, and hardware structures, as well as organizational responsibilities (Alahmari and Duncan 2020). These processes are particularly crucial to ensure the integrity and confidentiality of defined processes such as Security Incident Management (SIM) and Risk Management. Further, CsM measures ensure adjustments of policies based on legal changes as well as project planning (International Organization for Standardization (ISO) 2016).

2.1.4 Cybersecurity Operations

Cybersecurity Operations (CsO) describe the key processes needed to ensure a strong cyber defense. According to Ehrnström (2018), enterprises need to master four crucial capabilities to

succeed at CsO. First, necessary security controls such as firewalls and endpoint protection are needed to prevent and protect against attacks. To ensure effectiveness, technologies and defined policies need to empower each other. Second, in order to detect both internal and external breaches, threat and vulnerability data has to be monitored and correlated. Third, incident management, disaster management, and business continuity are essential to address the breach fast and accurate to limit the damage. And fourth, the constant adaption of cybersecurity capabilities to incidents and external as well as internal changes. This includes measuring the effectiveness of efforts, adjusting to new technologies such as mobile and remote working systems, and mechanisms that detect external threats.

2.2 The Portuguese Water Sector

The Portuguese water sector is characterized by its diversity in scale and resources of distinct players and their management model. In general, the sector includes the following activities: water harvesting, treatment, and distribution of water for public consumption (Vitorino 2002).

There are three models of management adopted by the Portuguese water sector: direct state management, delegation, and concession. Direct state management operated players only operate downstream, dealing directly with private households (Reis, Ribeiro, and Sarmento 2012). Governmental services such as Municipality Services and Inter-Municipality Services are responsible for the provision of services as well as for system development and funding requirements. The second management model, delegation, refers to state-owned companies. Municipalities or association of Municipalities (Intermunicipalities) incorporate companies for the distribution of water (Vitorino 2002). According to the World Bank (2009), this management model brings services closer to the customer, minimizes administrative costs, and helps improve utility performance. The third management model, concessions, enables the entrance of privately-owned companies through tenders. Municipalities or Multi-

Municipalities launch concessions to attract know-how and funding to improve their services (AEPSA 2020). Technical solutions are not only developed but also operated by the private sector, so the government often does not have the necessary expertise to perform tasks and take appropriate action. As a result, public organizations decided to establish private-public relationships (PPPs) (Suter 2012). The concessionaires are responsible for the establishment, operations, and maintenance of facilities. Further, they need to secure their contractual compliance, including meeting fixed technological requirements (Vitorino 2002).

Following Reis, Ribeiro, and Sarmento (2012), particularly private concessions are more likely to operate more efficiently with an improved quality of service output. The comparison of management models in prior research further shows that cybersecurity seems to be at a lower level in the public sector, which is not handed over to private organizations, compared to the private sector (Bossong and Wagner 2017).

2.3 Cyber Risks and Challenges in the Water Sector

As the focus of the study is on the water sector, the following literature results on cybersecurity are only related to the water sector or similar crucial public sectors. Cybersecurity should have the highest priority in the digital age. According to the European Commission, a robust and stable program is critical for the provision of services to the population and public health (European Commission 2020). Especially in the water sector, the often-outdated systems offer easy access to the water valves and flow operations. This makes it very easy to manipulate the water flow and the number of chemicals used for water treatment. By accessing the online payment systems of the water companies, potential attackers find their weak points in the water network (Germano 2018). Following the article of Panguluri et al. (2019), there are four main challenges posed by the interdisciplinary processes. 1) the increasing interconnection of their business and control system networks, 2) the wide variety of proprietary industrial control

devices in use, 3) the multiplicity of cross-sector cybersecurity standards, and 4) the different approaches of device manufacturers to meeting these security standards. This shows that attacks in the water sector are possible in many places and that it is often easy to reach critical points due to the fragmentary and decentralized structure. The actual access to the system is usually very easy since SCADA systems, especially the older ones, are not sufficiently protected (Colbert and Kott 2016).

The following incidents are well-known documentations from the literature to show that the named risks have already led to damage in practice. Even though these are only a few examples, they represent the potential threats the water sector is confronted with and emphasize the need for accurate cybersecurity measures. As early as 2000, an attack on a wastewater plant in Australia was documented. In this case, an external consultant misused the access codes known to him for the wireless transmission systems to compromise the plant (Slay and Miller 2007). In 2018, security researchers from Germany describe that they were able to gain unrestricted online access via the web interface to wastewater treatment plants with administrator rights (Tremmel 2018). In the latest case, a European water utility commissioned a critical infrastructure security company, Radiflow, to monitor its network. Investigations revealed that foreign IP addresses were on the network. However, these did not lead to a malicious site but to the MinerCircle Monero pool. The findings, in this case, were the discovery of crypto-mining malware on the water utility's OT network (Hassanzadeh et al. 2020).

3. CONCEPTUALIZATION

This chapter provides an overview of the framework used as a base for this study. All literature reviewed is presented and conceptualized based on a modified Cybersecurity Maturity Assessment Framework (CMAF), which allows for the classification of all literature reviewed.

3.1 Cybersecurity Maturity Assessment Framework

The Cybersecurity Maturity Assessment Framework was built by the Greek government to support organizations of essential services and digital service providers to evaluate their cybersecurity maturity. The goal of this framework is the creation of a tool that can be used for self-assessment, as a basis for audits, for benchmarking in a certain industry, or as a guide for security measures implementation (Drivas et al. 2020). The requirements are based on the EU NIS Directive, which was issued by the European Commission and the European Union Agency for Network and Information Security (ENISA) in 2016 (European Parliament, Council of the European Union 2016). The aim of the framework is to identify the strengths and weaknesses of an organization's processes and to assess how compatible these processes are compatible with the relevant best practices or guidelines. The assessment framework consists of the safety requirements against which the organization's processes are assessed and the scale against which the degree of compliance of the organization's processes is assessed. According to Drivas et al. (2020), the CMA framework has features such as covering the full scope of security requirements, fulfilling the obligations of the NIS Directive, and aiming for clear results regarding the level of security as well as easy transferability to similar areas.

3.2 ISFAM

Secondly, the Information Security Focus Area Maturity Framework was used to evaluate the results gathered in the survey regarding the dependencies between the 16 focus areas in the questionnaire. Researchers at the University of Utrecht in the Netherlands have set up the model in order to better explain the relationships between different aspects of information security and to achieve an improvement in information security maturity (Appx. 2). The 13 focus areas of the researchers are partly very similar to the areas investigated in this research. The model was evaluated through a case study with a medium-sized telecommunication company (Spruit and Röling 2014).

3.3 Cybersecurity Maturity Assessment Framework for the Water Sector

On this basis, an adapted framework was developed to explore cybersecurity maturity in the Portuguese water sector. The framework models for the security requirements have been fundamentally adopted. This content has been published by organizations such as ENISA, the European Union, NIST, and others. Here the main objective was to bring the model into line with the NIS directive. At the same time, efforts were made to integrate the factors from directive DL65/2021 and to expand the assessment based on these requirements. Based on this, the framework was made up of 73 security requirements, which serve as a reference point, and six maturity levels, which serve as a qualitative measurement scale (see 3.4). For a comprehensive overview, the requirements are divided into three groups. The first focus area, "Cybersecurity Governance" (CsG), contains ten requirements and aims at providing strategic direction, mitigating risks, and allocating resources responsibly. This enables the organization to focus its efforts and manage its processes and resources effectively and efficiently (Bodeau et al. 2010). The "Cybersecurity Management" (CsM) focus area includes an enterprise's capability to secure and protect information resources from internal and external threats. It comprises recommended strategies and control instances such as processes, procedures, software, and hardware structures, as well as organizational responsibilities (Alahmari and Duncan 2020). The third focus area deals with "Cybersecurity Operations" (CsO). These requirements are necessary security controls such as firewalls and endpoint protection are needed to prevent and protect against attacks. The controls selected for this category should also focus on mitigating the impact of an incident and restoring essential services to an acceptable and predefined level (Drivas et al. 2020).

The following requirements were included for the expansion and adaptation to the water supply. Many of them are very focused on the topic of OT and asset management, as many vulnerabilities are found in the water sector at this level. The first important point is the security

of Industrial Control Systems (ICS), which mainly concern valves and pumps. Many of these systems are very old and partly only secured with simple one-time passwords (Colbert and Kott 2016). There are often higher costs for procurement, deployment, and integration of the different systems. The system must remain in operation over a long period of time for the costs of this investment to be amortized. For example, relays in power supply systems are typically expected to be in operation for over 20 years (Colbert and Kott 2016). In addition, the dependencies on vendors and manufacturers must be considered. It often happens that systems are only supported up to a certain age. Furthermore, systems are often tied to the manufacturer's own systems and can only be maintained by certified technicians, which increases costs and waiting times (Colbert and Kott 2016). However, also general support activities like human resource management are incorporated to get a broad picture of the value chain.

3.4 Maturity Level Scale

Following the CMA framework, a 6-point scale was utilized to measure the maturity of the organizations. Level 0 is the lowest value and equals "Incomplete - Not existing." Level 5 is the highest rank and indicates "Efficient - Optimized." The maturity levels can be described as follows based on the pre-established definitions of Drivas et al. (2020):

Level 0 – Does not have – Not existing: The requirement under review is not implemented or is implemented only in part or ad hoc.

Level 1 – Incompletely and informally – Reactive: The organization has started to implement the requirement, but the degree of implementation is either partial or reactive.

Level 2 – Formalised minimum – Managed: There is a definite plan to comply with the requirement. The necessary controls are implemented but are only partially measured and partially controlled.

Level 3 – Complete and formal way – Defined: There is a standardized procedure for meeting the requirement. The required controls are implemented, measured, and verified at the level described.

Level 4 – Complete, formal, and measures effectiveness - Quantitatively Managed: There is a standardized procedure for meeting the requirement. The required controls are implemented, measured, and verified at the level described

Level 5 - Complete, formal, and measures effectiveness and improves periodically – Optimized: Continuous improvement of the implemented controls and the organization's level of security. A fully risk-based approach is followed, and a cost-benefit balance is applied. The necessary controls are implemented, measured, and controlled at the level described.

4. METHODOLOGY

This chapter explains the methodology used to explore the research objectives in this study. In the first step, a comprehensive literature review was conducted to assess the sixteen crucial focus areas to assess the Portuguese water sector's maturity level (Creswell 1994). Next, a quantitative research approach to collect data was chosen to gain holistic insights. The survey method was used to examine the maturity level of cybersecurity in the Portuguese water sector. The decision to conduct an online questionnaire was made in order to ensure reaching the majority of participants in a straightforward and anonymous way.

An online questionnaire was designed based on the literature reviewed, structured on the CMA framework, and clustered into three categories (CsG, CsM, and CsO) with multiple requirements and sub-requirements defined (Appx. 3). To capture the intensity of respondents' answers ensure reliability, the 6-point Likert scale was considered appropriate to match the CMAF maturity scale (Preston and Colman 2000).

A preliminary questionnaire was tested with a sample consisting of academic professors and experts of the ERSAR to ensure validity and reliability (Saunders, Lewis, and Thornhill 2007). The units of analysis were organizations of the Portuguese water sector that are related to the sector in any way. To assess the relevant population, the survey link was shared directly with all water operators in Portugal, ensuring data from three operating areas, retail population sizes, and three different management models (Harrigan, Rosenthal, and Scherer 2008). In total, the questionnaire comprised 73 questions clustered into 16 focus areas and three main categories. Finally, all data were analyzed with Python and SPSS 26.

In order to assure confirmability and consistency, the data collection processes are described in detail (Bhattacherjee 2012). Further, validity was maintained by basing the survey structure on literature and prior frameworks as well as by extensive pilot testing. Nevertheless, bias cannot be completely precluded as all answers depend on the respondent's individual situation and perception. Moreover, this study is limited by the number of respondents the diversity of enterprises involved, including factors such as management models, retail population size, and water operations.

5. RESULTS AND DISCUSSION

5.1 Results

To gather quantitative insights into the current level of cybersecurity maturity in the Portuguese water sector, a survey was conducted with 226 employees from three different departments of 115 water operators in the water harvesting, water treatment, or water distribution sector. Solely 70 unique operators were considered out of 113 valid responses after removing non-valid answers.

To test the reliability of the questionnaire, Cronbach's Alpha was adduced to measure the level to which the questions are related to each other (Saunders, Lewis, and Thornhill 2019). The overall Cronbach's Alpha of 0.974 highlights the strong reliability of this questionnaire, with inner-item consistencies ranging from 0.723 to 0.921 (Appx.4). Subsequently, descriptive

statistics are examined and displayed for each individual question as well as on a grouped level. Therefore, all Likert-scaled maturity level data were treated as interval data, based on the research of Kenny (1986), who pointed out that they can be considered as having metric properties under the conditions of this study. Next, to determine which factors of the organizations influence the maturity level, a one-sided ANOVA was applied to the grouped focus areas. Afterward, a post-hoc test by Hochberg was conducted due to similar variances but a strongly varying number of cases within one subgroup (Field 2013).

The organizations surveyed operate based on three management models, which can be further partitioned into two sub-models each (Appx.5). The largest group has a Direct Management model (43.4%) with a Municipality Service sub-management model (37.2%). The respondent's organizations serve regions of varying sizes, which are divided into three groupings of a retail population of over 100,000, between 20,000 and 100,000, and under 20,000 people. Areas under 100,000 barely differ in the number of responses, while municipalities over 100,000 contribute only 24.8% (Appx.6). The largest share in the Area of Operation, 56.6%, are organizations that are solely responsible for water distribution (Appx.7). Further, more than half (50.4%) of all responses are employees from Corporate RSI (IT), and 36.3% work for an Operational Technology department (Appx.8).

5.2 RQ1: Level of Cybersecurity Maturity in the Portuguese Water Sector

5.2.1 Level of Cybersecurity Maturity

Following the European Commission's proposal for the directive on the resilience of critical entities, cybersecurity should be a top priority in essential public sectors, such as water supply (European Commission 2020). The results of this study show that the maturity level in various fields is not yet high enough to maintain resilience against cyber-attacks. Insights point towards a total average maturity level of 1.509 points (Appx.9) from the scale of 0 to 5 points. This

indicates that the average Portuguese organization in the water sector has implemented measures partially but only formalized at a minimum (Drivas et al. 2020).

Further, all 16 focus areas range on average between 1.030 and 2.482 points. Hence, in no area is sufficient coverage of cybersecurity measures is guaranteed (Appx.10). Looking at the maturity of the CsG and CsM focus area, similar numbers to the overall maturity level can be derived. Hence both measures related to CsG and CsM are formalized across the whole Portuguese water sector yet solely to a minimum.

In contrast, there are greater deviations in the groups of the CsO focus area. The highest maturity level is achieved by the mobile and remote working systems with a mean value of 2.482 points, indicating that remote working mechanisms and mobile working security mechanisms are implemented on the road to a complete and formal way (Appx.10). One possible explanation could be the rapid digitalization and use of mobile devices in the home office due to COVID-19. Furthermore, the focus area "Management of security operations" is still in the minimally formalized stage of maturity level 2, according to the definition. An individual analysis of the questions shows that a high level of maturity is primarily indicated for the capacity management process, activity logging, and control of operational software. However, since basic IT equipment is equipped with essential technology nowadays, a minimally formal process is already given even without additional measures from the respective enterprise (Appx.11). The third most mature area is “Communications management”. Factors such as the implementation of network controls, for example, firewalls and network security architecture, were surveyed. With an average maturity of 3.150 points, the first question about network controls clearly raises the average (Appx.12). However, as today's quality for network controls are internationally standardized, and basically every operating system has an integrated control function, this result is to be expected.

Hiring/HR, on the other hand, is the focus area with the lowest maturity (1.030 points), where all topics related from pre-employment validation to education and awareness training regarding cybersecurity are asked. With 0.796 points, "Condition of Engagement include cybersecurity requirements" has the least maturity in this area. An explanation for this fact could be the high effort and a sophisticated human resource management system connected with this task (Appx.13). With a maturity level of 1.074 points, the area of “Classification of Information and Operation Support Assets” (Appx.14) comes unswervingly behind the Hiring area. Drilling down this area shows an overall bad level of maturity for all questions related to this topic. Using encryption mechanisms (1.062 points) or having an asset security level classification mechanism (1.009 points) requires new and often more expensive assets, which corresponds to the findings of Colbert and Kott (2016).

Traditionally, cybersecurity has been a task of IT and security departments (Bodeau et al. 2010). However, due to the rapid digitalization, every employee now has to become familiar with the potential risks and should be trained accordingly. With 1,407 points, the question "Develops training, education, and awareness in cybersecurity" was answered below the average level of maturity. This result shows that in the Portuguese water sector, it is not yet understood that cybersecurity should be established in the whole company culture (Hewitt 2019). Also, the organizational structure and policies must not only be oriented towards software and hardware but also towards human factors (Hewitt 2019).

5.2.2 Dependencies of Cybersecurity Maturity

Since interdependencies between the focus areas cannot be ruled out, they will be examined in a PLS analysis (Appx. 15) to show that the order of cybersecurity measures plays an important role in the implementation of new elements. This analysis is based on the research of the ISFAM framework of the Utrecht University in the Netherlands, which shows the dependencies of similar focus areas in a case study (Spruit and Röling 2014). The goal of the PLS evaluation

is to calculate the correlations between the 16 focus areas analyzed. According to Bodeau et al. (2010), CsG determines both CsM and CsO through the enterprise-wide defined organizational structures, guidelines, and policies. Further, procedures and control measures of CsM influence activities in CsO (Alahmari and Duncan 2020).

Following Bodeau et al. (2010), the analysis of the latent variables shows a strong relationship of governance to CsM (path coefficient (pc)=0.897; p=0.000), but less so to CsO (pc=0.639; p=0.000). However, a correlation between CsM and CsO does not seem to exist (pc=0.320; p=0.001). CsG is represented by ten questions in this research, as seen in Appx. 15, covering different areas. In the result analysis of the cybersecurity governance factors, the outer loadings (ol) show a particularly strong tendency for the questions "Has a Cybersecurity Policy" (CSG1; ol=0.855; p=0.000), "Has a Security Organization defined" (CSG2; ol=0.892; p=0.000), "It has a Cybersecurity Architecture" (CSG4; ol=0.852; p=0.000) und "It has a Management System that supports Security Management" (CSG5; ol=0.854; p=0.000). Comparing this outcome with the dependencies from the ISFAM model, there are clear similarities, especially with regards to policy development and security organization (Appx. 16). In accordance with Spruit and Röling (2014), the strong correlation can be explained by the fact that all five have the highest impact on a company's maturity level. Thus, in the Portuguese water sector, it is particularly these measures that influence the maturity level of the CsG. The ISFAM model also shows that a level in "Policy Development" and "Organizing Information Security" is a basic condition that influences almost all other factors (Appx. 17).

For the focus area CsM, the three questions of “It has a Security Incident Management Process” (CSM1; ol=0.914; p=0.000), “Has defined Roles and Responsibilities in Information Security Management” (CSM3; ol=0.925; p=0.000) and “Manages Cybersecurity in Projects” (CSM7; ol=0.897; p=0.000) stand out with a higher correlation. As these questions refer to quite basic measures explaining the CsM maturity level, this result supports the minimally formalized

maturity level of the Portuguese water sector. Further, considering the CsO cluster, the key areas of the Portuguese water sector's operational structure become clear. The areas “Security Incident Management” (ol=0.910; p=0.000), “Relationship with Suppliers” (ol=0.887; p=0.000) and “Business Continuity, Disaster Management and Information Security” (ol=0.866; p=0.000) prove to be particularly strongly correlated. Moreover, the outer model indicates that elementary functions relating to cybersecurity “Incident Management” have an enormous influence on maturity. In addition, “Business continuity”, “Disaster Management”, and “Information Security Management” complement the topic around incidents. This leads to the assumption that strengthening the measures related to incident management is a crucial factor to advance the cybersecurity maturity level of the Portuguese water sector rapidly.

Finally, in accordance with the ISFAM framework, these insights emphasize the need to increase the maturity level of the different focus areas in sequence, starting with CsG and CsM in order to increase the cybersecurity maturity level sustainably (Spruit and Röling 2014).

5.3 RQ2: Limiting Factors of Cybersecurity Maturity in the Portuguese Water Sector

In this step, the limiting factors of cybersecurity maturity are identified and analyzed. For this purpose, three factors of the organizations are examined: management model, retail population, and the area of operation.

Management Model: The organizations surveyed can be divided into subgroups of the three management models: delegation, concession, and direct management. According to the study, there are significant differences between all three management models across various focus areas.

First, the responses of organizations that are linked with the concession management model are consistently rated higher across all 16 focus areas. The second-best performing management

model is delegation, followed by the direct management model rated with the overall lowest maturity of all management models (Appx. 18).

However, the focus areas "Classification of Information and Operation Support Assets" (p=0.103), "Management of Security Operations" (p=0.218), and "Communications Management" (p=0.103) are not significant when it comes to the evaluation of the management model (Appx.19). Based on these results, it can be concluded that all three non-significant areas are not dependent on the management model and must become more advanced as a general element. Thus, it can be concluded that the management model determines many factors but that these are consequences of assets that cannot be directly influenced by the organization. If a specific question in the focus area of “Communications management” or “Management of Security Operations” is picked out, correlations to the assets can be established. For example, many of these are from external manufacturers with standardized software and no customizable functions. Backups or logging processes are predetermined by the technology and can only be changed with difficulties by the organization. In summary, there is a high potential for improvement across all management models; thus, they do not constitute a limiting factor for these measures.

Given that a concession management model relies on the know-how and investment of private companies, it is to assume that profit-oriented companies already have a higher level of cybersecurity (Vitorino 2002). This can be evidenced by the effect of competition in a market economy since in the event of bad performance, and other competing companies would be chosen otherwise. Furthermore, the outcome of the first research question showed that the Portuguese water sector operates very traditionally, and cybersecurity is still under the supervision of IT and Tech departments rather than an organization-wide established method (Hewitt 2019).

Further, the post-hoc test's results show that there are significant differences between the three management models, especially for the focus area "Relationship with Suppliers". The maturity levels for this focus area particularly differ between concession and direct management model with an MD of 2.017 (p=0.000). This emphasizes again the positive impact of private companies that, in this case, influence the external relationships as well as digitalization level compared to other management models (Appx. 19). These challenges can be optimized with a better process chain and clear responsibilities (Bossong and Wagner 2017). Similar differences exist in "IT, OT, and IoT asset management" and "Security incident management", for which a high level of subject matter expertise is required (Suter 2012). However, in order to minimize the gap between the maturity levels in these focus areas, it is required to further explore the differences between the different management models in-depth.

Retail Population: The ANOVA, which considers the retail population divided into three clusters, does not yield significant results for any focus area. In view of these results, the retail population size of the service region does not give any indication of a lower or higher implementation of cybersecurity measures and thus of an increased maturity level (Appx. 20). This might be related to the fact that small regions are jointly served by a larger organization or that small regions are attached to larger municipalities (Reis, Ribeiro, and Sarmento 2012). However, further research is needed to allow for more holistic insights on this subject's manner.

Area of Operation: The analysis of the factor area of operation does not show a significant difference in mean. As this was not highlighted in prior literature, this finding, however, is to be expected. Neither organizations in harvesting and treatment nor organizations that only take care of distribution differ significantly in their maturity level (Appx. 21). Finally, organizations that work across the entire value chain are not significantly ahead when it comes to cybersecurity maturity. Contradicting the statements of Panguluri et al. (2011), the value chain thus seems to be balanced when it comes to the level of cybersecurity maturity.

6. IMPLICATIONS

This chapter deals with the theoretical and practical implications that can be adopted on the basis of this research and how they can be extended.

The main objective of this study was to reduce the gap of research knowledge regarding the evaluation and connection of measures for cybersecurity, especially in the water sector of Portugal. Due to the quantitative approach of this research, it is possible to statistically generalize the findings from a small population to a larger one. Thus, stakeholders from other sectors and organizations can easily adapt the findings to their individual challenges, as well as break down emerging effects from the results as a whole. The findings of the first research question show that cybersecurity is not yet treated with the authority and priority that would be appropriate and necessary to strengthen against cyberattacks as defined by the EU's directive. Since the technology for enterprises has developed so rapidly in recent years, it is also very challenging to implement all changes and innovations properly and quickly (ISACA 2020). In order to speed up the process, it is important that cybersecurity becomes more of a top management responsibility and not a traditional responsibility of the tech or IT departments (Hewitt 2019). Understanding that cybersecurity is a company-wide challenge and also affects supporting departments such as human resources requires a new company culture as well as new structures in strategic planning and alignment (Nigro 2020).

A second important implication of the study derives from the findings on the dependencies between the focus areas. As shown in the ISFAM model, successful implementation always starts with management commitment and having sufficient resources available (Spruit and Röling 2014). It is important to understand that maturity can be increased much faster if improvements are made in the right places. The outcome indicates the necessity of a basic organizational structure for cybersecurity and that this also leads to a higher maturity level. For

instance, it is essential that policies need to be aligned prior to introducing a new encryption model (ENISA 2008).

A third implication stems from the second research question, how the characteristics of the organizations affect the maturity level. The results suggest that the influence of the management model exposes significant differences. As public sectors often lack the expertise and resources to deal with cybersecurity, more extensive research is required to assess comprehensively how private organizations differ from the public sector and which processes can be adopted and thus improved in the relationship with suppliers, as exemplified (Suter 2012). The area of operation in the water sector, as well as the retail population, turns out not to be significant in the analysis of the results. Accordingly, this could imply that these outcomes are independent of the area of operation in the water sector and transferable to other utility sectors in the same way.

7. CONCLUSION

Cybersecurity is undoubtedly one of the buzzwords of this decade, changing many processes in the public sector and describing an integral threat when it comes to public health and essential services (Clark et al. 2017). In the US, the protection of the water utility sector has even become a national priority (The White House - Office of the Press Secretary 2013). Nevertheless, the maturity of cybersecurity in public sectors in Europe is still rather at an early stage, which according to this study, also applies to the Portuguese water sector.

The reason for this research was to determine the maturity level and to assess the reason for the current state of cybersecurity in the Portuguese water sector. Using the CMA framework, significant focus areas were identified, providing in-depth insights into the responsible organizations, and highlighting the biggest gaps. Primarily due to increasing digitalization and the adoption of IoT, water utility providers were quickly inundated with growing complexity for security mechanisms (Tuptuk et al. 2021). The findings of this study indicate that the

general maturity across the Portuguese water sector is very low and, on average, has not yet adopted a formal minimum. Instead, it is still on a reactive level. Especially the efforts in the supporting areas of the organizations must be increased to guarantee overall security. Furthermore, the results imply the importance of implementing improvements in a certain sequence to use elementary processes or structures as a basis for change in more specific areas and operations. Another significant finding was the influence of the management model on the progress and maturity of cybersecurity. The analysis of the results points out how public-private partnerships positively influence the level of cybersecurity maturity. The fact that many public organizations have less expertise than private organizations also shows that resources in the public sector are sometimes lacking or used in the wrong places (Suter 2012).

Finally, this research provides guidance to the Portuguese respondents as well as to organizations in other public sectors, providing starting points on how to advance cybersecurity. In addition, the developed model can be adopted as a tool for assessing cybersecurity maturity in the water sector or support other sectors as a template. Most importantly, the results obtained should stimulate a discussion at the management level on better measures and update the public sector regarding cybersecurity.

For more detailed insights, this quantitative approach serves as a basis to conduct case studies to deal with specific challenges and to assess how to successfully overcome these. Organization-specific factors can be addressed to identify the most important areas and the best approach to solve them. In addition, further research can analyze the relationship between several crucial public sectors and possibly implement holistic solutions across sectors. On another note, the organizations surveyed limit the results. The organizations' factors can be further expanded, allowing for a much more comprehensive analysis. In addition, the identified barriers are limited by the literature reviewed.

8. BIBLIOGRAPHY

AEPSA. 2020. “Mandate of the Special Rapporteur on the Human Rights to Safe Drinking Water and Sanitation Report to the 75th Session of the UN General Assembly in 2020.”

Alahmari, Abdulmajeed, and Bob Duncan. 2020. “Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence.” In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5. Dublin, Ireland: IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638.

Bodeau, Boyle, Fabius-Greene, and Graubart. 2010. “Cyber Security Governance - A Component of MITRE’s Cyber Prep Methodology.”

Bossong, Raphael, and Ben Wagner. 2017. “A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU.” *Crime, Law and Social Change* 67 (3): 265–88. https://doi.org/10.1007/s10611-016-9653-3.

Bruijn, Hans de, and Marijn Janssen. 2017. “Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies.” *Government Information Quarterly* 34 (1): 1–7. https://doi.org/10.1016/j.giq.2017.02.007.

Clark, Robert M., Srinivas Panguluri, Trent D. Nelson, and Richard P. Wyman. 2017. “Protecting Drinking Water Utilities From Cyberthreats.” *Journal - American Water Works Association* 109 (February): 50–58. https://doi.org/10.5942/jawwa.2017.109.0021.

Colbert, Edward J. M., and Alexander Kott, eds. 2016. *Cyber-Security of SCADA and Other Industrial Control Systems*. Vol. 66. Advances in Information Security. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-32125-7.

Craigen, Dan, Charles Leslie Stevenson, Nadia Diakun-Thibault, and Randy Purse. 2014. “Defining Cybersecurity.” *Technology Innovation Management Review*, 9.

Creswell, John W. 1994. *Research Design: Qualitative & Quantitative Approaches*. Thousand Oaks, Calif: Sage Publications.

Drivas, George, Argyro Chatzopoulou, Leandros Maglaras, Costas Lambrinoudakis, Allan Cook, and Helge Janicke. 2020. "A NIS Directive Compliant Cybersecurity Maturity Assessment Framework." In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1641–46. Madrid, Spain: IEEE. https://doi.org/10.1109/COMPSAC48688.2020.00-20.

Ehrnström, Oskar. 2018. "4 Key Capabilities That Every Successful Cybersecurity Operations Possesses."

ENISA. 2008. "Der Neue Leitfaden Für Die Praxis: Juli Wege Zu Mehr Bewusstsein Für Informationssicherheit."

European Commission. 2020. "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Resilience of Critical Entities." 2020. https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

European Parliament, Council of the European Union. 2016. "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016." In *Core EU Legislation*. https://doi.org/10.1007/978-1-137-54482-7_33.

Evans, Corbin, and Christopher Smith. 2019. "A Report of the NDIA Policy Department," 27.

Field, Andy P. 2013. *Discovering Statistics Using IBM SPSS Statistics: And Sex and Drugs and Rock "n" Roll*. 4th edition. Los Angeles: Sage.

Fraunhofer Institute for Integrated Circuits IIS. 2021. "Cyber Security for IoT." Fraunhofer Institute for Integrated Circuits IIS. 2021. https://www.iis.fraunhofer.de/en/ff/lv/iot-system/tech/cybersecurity.html.

Gartner Information Technology Glossary. 2021a. “Definition of Information Technology (IT) - Gartner Information Technology Glossary.” Gartner. 2021. https://www.gartner.com/en/information-technology/glossary/it-information-technology.

———. 2021b. “Definition of Internet Of Things (Iot) - Gartner Information Technology Glossary.” Gartner. 2021. https://www.gartner.com/en/information-technology/glossary/internet-of-things.

———. 2021c. “Definition of Operational Technology (OT) - Gartner Information Technology Glossary.” Gartner. 2021. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

Germano, Judith H. 2018. “CYBERSECURITY RISK & RESPONSIBILITY IN THE WATER SECTOR.”

Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and Katherine Banks. 2020. “A Review of Cybersecurity Incidents in the Water Sector.” *Journal of Environmental Engineering* 146 (5): 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

Hewitt, Kasey. 2019. “11 Considerations of Effective Cybersecurity Risk Management.” SecurityScorecard. 2019. https://securityscorecard.com/blog/10-considerations-for-cybersecurity-risk-management.

International Organization for Standardization (ISO). 2016. “IT Governance and The International Standard, ISO/IEC 38500.”

International Telecommunication Union. 2008. “SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication Security Overview of Cybersecurity.”

ISACA. 2020. “Managing Cybersecurity Risk: A Crisis of Confidence.”

Kenny, Graham K. 1986. “The Metric Properties of Rating Scales Employed in Evaluation Research: An Empirical Examination.” *Evaluation Review* 10 (3): 397–408. https://doi.org/10.1177/0193841X8601000309.

Kullik, Jakob. 2014. *Vernetzte (Un-)Sicherheit? eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik*. Chemnitzer Schriften zur europäischen und internationalen Politik 7. Hamburg: Kovač.

Margetts, Helen. 2012. *Information Technology in Government: Britain and America*. 0 ed. Routledge. https://doi.org/10.4324/9780203020944.

Nigro, Pam. 2020. “Cybersecurity Governance: A Path to Cyber Maturity.”

Panguluri, Srinivas, William Phillips, and John Cusimano. 2011. “Protecting Water and Wastewater Infrastructure from Cyber Attacks.”

Preston, Carolyn C, and Andrew M Colman. 2000. “Optimal Number of Response Categories in Rating Scales: Reliability, Validity, Discriminating Power, and Respondent Preferences.” *Acta Psychologica* 104 (1): 1–15. https://doi.org/10.1016/S0001-6918(99)00050-5.

Reis, Ricardo Ferreira, João Gonçalo Ribeiro, and Sarmento. 2012. “An Assessment of Water Utilities Efficiency Using the Portuguese Case.”

Saunders, M. N. K., Philip Lewis, and Adrian Thornhill. 2019. *Research Methods for Business Students*. Eighth Edition. New York: Pearson.

Slay, Jill, and Michael Miller. 2007. “Lessons Learned from the Maroochy Water Breach.” In *Critical Infrastructure Protection*, edited by Eric Goetz and Sujeet Shenoi, 253:73–82. IFIP International Federation for Information Processing. Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-75462-8_6.

Spruit, Marco, and Martijn Röling. 2014. *Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014*. S. l.: AISeL. http://aisel.aisnet.org/ecis2014/.

Suter, Manuel. 2012. "The Governance of Cybersecurity: An Analysis of Public-Private Partnerships in a New Field of Security Policy." Application/pdf. ETH Zurich. https://doi.org/10.3929/ETHZ-A-007319319.

The White House - Office of the Press Secretary. 2013. "Presidential Policy Directive - Critical Infrastructure Security and Resilienc."

Tremmel, Moritz. 2018. "Per Weblogin Ins Klärwerk." https://www.golem.de/news/schwachstellen-aufgedeckt-per-weblogin-ins-klaerwerk-1812-138363.html.

Tuptuk, Nilufer, Peter Hazell, Jeremy Watson, and Stephen Hailes. 2021. "A Systematic Review of the State of Cyber-Security in Water Systems." *Water* 13 (1): 81. https://doi.org/10.3390/w13010081.

Vitorino, Macedo. 2002. "Portugal: Opportunities in the Portuguese Water Market."

World Bank. 2009. "Improving Water Utility Services through Delegated Management: Lessons from the Utility and Small-Scale Providers in Kisumu, Kenya."

9. APPENDICES

Appendix 1: Borders of IT adapted by Colbert and Kott (2016)

*Click **here** to return to the document*

Area of control	Borders of OT
System Configuration	Organizations may not have sufficient control over system configuration, for example, hard-coded permissions or locked down.
Authentication	Many systems do not yet provide multi-level authentication or support for authentication servers (e.g., LDAP)/authentication protocols (e.g., RADIUS) and offer only short passwords.
External Communication	A lack of solid security algorithms leads to insufficient protection during data communication processes.
System Integrity	The systems verification deficit includes, e.g., mechanisms for patches, support for malware protection, or mechanisms to verify the integrity of a system.

Appendix 2: Overview of the Information Security Focus Area Maturity (ISFAM) model – adapted by Spruit and Röling (2014)

*Click **here** to return to the document*

Focus Area: / Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
1. Risk Management				A		B		C			D		
2. Policy Development			A		B						C		
3. Organizing Information Security		A			B					C		D	
4. Human Resource Security				A		B		C		D			
5. Compliance				A		B						C	
Technical													
6. Identity and access management					A		B		C		D		
7. Secure software development					A		B			C		D	
Organizational and Technical													
8. Incident management			A			B			C			D	
9. Business Continuity Management				A		B		C			D		E
10. Change Management				A		B		C		D			
Support													
11. Physical and environmental security						A		B		C			D
12. Asset Management			A				B			C		D	
13. Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Appendix 3: Overview of Questions included in the online questionnaire

*Click **here** to return to the document*

'- Para cada questão, a resposta deve ser dada relativamente a cada um dos pilares: IT, OT e IOT. - Para cada questão, a resposta associada a cada um dos pilares, IT, OT e IOT deve ser dada por quem gere essa infraestrutura - Sempre que se leia sistema, pode ser entendido como sistema de informação, quer seja de caráter corporativo ou de caráter operacional, mas também se refere aos sistemas e subsistemas de abastecimento de água, nas suas componentes tecnológicas. - Sempre que se leia Segurança, pode ser entendido como Segurança de Informação em sentido lato (incluindo segurança tecnológica) ou Cibersegurança - Para cada Pilar (IT, OT e IoT) deve ser identificada a função e a posição hierárquica na organização

Corporate Information Systems (IT) Networks							
0 - Does not have	**1 - Has/uses incompletely and informally**	**2 - Have/use a formalised minimum**	**3 - Has/uses in a complete and formal way**	**4 - Has complete, formal, and measures effectiveness**	**5 - It is complete, formal, measures effectiveness and improves periodically**	**N/A**	**Doesn't know/doesn't intend to answer**

Cyber Security Governance	
	Has a Cybersecurity Policy (M)
	Has a Security Organization defined
	It has a Safety Officer (M)
	It has a Cybersecurity Architecture

	It has a Management System that supports Security Management
	Top Management takes a perspective on the risk that connected technologies pose to essential service delivery
	Decisions associated with IT, OT and IoT technologies are taken in an integrated way, for example with a project management committee.
	It considers it has adequate funding to meet cybersecurity requirements (whether in IT, OT or IoT)
	It considers having adequate funding to hire HR or specialist subcontracting to meet cybersecurity requirements (whether in IT, OT or IoT)
	Considers that there is Top Management commitment to the sustainability of cybersecurity management
Cyber Security Management	
	It has a Security Incident Management Process (M)
	Has a Safety Point of Contact (M)
	Has defined Roles and Responsibilities in Information Security Management
	Performs Function Segregation (separation of functions with conflicting roles, e.g. an approver being the executor of a risk activity)
	It has a Risk Management (M)
	Contacts with Authorities (M)
	Manages Cybersecurity in Projects
Cybersecurity Operations	

a) Mobile and Remote Working Systems	Has Security mechanisms implemented in Mobile Systems (e.g. laptops, mobile phones, mobile equipment with processing capacity)
	Uses Remote Working Mechanisms (e.g. VPN, remote management systems)
b) Classification of Information and Operation Support Assets	
	It has a process of Asset Identification by security level
	It has an Asset Security Level Classification mechanism (e.g. an asset being considered essential already presupposes a classification of the security level of the asset)
	Uses removable media to support and transport data and information securely or with embedded security mechanisms (e.g. encryption)
c) Access Control (Partially)	
	It has mechanisms to control logical access to networks, information systems and connected equipment
	It has a registration and configuration of Users
	Manages and reviews Users' privileges
d) Management of security operations (M partially)	
	Has an Asset Change Management Process that assesses risk and authorises changes to assets
	It has a Capacity Management Process used in the assets (when applicable)

	Performs segregation of development, test, quality and production environments
	Performs segregation of Corporate, Operational and Connected Equipment environments
	Backs up and safeguards data, information and systems
	It has activity logging processes (Logs)
	It has a control of the Operational Software Used or a control of its use (e.g. software that allows the management of the configuration of the assets in its operation)
	Has a record of the Security Controls (i.e. mechanisms that guarantee the logical and physical security of the IT, OT or IOT)
e) Communications Management (partial M)	
	Has implemented Network Controls (Firewall, IPS, IDS, etc.)
	Has implemented a Network Security Architecture
	It has an Information and Data Transfer Policy
	Uses NDA Confidentiality Agreements
f) Safety in systems development, acquisition, and maintenance (IT, OT or IOT networks and information systems, water supply systems and subsystems)	
	Software development projects include cybersecurity requirements
	The technology (equipment or software) acquisition processes include cybersecurity requisites
	System maintenance contracts (IT, OT or IOT networks and information systems, water supply systems and subsystems) include cybersecurity requirements

g) Security Incident Management (M)	
	It has Security Incident Management Procedures
	Has a Security Incident Reporting Process
	It has a Fragility Reporting Process
	Has Rules of Assessment and Decision Making in Security Incidents
	It has a Security Incident Response Process
	It has mechanisms for gathering evidence in the event of a Security Incident
h) Hiring HR	
	Has pre-employment verification mechanisms in place for key cybersecurity roles (e.g. criminal record validation, and CV checks)
	Conditions of Engagement include cybersecurity requirements
	Develops Training, Education and Awareness in cybersecurity
	The use of Disciplinary Procedures is foreseen
	On termination of employment, it imposes cybersecurity requirements on former employees (e.g. the responsibility to safeguard and not disseminate knowledge about the infrastructure and accesses for a certain period of time)
i) IT, OT and IOT asset management	
	Has appointed Asset Managers in the IT or OT or IOT components
	Has and updates an Asset Inventory with the respective security classification

	It has procedures that define the Adequate Use of Assets
j) Management of safety zones	
	Carries out Security Management considering physical Perimeters
	It has Physical Access Control
	It has mechanisms to detect and protect against environmental threats (e.g. fires, floods, extreme phenomena, etc.)
	Work is carried out in Safe Grading Zones
k) Protection of IT, OT and IOT equipment	
	It has protection mechanisms for remote and isolated operation equipment
	It has mechanisms to protect the support infrastructures (e.g. energy, air conditioning)
	It has mechanisms for the Protection and Security of Cables and radio-frequency communication systems
	It provides for the periodic maintenance of equipment, namely remote equipment in isolated operation
	It has procedures for the destruction of obsolete equipment (equipment that retains information or can be reused by third parties after its release and that may constitute a risk to the operation)
l) Relationship with Suppliers	
	Put Safety Requirements in Agreements with Suppliers

	Has Safety mechanisms planned and implemented in the electronic Value Chains (i.e. services provided electronically by suppliers, e.g. remote maintenance of systems)
	Applies security procedures in managing and changing Suppliers
m) Business Continuity, Disaster Management, and Information Security	
	Carries out cyber-security planning in the event of a disaster
	In the event of a contingency situation, it has mechanisms to ensure that the levels of cybersecurity required in normal operation are maintained
	Conducts Verifications (e.g. testing) and Reviews (e.g. auditing) on Continuity of Cyber Security
n) Compliance with legislation and contractual requirements	
	It has mechanisms to identify legislation and to identify applicable contractual requirements that allow for the identification of cybersecurity requirements
	It has mechanisms for the Protection of Records (e.g. Logs) and Data Protection
	Conducts independent reviews (e.g. Audit) of security
	Performs technical reviews (e.g. Intrusion audits)

Appendix 4: Cronbach's Alpha - Reliability Statistics

*Click **here** to return to the document*

Cronbach's Alpha	N of Items
0.974	16

Cronbach's Alpha - Item Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation
CsG	23.2765	258.802	0.921
CsM	23.3671	255.917	0.881
Mobile and Remote Working Systems	22.208	256.544	0.799
Classification of Information and Operation Support Assets	23.708	260.026	0.773
Access Control (Partially)	23.6889	259.552	0.883
Management of safety operations (M partially)	22.6044	263.369	0.723
Communications Management (partial M)	22.5794	259.975	0.772
Security in systems development, acquisition and maintenance	23.0937	257.394	0.814
Security Incident Management (M)	23.577	254.539	0.889
Hiring HR	23.7737	262.443	0.815
IT, OT and IOT asset management	23.2461	252.64	0.857
Management of security zones	23.183	263.865	0.725
Protection of IT, OT and IOT equipment	23.2708	263.359	0.794
Relationship with Suppliers	23.4461	254.311	0.873
Business Continuity, Disaster Management and Information Security	23.7032	261.154	0.852
Compliance with legislation and contractual requirements	23.3937	256.117	0.857

Appendix 5: Descriptive Analysis Management Models

*Click **here** to return to the document*

Management Model (Sub Model)	Responses	Relative Responses
Concession	**31**	**27.4%**
MultiMunicipal Concessionaire	6	5.3%
Municipal Concessionaire	25	22.1%
Delegation	**33**	**29.2%**
Municipal or Intermunicipal Company	26	23.0%
State/Municipality Partnership	7	6.2%
Direct Management	**49**	**43.4%**
Municipality Service	42	37.2%
Municipalized or Intermunicipalized Service	7	6.2%
Grand Total	**113**	**100.0%**

Appendix 6: Descriptive Analysis retail population

*Click **here** to return to the document*

Retail Population	Responses	Relative Responses
<20000	43	38.1%
20000-100000	42	37.2%
>100000	28	24.8%
Grand Total	**113**	**100.0%**

Appendix 7: Descriptive Analysis Area of Operation

*Click **here** to return to the document*

Area of Operation	Responses	Relative Responses
Water distribution	64	56.6%
Water gathering and treatment	12	10.6%
Water gathering, treatment and distribution	37	32.7%
Grand Total	**113**	**100.0%**

Appendix 8: Descriptive Analysis Pillars

*Click **here** to return to the document*

Pillar	Responses	Relative Responses
Corporate RSI (IT)	57	50.4%
RSI and Operational Technology (OT)	41	36.3%
Sensing, Robotics and Connected Technology (IoT)	15	13.3%
Grand Total	**113**	**100.0%**

Appendix 9: Overall Maturity Level

*Click **here** to return to the document*

Focus Area	Total Maturity Level
Average	1.509
Standard Deviation	0.111

Appendix 10: Maturity Level by Focus Area

*Click **here** to return to the document*

Focus Area	**Total Maturity Level**	Cyber Security Governance	Cyber Security Management		
Average	**1.509**	1.485	1.405		
Standard Deviation	**0.111**	1.165	1.257		
Focus Area	a) Mobile and Remote Working Systems	b) Classification of Information and Operation Support Assets	c) Access Control (Partially)	d) Management of security operations (M partially)	e) Communications Management (partial M)
Average	2.482	1.074	1.106	2.158	2.088
Standard Deviation	1.510	1.303	1.188	1.327	1.352
Focus Area	f) Safety in systems development, acquisition, and maintenance (IT, OT or IOT networks and information systems, water supply systems and subsystems)	g) Security Incident Management (M)	h) Hiring HR	i) IT, OT and IOT asset management	j) Management of security zones

Average	1.649	1.180	1.030	1.507	1.624
Standard Deviation	1.371	1.314	1.142	1.454	1.227
Focus Area	k) Protection of IT, OT and IOT equipment	l) Relationship with Suppliers	m) Business Continuity, Disaster Management, and Information Security	n) Compliance with legislation and contractual requirements	
Average	1.522	1.336	1.133	1.361	
Standard Deviation	1.169	1.435	1.207	1.311	

Appendix 11: Maturity Level of d) Management of security operations (M partially)

*Click **here** to return to the document*

Question	Has an Asset Change Management Process that assesses risk and authorizes changes to assets	It has a Capacity Management Process used in the assets (when applicable)	Performs segregation of development, test, quality, and production environments	Performs segregation of Corporate, Operational and Connected Equipment environments	Backs up and safeguards data, information, and systems	It has activity logging processes (Logs)	It has a control of the Operational Software Used or a control of its use (e.g. software that allows the management of the configuration of the assets in its operation)	Has a record of the Security Controls (i.e. mechanisms that guarantee the logical and physical security of the IT, OT or IOT)
Average	1.664	2.912	2.124	1.566	1.513	2.522	2.655	2.310
Standard Deviation	1.596	1.854	1.553	1.540	1.513	1.717	1.700	1.621

Appendix 12: Maturity Level of e) Communications Management (partial M)

*Click **here** to return to the document*

Question	Has implemented Network Controls (Firewall, IPS, IDS, etc.)	Has implemented a Network Security Architecture	It has an Information and Data Transfer Policy	Uses NDA Confidentiality Agreements
Average	3.182	2.327	1.554	1.418
Standard Deviation	1.759	1.639	1.570	1.595

Appendix 13: Maturity Level of h) Hiring HR

*Click **here** to return to the document*

Question	Has pre-employment verification mechanisms in place for key cybersecurity roles (e.g. criminal record validation, and CV checks)	Conditions of Engagement include cybersecurity requirements	Develops Training, Education and Awareness in cybersecurity	The use of Disciplinary Procedures is foreseen	On termination of employment, it imposes cybersecurity requirements on former employees (e.g. the responsibility to safeguard and not disseminate knowledge about the infrastructure and accesses for a certain period of time)
Average	0.956	0.796	1.407	1.159	0.832
Standard Deviation	1.270	1.189	1.694	1.533	1.329

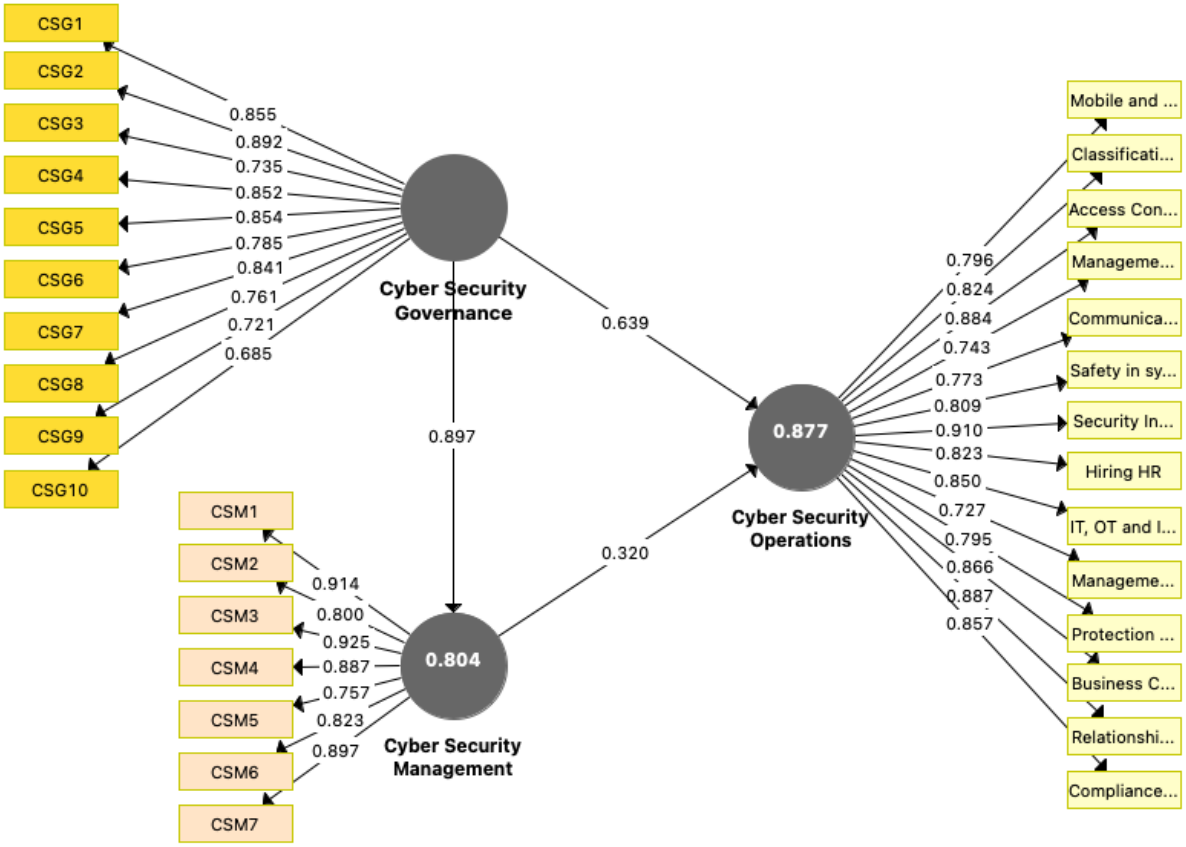
Appendix 14: Maturity Level of b) Classification of Information and Operation Support Assets

*Click **here** to return to the document*

Question	It has a process of Asset Identification by security level	It has an Asset Security Level Classification mechanism (e.g. an asset being considered essential already presupposes a classification of the security level of the asset)	Uses removable media to support and transport data and information securely or with embedded security mechanisms (e.g. encryption)
Average	1.150	1.009	1.062
Standard Deviation	1.495	1.473	1.378

Appendix 15: Dependencies between CsG, CsM and CsG – PLS analysis

*Click **here** to return to the document*



Path Coefficient Matrix – PLS

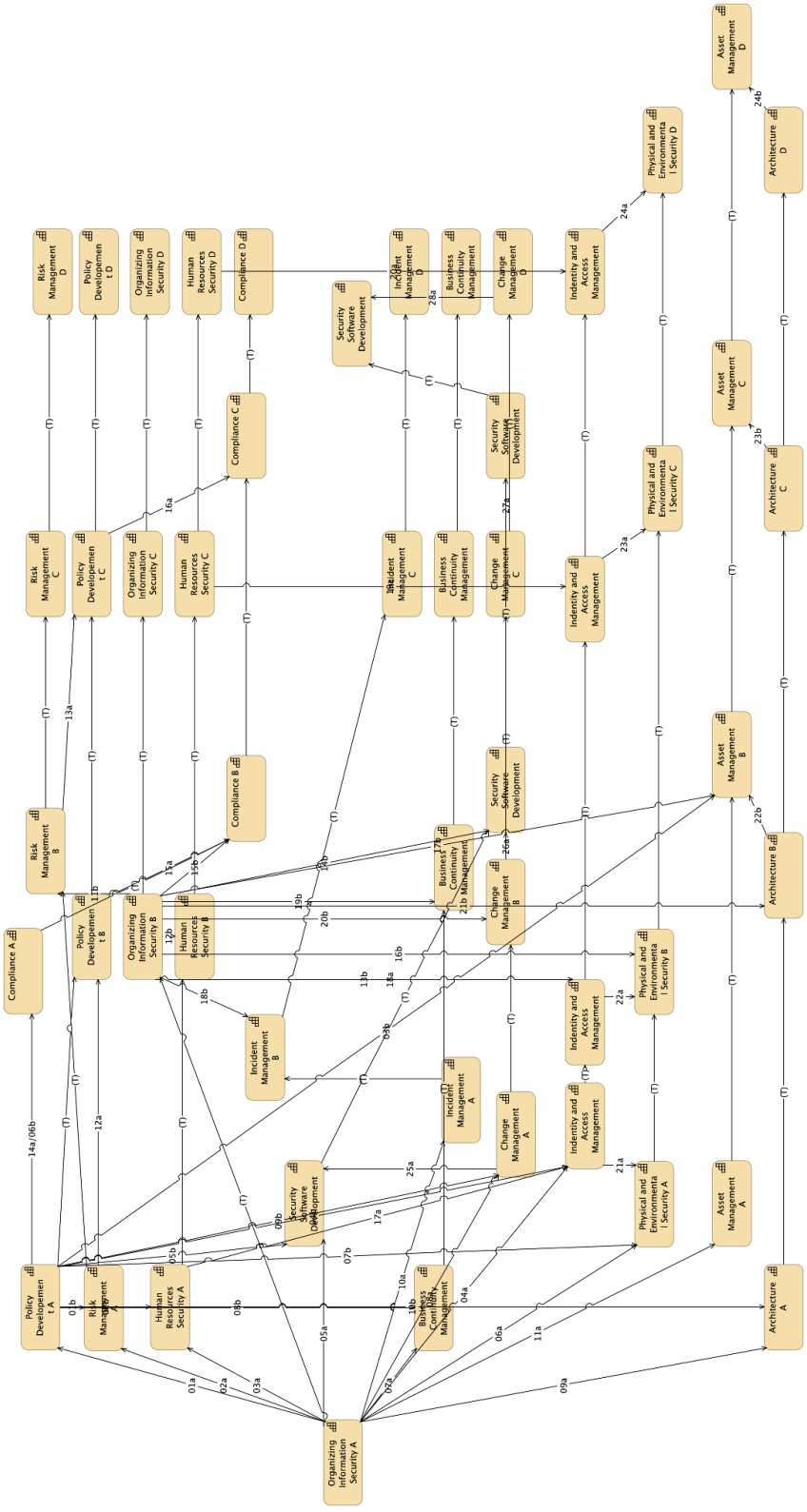
	CsG	CsM	CsO
CsG		0.897	0.639
CsM			0.320
CsO			

Path Coefficient - PLS – Bootstrapping

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
CsG -> CsM	0.897	0.899	0.025	35.735	0.000
CsG -> CsO	0.639	0.637	0.091	6.982	0.000
CsM -> CsO	0.320	0.323	0.092	3.490	0.000

Appendix 16: ISFAM dependencies – adapted by Spruit and Röling (2014)

*Click **here** to return to the document*



Appendix 17: PLS Analysis - Outer Loadings

*Click **here** to return to the document*

	CsG	CsM	CsO
CSG1	0.855		
CSG2	0.892		
CSG3	0.735		
CSG4	0.852		
CSG5	0.854		
CSG6	0.785		
CSG7	0.841		
CSG8	0.761		
CSG9	0.721		
CSG10	0.685		
CSM1		0.914	
CSM2		0.800	
CSM3		0.925	
CSM4		0.887	
CSM5		0.757	
CSM6		0.823	
CSM7		0.897	
Mobile and Remote Working Systems			0.796
Classification of Information and Operation Support Assets			0.824
Access Control (Partially)			0.884
Management of safety operations (M partially)			0.743
Communications Management (partial M)			0.773
Security in systems development, acquisition and maintenance			0.910
Security Incident Management (M)			0.809
Hiring HR			0.823
IT, OT and IOT asset management			0.850
Management of security zones			0.727

Protection of IT, OT and IOT equipment			0.795
Relationship with Suppliers			0.881
Business Continuity, Disaster Management and Information Security			0.866
Compliance with legislation and contractual requirements			0.857

Outer Loadings - PLS - Bootstraping

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
CSG1	0.855	0.852	0.034	25.336	0.000
CSG2	0.892	0.892	0.023	38.080	0.000
CSG3	0.735	0.729	0.077	9.489	0.000
CSG4	0.852	0.851	0.044	19.574	0.000
CSG5	0.854	0.852	0.041	20.778	0.000
CSG6	0.785	0.784	0.054	14.550	0.000
CSG7	0.841	0.840	0.039	21.366	0.000
CSG8	0.761	0.761	0.074	10.235	0.000
CSG9	0.721	0.714	0.067	10.714	0.000
CSG10	0.685	0.685	0.070	9.776	0.000
CSM1	0.914	0.912	0.027	33.279	0.000
CSM2	0.800	0.793	0.059	13.543	0.000
CSM3	0.925	0.925	0.026	35.287	0.000
CSM4	0.887	0.886	0.034	26.351	0.000
CSM5	0.757	0.757	0.066	11.411	0.000
CSM6	0.823	0.822	0.044	18.788	0.000
CSM7	0.897	0.896	0.025	35.515	0.000
Mobile and Remote Working Systems	0.796	0.796	0.044	18.110	0.000
Classification of Information and Operation Support Assets	0.824	0.823	0.042	19.733	0.000
Access Control (Partially)	0.884	0.883	0.024	36.294	0.000
Management of safety operations (M partially)	0.743	0.741	0.065	11.488	0.000
Communications Management (partial M)	0.773	0.769	0.051	15.166	0.000

Security in systems development, acquisition and maintenance	0.910	0.910	0.019	48.672	0.000
Security Incident Management (M)	0.809	0.807	0.046	17.608	0.000
Hiring HR	0.823	0.820	0.043	18.939	0.000
IT, OT and IOT asset management	0.850	0.847	0.040	21.143	0.000
Management of security zones	0.727	0.725	0.059	12.313	0.000
Protection of IT, OT and IOT equipment	0.795	0.793	0.050	15.883	0.000
Relationship with Suppliers	0.887	0.887	0.023	37.863	0.000
Business Continuity, Disaster Management and Information Security	0.866	0.867	0.026	32.746	0.000
Compliance with legislation and contractual requirements	0.857	0.858	0.027	31.772	0.000

Effect Size - PLS

	R Square	R Square Adjusted
CsM	0.804	0.801
CsO	0.877	0.874

Appendix 18: Results of one-sided ANOVA– between the three management models

*Click **here** to return to the document*

		Sum of Squares	df	Mean Square	F	Sig.
CsG	Between Groups	27.791	2	13.895	15.050	0.000
	Within Groups	61.86	67	0.923		
	Total	89.651	69			
CsM	Between Groups	37.386	2	18.693	16.220	0.000
	Within Groups	77.216	67	1.152		
	Total	114.602	69			
Mobile and Remote Working Systems (CsO)	Between Groups	25.713	2	12.856	8.081	0.001
	Within Groups	106.587	67	1.591		
	Total	132.3	69			

Classification of Information and Operation Support Assets (CsO)	Between Groups	7.542	2	3.771	2.352	0.103
	Within Groups	107.425	67	1.603		
	Total	114.967	69			
Access Control (Partially) (CsO)	Between Groups	30.477	2	15.239	16.415	0.000
	Within Groups	62.198	67	0.928		
	Total	92.675	69			
Management of safety operations (M partially) (CsO)	Between Groups	4.682	2	2.341	1.560	0.218
	Within Groups	100.542	67	1.501		
	Total	105.224	69			
Communications Management (partial M) (CsO)	Between Groups	7.594	2	3.797	2.356	0.103
	Within Groups	107.999	67	1.612		
	Total	115.593	69			
Security in systems development, acquisition and maintenance (CsO)	Between Groups	33.703	2	16.851	12.810	0.000
	Within Groups	88.139	67	1.316		
	Total	121.841	69			
Security Incident Management (M) (CsO)	Between Groups	32.474	2	16.237	12.256	0.000
	Within Groups	88.765	67	1.325		
	Total	121.238	69			
Hiring HR (CsO)	Between Groups	12.76	2	6.38	5.546	0.006
	Within Groups	77.077	67	1.15		
	Total	89.838	69			
IT, OT and IOT asset management (CsO)	Between Groups	43.506	2	21.753	14.680	0.000
	Within Groups	99.282	67	1.482		
	Total	142.787	69			
Management of security zones (CsO)	Between Groups	15.223	2	7.611	5.913	0.004
	Within Groups	86.246	67	1.287		
	Total	101.469	69			
Protection of IT, OT and IOT equipment (CsO)	Between Groups	14.619	2	7.31	6.598	0.002
	Within Groups	74.224	67	1.108		
	Total	88.843	69			
Relationship with Suppliers (CsO)	Between Groups	45.832	2	22.916	18.955	0.000
	Within Groups	81	67	1.209		
	Total	126.832	69			
Business Continuity, Disaster Management and Information Security (CsO)	Between Groups	19.44	2	9.72	9.243	0.000
	Within Groups	70.459	67	1.052		
	Total	89.898	69			
Compliance with legislation and contractual requirements (CsO)	Between Groups	33.516	2	16.758	13.117	0.000
	Within Groups	85.595	67	1.278		
	Total	119.111	69			
*The mean difference is significant at the 0.05 level						

Appendix 19: Results of Hochberg's Post-hoc test – between the three management models

*Click **here** to return to the document*

Maturity Stage in Cybersecurity Governance

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.00037*	0.33469	0.012	0.1815	1.8192
Concession - Direct Management	1.57382*	0.2875	0.000	0.8704	2.2772
Delegation - Direct Management	0.57345	0.28154	0.13	-0.1154	1.2623
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Management

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.37973*	0.37393	0.001	0.4649	2.2946
Concession - Direct Management	1.82601*	0.32121	0.000	1.0401	2.6119
Delegation - Direct Management	0.44629	0.31455	0.405	-0.3233	1.2159
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Mobile and Remote Working Systems

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.82904	0.43933	0.177	-0.2458	1.9039
Concession - Direct Management	1.49916*	0.37739	0.001	0.5758	2.4225
Delegation - Direct Management	0.67011	0.36956	0.205	-0.2341	1.5743
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Classification of Information and Operation Support Assets

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.40931	0.44105	0.73	-0.6697	1.4884
Concession - Direct Management	0.80518	0.37887	0.107	-0.1218	1.7321
Delegation - Direct Management	0.39587	0.37101	0.638	-0.5118	1.3036
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Access Control

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	.99387*	0.3356	0.013	0.1728	1.8149
Concession - Direct Management	1.64358*	0.28829	0.000	0.9383	2.3489
Delegation - Direct Management	0.64971	0.28231	0.071	-0.041	1.3404
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Management of safety operations

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.1273	0.42669	0.987	-0.9166	1.1712
Concession - Direct Management	0.57622	0.36653	0.317	-0.3205	1.473
Delegation - Direct Management	0.44893	0.35893	0.513	-0.4292	1.3271
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Communications Management

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.35202	0.44223	0.811	-0.7299	1.434
Concession - Direct Management	0.79519	0.37988	0.115	-0.1342	1.7246
Delegation - Direct Management	0.44316	0.372	0.553	-0.467	1.3533
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Security in systems development, acquisition and maintenance

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.17157*	0.3995	0.014	0.1942	2.149
Concession - Direct Management	1.73649*	0.34318	0.000	0.8969	2.5761
Delegation - Direct Management	0.56492	0.33606	0.262	-0.2573	1.3871
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Security Incident Management

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.17157*	0.40092	0.014	0.1907	2.1524
Concession - Direct Management	1.70495*	0.3444	0.000	0.8624	2.5476
Delegation - Direct Management	0.53339	0.33725	0.312	-0.2917	1.3585
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Hiring HR

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.10221	0.37359	0.99	-0.8118	1.0162
Concession - Direct Management	.90507*	0.32092	0.019	0.1199	1.6902
Delegation - Direct Management	.80286*	0.31427	0.038	0.034	1.5717
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - IT, OT and IOT asset management

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.36887*	0.424	0.006	0.3315	2.4062
Concession - Direct Management	1.97354*	0.36423	0.000	1.0824	2.8647
Delegation - Direct Management	0.60466	0.35667	0.256	-0.268	1.4773
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Management of security zones

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.7454	0.39519	0.177	-0.2215	1.7123
Concession - Direct Management	1.16512*	0.33948	0.003	0.3346	1.9957
Delegation - Direct Management	0.41971	0.33243	0.505	-0.3936	1.233
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Protection of IT, OT and IOT equipment

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.48456	0.36661	0.466	-0.4124	1.3815
Concession - Direct Management	1.10236*	0.31493	0.002	0.3319	1.8729
Delegation - Direct Management	0.61781	0.30839	0.139	-0.1367	1.3723
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Relationship with Suppliers

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.23897*	0.38298	0.006	0.302	2.176
Concession - Direct Management	2.01745*	0.32899	0.000	1.2126	2.8224
Delegation - Direct Management	0.77848	0.32216	0.054	-0.0097	1.5667
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Business Continuity, Disaster Management, and Information Security

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	0.82353	0.35719	0.071	-0.0504	1.6974
Concession - Direct Management	1.31532*	0.30684	0.000	0.5646	2.066
Delegation - Direct Management	0.49179	0.30047	0.284	-0.2433	1.2269
*The mean difference is significant at the 0.05 level					

Maturity Stage in Cybersecurity Operations - Compliance with legislation and contractual requirements

	Mean Difference (I - J)	Std. Error	Sig.	Lower Bound	Upper Bound
Concession - Delegation	1.36213*	0.39369	0.003	0.3989	2.3253
Concession - Direct Management	1.72382*	0.33819	0.000	0.8964	2.5512
Delegation - Direct Management	0.36169	0.33118	0.621	-0.4486	1.1719
*The mean difference is significant at the 0.05 level					

Appendix 20: Results of one-sided ANOVA– between the three retail population sizes

*Click **here** to return to the document*

		Sum of Squares	df	Mean Square	F	Sig.
CsG	Between Groups	1.287	2	0.643	0.488	0.616
	Within Groups	88.364	67	1.319		
	Total	89.651	69			
CsM	Between Groups	5.389	2	2.694	1.653	0.199
	Within Groups	109.213	67	1.63		
	Total	114.602	69			
Mobile and Remote Working Systems (CsO)	Between Groups	2.207	2	1.103	0.568	0.569
	Within Groups	130.093	67	1.942		
	Total	132.3	69			
Classification of Information and Operation Support Assets (CsO)	Between Groups	1.416	2	0.708	0.418	0.660
	Within Groups	113.551	67	1.695		
	Total	114.967	69			
Access Control (Partially) (CsO)	Between Groups	0.657	2	0.328	0.239	0.788
	Within Groups	92.018	67	1.373		
	Total	92.675	69			
Management of safety operations (M partially) (CsO)	Between Groups	1.325	2	0.662	0.427	0.654
	Within Groups	103.899	67	1.551		
	Total	105.224	69			
Communications Management (partial M) (CsO)	Between Groups	2.377	2	1.188	0.703	0.499
	Within Groups	113.216	67	1.69		
	Total	115.593	69			
Security in systems development,	Between Groups	5.563	2	2.781	1.603	0.209
	Within Groups	116.279	67	1.736		

acquisition and maintenance (CsO)	Total	121.841	69			
Security Incident Management (M) (CsO)	Between Groups	3.394	2	1.697	0.965	0.386
	Within Groups	117.844	67	1.759		
	Total	121.238	69			
Hiring HR (CsO)	Between Groups	1.341	2	0.671	0.508	0.604
	Within Groups	88.497	67	1.321		
	Total	89.838	69			
IT, OT and IOT asset management (CsO)	Between Groups	0.672	2	0.336	0.158	0.854
	Within Groups	142.115	67	2.121		
	Total	142.787	69			
Management of security zones (CsO)	Between Groups	1.211	2	0.605	0.405	0.669
	Within Groups	100.258	67	1.496		
	Total	101.469	69			
Protection of IT, OT and IOT equipment (CsO)	Between Groups	4.428	2	2.214	1.757	0.180
	Within Groups	84.416	67	1.26		
	Total	88.843	69			
Relationship with Suppliers (CsO)	Between Groups	1.844	2	0.922	0.494	0.612
	Within Groups	124.988	67	1.865		
	Total	126.832	69			
Business Continuity, Disaster Management and Information Security (CsO)	Between Groups	2.636	2	1.318	1.012	0.369
	Within Groups	87.263	67	1.302		
	Total	89.898	69			
Compliance with legislation and contractual requirements (CsO)	Between Groups	2.041	2	1.021	0.584	0.560
	Within Groups	117.07	67	1.747		
	Total	119.111	69			
*The mean difference is significant at the 0.05 level						

Appendix 21: Results of one-sided ANOVA– between the three areas of operations

*Click **here** to return to the document*

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CsG	Between Groups	0.761	2	0.38	0.287	0.752
	Within Groups	88.89	67	1.327		
	Total	89.651	69			
CsM	Between Groups	3.859	2	1.93	1.167	0.317
	Within Groups	110.742	67	1.653		
	Total	114.602	69			
	Between Groups	0.721	2	0.36	0.184	0.833
	Within Groups	131.579	67	1.964		

Mobile and Remote Working Systems (CsO)	Total	132.3	69			
Classification of Information and Operation Support Assets (CsO)	Between Groups	2.339	2	1.169	0.696	0.502
	Within Groups	112.628	67	1.681		
	Total	114.967	69			
Access Control (Partially) (CsO)	Between Groups	1.154	2	0.577	0.423	0.657
	Within Groups	91.52	67	1.366		
	Total	92.675	69			
Management of safety operations (M partially) (CsO)	Between Groups	0.427	2	0.214	0.136	0.873
	Within Groups	104.797	67	1.564		
	Total	105.224	69			
Communications Management (partial M) (CsO)	Between Groups	0.613	2	0.306	0.179	0.837
	Within Groups	114.98	67	1.716		
	Total	115.593	69			
Security in systems development, acquisition and maintenance (CsO)	Between Groups	0.315	2	0.158	0.087	0.917
	Within Groups	121.526	67	1.814		
	Total	121.841	69			
Security Incident Management (M) (CsO)	Between Groups	1.487	2	0.744	0.416	0.661
	Within Groups	119.751	67	1.787		
	Total	121.238	69			
Hiring HR (CsO)	Between Groups	0.048	2	0.024	0.018	0.982
	Within Groups	89.79	67	1.34		
	Total	89.838	69			
IT, OT and IOT asset management (CsO)	Between Groups	1.445	2	0.723	0.343	0.711
	Within Groups	141.342	67	2.11		
	Total	142.787	69			
Management of security zones (CsO)	Between Groups	0.694	2	0.347	0.231	0.795
	Within Groups	100.775	67	1.504		
	Total	101.469	69			
Protection of IT, OT and IOT equipment (CsO)	Between Groups	0.468	2	0.234	0.177	0.838
	Within Groups	88.376	67	1.319		
	Total	88.843	69			
Relationship with Suppliers (CsO)	Between Groups	0.389	2	0.195	0.103	0.902
	Within Groups	126.443	67	1.887		
	Total	126.832	69			
Business Continuity, Disaster Management and Information Security (CsO)	Between Groups	0.382	2	0.191	0.143	0.867
	Within Groups	89.517	67	1.336		
	Total	89.898	69			
Compliance with legislation and contractual requirements (CsO)	Between Groups	3.021	2	1.511	0.872	0.423
	Within Groups	116.089	67	1.733		
	Total	119.111	69			
*The mean difference is significant at the 0.05 level						