information

MDPI

Article

Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study

Manuel Domínguez-Dorado [1,*], Francisco J. Rodríguez-Pérez [2], Javier Carmona-Murillo [2], David Cortés-Polo [2] and Jesús Calle-Cancho [3]

[1] Department of Domains, Information Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain
[2] Department of Computing and Telematics Systems Engineering, University of Extremadura, 10003 Cáceres, Spain
[3] Extremadura Research Center for Advanced Technologies (CETA-CIEMAT), 10200 Trujillo, Spain
* Correspondence: manuel.dominguez@red.es; Tel.: +34-747-756-532

Abstract: Public sector organizations are facing an escalating challenge with the increasing volume and complexity of cyberattacks, which disrupt essential public services and jeopardize citizen data and privacy. Effective cybersecurity management has become an urgent necessity. To combat these threats comprehensively, the active involvement of all functional areas is crucial, necessitating a heightened holistic cybersecurity awareness among tactical and operational teams responsible for implementing security measures. Public entities face various challenges in maintaining this awareness, including difficulties in building a skilled cybersecurity workforce, coordinating mixed internal and external teams, and adapting to the outsourcing trend, which includes cybersecurity operations centers (CyberSOCs). Our research began with an extensive literature analysis to expand our insights derived from previous works, followed by a Spanish case study in collaboration with a digitization-focused public organization. The study revealed common features shared by public organizations globally. Collaborating with this public entity, we developed strategies tailored to its characteristics and transferrable to other public organizations. As a result, we propose the "Wide-Scope CyberSOC" as an innovative outsourced solution to enhance holistic awareness among the cross-functional cybersecurity team and facilitate comprehensive cybersecurity adoption within public organizations. We have also documented essential requirements for public entities when contracting Wide-Scope CyberSOC services to ensure alignment with their specific needs, accompanied by a management framework for seamless operation.

Keywords: cyberSOC outsourcing; holistic cybersecurity; public sector cyber-resilience; tactical-operational cybersecurity management; wide-scope cyberSOC

check for updates

Citation: Domínguez-Dorado, M.; Rodríguez-Pérez, F.J.; Carmona-Murillo, J.; Cortés-Polo, D.; Calle-Cancho, J. Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study. *Information* **2023**, *14*, 586. https://doi.org/10.3390/info14110586

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 12 September 2023
Revised: 17 October 2023
Accepted: 23 October 2023
Published: 25 October 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A multitude of definitions exist for the concept of cybersecurity. One of the wider definitions can be located in the work of Domínguez-Dorado et al. [1], which is closely intertwined with the notion of cyberspace. Cyberspace, defined as a network comprising interconnected information systems facilitated by communication networks, serves as the arena where individuals and entities interact and carry out their activities. This environment possesses distinct attributes, including high dynamism, common ground where each organization exercises control over a portion, a substantial reliance on third parties, and a necessity to prioritize not only information, but also the continuity of business processes and assets. Furthermore, it demands a focus on cyber resilience, among other considerations. Within this context, cybersecurity emerges as the discipline entrusted with the responsibility of managing and mitigating the threats, risks, and circumstances originating from this intricate cyberspace. A cyberattack, one of the most common of the mentioned cyber threats, encompasses any deliberate endeavor aimed at illicitly acquiring, disclosing, modifying, incapacitating, or annihilating data, applications, or other assets by means of unauthorized access to a network, computer system, or digital device. Furthermore, it is worth noting that attackers need not always gain access to any element within the organization's infrastructure. A mere misinformation campaign can suffice to tarnish the organization's reputation and trustworthiness. It is widely recognized that in the 21st Century, cybersecurity must be approached holistically. However, many organizations still struggle to effectively implement this approach due to a lack of alignment with traditional information security standards and practices. While an information security approach permits handling the cybersecurity aspects in many cases, it might be insufficient, alone, to address some of the risks and threats that emerge from cyberspace and for that reason, it is sometimes recommended to the adopt a more suitable cybersecurity approach as explained in von Solms and van Niekerk [2], and Reid and van Niekerk [3]. Therefore, achieving true holism and effective cybersecurity in practice remains a challenge for many organizations.

In various instances, the obstacles in achieving holistic cybersecurity deployment stem from issues tied to the cross-functional cybersecurity workforce and their capacity to establish a holistic approach to address the ever-evolving cyber threats landscape. This will be further elucidated in the forthcoming sections. For instance, one of the reasons that public sector organizations often outsource their cybersecurity needs, such as managed cybersecurity services or CyberSOC services, is the difficulty in recruiting and retaining civil servants with the necessary cybersecurity skills as stated in works as Furnell [4], De Zan [5], Reeder and Alan [6], or DeCrosta [7]. This is a problem faced by organizations across the public and private sectors, but it is particularly acute in the public sector for which we recommend the studies of Shava and Hofisi [8], Ngwenyama et al. [9], or Nizich [10], where the high demand and high salaries for cybersecurity professionals in the private sector can make it difficult to attract and retain talent. Additionally, when it comes to externalized CyberSOC contracts, these contracts must be renewed on a periodic basis, which can make it difficult to retain talent even when outsourcing these services. As a result, public sector organizations may struggle to maintain a consistent and effective approach to cybersecurity.

Relying heavily on outsourced services for their operational needs is also an impediment to focusing on a holistic framework, Reh Lee et al. [11]. Public sector entities often have a large number of highly skilled managers at various levels, but the hands-on work is frequently carried out by personnel from outsourced services providers. As a result, tactical-operational teams in these organizations are often composed of a mix of in-house staff and personnel from external service providers. These outsourced services are typically focused on specific areas, such as communications, software development, legal advising, human resources, or facilities management, and are typically only available to the specific area that contracted them. This fragmented approach creates obstacles to achieving holistic cybersecurity. Nevertheless, when a decision has been made to outsource a CyberSOC, this situation can be tapped as the foundation for building a truly holistic approach to cybersecurity, particularly in public sector organizations. To achieve this goal, the CyberSOC should be able to propose cybersecurity actions that can be implemented across the organization to achieve the necessary level of holism. This requires a cross-functional vision, as the nature of cybersecurity is inherently holistic. At the same time, the tactical-operational teams responsible for implementing these cybersecurity measures must be skilled in their respective areas of expertise to effectively design and implement cybersecurity safeguards in the "last mile". Unfortunately, it is often the case that neither the CyberSOC is adequately equipped to prescribe cybersecurity actions across all domains, nor are tactical-operational teams trained to apply their expertise to cybersecurity holistically, Onwibiko and Ouazzane [12].

Taking the aforementioned considerations into account, in this work, we address the enhancement of the organization's cybersecurity workforce capabilities to implement and maintain holistic cybersecurity. Our study commences with the necessity of implementing a model for managing holistic cybersecurity from the lower levels of a Spanish public organization. To attain this objective, we initiated a thorough examination of the existing literature, aiming to identify aspects highlighted in a prior work [1] and potential requisites for its practical application within the context of public sector. Subsequently, we conducted an in-depth analysis of the participating entity, which agreed to serve as a case study that could be generalized aid similar organizations. In this sense, the participating public entity contributed not only by providing information for analysis at the beginning of the study, but also actively participated in defining the solution presented in this paper. They shared their firsthand expertise and played a crucial role in identifying and addressing early implementation issues, adding substantial value to the research effort. The purpose of this analysis was to confirm the presence of insights we had identified as common during our examination of the existing literature, within the studied public organization. If these insights are indeed present, the same strategies devised for our specific use case should prove advantageous for public sector entities on a broader scale.

As a result of our investigation in cooperation with the participating entity, and in order to couple with the features of public sector organizations, we suggest introducing a new category of outsourced CyberSOC, which we refer to as the Wide-Scope CyberSOC. This innovative CyberSOC not only needs to incorporate a holistic cybersecurity approach into its daily operations, but also must possess the capability to convey this perspective and knowledge to every member of the cross-functional, diverse cybersecurity team, thereby empowering them to actively engage in this collaborative approach. As part of our study, we identify the key elements and requirements that a public organization should demand from the provider offering such a Wide-Scope CyberSOC service. This ensures that it facilitates the improvement of worker capabilities in the context of holistic cybersecurity.

As part of this endeavor, we draw upon existing frameworks and prior knowledge, such as the CyberTOMP framework and previous research on outsourcing and workforce training, among others. By amalgamating these resources with additional components, we streamline the process of implementing comprehensive cybersecurity measures within public organizations.

The remainder of this document is organized as follows: In Section 2, a review of research relevant for our proposal are carried out. Section 3 provides a detailed description of the methodology and steps employed in our study, including a literature review as an expanded and detailed version of the introduction. Section 4 presents the key findings obtained throughout the research and Section 5 summarizes the most significant conclusions of our study and presents the future lines of work that arise from it.

2. Analysis of the State of the Art

Starting at this juncture, we initiated an analysis of the existing literature. Our aim was to select relevant works that could facilitate an expansion of our knowledge, particularly regarding insights derived from one of our prior studies [1]. Additionally, we sought to identify any unique requirements or specific needs that might surface when applying the aforementioned work to a public sector organization. At this stage, our primary objective was to pinpoint common features, requirements, or needs that were shared by public organizations on a global scale. Table 1 provides a comprehensive overview of the collection of works we analyzed. However, a detailed contextualization of these works is provided in the subsequent paragraphs.

In recent decades, there has been a growing consensus regarding the meaning of cybersecurity and how it differs from previous approaches such as technology security and information security, represented by the works of Schatz et al. [2,13]. Cybersecurity emerges from the concept of cyberspace, which is a network of interconnected information services that allows people and organizations to conduct their activities and businesses beyond the physical boundaries of traditional organizations. As a result, much of the ecosystem in which organizations operate falls outside of their control, and the dependence of business activities on this “uncontrolled” part has increased over time. This new environment gives rise to new threats, risks, and countermeasures that must be properly addressed; Ghelani addresses this problem in [14].

Table 1. Studies examined to ascertain whether the identified characteristics could be extrapolated to the entire Public Sector.

Topic	Analyzed Source
Holistic cybersecurity foundations and cybersecurity context in public sector	[2,3,13,15–34]
Tactical-operational cybersecurity workforce management	[1,35–47]
Cybersecurity talent development and retention	[4–10,48–66]
Outsourcing in public sector	[11,67–88]
Outsourcing CyberSOC services	[89–95]

Slowly but surely, organizations are beginning to adopt practical approaches to cybersecurity management. However, these efforts are often limited to the strategic level and rely on information security standards rather than specific cybersecurity frameworks, as analyzed by Sulistyowati et al. in [15]. There has been relatively little progress in applying cybersecurity management to lower levels, which are crucial for achieving effective cybersecurity.

The situation in the public sector is even more challenging. Private companies are often early adopters of new technologies and approaches, while public sector organizations are typically slower to adopt these innovations due to a variety of constraints such as regulatory frameworks, contracting timeframes, hiring restrictions, career development opportunities, and excessive bureaucracy; Srinivas et al. goes deep in this topic in [16]. As a result, public sector entities may struggle to adapt nimbly to changes in the cybersecurity landscape. In many cases, they resort to outsourcing services in order to alleviate these challenges.

2.1. The Importance of a Holistic Approach to Cybersecurity

Cybersecurity differs from previous approaches in several ways, with the main differences stemming from the emergence of a new environment: the cyberspace. As a critical component in every digitized organization, cyberspace poses unique challenges since organizations cannot have complete control over it but have near complete dependency. As mentioned in the introduction "*a mere misinformation campaign can suffice to tarnish the organization's reputation and trustworthiness*". The threats and risks that emerge from this environment require unity of action and a broader holistic approach as studied in Ahmed et al. [17], and while some research has been conducted in this area as described by Atoum et al. in [18], much more work remains to achieve an acceptable level of holism, something that is covered by Kranemburg and Le Gars [19], and to cover those specific threats emanating from cyberspace for which an information security approach does not fit well. Recent studies also suggest the need to extend this holism not only within the organization itself, but also to its network of collaborators, civil organizations, government entities, and citizens, in order to provide the necessary unity of action to effectively respond to threats and risks, as investigated in [20] by Del-Real and Díaz-Fernández.

In order to effectively respond to risks and threats emanating from cyberspace, a holistic approach to cybersecurity must involve all functional areas of the organization. This requires a cross-functional approach that considers the unique perspectives and challenges of each area in order to develop comprehensive and effective cybersecurity strategies and, of course, it requires that the involved cross-functional cybersecurity workforce poses a high level of awareness regarding their potential contribution to the overall cybersecurity. Moreover, holism should not be a merely theoretical concept but had better instead to focus on practical implementation. While there have been some advances in achieving this holism in practice, most of these efforts have focused on the strategic level, with less attention given to bringing holism down to the tactical and operational levels of the organization. It is at these lower levels that the necessary safeguards for effective cybersecurity are implemented, though, and thus, it is essential to address the obstacles that prevent organizations from achieving true holism in their tactical-operational approach to cybersecurity.

2.2. Tactical-Operational Cybersecurity Workforce Management

There are several works that address cybersecurity management from different points of view: Rothrock et al. examine it from the board of director's perspective in [45]; the municipalities' points of view are reviewed by Preis and Susskind in [41]; the work by Limba et al. in [46] is centered in critical infrastructures; Yigit et al. focus on the assessment of cybersecurity capabilities in [37]; Rajan et al. focused on cross-functional collaboration in [38]; etc. All of these are very useful studies that have made possible several advances in cybersecurity. However, none of them are comprehensive models that can be used within an organization to handle cybersecurity at tactical and operational levels with a managerial approach. From our perspective, holism can only be achieved by designing and applying managerial techniques not only to lower levels, but also from lower levels, from those who must cooperate in the short and medium term to execute and design cybersecurity safeguards in the last mile, as considered by Axon et al. in [39].

While there are a few existing works that address holism at different levels, including the tactical and operational levels, there is still a need for further research and development in this area in order to effectively manage cybersecurity at these levels.

In [40], a work by Antunes et al., a good analysis is carried out after a practical implementation of an information security and a cybersecurity program in small and medium-size enterprises (SMEs) in Portugal. It takes into account the required controls and their degree of implementation, and profiles SMEs to apply proportional security measures. However, it does not provide details on the coordination mechanism for the multidisciplinary cybersecurity workforce and is based on the ISO 27001 standard for information security rather than cybersecurity. The authors themselves recognize this as a limitation. This analysis focuses on characterizing the participating SMEs in order to align the various safeguards with their specific needs.

The work developed by Domínguez-Dorado et al. in [1] proposed a more comprehensive set of procedural elements that explicitly enable cybersecurity management at the tactical and operational levels is defined as CyberTOMP framework. It is based on the most important cybersecurity frameworks and initiatives, and its authors have created a unified list of potential cybersecurity actions. These actions, also called "expected outcomes", are clustered into three implementation groups that can be applied to business assets with different cybersecurity needs, making it easier to select the appropriate cybersecurity controls, a selection of controls mechanism that is also covered by Breier and Hudec in [47].

While this framework is designed specifically for managing cybersecurity at the tactical and operational levels, it also allows for alignment with strategic cybersecurity goals through the use of the business impact analysis, that, according to Quinn et al. in [36], is a good tool to inform risk prioritization, and the cybersecurity master plan as hooks, which allows unifying cybersecurity and business continuity in a single framework, something described in [43] by Phillips and Tanner. This approach allows organizations to maintain a focus on their overall cybersecurity objectives while also addressing the specific challenges and needs at the tactical and operational levels and this allows the framework to be independent of the strategic standard chosen by the organization, while still providing complementary support. The study of Domínguez-Dorado et al. in [1] follows a practical approach and provides step-by-step processes, procedures, and guidance for identifying cybersecurity actions through a collaborative process that engages all functional areas of the organization. It is additionally supported by tools that facilitate the attainment of agreements on the necessary set of cybersecurity actions [35]. This approach allows for the development of holistic cybersecurity actions that are agreed upon and assigned to the functional areas involved in cybersecurity. The focus of this framework on business assets, which are understood as manageable and understandable units of cybersecurity, is a growing trend in the field as can be extracted from the works of Clark et al. [42] and Kure and Islam [44].

Nonetheless, although this framework provides a useful approach for managing cybersecurity at the tactical and operational levels, there is room to improve. For instance, it can be enhanced to identify the skills and training required by different functional areas of the organization in order to effectively carry out their cybersecurity tasks. Without the necessary skills and training, it is difficult for organizations to fully implement this framework and achieve the desired results.

Summarizing, to ensure the effectiveness of tactical and operational cybersecurity management, it is essential to develop mechanisms that can provide the necessary capabilities and expertise at these levels. This can be achieved through training programs, hiring qualified personnel, and implementing systems and processes that support the effective management of cybersecurity at the tactical and operational levels, or it can be achieved by acquiring this knowledge from specialized third parties. By taking these steps, organizations can better prepare themselves to effectively manage cybersecurity risks and threats and ensure that their overall cybersecurity efforts are successful.

2.3. Cybersecurity Talent Development and Retention

The development and retention of cybersecurity talent is a pressing issue in today's world. The rapid expansion of the cyberspace and the growing dependence of organizations on it have led to a shortage of cybersecurity professionals. The pandemic of COVID-19 has exacerbated this situation, as organizations have had to provide remote access and services to their employees, making them more vulnerable to cyber-attacks. This has motivated an increased demand for cybersecurity specialists, as organizations strive to protect themselves against these threats.

The shortage of cybersecurity talent has an indirect effect on organizations: in high-demand conditions, organizations are less able to retain cybersecurity-skilled personnel because many companies are competing for the same talent.

Training the existing workforce is an option, but it comes with the risk of losing skilled personnel due to the high demand for cybersecurity professionals. Despite this, providing training to the existing workforce can be beneficial in the short term, as it allows organizations to develop the skills of their employees and improve their ability to manage cybersecurity risks and threats. However, it is important for organizations to carefully consider their training strategies, as they need to ensure that they can retain their trained personnel in the long term. It is likely that more educated, motivated, and well-paid public employees will be easier for organizations to retain, as identified by Dahlstöm et al. [64].

There is an increasing number of research works that address this situation from different perspectives; for instance, in [4], the authors present evidence of the cybersecurity workforce shortage and the different forms of qualification that are available to meet the needs. The work presented in [5] show that this shortage is due in part to the high demand for cybersecurity specialists, as well as the limited availability of relevant training programs and qualifications. In response to this problem, some public organizations have turned to national skills competitions to create interest in cybersecurity and attract qualified personnel. In a work by Ahmad et al. [62], the authors propose to use incident management as a way to improve organizational learning in cybersecurity topics. This approach focuses on using real-life incidents to provide practical experience and training for cybersecurity personnel, with the aim of increasing their knowledge and expertise. The research carried out in [56] by Ahmad et al. highlights the need for interdisciplinary cybersecurity education and proposes a curriculum roadmap that integrates cybersecurity across technical and non-technical curricula. This approach seeks to address the current shortage of cybersecurity talent by providing a more comprehensive education on the subject. The research presented in [6] proposes three promising approaches to identify, recruit, and develop cybersecurity talent from both technical and non-technical personnel. These approaches aim to address the shortage of skilled cybersecurity professionals and improve organizations' ability to retain their talent. In [57], Chowdhury and Gkioulos identify cybersecurity training offerings for critical infrastructure protection and the key performance indicators that allow evaluating their effectiveness. In research by Noche [58], a comprehensive review of empirical studies aimed at developing the cybersecurity workforce is presented. Gamification is proposed as a method to improve the cybersecurity training of individuals responsible for protecting critical infrastructure in [54] by Ashley et al. In [60], a study by Kävrestad and Nohlberg, a review of evaluation strategies for cybersecurity training is presented with the aim of minimizing the impact of human factors on cyberattacks. In an investigation by Hulatt and Stavrou [59], the authors present the need for a multidisciplinary cybersecurity workforce that includes professionals from various backgrounds beyond traditional ones such as computing and Information Technology (IT). The authors of [55], Justice et al., analyze the future needs of the cybersecurity workforce. In [61], Maurer et al. identify the specific cybersecurity and professional skills required by those responsible for cybersecurity. These skills are necessary to ensure the effectiveness of tactical and operational cybersecurity management. Finally, in [7], the study analyses the quantitative and qualitative factors that contribute to the current shortage of cybersecurity professionals.

Overall, the shortage of cybersecurity talent is a growing concern for organizations, as it reduces their ability to effectively manage cybersecurity risks and protect against potential threats. This shortage is particularly acute at the tactical and operational levels, where hands-on skills are essential. Intense competition for skilled personnel has made it difficult for organizations to attract and retain the talent they need, leading to further declines in their ability to manage cybersecurity effectively. In order to address this issue, organizations must develop effective strategies to attract and retain cybersecurity talent, particularly at the tactical and operational levels. This will require a comprehensive approach that includes training programs, hiring qualified personnel, and implementing systems and processes that support effective cybersecurity management.

2.4. Outsourcing in Public Sector

There are various forms of potential collaboration in public service delivery, as Kekez et al. analyze in [85], with outsourcing being one of the most common. The decision to outsource is often driven by a desire to reduce costs, as investigated by Santos and Fontana in [71] and improve efficiency. By transferring certain business processes or functions to an external provider, a company can benefit from their expertise and specialized capabilities. Additionally, outsourcing can provide access to a global talent pool, allowing companies to tap into a wider range of skills and knowledge. In addition to cost savings and access to specialized skills, outsourcing can also help a business to focus on its core competencies and drive growth. As such, this is a strategy that is often considered by public organizations looking to streamline their operations and improve their public services.

Although there are some differences between public and private outsourcing, which is explored in [87] by Burnes and Anastasiadis, the motivations for outsourcing are similar across both public and private sectors, with cost control and reduction, focus on core capabilities, and access to supplier expertise and technologies being among the key drivers as supported by works carried out by Marco-Simó and Pastor-Collado [74] or Bogoviz et al. [77], but also to face exceptional situations like the pandemic of COVID-19 as analyzed in [75] by van der Wal. Public organizations are generally well-equipped with individuals who have the necessary skills and expertise to manage tasks and processes effectively. However, they frequently face challenges when it comes to staffing the most technical and operational tasks, which require specialized knowledge and expertise. As a result, these organizations may struggle to effectively perform these tasks, leading to reduced efficiency and performance.

In order to overcome these challenges, many public organizations turn their strategic plans to outsourcing through public-private contracts, as examined in Pavelko et al. [70]. These contracts provide a legal framework for defining the roles and responsibilities of each party, as well as the terms of the relationship between the public and private sectors. They also help to ensure that the activities and services provided under the contract are organized and carried out in a manner that is consistent with the parties' respective rights and obligations, something studied in the research of Bloomfield et al. [78]. The accurate definition of service requirements within these contracts is a key factor for Proscovia in [79] to successful outsourcing, which will later depend on managing the outsourcing relationship well after the decision is made, which is evaluated in [69] by Heikkilä and Cordon. The lack of service requirements definitions when outsourcing in public sector led to a falling quality of the provided public services.

Outsourcing is a controversial topic. There are many interesting works that discuss the pros and cons of outsourcing in the public sector under different circumstances such as those carried out by Tayauova, Lobao et al., Aswini, Sánchez, Rizwan and Bhatti, Johansson and Siverbo, and Andersson et al. in [76,81–83,86,88] or [80], respectively, among others. Although this debate is outside the scope of our study, we mention them here to highlight the significance of the outsourcing approach for public sector entities.

While outsourcing can have a slight negative effect on the performance and perception of in-house employees [11], it is often necessary in order to ensure that tactical-operational teams have the necessary skills and expertise. But as a result of outsourcing, tactical-operational teams in the public sector are often composed of a mix of public sector employees and outsourced or insourced personnel.

It is also important to note that by outsourcing any service, the outsourcing organization is expanding its supply chain, which can lead to additional risks, including in the realm of cybersecurity. Some of these topics are covered in Nasrulddin et al. [72] and Repetto et al. [73].

2.5. Outsourcing CyberSOC Services

A CyberSOC, is a specialized unit that is focused on monitoring, detecting, and responding to cyber threats in real time. Among the main duties of a CyberSOC the following are included, as determined in Saraiva and Mateus-Coelho [90]:

- Continuous monitoring of an organization's networks and systems for signs of potential cyber threats;
- Detection of cyber threats through the use of advanced technology and analysis of security data;
- Response to detected threats, including implementing countermeasures to prevent or mitigate the impact of the threat;
- Communication with relevant stakeholders, such as the organization's leadership and other security teams, about detected threats and response efforts;
- Ongoing analysis of security data to identify patterns and trends that can help improve the organization's overall security posture.

In addition to these core duties, a CyberSOC may also be responsible for providing training and education to the organization's staff on cybersecurity best practices, as well as collaborating with other security teams and external partners to share information and coordinate efforts to defend against cyber threats. Overall, the role of a CyberSOC is essential in helping organizations protect themselves from the constantly evolving threat landscape of the digital world, as analyzed in [91] by Shutock and Dietrich, and assess their readiness level, something evaluated in [92] by Georgiadou et al.

From our perspective, this set of capabilities and responsibilities, especially the non-core ones, can be tapped by the organization to turn the CyberSOC into the cornerstone over which develop real holistic cybersecurity. Although in public administration, where outsourcing is something very common, this possibility cannot be extrapolated directly, due to the existence of cross-functional tactical and operational teams composed by employees and outsourced workforce.

From a cybersecurity perspective, the presence of mixed multidisciplinary in-house/outsourced tactical and operational teams, which experience high levels of turnover every few years, is not necessarily a problem, but it does present a challenging situation that must be managed carefully in order to ensure effective holistic cybersecurity across the organization.

The above could be even more challenging if the CyberSOC service itself is outsourced, which is also a common practice in public sector and involves roles with high cybersecurity skills, as questioned in Nugraha [94]. Although outsourcing also has advantages, as mentioned in previous paragraphs, the cons are relevant in this case, according to Ti Dun et al. [93], and several efforts have to be made to enhance the communication between the public entity's manager and the provider of CyberSOC services, which is analyzed in [95] by Kokulu et al. In view of the above, we are of the opinion that one potential disadvantage of outsourcing a CyberSOC is the loss of control over the security of the organization's systems and data. When a CyberSOC is managed by an external provider, the organization loses the ability to directly oversee and manage the security measures in place to protect its systems and data. This can make it difficult to ensure that the necessary security protocols are being followed and can increase the risk of security breaches or other incidents. Another disadvantage is the potential for reduced flexibility and responsiveness. When a CyberSOC is outsourced, the organization is reliant on the external provider for the timely detection and response to security threats. If the provider is unable to respond quickly or effectively, this can leave the organization vulnerable to security breaches or other incidents. Lastly, assigning an outsourced CyberSOC to prescribe cybersecurity tasks for all of the organization's functional areas that are also partially outsourced can lead to conflicts and a lack of coordination between service providers. This can potentially be challenging to resolve and can impact the organization's cybersecurity strategy.

As previously mentioned, there are several situations in which public sector organizations may need to outsource their CyberSOC services. In order for these outsourced CyberSOCs to be able to provide cybersecurity recommendations for all of the organization's functional areas and support their implementation, the outsourcing public entity must put in some effort upfront to identify the necessary capabilities of the CyberSOC and include them as requirements in the related technical specifications. However, these public organizations are often outsourcing their CyberSOC services due to a lack of knowledge and skills, making it difficult for them to identify the necessary requirements. It is necessary to simplify this process in order to ensure that the requirements for the service provider of an outsourced CyberSOC align with the needs of the public organization to develop effective, comprehensive cybersecurity.

2.6. Insights after Reviewing the State of the Art

After conducting a thorough review to identify the unique circumstances and issues that prevent the achievement of effective, comprehensive cybersecurity in public sector organizations, we found that:

- The role of tactical-operational cross-functional teams in cybersecurity management is crucial, as they are responsible for implementing the actual cybersecurity countermeasures within the organization and provide the corresponding holism. There is a dearth of research studies that examine this specific niche from a managerial standpoint, thereby creating a void that hampers the implementation of a comprehensive cybersecurity management approach. It is imperative that such an approach be undertaken at these levels to prevent the formation of isolated units, both within the public and private sectors;
- Currently, there is a shortage of cybersecurity professionals that is expected to continue in the short and medium term. This shortage is particularly acute in public sector organizations, which often have personnel capable of managing at all levels but lack technical staff with hands-on expertise. Therefore, it is imperative to undertake certain actions aimed at raising awareness among the cross-functional cybersecurity workforce regarding the implications of their specific areas of expertise in the broader realm of cybersecurity. This will enable them to become personnel who possess the necessary expertise and managerial acumen to effectively confront the prevailing cyber threats;
- Public sector entities heavily rely on the practice of outsourcing. One of the reasons for that is to gain access to technical staff with hands-on expertise, trying to avoid the mentioned workforce shortage. As a result, their cross-functional tactical-operational teams are often composed of a mix of employees and outsourced workers, which are frequently replaced as their outsourcing contracts come to an end. It is common for public organizations to also outsource CyberSOC services. Although outsourcing appears to be a necessary step in many instances, it is crucial that it is executed in a manner that ensures the service provider aligns with the cybersecurity requirements

of the business. Specifically, it must be capable of facilitating the implementation of a comprehensive tactical-operational cybersecurity management approach.

3. Method

The present research is driven by the real need of a public sector entity, at its own initiative, to undertake an ambitious program to implement a tactical-operational management model for cybersecurity, providing the required holism to tackle current cyber threats. The mentioned organization is a Spanish public organization, which is involved in promoting technology in all spheres of society. It employs approximately 300 individuals and comprises five departments along with sixteen primary functional areas. Exploiting this need and in mutual agreement with the involved organization, we conducted a research project aimed at providing a series of valuable contributions not only to that organization, but also to other public entities with similar needs.

We undertook the research employing a business analysis methodology, evaluating the capacities of the public entity to effectively implement a comprehensive tactical-operational cybersecurity management approach, which holds the potential to foster a substantial transformation in the cybersecurity culture. Our study was divided into four phases grouped in two stages:

- Stage 1. Pre-study of public sector requirements and context
    - Phase 1. In this phase, after a systematic analysis of the existing literature was carried out, the corresponding insights were analyzed and organized to detect whether the features, requirements, and impediments to deploy a truly holistic cybersecurity management model are shared by different public sector organizations worldwide; this phase corresponds to the work described in Section 2.
    - Phase 2. During this phase, a series of meetings were conducted with the participating organization to discuss the prerequisites for implementing a comprehensive cybersecurity management model. These discussions aimed to enable the organization to assess challenges and barriers that could impede the adoption of such a model. Additionally, the organization shared anonymously, and whenever possible, information about other public entities it is related to, which allowed gathering relevant insight both directly and indirectly. This phase focused on determining the organization's capability to fulfill the model's requirements and identify potential obstacles. Continuing with our work, the information retrieved in the mentioned meetings was channelized using the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis technique described by Benzaghta et al. in [96] to analyze deeply and systematically de current circumstances of the participating public entity. We also determine at this point whether the resulting insights coincide with the common features identified for public organizations in a wider context.
    - Phase 3. At this stage, we identified a specific set of actionable strategies that we understood as universally applicable to all public sector entities due the fact that they share common root characteristics as determined in Phase 1 and Phase 2. These strategies were aimed at the successful implementation of a comprehensive tactical-operational cybersecurity management model. This model takes into consideration the distinctive attributes of the public organizations identified in the previous phase and we use the Threats, Opportunities, Weaknesses, and Strengths (TOWS) matrix technique, described in Pasaribu et al. [97], to analyze the external opportunities and threats and compare them to the organization's strengths and weaknesses, resulting in a set of actionable strategies. The combined use of SWOT–TOWS analysis is common to analyze and interpret systems, especially to develop strategies; the work of Hattangadi in [98] analyzes them together.
- Stage 2. Model development.
    - Phase 4. Finally, we carried out our proposal to develop the identified strategies, that would allow public entities to seamlessly adopt a holistic management model

of cybersecurity, taking into account and incorporating the previously identified peculiarities and facing the existing specific challenges of public entities. Throughout the duration of this phase, the research team benefited from the active engagement of the participating public entity. Their involvement enriched the solutions devised by providing insights from the perspective of the recipient institution.

3.1. Stage 1: Pre-Study of Public Sector Requirements and Context

During this stage, encompassing all tasks within phases 1, 2, and 3, we conducted a comprehensive preliminary study to systematically analyze the context surrounding public sector entities. This analysis extended to the international perspective through a state-of-the-art review and to our specific Spanish case study. The overarching objective at this stage was to acquire an in-depth understanding of the requirements and characteristics unique to public sector organizations, enabling them to effectively address the challenges faced by the cross-functional cybersecurity workforce in implementing holistic cybersecurity. Armed with this knowledge, we aimed to identify the most advantageous strategies for any model seeking to address these challenges and seamlessly integrate with public sector entities. We leveraged these identified strategies in the subsequent development of our proposal.

In phase 2, several meetings were held with the participating organization, aimed at discussing the requirements that need to be met to implement a holistic cybersecurity management model. The main purpose of these meetings was to analyze its specific context, gathering relevant information about its strengths and weaknesses, as well as the existing opportunities and threats in relation to the implementation of a holistic cybersecurity model. Moreover, throughout the entire process, the participating organization provided anonymous information concerning other similar public entities with which it had relationships, pertaining to the same aspects being analyzed in its case. As a result, the study incorporates direct information provided by the organization itself, as well as secondary information concerning third parties, provided by the organization but in an indirect way, thus necessitating a more in-depth subsequent analysis. Based on these, and with the gathered information, a SWOT analysis was conducted, which succinctly represented the characteristics of the organization and its starting conditions to address the process of deploying a holistic model that enables the enhancement of its cybersecurity (Table 2).

Table 2. SWOT analysis based on the information provided by the participating entity regarding its own strengths, weaknesses, opportunities, and threats, as well as those of third-party public entities.

	Strengths	**Weakness**
Internal	• Their personnel are highly skilled as managers; • Have much experience in outsourcing processes and can contract the required skilled service providers if needed; • Can provide long term stable employment; • They are not necessarily under the pressure of a profit goal but driven by the vocation of public utility.	• Have difficulty to retain and develop the career of cybersecurity personnel; • Lack of personnel skilled in hands-on tasks; • Their teams are often composed by in-house and outsourced personnel; • They are silo-based organizations where cross-domain collaboration is difficult.
	Opportunities	Threats
External	• There is an increasing interest that public organizations enhance their cybersecurity capabilities; • Can partner with private sector organizations to leverage their expertise and technology to improve cybersecurity; • Those public organizations able to offer cyber-resilient services will be more valued; • More funding is available for public organization to modernize in terms of cybersecurity.	• Private sector can attract potential employees more effectively; • Regulations hinder to contract the same service providers continuously; • The number of cyber criminals seeking to target public sector organizations is increasing; • Cyber threats are constantly evolving, and the public sector may struggle to keep up with the latest threats and technologies. This can lead to a reactive approach to cybersecurity rather than a proactive one.
	Positive	Negative

From this phase, we obtained a comprehensive understanding of the organization's potential to implement the intended model. The positive aspects can be summarized as a high capacity for management and expertise in outsourcing, coupled with a growing interest and allocation of budget towards enhancing cybersecurity in the public sector. The negative aspects primarily revolve around the public entity's challenges in developing and retaining technical cybersecurity talent, as well as difficulties in adapting to highly dynamic changes or implementing a collaborative internal working system.

In conclusion of this stage, we have come to the realization that the common characteristics we found in the analysis of the state of the art are also present in the participating entity and the rest of entities we analyzed indirectly. Extensive literature exists that describes similar circumstances in public organizations worldwide. Henceforth, we possessed sufficient confidence to perceive this situation as a widespread phenomenon within public sector organizations aspiring to implement a comprehensive tactical-operational cybersecurity management approach. At this point in our study, we had gathered sufficient evidence to suggest that the participating organization exhibited similar characteristics to other public entities worldwide in terms of their potential to implement a holistic cybersecurity management model. This encouraged us to believe that the solution we were developing for the participating entity could also be beneficial to other organizations with similar profiles.

Finally, in the third phase, we employed the prior analysis as an input to a TOWS matrix with the objective of translating the insights from Phase 1 and Phase 2 into actionable strategies. The resulting strategies were:

- Strengths and Opportunities (SO) strategies, commonly referred to as the "Maxi-Maxi Strategy", encompass the utilization of strengths to optimize opportunities. In a TOWS analysis, this type of strategy is considered highly proactive and has a higher likelihood of yielding success. In our case, the public organization could leverage its expertise, skills, and capabilities in public procurement and outsourcing to effectively utilize the available funding. By establishing public-private contracts, the organization can transform itself into a resilient entity in the field of cybersecurity and provide better and more secure public services;
- Strengths and Threats (ST) strategies, commonly referred to as the "Maxi-Mini Strategy", involve leveraging strengths to mitigate threats. In our study, by leveraging the growing allocation of funds for cybersecurity enhancements and the heightened focus on modernizing and fortifying public entities and services, the public organization can seize the opportunity to engage public sector companies. This strategic move aims to facilitate the organization's adaptation to the dynamic, challenging, and rapidly evolving contexts of cybersecurity and cyber threats;
- Weakness and Opportunities (WO) strategies, commonly referred to as the "Mini-Maxi Strategy", encompass the approach of minimizing weaknesses by capitalizing on available opportunities. In our work, the growing allocation of funds for cybersecurity enhancements, coupled with the heightened emphasis on modernizing and fortifying public entities and services, presents an opportunity for the public organization to utilize outsourced personnel, augment the cybersecurity skills and career progression of its existing employees, and establish methodological foundations to foster true holism;
- Weaknesses and Threats (WT) strategies, also recognized as the "Mini-Mini Strategy", are employed to minimize weaknesses and evade threats. Within a TOWS analysis, this type of strategy is considered highly reactive/defensive and may not be as reliable in generating success. Due to this rationale, this strategy is not deemed conducive to steering the advancement of our proposal.

In summary, our objective in this research was to find a mechanism that would facilitate the development of the described strategies, namely, the SO, ST, and WO strategies. Essentially, this mechanism should be based on the outsourcing of services, leveraging existing resources and the interest in cybersecurity within the context of public sector entities. Its purpose would be to enhance the cybersecurity skills of various functional areas within the organization, improve its talent retention capabilities, implement a holistic model, and establish a cybersecurity management context that seamlessly orchestrates all these elements.

3.2. Stage 2: Model Development

The second stage of our research began with the inputs from stage 1, namely, the strategies required for a model aiming to address the challenges of deploying holistic cybersecurity by the cross-functional cybersecurity workforce in public sector organizations. In this specific context, the strategies previously defined were adjusted to accommodate the unique characteristics of public entities, ensuring that the resulting model would be well-suited to their needs.

Throughout Phase 4, we formulated our proposal to execute the strategies delineated in the preceding stage. Following thorough deliberations, we made the strategic choice to harness the outsourcing capabilities of public sector entities and establish a novel type of outsourced CyberSOC. This strategic decision was aimed at bolstering the cybersecurity proficiency of the cross-functional workforce while aligning with the specific contextual considerations, strengths, and weaknesses unique to public sector organizations. The outcome of this phase, as detailed in the following sections, are the results of our research: a novel concept called the "Wide-Scope CyberSOC" along with the essential documentation and procedural elements for its easy and efficient implementation within public sector organizations.

As mentioned, our proposal involves the utilization of an outsourced CyberSOC service, equipped with specialized capabilities that serve as the foundation for fostering a holistic approach to cybersecurity management within the organization. We designated this novel CyberSOC type as "Wide-Scope CyberSOC".

In order to materialize this Wide-Scope CyberSOC, we deemed it imperative to consider several pivotal aspects, as depicted in Figure 1:

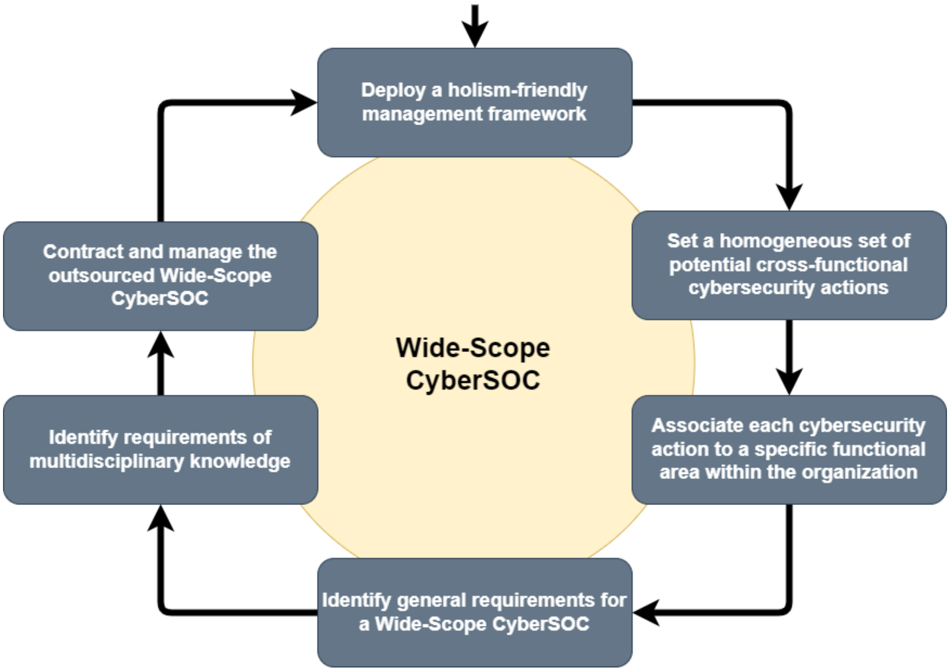
Deploy a holism-friendly management framework
Set a homogeneous set of potential cross-functional cybersecurity actions
Associate each cybersecurity action to a specific functional area within the organization
Identify general requirements for a Wide-Scope CyberSOC
Identify requirements of multidisciplinary knowledge
Contract and manage the outsourced Wide-Scope CyberSOC
Wide-Scope CyberSOC

Figure 1. Key aspects to be taken into consideration to seamlessly integrate a Wide-Scope CyberSOC into the organization, enabling a holistic management of cybersecurity.

- The establishment of a cybersecurity management framework that can deliver the necessary holism at lower organizational levels is imperative. Contracting a Wide-Scope CyberSOC to assist the organization in overcoming silos and adopting a holistic approach would be futile if the procedural foundations to support such an extended CyberSOC have not been put in place. Consequently, based on the reasons outlined in Section 2.2, we opted for the CyberTOMP framework.

- Since the Wide-Scope CyberSOC is intended to provide guidance and assistance in designing and implementing multidisciplinary cybersecurity measures, it is essential to pre-identify the potential set of such cybersecurity actions. This enables us to contractually demand support for each of these actions. As our proposal is based on CyberTOMP, this set of actions is already identified within this framework. The Unified List of Expected Outcomes (ULEO) of CyberTOMP (Table 3) precisely represents a compilation of potential cybersecurity actions. There, every unified expected outcome is represented together with its corresponding function and category from the cybersecurity framework of National Institute of Standards and Technology (NIST). Each expected outcome in the ULEO has its own identifier. Expected outcomes from [99] are identified with the prefix "9D", those from [100] are identified with the prefix "CSC", and the remainder are identified using the original terminology from [101]. Furthermore, the associated Implementation Groups (IGs), to which the unified expected outcome should be applied, are determined. This enables the development of a proportionate cybersecurity approach, as lower IGs define the unified expected outcomes applicable to assets of lower criticality, while higher IGs pertain to assets with greater criticality. Additionally, leveraging this list for our proposal allows us to utilize the associated set of metrics concerning its implementation and the cybersecurity status of each asset to which they are applied.

Table 3. A fragment of the ULEO, as defined in the CyberTOMP framework, included for informational purposes.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3
Protect	PR.PT	9D-4		√	√
Protect	PR.PT	CSC-4.12			√
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
Protect	PR.PT	PR.PT-5	√	√	√

- It is also crucial to identify which functional area should be responsible for each of these cybersecurity actions, ensuring that the contribution of each functional area to overall cybersecurity enables genuine holistic cybersecurity. Furthermore, this allows the Wide-Scope CyberSOC to focus its efforts on supporting each area in developing specific cybersecurity actions from the perspective of its specialized field. During our research efforts, we conducted a detailed analysis of the various functional areas involved in cybersecurity, as defined in CyberTOMP (Table 4). We also examined the specific scope of each cybersecurity action and established the association between functional areas and corresponding actions in all cases, as described in [99,100,102]. The comprehensive results of our investigation can be found in Appendix A.

Table 4. Functional areas of the organization involved in holistic cybersecurity, as defined in the reference framework used in our proposal.

Area ID	Area's Main Cybersecurity Responsibilities
FA1	In charge of the security of Internet of Things (IoT) devices.
FA2	Implementation of active defense measures, vulnerabilities management, threat hunting, Security Information and Event Management (SIEM) operation, activities within a CyberSOC, and incident response.
FA3	Human resources preparation regarding cybersecurity threats through continuous training and its reinforcement, as well as the design and execution of practical cybersecurity exercises

Table 4. *Cont.*

Area ID	Area's Main Cybersecurity Responsibilities
FA4	Analysis of internal and external threats, exchange of threat intelligence with third parties, and preparation and incorporation of Indicators of Compromise (IoCs).
FA5	Surveillance of the applicable regulation and its incorporation into cybersecurity. Key Performance Indicators (KPI) monitoring, establishment of strategies, policies, standards, processes, procedures, and corporate instructions.
FA6	Risk treatment, business continuity management, crisis management, establishing the organization's position regarding cyber risks, insurance contracting, risk registration, auditing, definition of groups of risk management, and definition of those responsible and owners of the processes and assets.
FA7	Cybersecurity risk analysis, vulnerability scanning, supply chain risk identification and analysis, asset inventory, risk monitoring, penetration testing of infrastructure, people, or information systems.
FA8	Leading the secure software development cycle, continuous integration and deployment, user experience security, software quality, API security, identification of information flows in information systems, management of the free software used and the static or dynamic analysis of the code.
FA9	Management, development, implementation, and verification of compliance with the standards and regulations defined at the corporate level for cybersecurity: CIS controls [100], CIS Community Defense Model [103], MITRE matrix [104,105], NIST framework [101] for the improvement of cybersecurity of critical infrastructures or the family of standards ISO27000, CyberTOMP.
FA10	Management, definition, implementation, operation, prevention, etc., in relation to cryptography, key and certificate management, encryption standards, security engineering, access controls with or without multiple authentication factors, single sign-on, privileged access management, identity management, identity federation, cloud security, container security, endpoint security, data protection and prevention of data leakage, network design to prevent distributed denial of service attacks, development and secure configuration of systems, patch and update management and the establishment of secure reference configurations.
FA11	Promote study, education and training, attendance at conferences and participation in related professional groups, training, or certification.
FA12	Internal and external corporate communication, social networks management, marketing and the establishment and maintenance of institutional relationship with interested third parties with whom the organization maintains some type of contact.

- Given that the Wide-Scope CyberSOC is going to be outsourced to third parties, it is highly advisable to establish a set of general requirements that clearly distinguish what is being contracted as a Wide-Scope CyberSOC and not merely a technologically focused CyberSOC. This is important because many service providers tend to offer traditional, technology-focused CyberSOC services by default. In the context of a public entity that has outsourced some of its workforce and has an external CyberSOC, we define a Wide-Scope CyberSOC as a CyberSOC with the following general requirements:
    - Must poses the necessary skills and capabilities to understand, design, prescribe, advise, and monitor cybersecurity actions that can be executed by every functional area within an organization that can contribute to the organization's strategic common effort, with a particular focus on those functional areas that fall outside of the realm of computing or information technologies;
    - Must be capable of positioning itself within the context of each organization's functional areas, and from this vantage point, be able to understand the implications (including what, how, where, when, and who) of these areas of expertise with regards to cybersecurity. In fact, a Wide-Scope CyberSOC must be an expert in all fields of knowledge that are relevant to cybersecurity. Not only in the most technological ones;
    - Must be aware that those functional areas that do not typically participate in cybersecurity may not be conscious of the fact that they can significantly contribute to improving the overall state of cybersecurity from within their own areas of expertise. As such, a Wide-Scope CyberSOC must also act as a mentor to enhance

  the awareness of these functional areas and develop their cybersecurity skills from the perspective of their areas of expertise;
    - Must be able to understand the organizational context and address circumstances where the functional areas with which it engages in cybersecurity may be partially outsourced and frequently renewed. Its mode of operation must be adapted to this situation in a seamless manner.

Drawing upon the characteristics of public entities that we have identified, and supported by the body of research we have examined and presented in Table 1, we have proposed the preceding paragraphs as general requirements for public entities when engaging a service provider for CyberSOC outsourcing.

This approach allows us to leverage the existing presence of an outsourced, technology-focused CyberSOC to offer a more comprehensive perspective on cybersecurity. Simultaneously, it enhances the awareness of the cybersecurity workforce regarding its potential contributions to the overall cybersecurity posture of the organization. While there may be alternative approaches, we believe that ours takes into account factors already prevalent in public organizations, which we have directly and indirectly analyzed in previous phases. These factors include the widespread adoption of outsourcing, the existence of mixed operational teams comprising both in-house and outsourced personnel, the challenges associated with acquiring cybersecurity talent, and the imperative need to augment cybersecurity skills to address the shortage in the cybersecurity workforce, among others. In our conception of a Wide-Scope CyberSOC, it must be proficient enough to serve as the cybersecurity reference unit within the organization and train cross-functional personnel applying a learning-by-doing approach, as explained in [106] by Deng et al., and also providing mentorship and coaching as needed, following the guidelines of [107–110] by Hamburg, Burrel, Ndueso et al., and Corradini, respectively. It is also necessary that the outsourced Wide-Scope CyberSOC has the ability of enhancing the cybersecurity awareness of workers, as in [65,66]. It should serve as a facilitating element that enables the continuous enhancement of cybersecurity capabilities and knowledge within each functional area involved in corporate cybersecurity, rather than solely designing and implementing these measures firsthand.

While it is not mandatory, it is advisable for the Wide-Scope CyberSOC to be viewed as a collective asset of the entire cross-functional cybersecurity workforce. Given that this new CyberSOC will be more deeply involved in the daily cybersecurity activities of various functional areas, we recommend positioning it within the organization in a way that minimizes the potential for any functional area to perceive conflicts of interest or biases, something identified by Monzelo and Nunes [111] or Badhwar [112], as shown in Figure 2.

- As a preliminary step before contracting the Wide-Scope CyberSOC service, it is also essential to turn the desired multidisciplinary capabilities, skills, and knowledge into explicit requirements for the service that any potential service provider must meet. These requirements will enable them to effectively mentor and provide the necessary support to the various functional areas contributing to cybersecurity. As part of our study, we have conducted this analysis and defined the necessary prerequisites, which can be directly incorporated into the technical specifications of the Wide-Scope CyberSOC. The specific knowledge requirements can be found in Appendix A;
- Finally, after addressing all the relevant points explained in this section, the public entity will be able to outsource the Wide-Scope CyberSOC service using its expertise in public procurement. Once the service is contracted, it should be managed using the existing procedures in the selected model, CyberTOMP. Figure 3 illustrates the specific activities of the tactical-operational cybersecurity management process defined in CyberTOMP, where the Wide-Scope CyberSOC should play a key role by contributing its expertise and acting as a cohesive element among the various functional areas of the organization. Furthermore, aside from the aforementioned aspect, which pertains exclusively to the set of steps/tasks delineated in the CyberTOMP proposal, the Wide-Scope CyberSOC must also undertake the activities typically associated with a

traditional CyberSOC. These activities may encompass actions within the realms of identify, protect, detect, respond, and recover approaches, as is customary.

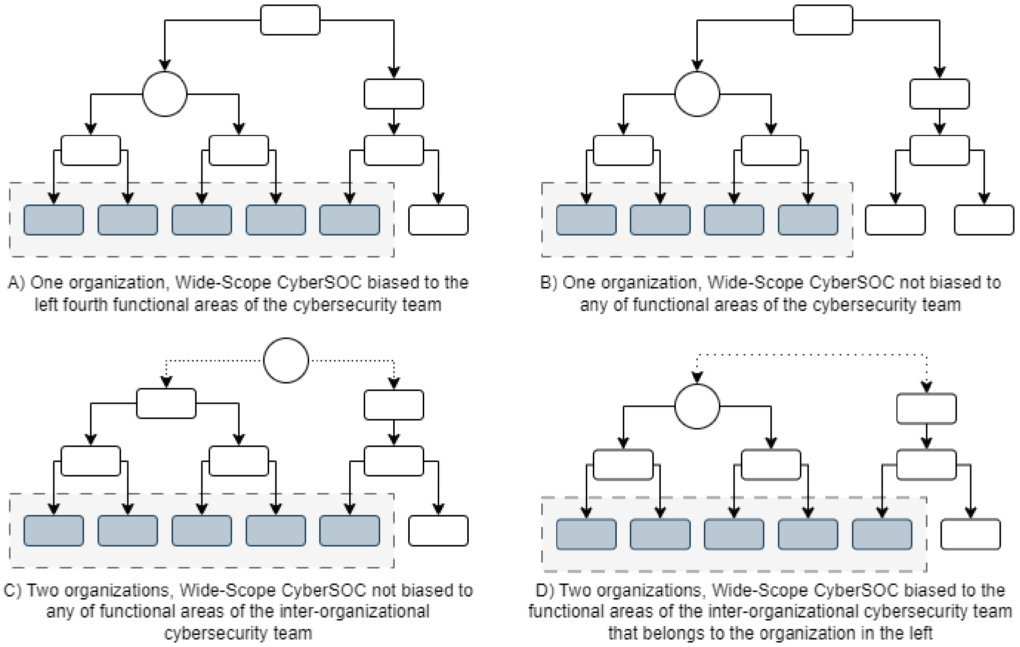
A) One organization, Wide-Scope CyberSOC biased to the left fourth functional areas of the cybersecurity team
B) One organization, Wide-Scope CyberSOC not biased to any of functional areas of the cybersecurity team
C) Two organizations, Wide-Scope CyberSOC not biased to any of functional areas of the inter-organizational cybersecurity team
D) Two organizations, Wide-Scope CyberSOC biased to the functional areas of the inter-organizational cybersecurity team that belongs to the organization in the left

Figure 2. Here are four examples of organizational structures. In (**B**,**C**), the Wide-Scope CyberSOC (represented by a circle) is less likely to be perceived as biased, as every functional area involved in cybersecurity (shown in gray) that makes up the multidisciplinary cybersecurity team (enclosed by a dashed rectangle) has direct access to it, even if they belong to different organizations. Conversely, this is not the case in scenarios (**A**,**D**).

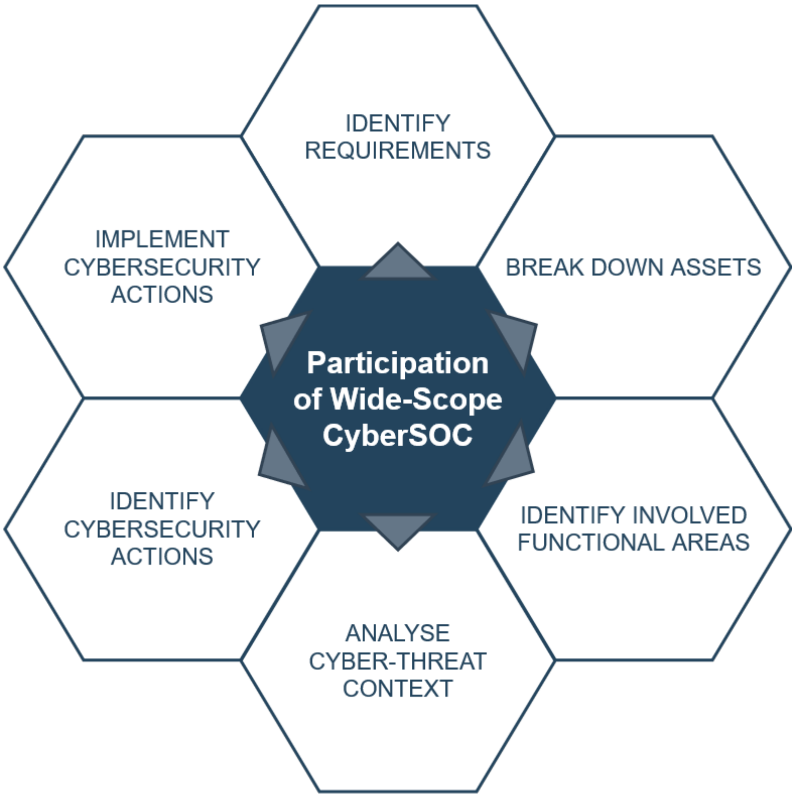
IDENTIFY REQUIREMENTS
IMPLEMENT CYBERSECURITY ACTIONS
BREAK DOWN ASSETS
Participation of Wide-Scope CyberSOC
IDENTIFY CYBERSECURITY ACTIONS
IDENTIFY INVOLVED FUNCTIONAL AREAS
ANALYSE CYBER-THREAT CONTEXT

Figure 3. Tasks defined within the CyberTOMP framework in which the Wide-Scope CyberSOC can assume a significant role.

3.3. Assessing the Wide-Scope CyberSOC Effect on the Deployment of Holistic Cybersecurity

The core objective of our proposal is to ease the implementation of holistic cybersecurity by enhancing the capabilities of the cross-functional cybersecurity workforce, which includes individuals from both the public and private sectors. Our aim is to empower them to better comprehend and apply their roles, leveraging their specific expertise to contribute effectively to the overall organizational cybersecurity strategy.

To achieve this goal, we advocate for the adoption of the innovative Wide-Scope CyberSOC. It is crucial to underscore that our ultimate objective is to fortify the cybersecurity situational awareness of the personnel involved. To this end, we believe that evaluating and measuring the situational awareness of the cybersecurity cross-functional team over time, post-implementation of the Wide-Scope CyberSOC within the organization, serves as a robust means of validating the effectiveness of the Wide-Scope CyberSOC in simplifying the deployment of holistic cybersecurity.

To facilitate this measurement, we propose the utilization of structured questionnaires tailored to assess personnel's situational awareness skills across four key areas, in line with the requirements we recommend imposing on the Wide-Scope CyberSOC:

1. Grasping the holistic nature of cybersecurity and the extensive spectrum of potential, applicable cybersecurity actions;
2. Recognizing the responsibilities associated with each functional area and appreciating the critical importance of collective engagement in achieving the highest cybersecurity standards;
3. Understanding the imperative need for proportional cybersecurity measures, aligned with the criticality of assets;
4. Acknowledging that various approaches can be employed to attain the same objectives, thus enabling the distribution of cybersecurity efforts and resources throughout the organization to foster collaborative equilibrium.

Given that situational awareness training is inherently an ongoing process, it may take a substantial amount of time before conclusive results are obtained. Nevertheless, successive measurements should exhibit an upward trend in these skills among the cross-functional cybersecurity workforce.

4. Results and Discussion

The current research project addresses a genuine need of a Public Sector entity engaged in defining and implementing a holistic cybersecurity management model: the necessity to attain a comprehensive level of cybersecurity awareness among their personnel. With the collaboration of this organization, we undertook this work with the intention of ensuring that the outcomes, tools, and elements developed could also be applicable to other public sector entities. Our motivation lies not only in a sense of public service but also in the potential for collaboration and further evolution of the proposal.

To ensure this, we conducted our work adhering to the standard formal or semi-formal methods as described: We conducted an analysis of a relevant set of research works found in the current literature. Our goal was to identify requirements stemming from one of our previous studies and the need emerging from its applicability to a public sector entity. Subsequently, through interviews and work sessions, we assessed the entity's situation and specific characteristics regarding the adoption of a holistic model for cybersecurity management. Concurrently, we indirectly gathered information on similar characteristics in other public organizations from the same organization. We employed SWOT analysis technique, to systematically organize and categorize these attributes, to confirm these characteristics were similar to the common ones, we analyzed scrutinizing the international literature. This was crucial to develop a proposal applicable to all public organizations, not just the study participant. The outcome confirmed shared characteristics, and for that reason, we assumed they share a common scenario and could benefit from our proposal. Using a TOWS analysis technique, we identified successful strategies, guiding a coherent approach in our proposal's design. To implement the identified strategies, and taking into account the features of public sector organizations, we designed an extended-capabilities CyberSOC that facilitates the adoption of the holistic model tactically and operationally by increasing the holistic cybersecurity awareness level of the cybersecurity workforce.

To the best of our knowledge, and after extensive periods of research, we have not encountered a study that addresses the development of holistic cybersecurity capabilities at the lower levels of the organization while also considering the specificities of public sector entities and their operational methods. Our proposal specifically targets this gap within public organizations.

As a contribution resulting from this study, we coined the new concept, "Wide-Scope CyberSOC", which defines such a CyberSOC with extended capabilities. This CyberSOC can be easily outsourced, thanks to our identification of a well-structured, common, and multidisciplinary set of cybersecurity actions that has been also associated with each organization's functional area involved in cybersecurity. We then transformed this set into directly applicable requirements when drafting technical specifications for the procurement of such services. As a result of this process, the outsourced Wide-Scope CyberSOC is managed and evaluated consistently, seamlessly integrated into a specific framework for the holistic, tactical-operational management of cybersecurity. These contributions can be found, summarized, and organized, in Appendix A.

The Wide-Scope CyberSOC will be capable of actively participating in and facilitating the tactical-operational cybersecurity team in various activities. These activities include identifying cybersecurity requirements, breaking down business assets, identifying functional areas involved in their cybersecurity, analyzing the cyber threat landscape, and adapting the organization accordingly. Additionally, the CyberSOC will be instrumental in designing and implementing cross-functional cybersecurity measures. This empowered CyberSOC will serve as a cornerstone, expediting the adoption of a multidisciplinary approach to cybersecurity management within the public organization.

As part of our study, in cooperation with the participating public entity, we have designed its first Wide-Scope CyberSOC. It underwent a public tender process, with various security service providers submitting their offers. The organization has since implemented and is currently managing its first Wide-Scope CyberSOC based on the guidelines outlined in this study. In the meanwhile, we are assessing the effect of introducing the Wide-Scope CyberSOC in this public sector organization following the method described in Section 3.3. Initial measurements show promise, but further data collection and maturation are required before presenting the results to the general public, which will take a considerable amount of time.

We devoted a substantial amount of effort to carefully plan our research approach, ensuring that the results would not only be beneficial for the participating public organization, but also applicable to other public sector organizations internationally. While we are confident that it aligns well with the Spanish case study, we conducted and took the necessary precautions to facilitate its applicability to a broader range of public organizations, and we acknowledge that no research is immune to the possibility of unintentional biases or errors. We have identified two potential areas where these unlikely events could occur:

- The generalization process in our research was built upon the presence of common features and circumstances identified in the global literature pertaining to public sector organizations, along with the parallel existence of these same insights within the public organization participating in our study. This alignment allowed us to establish a connection that led us to recognize that the insights from our case study are applicable to other public organizations worldwide. To ensure the reliability of our approach, we deliberately selected a comprehensive array of research works for the analysis of current literature concerning public sector organizations. This approach was taken specifically to reduce the risk of selecting only a few sources that might not accurately represent these public organizations. Nonetheless, despite our efforts, there is a slight possibility that our selection of research works may have been influenced by unconscious bias;

- On the other hand, we have introduced a method to evaluate the effectiveness of our proposal, which we are currently applying to the participating organization in our study. The initial results appear promising, but they require extended assessment over time to thoroughly ascertain the model's benefits. Furthermore, since this is a generalization based on a single case study, the only application thus far has been the one conducted as part of our research. Additional applications will offer valuable data to refine our proposal if necessary.

While we have not identified any of the situations mentioned, and despite our vigilance and awareness, we acknowledge that these could be two points where additional checks could be beneficial to strengthen our work. Therefore, we encourage third parties to independently analyze the generalization process we conducted and implement the model in other public organizations to verify the results or propose enhancements that contribute to the body of knowledge related to holistic cybersecurity management in public sector organizations.

5. Conclusions and Future Work

As highlighted in the introduction, organizations across various sectors, both public and private, are becoming increasingly reliant on cyberspace, a realm beyond complete control, rendering them susceptible to dynamic cyber threats. This vulnerability exposes organizations to potential risks, including business disruptions and sensitive data breaches. For public entities, such risks translate into an inability to deliver essential public services and a failure to safeguard citizens' data and privacy. To address this challenge effectively, an enhanced cybersecurity awareness among the cybersecurity workforce is essential. We have identified common characteristics among public sector organizations, enabling us to propose a comprehensive solution that equips them to navigate cyberspace securely. Our proposal introduces a novel outsourced CyberSOC, the Wide-Scope CyberSOC, designed to facilitate the development of holistic cybersecurity skills within the workforce and streamline holistic cybersecurity management in public sector organizations. This work offers a valuable framework applicable to any public entity, particularly those heavily engaged in digital citizen services, where the exposure to the expanding cyber threats landscape is significant. Additionally, we have outlined the comprehensive set of requirements that public organizations should request from Wide-Scope CyberSOC service providers to ensure the fulfillment of necessary functionalities. As part of future work, we are exploring the development of specific tools to simplify the operations of Wide-Scope CyberSOCs and enhance the holistic cybersecurity awareness of cross-functional cybersecurity teams.

Author Contributions: Conceptualization, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; methodology, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; software, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; validation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; formal analysis, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; investigation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; resources, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; data curation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; writing—original draft preparation, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; writing—review and editing, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; visualization, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; supervision, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; project administration, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C.; funding acquisition, M.D.-D., F.J.R.-P., J.C.-M., D.C.-P. and J.C.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by TED2021-131699B-I00/ MCIN/AEI/10.13039/501100011033/ European Union NextGenerationEU/PRTR.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

Table A1. Knowledge Requirements to Contract Wide-Scope CyberSOC Services.

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Identify	ID.AM	CSC-1.1	√	√	√	FA7	Establishing and maintaining a detailed enterprise asset inventory with the potential to store or process data.
Identify	ID.AM	CSC-12.4		√	√	FA10	Establishing and maintaining architecture diagrams.
Identify	ID.AM	CSC-14.1	√	√	√	FA3	Establishing and maintaining a security awareness program.
Identify	ID.AM	CSC-2.2	√	√	√	FA8	Ensuring that only authorized, supported software is used.
Identify	ID.AM	CSC-3.1	√	√	√	FA5	Establishing and maintaining a process for data management
Identify	ID.AM	CSC-3.2	√	√	√	FA10	Establishing and maintaining a data inventory.
Identify	ID.AM	CSC-3.6	√	√	√	FA10	Identifying data on end-user devices that has encryption requirements.
Identify	ID.AM	CSC-3.7		√	√	FA9	Establishing and maintaining a data classification scheme
Identify	ID.AM	ID.AM-1	√	√	√	FA7	Establishing and maintaining detailed inventory of physical devices and systems.
Identify	ID.AM	ID.AM-2	√	√	√	FA8	Inventorying all software platforms and applications within the organization.
Identify	ID.AM	ID.AM-3		√	√	FA8	Mapping organizational communication and data flows.
Identify	ID.BE	9D-1		√	√	FA7	Analyzing the business environment to determine potential ways of deterring attacks.
Identify	ID.BE	ID.BE-1			√	FA6	Identifying and communicating the organization's role in the supply chain.
Identify	ID.BE	ID.BE-2			√	FA6	Identifying and communicating the organization's place in critical infrastructure and its industry sector.
Identify	ID.BE	ID.BE-3			√	FA5	Establishing and communicating priorities for organizational mission, objectives, and activities.
Identify	ID.BE	ID.BE-4			√	FA5	Establishing dependencies and critical functions for delivery of critical services.
Identify	ID.BE	ID.BE-5			√	FA5	Establishing resilience requirements to support delivery of critical services for all operating states.
Identify	ID.GV	CSC-17.4		√	√	FA5	Establishing, maintaining an incident response process.
Identify	ID.GV	ID.GV-1	√	√	√	FA5	Establishing and communicating organizational cybersecurity policy.
Identify	ID.GV	ID.GV-2		√	√	FA9	Coordinating and aligning cybersecurity roles and responsibilities with internal roles and external partners.
Identify	ID.GV	ID.GV-3			√	FA5	Understanding and managing legal and regulatory requirements regarding cybersecurity.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Identify	ID.GV	ID.GV-4			√	FA5	Ensuring governance and risk management processes address cybersecurity risks.
Identify	ID.RA	9D-1		√	√	FA7	Ensuring that the organization understands the risk of vulnerabilities and the necessity of deterring their exploitation.
Identify	ID.RA	CSC-18.2		√	√	FA7	Conducting periodic external penetration tests in order to enhance understanding of cyber risks.
Identify	ID.RA	CSC-18.5			√	FA7	Conducting periodic internal penetration tests in order to enhance understanding of cyber risks.
Identify	ID.RA	CSC-3.7		√	√	FA9	Assessing the current validity of the data classification scheme in relation to existing risks.
Identify	ID.RA	ID.RA-1	√	√	√	FA7	Identifying and documenting assets vulnerabilities.
Identify	ID.RA	ID.RA-2			√	FA4	Ensuring cyber threat intelligence is received from information sharing forums and sources.
Identify	ID.RA	ID.RA-3			√	FA4	Identifying and document threats, both internal and external.
Identify	ID.RA	ID.RA-4			√	FA6	Identifying potential business impacts and likelihoods.
Identify	ID.RA	ID.RA-6			√	FA6	Identifying and prioritizing risk responses.
Identify	ID.RM	9D-8		√	√	FA2	Comprehending the potential risks that necessitate redirecting attackers to alternative targets.
Identify	ID.RM	ID.RM-1			√	FA6	Ensuring risk management processes are established, managed, and agreed to by organizational stakeholders.
Identify	ID.RM	ID.RM-2			√	FA6	Determining and clearly expressing organizational risk tolerance.
Identify	ID.RM	ID.RM-3			√	FA6	Informing the organization's risk tolerance by its role in critical infrastructure and sector specific risk analysis.
Identify	ID.SC	ID.SC-1		√	√	FA5	Identifying, establishing, assessing, and managing cyber supply chain risk management processes.
Identify	ID.SC	ID.SC-2	√	√	√	FA5	Identifying, prioritizing, and assessing third party partners of information systems, components, and services, using a cybersecurity supply chain risk assessment process.
Identify	ID.SC	ID.SC-3		√	√	FA9	Ensuring contracts with suppliers and third-party are designed to meet the goals of an organization's cybersecurity program and cybersecurity supply chain management plan.
Identify	ID.SC	ID.SC-4			√	FA6	Auditing, testing, and evaluating suppliers and third-party partners to confirm they are meeting their contractual obligations.
Identify	ID.SC	ID.SC-5	√	√	√	FA9	Conducting response and recovery planning and testing with suppliers and third-party providers.
Protect	PR.AC	CSC-12.5		√	√	FA10	Centralizing network authentication, authorization, and auditing.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Protect	PR.AC	CSC-12.6		√	√	FA10	Employing secure network management and communication protocols.
Protect	PR.AC	CSC-13.4		√	√	FA10	Conducting traffic filtering between network segments
Protect	PR.AC	CSC-4.7	√	√	√	FA10	Managing default accounts on enterprise assets and software.
Protect	PR.AC	CSC-5.2	√	√	√	FA10	Using unique passwords for all enterprise assets.
Protect	PR.AC	CSC-5.6		√	√	FA10	Centralizing account management.
Protect	PR.AC	CSC-6.8			√	FA10	Deploying and maintaining Role-Based Access Control (RBAC)
Protect	PR.AC	PR.AC-1	√	√	√	FA10	Ensuring identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
Protect	PR.AC	PR.AC-2			√	FA7	Ensuring physical access to assets is managed and protected.
Protect	PR.AC	PR.AC-3	√	√	√	FA10	Ensuring remote access is managed.
Protect	PR.AC	PR.AC-4	√	√	√	FA10	Ensuring access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
Protect	PR.AC	PR.AC-5	√	√	√	FA10	Ensuring network integrity is protected.
Protect	PR.AC	PR.AC-6			√	FA10	Ensuring identities are proofed and bound to credentials and asserted in interactions.
Protect	PR.AC	PR.AC-7	√	√	√	FA10	Ensuring users, devices, and other assets are authenticated commensurate with the risk of the transaction.
Protect	PR.AT	CSC-14.9		√	√	FA3	Conducting role-specific security awareness and skills training.
Protect	PR.AT	CSC-15.4		√	√	FA5	Ensuring service provider contracts include security requirements.
Protect	PR.AT	PR.AT-1	√	√	√	FA3	Ensuring all users are informed and trained.
Protect	PR.AT	PR.AT-2		√	√	FA3	Ensuring privileged users understand their roles and responsibilities.
Protect	PR.DS	9D-6			√	FA8	Dispersing protective measures throughout the payload to safeguard the data.
Protect	PR.DS	CSC-3.4	√	√	√	FA10	Enforcing data retention in accordance with the risk strategy.
Protect	PR.DS	PR.DS-1		√	√	FA10	Ensuring data-at-rest is protected.
Protect	PR.DS	PR.DS-2		√	√	FA10	Ensuring data-in-transit is protected.
Protect	PR.DS	PR.DS-3	√	√	√	FA10	Ensuring assets are formally managed throughout removal, transfers, and disposition.
Protect	PR.DS	PR.DS-4			√	FA10	Adjusting capacity to ensure availability is maintained.
Protect	PR.DS	PR.DS-5			√	FA10	Ensuring protections against data leaks are implemented.
Protect	PR.DS	PR.DS-6		√	√	FA10	Ensuring integrity checking mechanisms are used to verify software, firmware, and information integrity.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in..."
Protect	PR.DS	PR.DS-7		√	√	FA10	Ensuring the development and testing environment(s) are separate from the production environment.
Protect	PR.DS	PR.DS-8			√	FA10	Ensuring integrity checking mechanisms are used to verify hardware integrity.
Protect	PR.IP	9D-3		√	√	FA2	Enhancing the difficulty of accessing the protected information beyond the attacker's skills.
Protect	PR.IP	9D-5		√	√	FA2	Investigating the threat in depth in order to prevent access to protected information using a multi-layered approach.
Protect	PR.IP	9D-8		√	√	FA2	Implementing measures to divert attackers in order to protect the information.
Protect	PR.IP	9D-9	√	√	√	FA2	Implementing measures in depth that become increasingly challenging and less visible as they approach the asset.
Protect	PR.IP	CSC-11.1	√	√	√	FA10	Establishing and maintaining a process for data recovery.
Protect	PR.IP	CSC-16.1		√	√	FA8	Establishing and maintaining a secure application development process.
Protect	PR.IP	CSC-16.14			√	FA4	Undertaking comprehensive threat modelling.
Protect	PR.IP	CSC-18.4			√	FA7	Validating the security measures deployed to protect information following each penetration test.
Protect	PR.IP	CSC-2.5		√	√	FA5	Creating an allow list of authorized software in order to protect information.
Protect	PR.IP	CSC-2.6		√	√	FA5	Creating an allow list of authorized libraries in order to protect information.
Protect	PR.IP	CSC-2.7			√	FA5	Creating an allow list of authorized scripts in order to protect information.
Protect	PR.IP	CSC-4.3	√	√	√	FA10	Configuring automatic session locking on enterprise assets to protect the information.
Protect	PR.IP	PR.IP-1	√	√	√	FA5	Ensuring a baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.
Protect	PR.IP	PR.IP-10		√	√	FA5	Ensuring response and recovery plans are tested.
Protect	PR.IP	PR.IP-11	√	√	√	FA11	Incorporating cybersecurity into human resources practices for information handling.
Protect	PR.IP	PR.IP-12		√	√	FA7	Developing and implementing a vulnerability management plan.
Protect	PR.IP	PR.IP-2		√	√	FA10	Implementing a system development life cycle to manage systems.
Protect	PR.IP	PR.IP-3			√	FA5	Designing a configuration change control process.
Protect	PR.IP	PR.IP-4	√	√	√	FA10	Ensuring backups of information are conducted, maintained, and tested.
Protect	PR.IP	PR.IP-5			√	FA5	Ensuring policy and regulations regarding the physical operating environment for organizational assets are met.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Protect	PR.IP	PR.IP-6	√	√	√	FA10	Ensuring data is destroyed according to policy.
Protect	PR.IP	PR.IP-7		√	√	FA5	Ensuring protection processes are improved.
Protect	PR.IP	PR.IP-8			√	FA2	Ensuring effectiveness of protection technologies is shared.
Protect	PR.IP	PR.IP-9	√	√	√	FA5	Ensuring response plans and recovery plans are in place and managed.
Protect	PR.MA	9D-5		√	√	FA2	Conducting maintenance activities on all layers of the asset.
Protect	PR.MA	9D-9		√	√	FA2	Carrying out maintenance tasks to ensure depth of defense.
Protect	PR.MA	CSC-12.1	√	√	√	FA10	Carrying out maintenance to ensure the network infrastructure is up to date.
Protect	PR.MA	CSC-12.3		√	√	FA10	Managing the network infrastructure with a security-oriented approach.
Protect	PR.MA	CSC-13.5		√	√	FA10	Carrying out maintenance actions to ensure assets remotely connecting to enterprise resources comply with the organization's requirements.
Protect	PR.MA	CSC-16.13			√	FA2	Performing root cause analysis on security vulnerabilities.
Protect	PR.MA	CSC-18.3		√	√	FA10	Remediating penetration test findings.
Protect	PR.MA	CSC-4.2	√	√	√	FA5	Carrying out tasks to securely configure the network infrastructure in accordance with established processes.
Protect	PR.MA	CSC-4.6	√	√	√	FA10	Carrying out security maintenance tasks on enterprise assets and software.
Protect	PR.MA	CSC-4.8		√	√	FA10	Uninstalling or disabling unnecessary services on enterprise assets and software.
Protect	PR.MA	CSC-4.9		√	√	FA10	Configuring trusted DNS servers on enterprise assets.
Protect	PR.MA	CSC-7.3	√	√	√	FA10	Performing automated operating system patch management.
Protect	PR.MA	CSC-8.1	√	√	√	FA5	Establishing and maintaining an audit log management process.
Protect	PR.MA	CSC-8.10		√	√	FA10	Retaining audit logs.
Protect	PR.MA	CSC-8.3	√	√	√	FA10	Ensuring adequate audit log storage.
Protect	PR.MA	CSC-8.9		√	√	FA10	Centralizing audit log collection and retention.
Protect	PR.MA	PR.MA-1			√	FA10	Ensuring maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
Protect	PR.PT	9D-4		√	√	FA2	Implementing differentiated protections to address each threat specifically.
Protect	PR.PT	9D-7			√	FA2	Employing decoys to distract attackers.
Protect	PR.PT	CSC-4.12			√	FA10	Separating enterprise workspaces on mobile end-user devices
Protect	PR.PT	CSC-4.4	√	√	√	FA10	Implementing and managing a firewall on servers

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Protect	PR.PT	CSC-4.5	√	√	√	FA10	Implementing and managing a firewall on end-user devices
Protect	PR.PT	CSC-9.5		√	√	FA10	Implementing DMARC.
Protect	PR.PT	PR.PT-1	√	√	√	FA10	Ensuring audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
Protect	PR.PT	PR.PT-2	√	√	√	FA10	Ensuring removable media is protected and its use restricted according to policy.
Protect	PR.PT	PR.PT-3			√	FA10	Ensuring the principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
Protect	PR.PT	PR.PT-4			√	FA10	Ensuring communications and control networks are protected.
Protect	PR.PT	PR.PT-5	√	√	√	FA10	Ensuring mechanisms are implemented to achieve resilience requirements in normal and adverse situations.
Detect	DA.AE	CSC-8.12			√	FA10	Collecting service provider logs to detect anomalies.
Detect	DA.AE	DE.AE-1		√	√	FA10	Establishing and maintaining a baseline of operations and expected data flows for users and systems.
Detect	DA.AE	DE.AE-2		√	√	FA2	Analyzing detected events to understand attack targets and methods.
Detect	DA.AE	DE.AE-3	√	√	√	FA2	Collecting and correlating event data correlated from multiple sources and sensors.
Detect	DA.AE	DE.AE-4			√	FA2	Determining impact of events.
Detect	DA.AE	DE.AE-5			√	FA2	Establishing incident alert thresholds.
Detect	DE.CM	CSC-13.1		√	√	FA2	Centralizing security event alerting
Detect	DE.CM	CSC-13.5		√	√	FA10	Monitoring access control for assets remotely connecting to enterprise resources.
Detect	DE.CM	CSC-3.14			√	FA10	Logging access to sensitive data.
Detect	DE.CM	DE.CM-1		√	√	FA2	Ensuring the network is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-2			√	FA1	Ensuring the physical environment is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-3			√	FA10	Ensuring personnel activity is monitored to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-4	√	√	√	FA2	Detecting malicious code.
Detect	DE.CM	DE.CM-5			√	FA2	Detecting unauthorized mobile code.
Detect	DE.CM	DE.CM-6			√	FA2	Monitoring external service provider activity to detect potential cybersecurity events.
Detect	DE.CM	DE.CM-7	√	√	√	FA2	Monitoring for unauthorized personnel, connections, devices, and software.
Detect	DE.CM	DE.CM-8		√	√	FA7	Conducting periodic vulnerability scans
Detect	DE.DP	CSC-17.1	√	√	√	FA5	Designating personnel, including key and backup, to manage incident handling.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Detect	DE.DP	CSC-17.4		√	√	FA5	Testing the incident response process to ensure it includes awareness of anomalous events.
Detect	DE.DP	CSC-17.5		√	√	FA5	Assigning key cross-functional roles and responsibilities in relation to incident response.
Detect	DE.DP	DE.DP-2			√	FA2	Ensuring detection activities comply with all applicable requirements.
Detect	DE.DP	DE.DP-3			√	FA10	Testing detection processes.
Detect	DE.DP	DE.DP-5			√	FA5	Continuously improving detection processes.
Respond	RS.AN	CSC-17.9			√	FA5	Establishing and maintaining security incident thresholds to ensure effective response.
Respond	RS.AN	RS.AN-1		√	√	FA2	Ensuring notifications from detection systems are investigated.
Respond	RS.AN	RS.AN-2			√	FA2	Ensuring the impact of the incident is understood.
Respond	RS.AN	RS.AN-3			√	FA2	Ensuring forensics are performed.
Respond	RS.AN	RS.AN-5		√	√	FA5	Ensuring processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources.
Respond	RS.CO	CSC-17.4	√	√	√	FA5	Communicating the incident response process.
Respond	RS.CO	CSC-17.5		√	√	FA5	Communicating key cross-functional roles and responsibilities in relation to incident response.
Respond	RS.CO	RS.CO-5			√	FA4	Ensuring voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Respond	RS.IM	RS.IM-1		√	√	FA5	Ensuring response plans incorporate lessons learned.
Respond	RS.IM	RS.IM-2		√	√	FA5	Response strategies are updated.
Respond	RS.MI	CSC-1.2	√	√	√	FA10	Ensuring that a process is in place to address unauthorized assets.
Respond	RS.MI	CSC-4.10		√	√	FA10	Enforcing remote wipe capability on portable end-user devices
Respond	RS.MI	CSC-7.7		√	√	FA10	Remediating detected vulnerabilities and weakness.
Respond	RS.MI	RS.MI-1			√	FA2	Containing incidents.
Respond	RS.MI	RS.MI-2			√	FA2	Mitigating incidents.
Respond	RS.MI	RS.MI-3			√	FA2	Mitigating newly identified vulnerabilities or documenting them as accepted risks.
Respond	RS.RP	CSC-17.6		√	√	FA5	Defining mechanisms for communicating during incident response.
Respond	RS.RP	RS.RP-1			√	FA2	Ensuring a response plan is executed during or after an incident.
Recover	RC.CO	RC.CO-1			√	FA12	Managing public relations.
Recover	RC.CO	RC.CO-2			√	FA12	Repairing the reputation after an incident.
Recover	RC.CO	RC.CO-3			√	FA12	Communicating recovery activities to internal and external stakeholders as well as executive and management teams.

Table A1. *Cont.*

NIST Function	NIST Category	Unified Expected Outcome	IG1	IG2	IG3	Main Area ID	Knowledge Requirement: "The Wide-Scope CyberSOC must be Skilled to Help Cross-Functional Teams in. . ."
Recover	RC.IM	RC.IM-1			√	FA5	Ensuring recovery plans incorporate lessons learned.
Recover	RC.IM	RC.IM-2			√	FA5	Ensuring recovery strategies are updated.
Recover	RC.RP	RC.RP-1			√	FA2	Ensuring a recovery plan is executed during or after a cybersecurity incident.

References

1. Domínguez-Dorado, M.; Carmona-Murillo, J.; Cortés-Polo, D.; Rodríguez-Pérez, F.J. CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels. *IEEE Access* **2022**, *10*, 122454–122485. [CrossRef]
2. von Solms, R.; van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
3. Reid, R.; van Niekerk, J. From information security to cyber security cultures. In Proceedings of the Information Security for South Africa, Johannesburg, South Africa, 13–14 August 2014.
4. Furnell, S. The cybersecurity workforce and skills. *Comput. Secur.* **2012**, *100*, 102080. [CrossRef]
5. De Zan, T. Mitigating the Cyber Security Skills Shortage: The Influence of National Skills Competitions on Cyber Security Interest. Ph.D. Thesis, Department of Education and Centre for Doctoral Training in Cyber Security, Linacre College, University of Oxford, Oxford, UK, 2021.
6. Reeder, F.; Alan, P. *What Works in Finding Elite Cybersecurity Talent: Promising Practices for Chief Information Officers*; CIO.org: Newport, UK, 2021.
7. DeCrosta, J. Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
8. Shava, E.; Hofisi, C. Challenges and Opportunities for Public Administration in the Fourth Industrial Revolution. *Afr. J. Public Aff.* **2017**, *9*, 203–215.
9. Ngwenyama, O.; Henriksen, H.Z.; Hardt, D. Public management challenges in the digital risk society: A Critical Analysis of the Public Debate on Implementation of the Danish NemID. *Eur. J. Inf. Syst.* **2023**, *32*, 108–126. [CrossRef]
10. Nizich, M. Preparing the Cybersecurity Workforce of Tomorrow. In *The Cybersecurity Workforce of Tomorrow (The Future of Work)*; Emerald Group Publishing Limited: Bingley, UK, 2023; pp. 117–146.
11. Lee, G.R.; Lee, S.; Malatesta, D.; Fernández, S. Outsourcing and Organizational Performance: The Employee Perspective. *Am. Rev. Public Adm.* **2019**, *49*, 973–986. [CrossRef]
12. Onwubiko, C.; Ouazzane, K. Challenges towards Building an effective Cyber Security Operations Centre. *Int. J. Cyber Situational Aware.* **2019**, *4*, 11–39. [CrossRef]
13. Schatz, D.; Bashroush, R.; Wall, J. Towards a More Representative Defifinition of Cyber Security. *J. Digit. Forensics Secur. Law* **2017**, *12*, 53–74.
14. Ghelani, D. Cyber Security, Cyber Threats, Implications and Future. *Am. J. Sci. Eng. Technol.* **2022**, *3*, 12–19.
15. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *Int. J. Inform. Vis.* **2020**, *4*, 225–230. [CrossRef]
16. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [CrossRef]
17. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
18. Atoum, I.; Otoom, A.; Ali, A.A. A holistic cyber security implementation framework. *Inf. Manag. Comput. Secur.* **2014**, *22*, 251–264. [CrossRef]
19. van Kranenburg, R.; Le Gars, G. The Cybersecurity Aspects of New Entities Need a Cybernetic, Holistic Perspective. *Int. J. Cyber Forensic Adv. Threat Investig.* **2021**, *1*, 2. [CrossRef]
20. Del-Real, C.; Díaz-Fernández, A.M. Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *Int. Cybersecur. Law Rev.* **2022**, *3*, 313–343. [CrossRef]
21. Oruj, Z. Cyber security: Contemporary cyber threats and national strategies. *Distance Educ. Ukr. Innov. Norm.-Leg. Pedagog. Asp.* **2023**, *1*, 100–116.
22. Sharikov, P. Contemporary Cybersecurity Challenges. In *The Implications of Emerging Technologies in the Euro-Atlantic Space*; Palgrave Macmillan: Cham, Switzerland; Basel, Switzerland, 2023; pp. 143–157.
23. Cavelty, M.D.; Smeets, M. Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *J. Eur. Public Policy* **2023**, *30*, 1330–1352. [CrossRef]
24. Kosseff, J. Upgrading Cybersecurity Law. *Houst. Law Rev. Forthcom.* **2023**, 1–33. [CrossRef]

25. Creemers, R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy. *J. Contemp. China* **2023**, 1–16. [CrossRef]
26. Mijwil, M.M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 1–6.
27. Abazi, B. Establishing the National Cybersecurity (Resilience) Ecosystem. *IFAC-PapersOnLine* **2022**, *55*, 42–47. [CrossRef]
28. ENISA. *ENISA Threat Landscape 2022*; European Union Agency for Cybersecurity: Heraclión, Greece, 2022.
29. Hinkley, S. *Technology in the Public Sector and the Future of Government Work*; UC Berkeley Labor Center: Berkeley, CA, USA, 2022.
30. Norris, D.F.; Mateczun, L.K.; Forno, R.F. What the Literature Says About Local Government Cybersecurity. In *Cybersecurity and Local Government*; Wiley Data and Cybersecurity: Hoboken, NJ, USA, 2022; pp. 47–66.
31. CCN-CERT. *Ciberamenazas y Tendencias: Eidición 2022*; Centro Criptológico Nacional: Madrid, Spain, 2022.
32. Farrand, B.; Carrapico, H. Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *Eur. Sefcurity* **2022**, *31*, 435–453. [CrossRef]
33. Al Mehairi, A.; Zgheib, R.; Abdellatif, T.M.; Conchon, E. Cyber Security Strategies While Safeguarding Information Systems in Public/Private Sectors. In *Electronic Governance with Emerging Technologies, Proceedings of the EGETC 2022, Tampico, Mexico, 12–14 September 2022*; Communications in Computer and Information Science; Springer: Cham, Switzerland, 2022; pp. 49–63.
34. Blondin, D.; Boin, A. Cooperation in the Face of Transboundary Crisis: A Framework for Analysis. *Perspect. Public Manag. Gov.* **2020**, *3*, 197–209. [CrossRef]
35. Domínguez-Dorado, M.; Cortés-Polo, D.; Carmona-Murillo, J.; Rodríguez-Pérez, F.J.; Galeano-Brajones, J. Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management. *Appl. Sci.* **2023**, *13*, 6327. [CrossRef]
36. Quinn, S.; Ivy, N.; Barrett, M.; Feldman, L.; Topper, D.; Witte, G.; Gardner, R.K. *Using Business Impact Analysis to Inform Risk Prioritization and Response*; NIST Interagency Report NIST IR 8286D; NIST: Gaithersburg, MD, USA, 2022.
37. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* **2021**, *1*, 119–139. [CrossRef]
38. Rajan, R.; Rana, N.P.; Parameswar, N.; Dhir, S.; Sushil; Dwivedi, Y.K.K. Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technol. Forecast. Soc. Change* **2021**, *170*, 120872. [CrossRef]
39. Axon, L.; Erola, A.; van Rensburg, A.J.; Nurse, J.R.C.; Goldsmith, M.; Creese, S. Practitioners' Views on Cybersecurity Control Adoption and Effectiveness. In Proceedings of the ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; ACM ICPS. ACM: New York, NY, USA, 2021; pp. 1–10.
40. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
41. Preis, B.; Susskind, L. Municipal Cybersecurity: More Work Needs to be Done. *Urban Aff. Rev.* **2020**, *58*, 614–629. [CrossRef]
42. Clark, M.; Espinosa, J.; Delone, W. Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020; pp. 4283–4292.
43. Phillips, R.; Tanner, B. Breaking down silos between business continuity and cyber security. *J. Bus. Contin. Emerg. Plan.* **2019**, *12*, 224–232.
44. Kure, H.I.; Islam, S. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 332–340. [CrossRef]
45. Rothrock, R.A.; Kaplan, J.; Van Der Oord, F. The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Manag. Rev.* **2018**, *59*, 12–15.
46. Limba, T.; Plėta, T.; Agafonov, K.; Damkus, M. Cyber security management model for critical infrastructure. *Entrep. Sustain. Issues* **2017**, *4*, 559–573. [CrossRef]
47. Breier, J.; Hudec, L. On Selecting Critical Security Controls. In Proceedings of the 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany, 2–6 September 2013; IEEE: New York, NY, USA, 2013; pp. 1–7.
48. Almoughem, K.A.B.M. The Future of Cybersecurity Workforce Development. *Acad. J. Res. Sci. Publ.* **2023**, *4*, 37–48. [CrossRef]
49. Shah, A.; Ganesan, R.; Jajodia, S.; Cam, H.; Hutchinson, S. A Novel Team Formation Framework based on Performance in a Cybersecurity Operations Center. *IEEE Trans. Serv. Comput. Early Access* **2023**, *16*, 2359–2371. [CrossRef]
50. Adetoye, B.; Fong, R.C.-W. Building a Resilient Cybersecurity Workforce: A Multidisciplinary Solution to the Problem of High Turnover of Cybersecurity Analysts. In *Cybersecurity in the Age of Smart Societies*; Springer: Cham, Switzerland, 2023; pp. 61–87.
51. Balon, T.; Baggili, I. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Educ. Inf. Technol.* **2023**, *28*, 11759–11791. [CrossRef]
52. Nadua, F.-D.-L.; Escandor, L.; Bangayan, M.; Vigonte, F.; Abante, M.V. Identifying Incentives to Address Attrition in the Government Cybersecurity Workforce. 2023; pp. 1–21. Available online: https://ssrn.com/abstract=4382110 (accessed on 16 October 2023).
53. Fisk, N.; Kelly, N.M.; Liebrock, L. Cybersecurity Communities of Practice: Strategies for Creating Gateways to Participation. *Comput. Secur.* **2023**, *132*, 103188. [CrossRef]
54. Ashley, T.D.; Kwon, R.; Gourisetti, S.N.G.; Katsis, C.; Bonebrake, C.A.; Boyd, P.A. Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access* **2022**, *10*, 112487–112501. [CrossRef]

55. Justice, C.; Sample, C.; Loo, S.M.; Ball, A.; Hampton, C. Future Needs of the Cybersecurity Workforce. In Proceedings of the 17th International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Academic Conferences International Limited: South Oxfordshire, UK, 2022; Volume 17, pp. 81–91.
56. Ahmad, N.; Laplante, P.A.; DeFranco, J.F.; Kassab, M. A Cybersecurity Educated Community. *IEEE Trans. Emerg. Top. Comput.* **2022**, *10*, 1456–1463. [CrossRef]
57. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 100361. [CrossRef]
58. Noche, E.B. A Literature Review of Empirical Studies on Cyber Security Workforce Development. *Asian J. Multidiscip. Stud.* **2021**, *4*, 65–73.
59. Hulatt, D.; Stavrou, E. The Development of a Multidisciplinary CybersecurityWorkforce: An Investigation. In *Human Aspects of Information Security and Assurance, Proceedings of the 15th IFIP WG 11.12 International Symposium, HAISA 2021*; Virtual, 7–9 July 2021, Springer: Cham, Switzerland, 2021; pp. 138–147.
60. Kävrestad, J.; Nohlberg, M. Evaluation Strategies for Cybersecurity Training Methods: A Literature Review. In *Human Aspects of Information Security and Assurance, Proceedings of the 15th IFIP WG 11.12 International Symposium, HAISA 2021*; Virtual, 7–9 July 2021, Springer: Cham, Switzerland, 2021; pp. 102–112.
61. Maurer, C.; Summer, M.; Mazzola, D.; Pearlson, K.; Jacks, T. The Cybersecurity Skills Survey: Response to the 2020 SIM IT Trends Study. In Proceedings of the SIGMIS-CPR'21: 2021 on Computers and People Research Conference, Virtual, 30 June 2021; ACM: Hamburg, Germany, 2021; pp. 35–37.
62. Ahmad, K.C.A.; Desouza, S.B.; Manyard, H.N.; Baskerville, R.L. How integration of cyber security management and incident response enables organizational learning. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 939–953. [CrossRef]
63. McNulty, M.; Kettani, H. On Cybersecurity Education for Non-technical Learners. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; IEEE: New York, NY, USA, 2020; pp. 413–416.
64. Dahlström, C.; Nistotskaya, M.; Tyrberg, M. Outsourcing, bureaucratic personnel quality and citizen satisfaction with public services. *Public Adm.* **2018**, *96*, 218–233. [CrossRef]
65. Affan, Y.; Lin, L.; Rubia, F.; Wang, J. Improving software security awareness using a serious game. *IET Softw. Spec. Issue Gamification Persuas. Games Softw.* **2019**, *13*, 159–169.
66. Rubia, F.; Affan, Y.; Lin, L.; Wang, J. Strategies for counteracting social engineering attacks. *Comput. Fraud. Secur.* **2022**, *2022*, 15–19. [CrossRef]
67. Aragão, J.P.S.; Fontana, M.E. Guidelines for public sector managers on assessing the impact of outsourcing on business continuity strategies: A Brazilian case. *J. Glob. Oper. Strateg. Sourc.* **2023**, *16*, 118–141. [CrossRef]
68. Gowun, P.; Brunjes, B.M. Engaging Citizens in Government Contracting: A Theoretical Approach for the Role of Social Service Nonprofits. *Perspect. Public Manag. Gov.* **2022**, *5*, 317–329.
69. Heikkilä, J.; Cordon, C. Outsourcing: A core or non-core strategic management decision? *Brief. Entrep. Financ.* **2022**, *11*, 183–193. [CrossRef]
70. Pavelko, O.; Lazaryshyna, I.; Dukhnovska, L.; Sharova, S.; Oliinyk, T.; Donenko, I. Construction Development and Its Impact on the Construction Enterprises Financial Results. *Stud. Appl. Econ.* **2021**, *39*, 1–11. [CrossRef]
71. Aragão, J.P.S.; Fontana, M.E. Outsourcing Strategies in Public Services under Budgetary Constraints: Analysing Perceptions of Public Managers. *Public Organ. Rev.* **2021**, *22*, 61–77. [CrossRef]
72. Latif, M.N.A.; Aziz, N.A.A.; Hussin, N.S.N.; Aziz, Z.A. Cyber security in supply chain management: A systematic review. *LogForum* **2021**, *17*, 49–57. [CrossRef]
73. Repetto, M.; Carrega, A.; Rapuzzi, R. An architecture to manage security operations for digital service chains. *Future Gener. Comput. Syst.* **2021**, *115*, 251–266. [CrossRef]
74. Marco-Simó, J.M.; Pastor-Collado, J.A. IT Outsourcing in the Public Sector: A Descriptive Framework from a Literature Review. *J. Glob. Inf. Technol. Manag.* **2020**, *23*, 25–52. [CrossRef]
75. van der Wal, Z. Being a Public Manager in Times of Crisis: The Art of Managing Stakeholders, Political Masters, and Collaborative Networks. *Public Adm. Rev.* **2020**, *80*, 759–764. [CrossRef] [PubMed]
76. Rizwan, H.; Bhatti, S.N. Impacts of Outsourcing on Quality: A Case Study of an Electronics Sector. *Bahria Univ. J. Manag. Technol.* **2020**, *2*, 16–23.
77. Bogoviz, A.V.; Berezhnoi, A.V.; Mezhov, I.S.S.; Titova, O.V.; Kryukova, O.G. Decision Making in Modern Business Systems by the Principles of Outsourcing. In *Specifics of Decision Making in Modern Business Systems*; Emerald Publishing Limited: Leeds, UK, 2019; pp. 141–148.
78. Bloomfield, K.; Williams, T.; Bovis, C.; Merali, Y. Systemic risk in major public contracts. *Int. J. Forecast.* **2019**, *35*, 667–676. [CrossRef]
79. Proscovia, S. The impact of new public management through outsourcing on the management of government information: The case of Sweden. *Rec. Manag. J.* **2019**, *29*, 134–151.
80. Andersson, F.; Jordahl, H.; Josephson, J. Outsourcing Public Services: Contractibility, Cost, and Quality. *CESifo Econ. Stud.* **2019**, *65*, 349–372. [CrossRef]
81. Soliño, A.S. Sustainability of Public Services: Is Outsourcing the Answer? *Sustainability* **2019**, *11*, 7231. [CrossRef]

82. Lobao, L.; Gray, M.; Cox, K.; Kitson, M. The shrinking state? Understanding the assault on the public sector. *Camb. J. Reg. Econ. Soc.* **2018**, *11*, 389–408. [CrossRef]
83. Aswini, K. Advantages and Disadvantages of Outsourcing. *Shanlax Int. J. Commer.* **2018**, *6*, 7–9.
84. Pupion, P.-C. Research on Public Strategic Management requiring a new theoretical framework. *Gest. Manag. Public* **2018**, *6*, 6–13.
85. Kekez, A.; Howlett, M.; Ramesh, M. Varieties of collaboration in public service delivery. *Policy Des. Pract.* **2018**, *1*, 243–252. [CrossRef]
86. Johansson, T.; Siverbo, S. The relationship between supplier control and competition in public sector outsourcing. *Financ. Account. Manag. Gov. Public Serv. Charities* **2018**, *34*, 268–287. [CrossRef]
87. Burnes, B.; Anastasiadis, A. Outsourcing: A public-private sector comparison. *Supply Chain Manag. Int. J.* **2016**, *8*, 355–366. [CrossRef]
88. Tayauova, G. Advantages and disadvantages of outsourcing: Analysis of outsourcing practices of Kazakhstan banks. *Procedia-Soc. Behav. Sci.* **2012**, *41*, 188–195. [CrossRef]
89. Schmid, A.U.; Knudsen, S.; Niehoff, T.; Schwietz, K. Planning Distributed Security Operations Centers in Multi-Cloud Landscapes A Systematic Approach, Generalized from A Case Study. *Res. Sq.* **2023**, 1–18. [CrossRef]
90. Saraiva, M.; Mateus-Coelho, N. CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Comput. Sci.* **2022**, *204*, 961–972. [CrossRef]
91. Shutock, M.; Dietrich, G. Security Operations Centers: A Holistic View on Problems and Solutions. In Proceedings of the 55th Hawaii International Conference on System Sciences, Virtual, 4–7 January 2022.
92. Georgiadou, A.; Mouzakitis, S.; Bounas, K.; Askounis, D. A Cyber-Security Culture Framework for Assessing Organization Readiness. *J. Comput. Inf. Syst.* **2022**, *62*, 452–462. [CrossRef]
93. Dun, Y.T.; Razak, M.F.A.; Zolkiplib, M.F.; Bee, T.F.; Firdaus, A. Grasp on next generation security operation centre (NGSOC): Comparative study. *Int. J. Nonlinear Anal. Appl.* **2022**, *12*, 869–895.
94. Nugraha, I. A Review on the Role of Modern SOC in Cybersecurity Operations. *Int. J. Curr. Sci. Res. Rev.* **2021**, *4*, 408–414. [CrossRef]
95. Kokulu, F.B.; Soneji, A.; Bao, T.; Shoshitaishvili, Y.; Zhao, Z.; Doupé, A.; Ahn, G. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In Proceedings of the CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; ACM: New York, NY, USA, 2019; pp. 1955–1970.
96. Benzaghta, M.A.; Elwalda, A.; Mousa, M.M.; Erkan, I.; Rahman, M. SWOT analysis applications: An integrative literature review. *J. Glob. Bus. Insights* **2021**, *6*, 55–73. [CrossRef]
97. Pasaribu, R.D.; Shalsabila, D.; Djatmiko, T. Revamping business strategy using Business Model Canvas (BMC), SWOT analysis, and TOWS matrix. *Herit. Sustain. Dev.* **2023**, *5*, 1–18. [CrossRef]
98. Hattangadi, V. SWOT & TOWS are Effective Tools for Strategic Formulation. *Eur. Econ. Lett.* **2023**, *13*, 977–981.
99. Wilson, K.S.; Kiy, M.A. Some Fundamental Cybersecurity Concepts. *IEEE Access* **2014**, *2*, 116–124. [CrossRef]
100. CIS. *CIS Critical Controls (R)*; Center for Internet Security: New York, NY, USA, 2021.
101. NIST. *Framework for Improving Critical Infrastructure Cybersecurity v1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
102. NIST. *Security and Privacy Controls for Information Systems and Organizations*; SP 800-53 Rev. 5; NIST: Gaithersburg, MD, USA, 2020.
103. Center for Internet Security. *CIS Community Defense Model v2.0*; Center for Internet Security: New York, NY, USA, 2021.
104. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *MITRE ATT and CK(C): Design and Philosophy*; Defense Technical Information Center: Fort Belvoir, VA, USA, 2018.
105. Kwon, R.; Ashley, T.; Castleberry, J.; Mckenzie, P.; Gourisetti, S.N.G. Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 19–23 October 2020; IEEE: New York, NY, USA, 2020; pp. 106–112.
106. Deng, S.; Guan, X.; Xu, J. The coopetition effect of learning-by-doing in outsourcing. *Int. J. Prod. Res.* **2021**, *59*, 516–541. [CrossRef]
107. Hamburg, I. Interdisciplinary Training and Mentoring for Cyber Security in Companies. In *Handbook of Research on Cyber Crime and Information Privacy*; IGI Global: Hershey, PA, USA, 2021; pp. 356–371.
108. Burrel, D.N. Assessing the value of executive leadership coaches for cybersecurity project managers. *Int. J. Hum. Cap. Inf. Technol. Prof.* **2019**, *10*, 20–32. [CrossRef]
109. John, S.N.; Noma-Osaghae, E.; Oajide, F.; Okokpujie, K. *Cybersecurity Education: The Skills Gap, Hurdle! In Innovations in Cybersecurity Education*; Springer: Cham, Switzerland, 2020; pp. 361–376.
110. Corradini, I. Training Methods. In *Building a Cybersecurity Culture in Organizations*; Studies in Systems, Decision and Control; Springer: Cham, Switzerland, 2020; Volume 284, pp. 115–133.
111. Monzelo, P.; Nunes, S. The Role of the Chief Information Security Officer (CISO) in Organizations. In *CAPSI 2019 Proceedings*; CAPSI: Toronto, ON, Canada, 2019; pp. 1–14.
112. Badhwar, R. *See Something, Do Something! In The CISO's Transformation*; Springer: Cham, Switzerland, 2021; pp. 45–53.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.