

Article

A Comprehensive Security Framework Proposal to Contribute to Sustainability

Javier Espinosa García ^{1,*} , Luis Hernández Encinas ^{1,2}  and Alberto Peinado Domínguez ³ 

¹ Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), 28006 Madrid, Spain; luis@iec.csic.es

² Higher Technical School of Engineering (ICAI), Comillas Pontifical University, 28015 Madrid, Spain

³ E.T.S. Ingeniería de Telecomunicación, Universidad de Málaga, 29071 Málaga, Spain; apeinado@ic.uma.es

* Correspondence: javier.espinosa@iec.csic.es

Abstract: Well-known international security frameworks try to eliminate or mitigate different kinds of risks on the assets covered by their scopes (e.g., people, goods, information, and reputation). To date, to the best of our knowledge, any of these approaches neither provide a comprehensive perspective on security (considered as the merge of physical and logical security) nor consider sustainability as one of the levers for their design, implementation, and execution. This work presents a comprehensive security proposal through a framework that fits to the organizational security needs and contributes to the achievement of the sustainability objectives of an organization by avoiding duplicities and large security gaps from disjointed approaches. The work is supported by a methodology, which is the result of the wide and long work experience of the co-authors on security over the years in different organizations, businesses, and scopes. As it is shown in the theoretical exemplification included in the paper, the proposed framework combines the complementary and joint action of various actors for the protection of assets capable of achieving efforts and dedication efficiency, by merging the aspects of physical and logical security.

Keywords: comprehensive security; security framework; security sustainability improvement



Citation: Espinosa García, J.; Hernández Encinas, L.; Peinado Domínguez, A. A Comprehensive Security Framework Proposal to Contribute to Sustainability. *Sustainability* **2021**, *13*, 6901. <https://doi.org/10.3390/su13126901>

Academic Editor: Zubair Baig

Received: 13 May 2021

Accepted: 15 June 2021

Published: 18 June 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 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

Nowadays, the term security has spread and risen to a big notoriety in our digital society. Since it is not an exact science, around the concept of security there are as many definitions or approaches as there are theories in international relations and political interests [1], mainly from a military defense perspective [2,3]. There is no universal definition of security [4], but in this work, the term security aligns with the analysis of [5] in terms of the protection of assets owned by an organization, regardless of their nature, either logical or physical.

In this work, we focus on a comprehensive protection of people, interests, goods, reputation, knowledge, and information of an organization, as well as the assets that support them. In other words, our work is about protecting the business of an organization and preventing losses by adding value and competitiveness by coordinated human and technological means, procedures, and information that supports the security strategy [6].

Security in organizations has become more complex, sophisticated, and necessary than ever, leaving behind the days when security in companies only meant having guards and cameras [7]. The demand for security will continue to grow hand in hand with society, adaptation and compliance with international standards will be required, the services provided will have to reach very high levels of quality and reliability, to the point that organizations will be, each time, more dependent on these security services [8–10].

However, the security of an organization must be approached from a global and integral perspective, avoiding old practices in which each element or class of value had its own particular protection strategy [11]. That is, strategic security planning must be

unique and specific in each organization to ensure the correct coordinated operation of security [12]. Security issues can hit an organization and cause real harm, no matter if the root cause is physical or logical [13].

Therefore, the essence of the comprehensive security considers threats and vulnerabilities of the business on all the assets of the organization. In this way, comprehensive security provides a convergent and orderly prism with which the efforts and the strategic, tactical, and operational decisions fits the needs and circumstances of the organization, in contrast to an independent and uncoordinated management with which chance and uncertainty play a stellar role [14]. From this point of view, a security strategy makes no sense anymore if the general services department leads the facilities protection strategy, human resources department leads the people protection strategy, marketing department leads the reputation, image, or brand protection strategy, studies department leads the knowledge protection strategy, or the information technology department leads the information protection strategy.

This paper proposes a comprehensive security framework that fits the generic protection needs of current organizations and the context that surrounds them, including sustainable development. The paper combines a complementary and joint action between the main actors and tools in pursuit of the protection of the assets, with special focus on intelligence and risk management as key roles for comprehensive security and sustainability development achievement. This way, based on a methodology product of more than 20 years of professional practice around almost every logical and physical security branch by providing services to the public and private sector, it is possible to optimize efforts to protect assets under the same organizational and functional model.

As stated in [15–19], comprehensive security is necessary for the sustainability development of businesses since security is a social and economic category within the sustainable development, which aims to counteract environmental threats as well as social threats.

The rest of this paper is organized as follows: Section 2 describes a brief background about security and its approaches in organizations that leads to comprehensive security and gives rise to the proposed framework. In Section 3, this paper presents a comprehensive security framework that is adjusted to the generic needs of current organizations aligned with sustainability development requirements, and the context that surrounds them, combining a complementary and joint action between the main actors in pursuit of the protection of their assets (tangible and intangible). In addition, in Section 4, this paper also presents an exemplification of the framework on a theoretical scenario with which to highlight the benefits provided by the framework, as well as the problems and inconveniences that are faced through its implementation and deployment. Finally, Section 5 brings the main conclusions about the proposed comprehensive security framework, paying special attention to the convenience of implementing the model to collaborate with sustainability, the difficulties to be faced during the first steps of its deployment in organizations, the benefits provided, and the main keys to be successful with the comprehensive security framework.

2. Background

Since its earliest origins [20], the demand of security by society has been a matter of fact, as well as the benefits derived from this symbiotic relationship. While, on the one hand, organizational, functional, or operational society advances have resulted in the definition, design, and implementation of the main components of security, on the other hand, innovation and constant gradual changes in security matters have led to direct or indirect improvements in society itself.

From the end of the 20th century to the present day [21], the change in the daily model of life is undeniable, from how people develop personal relationships to how business is done in organizations, through how doubts are consulted, plane seats are reserved, or food and groceries are ordered. We live in the age of digital information. The Internet has gone from being a tool limited to a small number of universities and official organizations to becoming a global network to which close to 60% of the world's population has access [22].

These massive irruptions offer infinite opportunities for innovation, growth, expansion, and development of new products and services for society. Internet and cyberspace are almost essential elements on a daily basis for millions of people who need to interact with their home (e.g., the refrigerator, the boiler, the air conditioning, the alarm system), their office (e.g., email, vending machines for coffee or snacks), or services providers (e.g., gym, shopping) [23]. Data has never been as valuable as it is today. For instance, personal data and those derived from the use of the Internet would allow to make a very precise profile of each individual thanks to their activity. Even the information of any organization (e.g., financial, operational, legal) circulates on digital supports that deal with huge amounts of bytes per second and can distribute them immediately to any of the billions of nodes in a global network such as the Internet. Since the industrial revolution of the 19th century, there has never been a change of such dimensions in which intangible assets represented more than 80% of the value of companies [24].

Today, there is no doubt that companies and institutions are increasingly complex, from both an organic and functional point of view, and that they move in a global and highly dynamic context where new technologies play a decisive and crucial role. In fact, when someone now asks about security in a company, the answers are usually divided, at least, into two blocks: one is physical security and the other is logical security. Since the human, technical, and material resources that organizations can devote to the protection of their assets are limited, the effectiveness of such resources should be maximized through a strategy that minimizes the likelihood of threats and the potential impact derived from their materialization. It is commonly accepted that information, understood as one of the main assets to be protected in any organization, resides primarily in electronic media that need to be physically protected, while ensuring the logical security of the physical media that contains it [25]. In other words, without the adequate physical security of an organization's assets, it would not be possible to guarantee their logical security, nor vice versa. In the same line, as the Internet started from a military network [26], the majority of current techniques and terms around it do come from physical world (e.g., kill chain, blue team, red team) and they are used in the same meaning and aspects but in a cyberspace [27]. Physical and logical worlds have been interacting long time: most of the use cases run in both worlds, similar techniques are used, skills and abilities are alike but end user tools are different.

Logical security or cybersecurity refers to the controls and measures necessary in an organization to preserve the confidentiality, integrity, availability, authenticity, traceability, and conservation of its information in digital format, as well as the information systems that collect, store, treat, maintain, use, share, distribute, or present it, against unauthorized access, use, disclosure, interruption, modification, or destruction of any asset [28].

A long time ago, professional areas such as telecommunications found it necessary and convenience to regulate the physical, electrical, and procedural characteristics of communication equipment to guarantee compatibility between equipment from different manufacturers [29]. In the case of the field of logical security, this has not been achieved until recently, as the computer industry field has traditionally tried to monopolize or captivate customers through hardware and/or software (e.g., IBM, Apple). Nevertheless, it is clear that the appearance, consolidation, and evolution of good practices or standards is directly linked to the existence of very specific regulations, as it can happen with quality, environmental protection, or occupational safety at the time of providing a certain service. Standards constitute a key pillar in optimizing resources and efforts within an organization with which to improve operation and make life easier for professionals.

The logical security management has evolved considerably over the last decades as a result of the rapid growth and dependence of business processes on information technology systems and the corresponding increase in associated risks [30]. Consequently, the number of publications of national and international standards on this matter has raised, becoming a clear set of good practices that can be referenced. The ISO 27000 family [31], NIST SP 800 series [32], NIST Cyber Security Framework [33], Department of Defense Cybersecurity

Maturity Model Certification (CMMC) framework [34], or Control Objectives for Information Technologies (COBIT) framework from ISACA [35] are some of the most relevant sources. These publications develop reference frameworks on which to implement logical security in an organization, with relative technological neutrality, taking as a reference the achievement of business objectives, legal and regulatory compliance, and systematic support in risk assessments when deploying any type of control or safeguard [36]. Besides, these frameworks are so much similar to each other so that it is possible to reach cross-references between them and identify the association of controls between one framework and another [37,38].

At this point, the presence of physical security in all these cybersecurity frameworks is limited to the mere protection of the information assets, the systems that process those information assets, the auxiliary equipment necessary for the information and systems, and the facilities and locations where all the previous elements are located [39]. In other words, logical security frameworks only safeguard the physical security of those items that are necessary for their assets scope (broadly speaking, information, technology systems, and communications), avoiding other valuable assets for organization such as people, goods, reputation, or knowledge.

Physical or corporate security is the function in charge of avoiding or mitigating a specific type of risks that affect an organization's personnel, goods, and knowledge through a wide range of activities, both preventive and reactive [40]. Unfortunately, unlike what happens with logical security, in the broad field of corporate security, there are very few and limited good practices or standards that, internationally complete, agreed, accepted, and recognized, are fully specified with which to comply. Maybe the most relevant and well-known ones are ANSI/ASIS International standards and guidelines regarding physical protection, such as ASIS Physical Asset Protection (PAP) [41] or ASIS Facilities Physical Security Measures (FPSM) [42]. As unfortunately as it has already been demonstrated, such good practices or standards are convenient travel companions when it comes to improving the trust and quality of the processes, services, or products offered by an organization [43]. As with cybersecurity frameworks, these standards only focus on the physical aspects of the assets (e.g., security lighting, barrier systems, video surveillance, security personnel) and not on a comprehensive perspective.

As previously stated, current security frameworks are segmented according to the assets they are focused on and define controls to safeguard them. These general frameworks define specific controls to safeguard their assets, but no complete framework envisages protecting an organization as a whole in terms of its assets. For instance, ISO 27001 [44] advises safeguarding employees, meanwhile, these handle or deal with information that must be protected across its Annex 7 (regarding human resources security) and Annex 11 (about ensuring secure physical and environmental areas), not due to employees, are key assets for an organization. Therefore, ISO 27001 controls regarding employees are not wide enough when an organization wants to protect its employees against kidnapping when they are abroad. Something similar happens with NIST SP800-53 [45] and the rest of the leading frameworks shown in Table 1.

The proposed comprehensive security framework provides a complete and total protection scope for an organization's assets (e.g., people, information, facilities, and goods).

Table 1. Types of assets covered by leading security frameworks.

Leading Security Frameworks	Assets Totally Covered	Assets Partially Covered (Framework Section)	Assets Not Covered
ISO 27001	Information Information Systems	People (A.7 and A.11) Facilities (A.11) Reputation (A.16, A.17, and A.18)	Non Information Technologies and Communications (ITC) Goods
NIST SP800-53 NIST Cyber Security Framework Department of Defense CMMC	Information Information Systems	People (PS, PL, SA, AT) Facilities (PE, AC, MA, MP) Reputation (IR, SI, AU, AT)	Non ITC Goods
ISACA COBIT	Information Information Systems	People (PO, DS) Facilities (A 13, DS 5, DS 11, DS 12) Reputation (DS 4, DS 5, DS 9)	Non ITC Goods
ASIS PAP	Facilities Goods People	Information (B.1, B.5) Reputation (B.9)	Information Systems
ASIS FPSM	Facilities	Goods People Information Reputation (3)	Information Systems

3. Comprehensive Security Framework Proposal

For some time now, the proliferation of terms such as integral, convergence, fusion, or merge, in the context of security, has confirmed that the complementation between physical security and logical security, throughout its entire value chain, provides more benefits than drawbacks [46]. Thus, Comprehensive Security (hereafter, CS) is the result of the assumption that physical security and logical security are interdependent and complementary, from a coordinated and combined perspective, leaving aside exclusions and rivalries that can only generate problems for the organization.

CS approach is neither unique nor universal. Depending on the circumstances that occur in each specific case, policies and mechanisms to be deployed will be one or the other. Nor can it be ignored that CS also has a human component that must be managed, since divisions and intrusive feelings can be generated between those who are in charge of physical security and those who are responsible for logical security [47]. Once again, it is necessary to emphasize that CS does not consist of a simple sum of logical security and physical security, but, regardless of the organizational and/or functional structure, it pursues the ultimate goal of protecting people, goods, knowledge, reputation, and interests of the organization. If physical security and logical security are at different hierarchical levels within the organization or if both are dependent on isolated executive areas, the disputes can be worrisome and cause greater issues (e.g., on budgets, functions and responsibilities). Therefore, decision-making in CS should be as judicious, objective, and impartial as possible, banishing prejudices or affinities for physical or logical aspects, in pursuit of a joint benefit for the organization. For this, it is not necessary to be an expert in both fields (physical and logical), but to have a valid enough criterion to carry out a

competent evaluation (understand and know) of what is being proposed, to keep in mind a joint vision of security risks, and internalize the way of collaboration or joint work.

With all of the above, coordination and communication are key pieces for which work groups or decision committees can be organized as a first forum for exchange, approach and consensus on risks, projects, investments, etc., where a CS strategy can begin to be outlined. All this must come from a mandate at the highest executive level within the organization to ensure permeability and have minimum guarantees of success in its deployment, in addition to setting and internalizing the mission and vision of security regarding the objectives to be achieved. CS, although it can be a challenge for an organization, generates an advantage, that of efficiency, which cannot go ignored from the moment when synergies are promoted within the security function in the organization, avoiding duplication and optimizing dedications and efforts. This efficiency in CS goes through convergent and efficient physical and logical securities. Along these lines, it should not be forgotten that CS provides a more complete vision when it comes to complying with normative and regulatory requirements that, gradually, approach the unification of security.

The absence of CS on any process of an organization is a serious drawback that directly affects its economic and social development: lack of trust and reputation of the organization; increased expenses on CS measures; or economic loss, whether local, national or global, among others. In this situation, it is necessary to provide such organization processes with CS to face these very real and tangible threats. For this reason, all the processes of an organization require a minimum CS measures that provide confidence and enable that processes, as well as a positive and direct impact on social and economic development.

As in software engineering, CS must be considered and incorporated into the business processes of the organization from the beginning, designing a program capable of meeting the security needs of the organization that does not negatively impact its operation or generate rejections. Security by design is a good starting point to address CS and thus reduce risks. In addition to the general functions of any department (e.g., personnel management or financial management), the true value that CS management brings to organizations lies in close coordination with other areas and institutions when it is directed through a set of activities aimed at safeguarding the organization's interests and valuable assets, both tangible and intangible. The scenario and context where any organization develops its business activities are complex, besides facing global threats (e.g., climate change, hybrid wars, and mass migrations) [48].

This section presents the main elements of CS (see Figure 1). Some of them are traditional ones for a biased view of physical or logical security, but this time they are considered as coordinated tools aimed to provide preventive and reactive protection to any asset of the organization, taking advantage of the power of each of these elements.

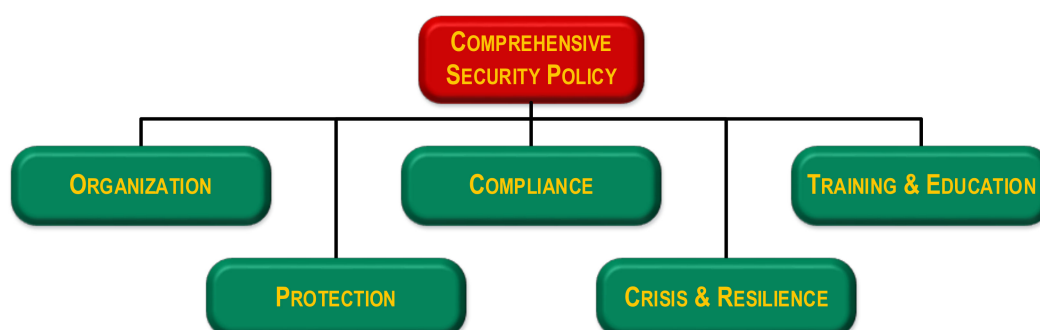


Figure 1. Comprehensive Security Framework overview.

3.1. Comprehensive Security Policy

The Comprehensive Security Policy (hereafter, CSP) corresponds to a declaration of high-level intentions which establishes the bases on which the entire CS function will be

developed in the organization, contributing to its homogenization and the rationalization of decision-making processes on security in the organization. The CSP will cover organizational, protection, compliance, crisis and resilience, and training and education principles in order to set CS bases.

The CSP, aligned with the mission, vision, and values of the organization, must establish its scope of application (e.g., employees, areas, processes), promote and encourage its knowledge and adoption among third parties, as partners, suppliers, contractors, collaborating organizations, etc., as well as decreeing possible coercive measures in case of non-compliance.

The CSP, among others, must:

- Determine which type of assets will be applied to (e.g., people, facilities, goods, information, reputation);
- Establish the CS goals (e.g., provide confidence to customers, achieve efficiency in protecting assets, comply with internal and external security requirements, ensure business continuity, improve internal security processes);
- Assign the responsibility of supporting and sponsorship of the CSP within the organization in terms of its development, implementation, and update;
- Settle the reference principles for CS in the organization (e.g., compliance with current legislation, respect for human rights, provision of resources, collaboration and coordination both internally and externally, the creation of a CS awareness, the promotion of a safe working environment).

3.2. Comprehensive Security Organization

In recent decades, the security function has escalated from depths to highest heights in executive offices within the structures of organizations. Despite some important obstacles, such as mergers or bankruptcies, security is now considered a vital part of most organizations, with professionals who report directly to the steering committees.

One of the main problems that arise around the structure of CS is related to its location within the chart of the organization so that the services provided are adequate, that is, who should be informed. The recognition of the need for CS within the entire spectrum of activities of any organization (since it directly or indirectly affects the final profit and loss statement), suggests greater responsibility and authority within the organizational structure. For this, CS must be placed in a high position within the organizational chart, close to the decision-making and management bodies of the organization. This could be either directly depending on the highest governing body of the organization (e.g., executive or management committee) or depending on a global area of the organization that does report directly to that governing body (e.g., a general management), thanks to which dynamism will be gained in the organization.

Once the CS is placed within the organization chart, the next step is to delve into the internal functional structure it should have. The proposal presented in Figure 2 is not limited to a mere fusion of models, but rather tries to organize those areas that present the greatest number of synergies in the context of CS. In the next subsections, the most relevant CS functions are described in detail.

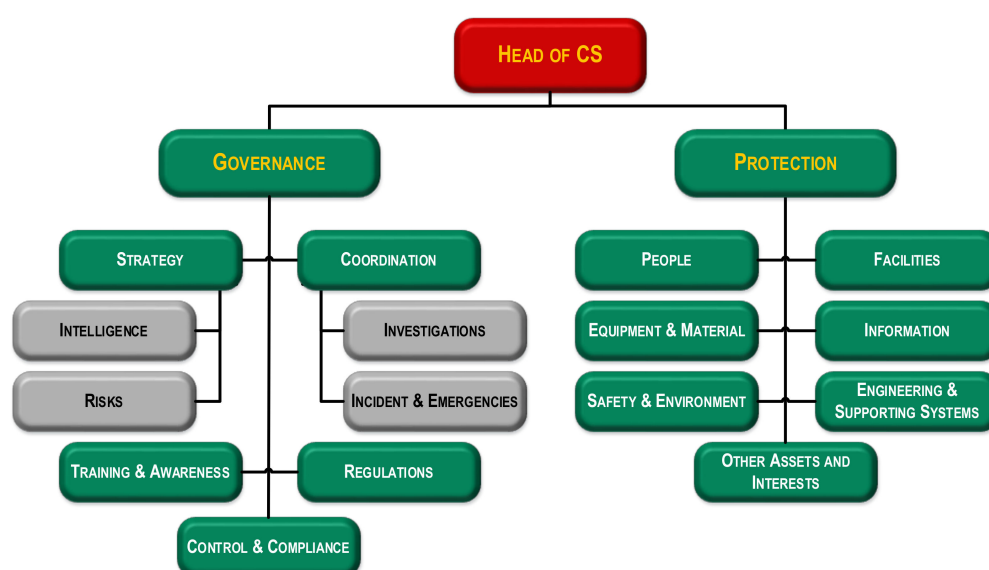


Figure 2. Comprehensive Security Functional overview.

3.2.1. Head of Comprehensive Security

The Head of CS is a key role that should pay more attention to the leadership of the area than to make operational decisions, no matter whether the Head of CS is member of the board of the organization or reports to a member of that board. That is, the Head of CS should promote an adequate working environment, mark the guidelines, suggest alternative solutions to problems, encourage and facilitate the professional growth of the team, etc.

Obviously, in those cases in which the organization is small, the Head of CS will have a more direct participation in the operational chapter. In the leadership role, the mark of success is directly associated with the ability to delegate responsibilities and an appropriate authority.

Outside its scope of natural action, the Head of CS must have sufficient presence and dynamism, preferably as part of the management team of the organization, with interests that go beyond CS and, in its relationship with the personnel of the area, be innovative, patient, exemplary, and able to guide and give useful advice.

3.2.2. Comprehensive Security Governance

The Governance of CS is a continuous cycle that must establish strategic, tactical, and operational responsibilities around a set of policies, norms, and procedures with which to direct, control, and supervise the protection of the organization's assets.

This Governance area must cover the specific needs of business that could be demanded at any time, as well as create a culture of CS and align the behavior of people, processes, and technologies to achieve the business objectives set by the organization.

Additionally, Governance must be the backbone responsible for ensuring the management, organization, and effectiveness of the security of the organization's assets in a coordinated, comprehensive, and joint manner. For this, Governance of CS has a whole set of resources with which to be able to, among others:

- Define, design, deploy, and monitor a complete security strategy according to the total assets to be protected. For this aim, tools such as intelligence and risk management should be available;
- Identify and implement specific internal CS procedures, keeping in mind those elements, such as regulations, laws or international frameworks and their changes or incoming ones, which are applicable in the organization and its business;
- Give coordinated due response to any type of CS incident or emergencies that may arise, from the early phases to its end and return to normality of such situations;

- Investigate any irregularity or sensitive situation in order to provide the necessary answers or conclusions;
- Improve the organization's security culture and sensitivity around CS through training and awareness;
- Carry out internal control over CS, determining a maturity degree of security within the organization (e.g., compliance, effectiveness).

3.3. Comprehensive Security Protection

Materializing the declaration of intentions contained in the CSP about protecting an organization's assets is not a trivial task. In order to comply with CSP, it is necessary to know and assimilate the business activities and context of the organization, so that it is possible to safeguard the people, goods, knowledge, and interests that support such activities against events that negatively impact them.

CS is a complex purpose, away from simplistic visions that assume a false and deceptive security by the mere fact of having a security guard at the entrance of a facility, a video surveillance system in the hallways, an antivirus in the computer, or a password on the mobile phone. It is necessary to know the activities of an organization and its value chain to protect all those key assets from a CS point of view.

An organization's assets could be grouped around categories such as People, Facilities, Equipment and Material, Information, Information Systems, and Other Intangible Assets (e.g., reputation, mark, confidence, interests). An organization achieves its business objectives through its critical resources, so the protection of such assets and business operations is essential. From a CS perspective, this protection implies the consideration of a wide range of threats of a very diverse nature, so the people and resources (i.e., budget) destined to these tasks must be multidisciplinary and wide ranged.

An organization's assets, in addition to being classified by their nature, must also be categorized according to their relevance for the organization, so that an asset must be considered critical, standard, or inconsequential depending on the impact for the organization when a threat materializes on said asset. Expert areas of the organization must define a minimum set with protection measures for each type of asset and its corresponding classification, always according to the risk assessment results and other factors such as costs, return on investment, legal requirements, or regulatory requirements, so that the organization's needs are covered with due flexibility.

3.4. Comprehensive Security Compliance

There is no doubt that any organization must have correctly identified all the CS requirements arising from laws, regulations, international standards, contractual commitments, or its own internal processes. These requirements must be included in the Comprehensive Security Framework (hereafter, CSF) as specific security controls or measures.

All employees must know about and apply all these CS requirements, so that they are not exempted from their responsibilities associated with their non-compliance by ignorance and/or lack of application thereof.

Thus, the organization must carry out regular assessments in order to verify its completeness and compliance with its CSF controls, and proactively identify any vulnerability that could put the CS of the organization at risk.

In this way, any organization must define a review plan to cover all applicable CS areas within its CSF in order to prevent potential incidents or deviations, and fix any finding according to its risk appetite.

3.5. Comprehensive Security Crisis and Resilience

Another element to consider in the proposed CSF is the security incident management. Depending on the intensity of a security incident, this can generate a serious organization crisis that could make necessary setting business continuity plans in motion.

For this reason, the organization CSF must:

- Provide systematic, accurate, and particularized procedures for security incident management, according to the organization needs;
- Identify those key players or roles that are involved in security incident management, defining and assigning responsibilities and authorities among them;
- Set communication channels and interfaces for security incidents;
- Define the relational model between those CSF roles that take part in the security incident management process;
- Agree on systematic evaluation criteria that avoid ambiguities when classifying security incidents;
- Keep updated records and details of each security incident that has occurred in order to get a complete knowledge database that allow to make incidents comparison;
- Establish priorities for the resolution of security incidents, by incident impact (i.e., relevance according to its effect on assets) and urgency (i.e., the maximum acceptable time of delay for its resolution). This way, a quick, effective, and organized response is ensured;
- Analyze root causes of incidents to define, plan, and implement solutions to avoid repetition of similar incidents;
- Monitor and control the evolution of security incidents from their detection to their resolution;
- Gather valid, necessary, and sufficient evidences to face subsequent audits, forensic analysis, negotiations, or even trials with basic guarantees.

3.6. Comprehensive Security Training and Education

CS is a multidisciplinary concept, aligned with current needs and trends, and understood as a holistic process shaped up with a wide cross section of several procedures, techniques and tools (e.g., scientific, technological, economic, financial, legal, social).

CS covers the most relevant fields of security, in strategic, tactical, and operational ways. Additionally, CS is aimed at preventing and avoiding any damage, danger, or risk that threatens any asset or element of value for an organization.

From this point of view, the organization must establish general guidelines to ensure that its employees are enough CS skilled to comply with its CS regulations on their duties.

Therefore, CS training and education supports many important organizational goals, allowing those who are instructed to be better able to

- Protect the organization assets, as the first and foremost purpose of training and education. Any other goal derives from this fundamental premise;
- Understand the relationship between CS and successful activities, enhancing awareness on the value and profitability of CS;
- Identify CS obligations for employees, showing such requirements in a reasonable and necessary way;
- Know the relationship between the CS objectives and deployed CS controls, proofing their utility, need, proportionality, and convenience;
- Find and locate those key areas to turn to in case of doubt, query, or an unforeseen event regarding CS within the organization;
- Comply with legal, regulatory, contractual, or internal requirements that could be applied in terms of CS by the organization;
- Minimize the responsibility of the organization, as a legal person, to counter negative events to its interest—even criminal or civil liability—by demonstrating that the organization watches over CS;
- Appreciate the CS function within the organization, providing a full valued service.

3.7. Comprehensive Security Framework Contributions

In first view, this CSF could look like a common existing governance framework that has been well established as a practice for quite some time now. However, this proposed

approach differs from current security governance frameworks over a single and full CS strategy, as it is shown in the following:

- Intelligence as an asset protection tool [49]. The main objective of intelligence as a process and result is to provide information and assessments that allow making the most accurate decisions possible. In this way, intelligence is able to explain to the decision-makers what has happened, what is happening, why, and what is most likely to happen in the future projected in the short, medium and/or long term. So far, no leading security framework has been identified that includes intelligence as a key tool or activity. The inclusion of intelligence function to the CSF returns high value when coordinates with other areas and organizations, in addition to providing robustness and completeness to the CS governance and management process. Additionally, intelligence avoids strategic and tactical surprises around CS; reduces the uncertainty that CS entails; and provides long-term experience on issues related to CS. For all that, the inclusion of a formal intelligence process in the proposed CSF provides a benefit that is either not present in current leading security frameworks or is not applied in CS;
- Unified and comprehensive security risk assessment on assets [50]. Risk assessments on physical security and logical security are a reality in the vast majority of the organizations [51–54]. However, each risk assessment has its own scope and particularities (e.g., assets, threats, vulnerabilities, and controls), fully aligned in pursuit of a common benefit for the organization. Thus, the CS aspects are addressed in a tangential way in the best of cases. This CSF proposes a CS risk assessment of the assets to be protected, where the total of threats, vulnerabilities, controls, and other conditions are examined in depth from a CS perspective. This means much more than join their specific catalogues (threats, controls, etc.). This implies a more complete and thorough analysis that goes beyond physical or logical partial considerations, directed towards covering security gaps. For instance, if financial fraud is considered, the Chief Information Security Officer looks at the problem from a logical point of view, while Chief Security Officer looks at it from a physical perspective, but a complete assessment requires knowledge and details from both perspectives to cover the entire spectrum and avoid gaps. This proposed approach would provide greater strength, resilience, and efficiency to the security process, which would go beyond a mere collaboration between the areas that shape it. All the mixture around risk assessment (e.g., threat, vulnerability, consequence, criterion, appetite, or treatment [55]) should not lose its objective and interfere in the process itself. Especially, taken into account that its main purpose is to provide the decision-making bodies or the organization with the necessary information to define and deploy a judicious CS strategy according to the business processes and the established business objectives. This CS strategy will consider sustainability development as a key factor to be considered, especially when efficiency and effectiveness parameters can vary over the time (i.e., it is useless to deploy a security measure, no matter how cheap it may be, if the organization will not be able to maintain it);
- Comprehensive security investigations from the same unit to face incidents [56]. Probably, investigations chapter constitutes one of the greatest challenges in the proposed CSF for organizations. One of the main work tools of CS to face operational, image and even criminal risks is investigation. The use of investigations techniques allow to keep the decision-makers informed or to complement ongoing actions of other units inside the organization (e.g., internal irregularities of employees, inappropriate behavior, fraud, commissions and bribes). Investigation corresponds to the fact of searching, observing, studying, clarifying, collecting, or examining, in a systematic and exhaustive way, information on certain elements (e.g., people, incidents, activities) to respond to a query or problem with the highest degree of certainty possible and to facilitate subsequent decision-making (e.g., hiring, firing, judicial process). Typically, according to the nature of the issue that arises, several investigation units appears

(e.g., cybersecurity and corporate security). During the parallel investigations, these units focus on their action and responsibility scopes, getting around those no-man's lands that could be critical. This CSF proposes that security investigations should be carried out by one specialized area that covers the whole scope. This investigations team would be able to answer basic questions (e.g., who, what, where, when, why, and how) and provide evidences that supports the findings;

- Alignment and integration of comprehensive security strategy in the sustainability development strategy of the organization. Sustainability is an effective strategic factor in establishing competitive differentiation in the markets through different sides, but a clear commitment to CS facilitates the achievement of an organization sustainability goal [57];
- Sustainability development of the CS aims to ensure that the protection of organization assets impact is neutral or positive, so a solid CS is not an individual goal, but is part of an organizational sustainability trend [58]. To date, security assessment has been based on efficiency and efficacy: on the one hand, necessary resources (e.g., time, money, material or human resources) are assessed against the achieved security levels; and on the other hand, those security levels are checked against the desired ones [59,60]. However, these two parameters are not enough for CS, which considers and adds its sustainability for the assessment, that is, the ability of CS measures to remain stable over time. It cannot be ignored that alignment with organization strategy is necessary. What good are security measures whose effectiveness decreases over time? What good are security measure whose maintenance is an ongoing costs increase? At this point, sustainability is once again a key factor in CS: management must be concerned with the resources that goes to CS and the obtained results, but the ability to keep these over time is of fundamental importance for CS.

3.8. Comprehensive Security Framework Benefits

It should be clear that a CS approach becomes a more complete and strong path than if different securities were carried out separately, since threats and vulnerabilities analysis on assets can provide more effective and efficient strategies for risk management. In addition, CS is able to provide rationalization to the general asset protection process and gain greater efficiencies, by deleting functional gaps and promoting cost savings, by either eliminating or reducing expenses.

The proposed CSF results in an improvement in the organization's security culture, which can positively influence the reduction of the number of security incidents, as well as their intensity. Finally, it is worth highlighting the benefit associated with this approach, such as the improvement in the reputation and image of the organization, both internally and externally.

The proposed CSF contributes to shape a business model where all the organization's value chain members (e.g., employees, stakeholders, partners, suppliers, customers) increase confidence with more reliable processes under a comprehensive security. This reinforce the social responsibility of the organization and improves the organization reputation and image.

At the same time, sustainability and its development within CSF are elements that have led to significant changes in security by incorporating the time as a new variable to determine the suitability of security controls. CSF makes a more optimized use of the necessary resources in the organization to identify security vulnerabilities and mitigate security risks on business processes with rational, sustainable and justified investments.

Finally, this CSF protects organization assets from both a physical and logical perspective, bringing down the number of frauds in the organization and, therefore, in the society. This minimizes the social and environmental risks that result in improving the functioning of society.

More detailed benefits are included in Section 5.

4. Case of Use

Any security framework based on a policy system is a part of high-level management and is necessary for corporate governance. Generally, the competitiveness of large/medium-sized enterprises must rely on a complete and effective security protection policy, and the complete practice of security framework can be used to demonstrate corporate performance. Small/medium-sized enterprises may slightly simplify the intensity of their practice due to work force or cost considerations, but if they have a complete security policy, supplemented by proper management, they should also be able to achieve the company's expected governance and protection goals. Several variables can determine the exemplification for the proposed CSF presented in Section 3.

Regarding the size of the organization and according to the data published by the Ministry of Industry, Commerce, and Tourism of the Government of Spain [61], the case of use will consider small/medium-size companies with 10–249 employees, which represents 5.93% of business fabric in Spain and 33% of employment in the country. The main reason for this decision is that the CSF implementation and execution will require human and financial resources, so most of the small and medium enterprises with up to nine employees will not be able to afford it. On the other hand, large companies with more than 250 employees are also ruled out because their size, organizational structure, or international presence would need a thorough analysis before the CSF deployment.

The problem that puts forward the case of use refers to a company where certain physical and logical security functions are internally carried out, not as primary activities but as secondary. That is, there are people within the company who are entrusted with certain professional duties that are performed in a complementary and almost random way. It is about an example where the security of the company's assets is not addressed in a complete, systematic, and homogeneous way. This is a representative example where an international business expansion is the driver to implement and operate de CSF. That is, the transformation begins because of a strategic business requirement and it makes all the sense.

So let us consider a theoretical small/medium-sized enterprise. This case is about an organization that decides to adopt CSF as a result of a strategic business approach where CS makes perfect sense. This is a scenario where the "canvas" is practically intact and the implementation of CS is simple and orthodox according to the CSF.

4.1. Introduction

Fictitious Business Name (hereafter, FBN) is a theoretical and small consulting company founded in Spain in 2003 by John Doe and Jane Doe. FBN helps its clients in the world of cryptographic security solutions with experience, rigor, innovation, quality, solvency, and balance against challenges, needs, and problems related to confidentiality, integrity, authentication, authorization, or non-repudiation that may be presented around the information of their businesses or organizations.

The catalog of services provided by FBN covers a wide spectrum around cryptography and its applications, both theoretical and practical. The company develops customized cryptographic tools and integrates them with technological platforms; executes "turnkey" projects regarding blockchain, machine learning, and specialized intelligence services; defines and puts into practice master, strategic, and research plans; provides top management advice as well as specialized training, awareness, and, in general, any other type of assistance required by its clients.

FBN, which has offices in Madrid, has exceeded the turnover of five million euros in the last fiscal year, with outstanding operating benefits and a positive EBITDA of 0.82 M EUR thanks to a workforce that has 25 professionals who provide their services to national and international clients.

Taking into account the typology of its services and its current foreign clients, FBN has considered its international consolidation as a strategic aspect. For this reason, FBN has decided, on the one hand, to start an orderly deployment in The Hague (Netherlands)

following some business opportunities with the Europol's EC3 (European Cybercrime Center) and, on the other hand, to restructure the company's security under a normalizing prism according to the proposed CSF. The new CSF of FBN should allow to

- Set strategic (long-term), tactical (medium-term), and operational (short-term) security objectives aligned with the level of security required by third parties (e.g., Public Administration, Europol) or the company itself;
- Plan and optimize costs and investments necessary to achieve the established objectives;
- Define lines of coordination and control in the area of security;
- Know and evaluate, objectively and homogeneously, the maturity of the security at FBN.

The implementation of this planned evolution in the security position of FBN towards the proposed CSF goes through reviewing the current security status of the company and analyzing the existing gap in front to the desired situation of CS, for then proceeding to adapt the company.

4.2. Current Security Status

FBN is a national reference for expert support in information security and cryptography that, even having a privileged position in the Spanish market, has decided to initiate the internationalization of the company towards other markets.

This decision implies new opportunities, needs, and, therefore, threats to its assets, which leads to evident requirements of proactive management of its CS. A CS that must be systematic, homogeneous, specialized, and aligned with the quality and trust that characterize the services offered by FBN.

4.2.1. Internal Analysis

From an internal point of view, the current organizational model of FBN in security matters (see Figure 3) is manifestly dispersed within the company. Since its launch, FBN has put the development and consolidation of other areas of the company—such as Research, Development, and Innovation (hereafter, R&D&I), business development, or finance—before a coherent, complete, and adjusted structure that fits real security requirements. The root cause of this fact is that security, as a whole, is not considered as a strategic function.

In this sense, the main actors for the internal CS services, articulated around the definition of the necessary security parameters for the development of the activity, the implementation of the defined security requirements, the operation of the activities of security around the business and the supervision or control of the proper functioning of such activities, are as follows.

- In the first place, the Chairman stands out as responsible for the physical security of FBN facilities. Specifically, the Chairman of FBN is the visible head of the company in terms of physical security for clients and the public administration, in charge of managing a contract with a security company that provides security for the company facilities and assets;
- On the other hand, the IT and Computing Manager is in charge of the cybersecurity of the information systems of FBN through the deployment and monitoring of basic protection measures, such as antivirus, access control to internal network, active directory permissions, server backup management, user provisioning, and credential management;
- Additionally, there is no approved security policy and no internal security regulation have been developed. Nevertheless, FBN has accredited international certifications in quality [62], environmental [63], and occupational health and safety [64] management. There is a quite few documented processes about security, as well as a minimum monitoring and control on security;
- Very few security activities exists in FBN and these are scattered all over Madrid offices, as well as the company's organizational structure. No formalized committee

or working group, supported by top management, coordinates security function. For instance, company assets have not been classified according to their criticality yet;

- Employee awareness regarding security is low or very low, and there is no evidence on audits or independent security reviews. This impact on the internal control of the security;
- Business continuity in FBN is oriented to disaster recovery on information technologies and communications, leaving aside business continuity as itself (i.e., business processes recovery according to people, facilities, critical providers, or information requirements).

It is clear that current maturity of FBN, in terms of CS, is in an initial stage, where certain controls are appreciated but without proper management or centralized coordination and, of course, an obvious organizational and functional lack regarding the proposed CSF.

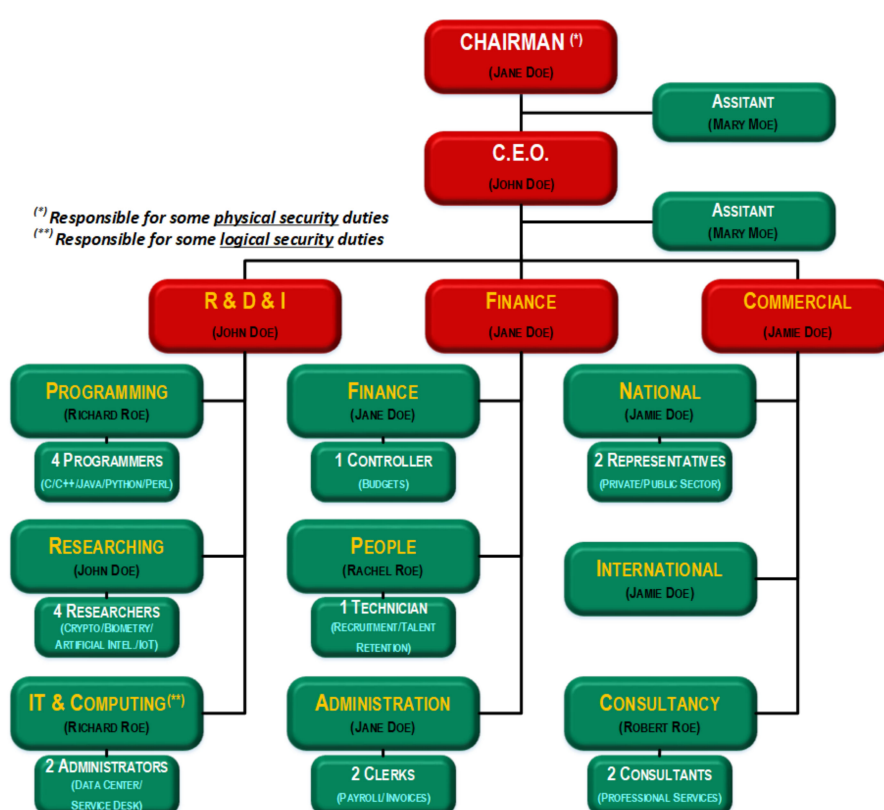


Figure 3. FBN Current Organization Chart.

4.2.2. External Analysis

From an external point of view, the security and sectoral environment of FBN has been analyzed in order to achieve a homogeneous criteria baseline. This baseline helps to determine the most efficient comprehensive security mechanisms and structures, resulting in the following conclusions:

- Security threats evolution that affect the main assets of FBN, such as intellectual property, its publications, and its cryptographic products, is very high, so it is highly recommended to take action on the daily operations of the company to manage and control vulnerabilities;
- Comprehensive security function must have a specific budget dedicated to the start-up, operation, maintenance, and control of security in the company's business processes;
- Comprehensive security function must be aligned with FBN's business units, holding all the company's existing asset protection functions;

- The pressure derived from regulatory requirements, both from the FBN sector as well as from its partners and clients, forces to improve the control and security levels provided by the company in its daily basis processes.

4.2.3. Strengths, Weaknesses, Opportunities, and Threat Analysis

Previous gathered information leads to conclusions that can be drawn through a Strengths, Weaknesses, Opportunities, and Threat Analysis:

- Strengths (i.e., positive elements that the company has in terms of CS): decision to adopt the CSF; acceptance of outsourcing services that provide little or no added value in CS to business processes; centralization of company's security processes under the new CS division (hereafter, CSD);
- Weaknesses (i.e., negative aspects that should be faced up to in the future, in terms of CS): lack of a business continuity plan; absence of a security policy; lack of an inventory of company assets; no documented and formal security procedures; low compliance with regulations; poor security training and awareness; limited number of employees with specific security experience;
- Opportunities (i.e., factors that are potential to develop or trends that positively affect business processes and the CS with which these must be provided): have a CSF; improve the current business model by incorporating new CS services; automate or outsource certain CS processes related to cybersecurity; align the CS strategy with the company's existing strategic plans; take advantage of synergies between all the company's business areas;
- Threats (i.e., negative forecasts or unfavorable trends for the CS improvement): loss of reputation due to security breaches; exposure to vulnerabilities and risks associated with the evolution and changes in the company's business strategy; compliance and regulatory pressure; lack of CS specialized personnel; lack of dedicated budgets for CS.

4.3. New Comprehensive Security Objectives

The fundamental basis on which the CS will be developed in FBN will have as a reference the following objectives:

- Guarantee the full protection of FBN business and its assets, both physical and logical nature ones;
- Incorporate CS in internal processes, with special attention to intelligence duties;
- Support company's security strategy in terms of CS risk management;
- Have an internal CS regulation that fits business needs;
- Have an optimal organizational structure regarding CS;
- Ensure compliance with regulations and other CS requirements that were applicable.

4.4. New Comprehensive Security Organization

The new CSD will be responsible for deploying the guidelines set by FBN with the appropriate human, material, and economic resources, directly reporting to the Chief Executive Officer of the company (see Figure 4), with sufficient visibility and voice on company matters such as planning, objectives, and decision-making processes.

In this case, since main business areas remain the same, the FBN organization does not change but the new CSD. As main responsible for the definition, planning, execution, monitoring, and control of the CS at FBN, the CSD must specify the objectives and corresponding security strategies on the company's assets, in addition to the management, governance, and protection functions.

For this, the new CSD at FBN must be adjusted to the reality of the organization (i.e., size, turnover, assets), so a basic organizational structure will be adopted, capable of covering the functional needs of CS and concentrated in the figure of the Head of CSD (hereafter, HCSD). The HCSD, organically and functionally dependent on the CEO of the company, will be a new employee that will have more than five years of work experience in similar positions.

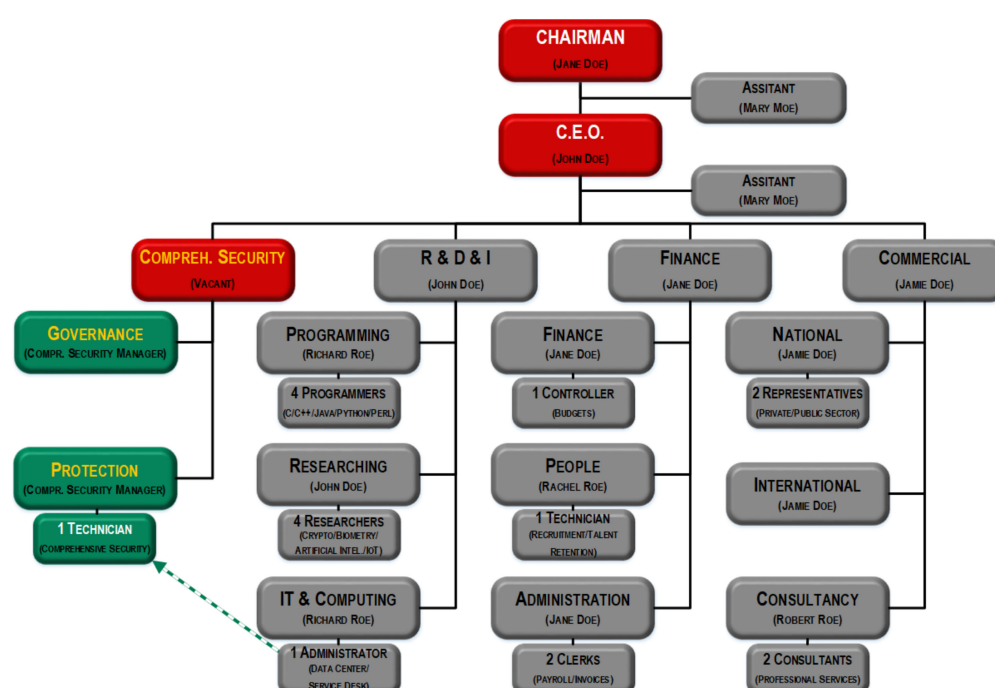


Figure 4. FBN New Organization Chart.

It is worth highlighting the main responsibilities of the new HCSD, as the highest authority and responsible for the CS governance and protection within the company:

- Deploy the new CSF within FBN;
- Specify and promote the approval of an internal regulatory body for CS;
- Manage CS risks of FBN;
- Ensure the adequacy and implementation of CS in the company in accordance with the strategy of FBN and with the appropriate solutions that are established, in technical, functional, and organizational ways;
- Define the CS strategy for FBN;
- Describe the roles and responsibilities for job positions at CSD;
- Provide a CS risk analysis and management methodology for FBN;
- Promote CS awareness and training within the company;
- Act as a consultative element for top management in case of any CS doubt or incident;
- Regularly inform top management about the company's CS status;
- Coordinate CS incidents that may occur and impact on the company's activity or assets;
- Supervise and evaluate the CS activity in FBN, ensuring the achievement of the objectives set;
- Maintain and coordinate existing continuity and contingency plans at FBN.

One IT and Computing administrator will be transferred to CSD as a new protection technician. This one will have to be "recycled", thus in a first and very precarious instance, this role could be limited to the protection of information assets and the management of supporting systems. However, in order to optimize the workload in CSD, this protection technician should receive complete training in CS.

In addition to all of the above, the CSD will establish an internal CS forum or committee where all company executives can express their needs or doubts on security. This way, FBN will take advantage of project synergies and provide enriching contribution for the company.

The HCSD will be in charge of the execution of a security analysis to identify protection measures to be addressed to mitigate existing risks over people, facilities, equipment, information, or reputation, among others.

4.5. Implementation Costs

The costs that FBN would have to assume to implement the proposed CSF would be very limited.

Maybe, the biggest cost corresponds to the personnel chapter. In this regard, the incorporation of a HCSD would represent almost a third of the total initial cost. In addition, it would be an annual recurring cost.

Other item with high weight in the costs lies in the implementation of technical security measures derived from risk assessment. Based on outsourced professional services, maybe this item does not need a high initial outlay but it would be a recurring cost.

5. Conclusions

Finally, this section brings the main conclusions about the proposed CSF, paying special attention to the convenience of implementing the model, the difficulties to be faced during the first steps of its deployment in organizations, the benefits provided by the CSF, and the main keys to be successful with the CSF.

Security is a necessary tool to avoid certain threats that negatively impact on the sustainability development of organizations. Whether referring to physical security attacks [65–67] or to cybersecurity attacks [68–70], organizations face a serious problem that grows exponentially and inexorably. Unfortunately, no one can say they are out of danger. Any asset of an organization or individual is susceptible to become a victim of an attack, no matter if this is either physical, logical, or cyber-physical nature. In the context of sustainable development, this situation could be framed within the chapter of social and global threats, so the adoption of a framework such as the CSF presented in this work contributes to the awareness of organizations on the security issues. Moreover, CSF is able to optimize the use of resources aimed at assets protection, address a greater range of action with the same resources, and avoid large security gaps because of disjointed approaches.

The following are the main conclusions:

- **Transparency and Agility.** This CSF proposal evolves the traditional concept of protection over the organization's assets and incorporates activities (e.g., strategy, intelligence, regulations, risks) on which it reduces complexity and even operational duplicity, with the consequent improvement of conflicts and confusions, and the optimization of resources and workloads. Given a situation that must be managed from security (e.g., financial fraud), the proposed CSF provides agility and responsiveness when it comes to urgent consultations or making security decisions within the organization, thanks to the reduction of uncoordinated decision or consultation elements. This can make the difference between success and failure while facing an incident;
- **Egos and Gangs.** Talking about assets protection, within most organizations, there are two high-level factions that come from two well-differentiated origins, whose composition is also very different and usually cohabit: they are physical security and logical security. At present, the vast majority of organizations still maintain parallel these structures, with separate and watertight operations, to address the security of their assets. Regardless of whether, in some cases, physical security and logical security can share elements such as people, intelligence, or infrastructure, the objectives of both areas remain disparate, work platforms remain unconnected, budgets remain independent, work standards are not coordinated, etc.;
- **Reality and Need.** Today, there are no isolated, exclusive or independent security problems in any area of organizations because any incident has different impact dimensions that must be analyzed by coordinated professionals capable of containing the incident and its negative implications. Perhaps when physical security departments investigate some case of fraud they do not request emails, personal computers or mobile phones of the organization in order to reach certain conclusions and, where appropriate, support a certain coercive action? Not to mention those circumstances where autonomy and confidentiality (e.g., internal investigations, judicial require-

ments), shared information, intelligence, and principles of action become an essential need for the organization under a CS vision;

- **Simplicity and Efficiency.** The CSF proposed in this work simplifies the development of the security function within the organization from a joint and singular perspective, away from mistrust of multiple complex disciplines and providing a normalization and demystification of security that allows organizations to focus on their priorities and make efficient use of their dedication and efforts in the face of serious problems. The day-to-day security is surrounded by problems. Problems of a very diverse nature and importance, whose impact can range from strategic aspects to other operational ones within the organization. This may affect tangible or intangible assets, whose resolution may be immediate or need several “iterations” to be solved, which require a lot of time and resources to face them or that, on the contrary, practically do not require dedication. The effort to fix any security problem will always be less from a CS level than from a divergent approach since, in the latter case the effort is managed from teams of different disciplines, while in the first case the resources are organized and coordinated. Therefore, the effort is managed through joint disciplines;
- **Resolve and Perseverance.** There is no single route to achieve the CSF within an organization, but it will depend on the characteristics of each organization, in terms of key business, volume of employees, customers, suppliers, existing organizational structure, etc. However, the fact of having a CSF such as the one presented here constitutes an interesting starting point to begin the journey towards the realization of CS within an organization. The challenges that arise in an organization when facing CS are not minor, but in no case should they block its implementation, especially if we take into account the resulting benefits through a global and general vision of the security of the assets of the organization. The presented concept of CS is undoubtedly familiar to most organizations and security professionals (regardless of whether they come from the physical or logical side). That, as it begins to materialize, is showing a set of benefits that, ultimately, result in greater and better protection of their assets, a rationalization of the media, an optimization of processes, an increase in productivity, an improvement in the image of the organization, and, of course, all this constitutes cost savings for the organization.

Author Contributions: Conceptualization, J.E.G., L.H.E. and A.P.D.; methodology, J.E.G., L.H.E. and A.P.D.; validation, J.E.G.; formal analysis, J.E.G. and L.H.E.; investigation, J.E.G., L.H.E. and A.P.D.; resources, J.E.G., L.H.E. and A.P.D.; writing—original draft preparation, J.E.G.; writing—review and editing, J.E.G., L.H.E. and A.P.D.; visualization, J.E.G.; supervision, L.H.E. All authors have read and agreed to the published version of the manuscript.

Funding: Department of Information and Communication Technologies (TIC) at Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research has been partially supported by the Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC). The authors would like to thank the anonymous reviewers for their valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pérez de Armino, K. Estudios de Seguridad: De la visión tradicional a los enfoques críticos. In *Teorías de las Relaciones Internacionales*; del Arenal Moyúa, C., Sanahuja Perales, J.A., Eds.; Revista Española de Derecho Internacional: Madrid, Spain, 2015; pp. 301–328.
2. Huysmans, J. Security! What Do You Mean? From Concept To Thick Signifier. *Eur. J. Int. Relat.* **1998**, *4*, 226–255. [[CrossRef](#)]

3. Jovanovic, M.; Burbiel, J. The evolving concept of security: A critical evaluation across four dimensions. In Proceedings of the 9th Security Research Conference Future Security, Berlin, Germany, 16–18 September 2014; pp. 502–506. Available online: https://www.researchgate.net/publication/278033393_THE_EVOLVING_CONCEPT_OF_SECURITY_A_CRITICAL_EVALUATION_ACROSS_FOUR_DIMENSIONS (accessed on 1 June 2021).
4. Williams, P.D. *Security Studies: An Introduction*; Routledge: London, UK, 2012. [CrossRef]
5. Baldwin, D.A. The concept of security. *Rev. Int. Stud.* **1997**, *23*, 5–26. [CrossRef]
6. Cabric, M. *From Corporate Security to Commercial Force: A Business Leader's Guide to Security Economics*; Butterworth-Heinemann: Boston, MA, USA, 2017. Available online: <https://www.sciencedirect.com/book/9780128051498/from-corporate-security-to-commercial-force> (accessed on 1 June 2021).
7. Hamilton, B.A. *Convergence of Enterprise Security Organizations. The Alliance for Enterprise Security Risk Management*; ASIS International: Alexandria, VA, USA, 2006; pp. 1–7. Available online: <https://pdfs.semanticscholar.org/9cb9/fe2450502b4e8bb4923978d9afc7198eab0b.pdf> (accessed on 1 June 2021).
8. FACT SHEET: President Biden's Leaders Summit on Climate. Available online: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/23/fact-sheet-president-bidens-leaders-summit-on-climate/> (accessed on 1 June 2021).
9. No Policy Maker Is an Island: The International Regulatory Co-Operation Response to the COVID-19 Crisis. Available online: <https://www.oecd.org/coronavirus/policy-responses/no-policy-maker-is-an-island-the-international-regulatory-co-operation-response-to-the-covid-19-crisis-3011ccd0/> (accessed on 1 June 2021).
10. Bernard, R. *Security Technology Convergence Insights*; Elsevier: Waltham, MA, USA, 2015. [CrossRef]
11. Contos, B.T.; DeRodeff, C.; Crowell, W.P.; Dunkel, D. *Physical and Logical Security Convergence: Powered by Enterprise Security Management*; Syngress: Rockland, MA, USA, 2007. [CrossRef]
12. Kinslow, J. Physical and IT Security: The Case for Convergence. *J. Secur. Educ.* **2006**, *2*, 75–91. [CrossRef]
13. Winterfeld, S. Chapter 4—Tools and Techniques. In *The Basics of Cyber Warfare*; Winterfeld, S., Ed.; Syngress: Rockland, MA, USA, 2013. [CrossRef]
14. Melendez, J.C.; Luse, A.; Townsend, A.M.; Mennecke, B. Convergence of Physical and Logical Security: A Pre-implementation Checklist. In Proceedings of the 3rd Annual Midwest Association for Information Systems Conference (MWAI 2008), Eau Claire, WI, USA, 23–24 May 2008; Paper 26. Available online: <https://aisel.aisnet.org/mwais2008/26> (accessed on 1 June 2021).
15. Pabian, A.; Pabian, B.; Reformat, B. E-Customer Security as a Social Value in the Sphere of Sustainability. *Sustainability* **2020**, *12*, 10590. [CrossRef]
16. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A.K.M.N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
17. Securing the Modern Economy: Transforming Cybersecurity through Sustainability. Available online: https://www.publicknowledge.org/assets/uploads/documents/Securing_the_Modern_Economy--Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_PK.pdf (accessed on 1 April 2021).
18. Security Shield: A Label to Support Sustainable Cybersecurity. Available online: <https://www.publicknowledge.org/documents/security-shield-a-label-to-support-sustainable-cybersecurity/> (accessed on 1 April 2021).
19. Vasiu, I.; Vasiu, L. Cybersecurity as an Essential Sustainable Economic Development Factor. *Eur. J. Sustain. Dev.* **2018**, *7*, 171–178. Available online: <https://ssrn.com/abstract=3262527> (accessed on 1 June 2021). [CrossRef]
20. Mithen, S. The Early Prehistory of Human Social Behaviour: Issues of Archaeological Inference and Cognitive Evolution. *Proc. Br. Academy* **1996**, *88*, 145–177. Available online: <http://publications.thebritishacademy.ac.uk/pubs/proc/files/88p145.pdf> (accessed on 1 June 2021).
21. Purpura, P.P. *Security and Loss Prevention: An Introduction*, 7th ed.; Butterworth-Heinemann: Boston, MA, USA, 2019. [CrossRef]
22. Digital 2021—Global Overview Report. Available online: <https://wearesocial.com/digital-2021> (accessed on 1 April 2021).
23. Data Never Sleeps 8.0. Available online: <https://www.domo.com/learn/data-never-sleeps-8> (accessed on 1 April 2021).
24. Financial Impact of Intellectual Property & Cyber Assets Report. Global Edition—2020. Available online: <https://www.aon.com/getmedia/6e200c08-c579-4333-b5f2-385ab6fbefde/Financial-Impact-of-Intellectual-Property-> (accessed on 1 April 2021).
25. Speed, T.J. *Asset Protection through Security Awareness*; Auerbach Publications: Boca Raton, CA, USA, 2019. [CrossRef]
26. Rohokale, V.M.; Prasad, R. Cyber Security for Intelligent World with Internet of Things and Machine to Machine Communication. *J. Cyber Secur.* **2015**, *4*, 23–40. [CrossRef]
27. Cyber Defense Guidelines for the Design, Planning, Implementation and Development of a Military Cyber Defense. 2020. Available online: https://www.iadfoundation.org/wp-content/uploads/2020/10/Cyber-defense_ing_v2.pdf (accessed on 1 April 2021).
28. National Institute of Standards and Technology. *NIST Special Publication 800-12—An Introduction to Information Security*; Revision 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
29. David, P.; Steinmueller, W. Economics of compatibility standards and competition in telecommunication networks. *Inf. Econ. Policy* **1994**, *6*, 217–241. [CrossRef]
30. Jones, R.V. *The Wizard War: British Scientific Intelligence, 1939–1945*; Echo Point Books & Media: Brattleboro, VT, USA, 2018. Available online: <https://www.echopointbooks.com/history/the-wizard-war> (accessed on 1 June 2021).

31. International Organization for Standardization. *ISO/IEC 27000:2018 Information Technology-Security Techniques-Information Security Management Systems-Overview and Vocabulary*; International Organization for Standardization: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/standard/73906.html> (accessed on 1 June 2021).
32. National Institute of Standards and Technology. NIST Special Publication 800-series General Information. 2021. Available online: <https://www.nist.gov/itl/nist-special-publication-800-series-general-information> (accessed on 1 April 2021).
33. National Institute of Standards and Technology. NIST Cyber Security Framework. Available online: <https://www.nist.gov/cyberframework> (accessed on 1 April 2021).
34. Department of Defense. Office of the Under Secretary of Defense for Acquisition and Sustainment. Cybersecurity Maturity Model Certification (CMMC) Framework. 2020. Available online: <https://www.acq.osd.mil/cmmc/> (accessed on 1 June 2021).
35. ISACA. *COBIT 2019 Framework: Introduction and Methodology*; ISACA: Schaumburg, IL, USA, 2018. Available online: https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fim (accessed on 1 June 2021).
36. Solms, S.H.; Solms, R. *Information Security Governance*; Springer: Boston, MA, USA, 2008. [CrossRef]
37. Framework for Improving Critical Infrastructure Cybersecurity Core. Available online: <https://www.nist.gov/document/framework-improving-critical-infrastructure-cybersecurity-corexlsx-1> (accessed on 1 April 2021).
38. National Institute of Standards and Technology. NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001. Available online: <https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx> (accessed on 1 April 2021).
39. International Organization for Standardization. 11 Physical and environmental security. In *ISO/IEC 27002:2013 Information Technology-Security Techniques-Code of Practice for Information Security Controls*; International Organization for Standardization: Geneva, Switzerland, 2013. Available online: <https://www.iso.org/standard/54533.html> (accessed on 1 June 2021).
40. Baillie, C.; Sennewald, C.A. *Effective Security Management*; Butterworth-Heinemann: Boston, MA, USA, 2016. [CrossRef]
41. American National Standards Institute; ASIS International. *ANSI/ASIS PAP.1-2012 Security Management Standard: Physical Asset Protection. Standards & Guidelines*; ASIS International: Alexandria, VA, USA, 2012. Available online: <https://webstore.ansi.org/Standards/ASIS/ANSIASISPA2012> (accessed on 1 June 2021).
42. ASIS International. *ASIS GDL FPSM-2009 Facilities Physical Security Measures Guideline*; ASIS International: Alexandria, VA, USA, 2019. Available online: <https://webstore.ansi.org/Standards/ASIS/ASISFPSMGDL2009> (accessed on 1 June 2021).
43. Clark, D.E.; McGibany, J.M.; Myers, A. The Effects of 9/11 on the Airline Travel Industry. In *The Impact of 9/11 on Business and Economics: The Business of Terror*; Morgan, M.J., Ed.; Palgrave Macmillan: New York, NY, USA, 2015; pp. 75–86. [CrossRef]
44. International Organization for Standardization. *ISO/IEC 27001:2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements*; International Organization for Standardization: Geneva, Switzerland, 2013. Available online: <https://www.iso.org/standard/54534.html> (accessed on 1 June 2021).
45. National Institute of Standards and Technology. NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations. 2020. Available online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> (accessed on 1 April 2021).
46. Rahman, S.M.; Donahue, S.E. Convergence of corporate and information security. *Int. J. Comput. Sci. Inf. Secur.* **2010**, *7*, 63–68. Available online: <https://arxiv.org/abs/1002.1950v1> (accessed on 1 June 2021).
47. Aleem, A.; Wakefield, A.; Button, M. Addressing the weakest link: Implementing converged security. *Secur. J.* **2013**, *26*, 236–248. [CrossRef]
48. World Economic Forum. The Global Risks Report 2021. Available online: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (accessed on 1 April 2021).
49. Andrew, C.; Jereys-Jones, R. *Eternal Vigilance? 50 years of the CIA (Studies in Intelligence)*; Routledge: London, UK, 2013. [CrossRef]
50. Allen, J.; Loyear, R. *Enterprise Security Risk Management: Concepts and Applications*; Rothstein Publishing: Brookfield, CT, USA, 2018. Available online: <https://www.rothstein.com/product/esrm/> (accessed on 1 June 2021).
51. Radanliev, P.; de Roure, D.; Walton, R.; van Kleek, M.; Montalvo, R.M.; Maddox, L.; Santos, O.; Burnap, P.; Anthi, E. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. *SN Appl. Sci.* **2020**, *2*, 1773. [CrossRef]
52. Radanliev, P.; De Roure, D.; Van Kleek, M.; Santos, O.; Ani, U.; Daniel, P. Artificial intelligence in cyber physical systems. *AI Soc.* **2020**. [CrossRef] [PubMed]
53. Esposito, C.; Moscato, V.; Sperli, G. Trustworthiness Assessment of Users in Social Reviewing Systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**. [CrossRef]
54. Han, Q.; Molinaro, C.; Picariello, A.; Sperli, G.; Subrahmanian, V.S.; Xiong, Y. Generating Fake Documents using Probabilistic Logic Graphs. *IEEE Trans. Dependable Secur. Comput.* **2021**. [CrossRef]
55. International Organization for Standardization. *ISO GUIDE 73:2009 Risk Management-Vocabulary*; International Organization for Standardization: Geneva, Switzerland, 2009. Available online: <https://www.iso.org/standard/44651.html> (accessed on 1 June 2021).
56. Gottschalk, P. *The Privatization of Fraud Investigation: Internal Investigations by Fraud Examiners*; Routledge: London, UK, 2019. [CrossRef]
57. Vision 2050: Time to Transform. Available online: <https://www.wbcsd.org/contentwbc/download/11765/177145/1> (accessed on 1 June 2021).
58. UN Sustainable Development Goal. Available online: <https://sdgs.un.org/goals> (accessed on 1 June 2021).

59. International Organization for Standardization. *ISO/IEC 27004:2016 Information Technology-Security Techniques-Information Security Management Systems-Monitoring, Measurement, Analysis and Evaluation*; International Organization for Standardization: Geneva, Switzerland, 2016. Available online: <https://www.iso.org/standard/64120.html> (accessed on 1 June 2021).
60. American National Standards Institute; ASIS International. *ANSI/ASIS PSC.1-2012 (R2017) Management System for Quality of Private Security Company Operations-Requirements with Guidance*; ASIS International: Alexandria, VA, USA, 2017. Available online: <https://webstore.ansi.org/Standards/ASIS/ANSIASISPSC2012R2017> (accessed on 1 June 2021).
61. Ministerio de Industria, Comercio y Turismo del Gobierno de España: Cifras PyME-Datos enero 2021. Available online: <http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-enero2021.pdf> (accessed on 1 April 2021).
62. International Organization for Standardization. *ISO 9001:2015 Quality Management Systems-Requirements*; International Organization for Standardization: Geneva, Switzerland, 2015. Available online: <https://www.iso.org/standard/62085.html> (accessed on 1 June 2021).
63. International Organization for Standardization. *ISO 14001:2015 Environmental Management Systems-Requirements with Guidance for Use*; International Organization for Standardization: Geneva, Switzerland, 2015. Available online: <https://www.iso.org/standard/60857.html> (accessed on 1 June 2021).
64. International Organization for Standardization. *ISO 45001:2018 Occupational Health and Safety Management Systems-Requirements with Guidance for Use*; International Organization for Standardization: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/standard/63787.html> (accessed on 1 June 2021).
65. UN Security Council Meets on Jerusalem but Holds off on Statement. Available online: <https://www.france24.com/en/live-news/20210510-un-security-council-meets-on-jerusalem-but-holds-off-on-statement> (accessed on 11 May 2021).
66. Many Dead After Shooting Spree, Explosion at School In Russia's Tatarstan. Available online: <https://www.rferl.org/a/kazan-school-shooting/31249135.html> (accessed on 11 May 2021).
67. Nigeria: Ten Worshippers Kidnapped in a Mosque in the Northwest. Available online: <https://www.africanews.com/2021/05/10/nigeria-ten-worshippers-kidnapped-in-a-mosque-in-the-northwest/> (accessed on 11 May 2021).
68. US Fuel Pipeline Hackers 'Didn't Mean to Create Problems'. Available online: <https://www.bbc.com/news/business-57050690> (accessed on 11 May 2021).
69. University Cancels Exams After Cyber-Attack. Available online: <https://www.infosecurity-magazine.com/news/university-cancels-exams-after/> (accessed on 11 May 2021).
70. The Most Significant Cyber Attacks from 2006–2020, by Country. Available online: <https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/> (accessed on 11 May 2021).