1290

UNIVERSIDADE Ð
COIMBRA

Pedro Miguel Osório Ferreira da Costa

IMPLEMENTING A FRAMEWORK FOR CONTINUOUS IMPROVEMENT IN CYBERSECURITY

Dissertation in the context of the Master in Informatics Security advised by Alberto Carnicero and Professor Marco Vieira, and presented to the Faculty of Sciences and Technology / Department of Informatics Engineering.

July 2022

1 2 9 0

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA
DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

Pedro Miguel Osório Ferreira da Costa

Implementing a Framework for Continuous Improvement in Cybersecurity

Dissertation in the context of the Master in Informatics Security advised by Alberto Carnicero and Professor Marco Vieira, and presented to the Faculty of Sciences and Technology / Department of Informatics Engineering.

July 2022

Acknowledgements

First of all, I would like to genuinely thank Alberto Caceres Carnicero for the trust given since the first day when I remotely knocked at his door with this challenge. Despite the distance between Portugal and Spain he was always available and receptive throughout this internship, to listen to me and give his best advice. His experience of more than thirty years in information systems has helped me to grow, both professionally and personally. *¡Muchas gracias!*

I would also like to thank Professor Marco Vieira for having accepted to be my advisor. Their vast experience in researching and developing secure systems gave me the necessary orientations to better organise my ideas. Placing each piece in its proper place, thus creating a conductive line that allowed this work, in my humble opinion, to be a success. Despite the distance, always available to guide me. I felt from our very first contact that he had full confidence in my work and with the objectives I had set myself.

Furthermore, I need to express my thanks to Professor Edmundo Monteiro and Professor Henrique Domingos for their comments during the intermediate defence in February 2022. I have taken them into consideration and I hope that this final report is more crystal clear.

I would like to thank Joana Ferreira for her unconditional support. Certainly, one of the most important pillars during all these months of internship. Always present, in the ups and downs, listening to my questions and doubts, such as: “Do you think I will achieve it?” where I always heard: “Of course you will! I am very proud of you”. Her belief in me has boosted my confidence, moving forward stronger and with motivation.

Last but not least, I need to mention my mother. She doesn’t understand what I am really doing in this world of cybersecurity and probably will never know. But one important thing I do know, is that she is genuinely proud of the person I have become and the achievements I have made during these 39 years of existence.

Abstract

Saint-Gobain is a French multinational company, founded in 1665, present in 75 countries with over 166,000 employees. It designs, produces and distributes materials and solutions that are fundamental to the well-being of each and every one of us. These solutions can be found in buildings, transports and many industrial applications.

As other large multinationals, such as Maersk or Merck, in 2017, Saint-Gobain, suffered a cyberattack due to the *NotPetya* ransomware, causing a significant disruption in the daily operations of its subsidiaries around the world. Since then and until the end of 2020, a strong and resilient cyber-defence plan has been followed with the main objective to better prepare the group's infrastructure for future cyberattacks. In 2021, after the last external audit, it was concluded by the auditors that the group has now a stable level of security. In many aspects, better prepared compared to similar companies. As a result, the group decided to move from a "Build" phase to a "Run" phase, following a set of controls inspired by the CIS Critical Controls version 8. This allowed the group to strengthen their security level and adapt their posture to evolving threats, materialised by the Cybersecurity Continuous Improvement Plan (CCIP).

In this internship we defined a strategy that allowed us to follow the CCIP and in parallel develop in-depth some of the objectives that this CCIP addresses. For this, we defined a main objective which is to implement a control framework for continuous improvement and two others that derive from the main one.

The main contributions towards these objectives were to familiarise with the subject and the state of the art regarding control frameworks, identifying the key requirements to undertake this internship and analysing the existing methodologies used by Saint-Gobain.

Implement and monitor the controls defined for our perimeter, analysing and remediating the gaps found, thus obtaining the evidence for each of these controls in order to verify their compliance with the policies defined by the group.

Follow a "*Security by Design*" methodology in all Information Technology and Operational Technology projects, identifying the main associated risks, as well as following the best practices from the very beginning of a project.

Develop and establish a Security Awareness Program that include all the relevant aspects that could help the reduction of unsecure behaviours by users with a special focus on phishing campaigns and user awareness sessions. Last but not least, a compilation of all the main recommendations and good practices learnt during this internship, which any small and medium company can follow.

Keywords

Cybersecurity, Security Controls, Security by Design, User Awareness, Risk Management

This page is intentionally left blank.

Resumo

A Saint-Gobain é uma empresa multinacional francesa, fundada em 1665, presente em 75 países com mais de 166.000 funcionários. Concebe, produz e distribui materiais e soluções que são fundamentais para o bem-estar de cada um de nós. Estas soluções podem ser encontradas em edifícios, transportes e muitas aplicações industriais.

Como outras grandes multinacionais, como a Maersk ou a Merck, em 2017, Saint-Gobain, sofreu um ataque cibernético devido ao ransomware NotPetya, causando uma perturbação significativa nas operações diárias das suas filiais em todo o mundo. Desde então e até ao final de 2020, foi seguido um plano de ciberdefesa forte e resistente com o objetivo principal de melhor preparar a infraestrutura do grupo para futuros ciberataques. Em 2021, após a última auditoria externa, os auditores concluíram que o grupo tem agora um nível de segurança estável. Em muitos aspetos, melhor preparado em comparação com empresas similares. Como resultado, o grupo decidiu passar de uma fase "*Build*" para uma fase "*Run*", seguindo um conjunto de controlos inspirados nos CIS Critical Security Controls na sua oitava versão. Isto permitiu ao grupo reforçar o seu nível de segurança e adaptar a sua postura à evolução das ameaças, materializada pelo Plano de Melhoria Contínua da Cibersegurança (CCIP).

Neste estágio definimos uma estratégia que nos permitiu seguir o CCIP e, paralelamente, desenvolver em profundidade alguns dos objetivos ele contempla. Para tal, definimos um objetivo principal que é o de implementar uma framework de controlos para a melhoria contínua e dois outros que derivam do principal.

As principais contribuições para estes objetivos consistiram na familiarização com o tema e o estado da arte no que diz respeito às frameworks de controlos, a identificação dos requisitos-chave para realizar este estágio e a análise das metodologias existentes utilizadas pela Saint-Gobain.

Implementar e monitorizar os controlos definidos para o nosso perímetro de atuação, analisando e remediando as lacunas encontradas, obtendo assim as evidências para cada um desses controlos a fim de verificar a sua conformidade com as políticas definidas pelo grupo.

Seguir uma metodologia de "Security by Design" em todos os projetos nas áreas das Tecnologias da Informação (IT) e Tecnologias Operacionais (OT), identificando os principais riscos associados, bem como seguir as melhores práticas desde a fase inicial de um projeto.

Desenvolver e estabelecer um Programa de Sensibilização para a Segurança que inclua todos os aspetos relevantes que possam ajudar a reduzir comportamentos inseguros por parte dos utilizadores, com especial ênfase em campanhas de *phishing* e sessões de sensibilização aos utilizadores. Por último, mas não menos importante, uma compilação de todas as principais recomendações e boas práticas aprendidas durante este estágio, que qualquer pequena e média empresa pode seguir.

Palavras-Chave

Cibersegurança, Controlos de segurança, Security by Design, Consciencialização dos utilizadores, Gestão de Risco

This page is intentionally left blank.

Contents

This page is intentionally left blank.

List of Abbreviations

2FA Two-factor authentication

AICT Availability, Integrity, Confidentiality and Traceability

ANSSI Agence Nationale de la Sécurité des Systèmes d'information

APT Advanced Persistent Threat

ATT&CK Adversarial Tactics, Techniques, and Common Knowledge

CAPEX Capital expenditures

CCTV Closed-circuit television

CCIP Cybersecurity Continuous Improvement Plan

CDP Cyber Defence Plan

CEO Chief Executive Officer

CIA Confidentiality Integrity Availability

CNCS Centro Nacional de Cibersegurança

CISA Cybersecurity and Infrastructure Security Agency

CIS Center for Internet Security

CISC CSC Center of Internet Security Critical Security Controls

CISO Chief Information Security Officer

COBIT Control Objectives for Information and Related Technologies

CMDB Configuration management database

CP Control Plan

CSF Cybersecurity Framework

CVE Common Vulnerabilities and Exposures

DAST Dynamic Application Security Testing

ENISA European Union Agency for Cybersecurity

GDPR General Data Protection Regulation

HIPPA Health Insurance Portability and Accountability

IaaS Infrastructure as a service

ICP Internal Control Plan

IG Implementation Groups

ISMS Information Security Management System

IEC International Electrotechnical Comission

IOA Indicators of Attack

ISO International Organization for Standardization

ISP Integration of Security into Projects

ITSM Information Technology Service Management

KPI Key Performance Indicator

MFA Multi-Factor Authentication

NDA Non-Disclosure Agreement

NIST National Institute of Standards and Technology

OS Operating System

OT Operational Technology

OWASP Open Web Application Security Project

PaaS Platform as a Service

PCI DSS Payment Card Industry Data Security Standard

PDCA Plan-Do-Check-Act

PII Personally identifiable information

PSAT Project Security Assessment Tool

PUM Potentially Unwanted Modifications

PUP Potentially Unwanted Programs

SaaS Software as a service

SAST Static application security testing

SG Saint-Gobain

SIEM Security information and event management

SIP Security Insurance Plan

SSO Single-Sign-On

TCP/UDP Transmission Control Protocol / User Datagram Protocol

VPN Virtual private network

WAS Web Application Scanner

This page is intentionally left blank.

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

Saint-Gobain (SG) is a worldwide leader in light and sustainable construction, that designs, manufactures and distributes materials and services for the construction and industrial markets. Like other large multinational companies, such as Maersk or Merck, in 2017, Saint-Gobain, suffered a cyber-attack related to *NotPetya* ransomware, causing a significant disruption in the daily operations of its subsidiaries around the world.

As we are facing with the Covid-19 pandemic, in the digital world, we are also finding that cyber threats are something that we will have to live with for a long time. As defenders, one of the main objective is to reduce the attack surface as much as possible. To achieve this objective, it's important to define and implement a set of actions that will reduce the likelihood of suffering pervasive and dangerous attacks [1]. There is a huge set of security requirements, regulatory mandates, risk management frameworks, compliance policies, and so forth; several recommendations and good practices shared by the community and experts. The open question is how to separate the wheat from the chaff.

The cyberattack that SG suffered in 2017, exploited, among others, the Server Message Block vulnerability [2], as well as a credential-stealing technique to spread and moving laterally, encrypting files and the computer's master boot record, rendering the machine unusable [3]. SG was one of those affected companies. In that year, they had decided starting a security program called: "Cyber Defence Plan" (CDP) to enhance the resilience based on the results of each annual external audits. Four audits had been carried out since 2017, achieving a significant cyber security improvement, leading to the company's decision in early 2021 to change the strategy. Therefore, it has been decided to replace the previous CDP by the Cybersecurity Continuous Improvement Plan (CCIP), highlighting the transition from a build phase to a run phase. The CCIP include the remaining actions of the last CDP as well as the new recommendations made by the external audit team, inspired by the CIS CSC version 8.

It is on the basis of the CCIP that this curricular internship will flow. It will address all the 18 CIS CSC and sub-controls which will have to be implemented and followed up during the first and second semester.

In parallel, all the new IT & OT projects will follow the principle of security by design on a basis of a specific methodology developed by SG, denominated Project Security Assessment Tool (PSAT). The PSAT document is both a methodological guide, a tracking tool and a deliverable to be completed as the project progresses. It gives the deliverables to be produced according to the nature of the project. Last but not least, during the internship, the implementation of a Security Awareness and Training Program will be carry out to ensure that all users understand and exhibit the necessary behaviours and skills to help ensure the security of the organization. All the recommendations and best practices learnt through this internship will also be compiled and included in this final report.

The defined objectives for this internship were achieved within a certain perimeter inside the SG group. Due to the fact that the group is present in more than 75 countries, they decided to organise the group's main activities in two different sectors, by four regions and by a specific market that are present in many of those countries.

The four consolidated **regions** are: Northern Europe, Southern Europe, Middle East, Africa (EMEA), Americas and Asia-Pacific. And **one global entity**: for High Performance Solutions (HPS) for leading-edge applications in global markets. For example, for automotive glass, civilian airborne satellite communications radomes, a range of textiles and coating technologies using fiberglass yarns, synthetic fibres, and natural fibres or even for single-use tubes for the pharmaceutical industry.

At a country level, this internship covers Spain, Portugal and Morocco and also the entities of HPS that are present in those countries. During this internship, the group decided to reorganize the structure for Digital & IT matters to improve support and align with the new digital trends, making the group more competitive. Thus, the organisational structure supporting Spain, Portugal and Morocco has been renamed to IT Services SPM (the abbreviations for these three countries).

Despite the organisation is subdivided into two different sectors, every entity is under the same umbrella. It means that everyone follows the same governance either in terms of strategy, global policies, technical norms, standards and guidelines. Everyone is rowing in the same direction and trying to keep up the same pace requested by the helmsman. Some of them not in the same maturity level, as each country have their own culture, their own rhythm, constraints and priorities. As we could better understand during this final report, we can confidently consider that our perimeter is one of those that has been reaching a high level of maturity, not only in terms of cybersecurity but also in other IT services (Governance, Infrastructures, Networking, User Support and related activities).

1.1 Cybersecurity Continuous Improvement Plan

The results of the last cybersecurity external audit in 2021 have shown a significant progress in all cybersecurity fields and faster than the average of the auditors' benchmark of similar companies, according to the auditing company. As mention before, with the success of the CDP, SG has now acquired the necessary cybersecurity foundations on which to build up future improvements. That is why it has been decided to move from a build to a run phase with the implementation of a continuous improvement plan which will be materialized by the CCIP replacing the CDP.

With the CCIP there is a need to focus on the three following priority topics:

- **Resilience**: hardening of servers, switches, firewalls, non-standard or obsolete assets, middleware, databases; implement and test the disaster recovery plan, conduct periodic crisis exercises; Implement standard solutions for storage and backups; Inventory of assets, segmentation of networks into bubbles with strict filtering;

- **Controls**: implementation of the 173 sub controls of which 95 apply to our perimeter; to find compliance gaps and continuous monitoring and remediation to prove the compliance on the next audit and of course to better secure the company;

- **Coordination of the cybersecurity community**: to ensure that everyone involved in the cybersecurity area follow harmonized guidelines, rules and frameworks established by the central team. Avoid the creation of silos inside the organization to let that business could implement their IT needs in an agile way, allowing that cybersecurity not to be seen as an inhibitor.

This will allow the company to strengthen the security level and adapt the posture to evolving threats. All the cybersecurity teams of the company are mobilized to implement these guidelines, in each of its spheres of action.

One of the main objective of this internship will orbit around the implementation and monitor of the priority topic: Controls. These controls are based, essentially, in the version 8 of the CIS CSC, that CIS launched on May 18, 2021, released at the global RSA Conference 2021.

1.2 Contributions

The main objective of this internship consists in the implementation of an Internal Control Plan, based on the CIS Critical Controls version 8. This is essential for any organisation by helping them to find compliance gaps, to put in place the necessary measures to remediate those observed gaps, monitoring them and prove compliance whenever needed. Control frameworks, such as CIS or ISO/IEC 27002, follows a recommended set of actions to improve an effective cyber defence posture. We decided to focus this internship in four different objectives. At the end, we should have been able to improve significantly our resilience within our perimeter allowing also that any organisation, whatever their size, can follow the same approach we followed.

The main contributions of this internship towards each objective, consist in the following actions which are linked with each other and that has inspired the title of the thesis:

- **A research and analysis of the different existing control frameworks** and understand what differentiates CIS CSC (that SG got inspired by) from the selected set of frameworks that have similarities: ISO 27001:2017, ISO/IEC 27002:2022, NIST Special Edition 800-52 revision 5 and NIST Cybersecurity Framework. Understand and highlight what can be learned from each one to improve or complement the actual control plan used by SG;

- **Collecting all the necessary information to implement the controls which apply to the scope of this internship**, find compliance gaps and remediate them, monitor and obtain appropriate evidences to prove compliance in case of audit. For each control there is an entire management to carry out through the use of specific tools that allows the monitoring of each one. Important to mention that this is the most important objective and the inspiration for the title of this master thesis. The below two objectives are included/mentioned in some of the controls;

- **Following the methodology of Integration of Security into Projects** defined by the group for all the projects concerned within this internship, identifying and managing the related risk, reducing the risk exposure. To accomplish this, the SG group created what they call Project Security Assessment Tool (PSAT) that is both a methodological guide, a tracking tool and a deliverable to be completed as the project progresses. It gives the deliverables to be produced according to the nature of the project. Either with direct links for each deliverable, either tab to use for deliverable integrated to the PSAT.

- **Develop and implementation of a Security Awareness Program** that will boost users' awareness, with training learning, cybersecurity awareness sessions, monthly newsletters, phishing campaigns, Intranet portal with awareness contents. Raise awareness for the risks that users are subject to, which could seriously compromise the company's entire information system. The creation and definition of this program, was carried out during the first semester, extended and improved during the second half.

At the beginning of this internship and after learning more about the methodology used by the SG group regarding the implementation of the internal control plan, we thought of a way to improve this methodology. A web based tool that could facilitate the way we can manage the internal control plan, inspired by the tool available on premise or in the Cloud, developed by CIS CSC. Actually, the group is working on to improve the way all of the Cyber Security Officers implement and monitor the controls. Their intention is to centrally manage the controls of each perimeter, instead of using local excel files that after will need to be integrated manually, developing a tool that will allow a better management.

At this moment, we have kept the same procedure for the implementation of controls, as will be better described in the respective chapter. The web-based platform will be for future work.

Important to note that the following three objectives:

- State-of-the-art of control frameworks
- Integration of Security into Projects
- Security Awareness Program

Revolve around the Internal Control Plan objective. That's why we selected the thesis title: "Implementing a Framework for Continuous Improvement in Cybersecurity". The implementation of a control framework, in our case, based on the CIS CSC in its eighth version, is a cornerstone for the development of a robust and resilient Information Security Management System. The internal control plan was designed and developed by the central team based on a risk assessment to define and better understand the nature of the risks that we could be exposed in our environment. It's a continuous process as new risks always arise.

1.3 Structure of the document

This document, in addition to chapter one, which presents the introduction, is structured with the following additional chapters:

Chapter 2 contains the state-of-the-art analysis of the different frameworks available with a special focus to the version 8 of the CIS CSC because is the foundation for the control plan implemented in SG. For each framework analysed, the main aspects of each one were described, so that, at the end it is possible to understand more clearly the difference between each one.

Chapter 3 describes the approach towards each objective. For each of them, the process followed to successfully achieve the proposed objectives. The risk analysis of this internship was also taken into consideration, as some objectives could be affected by some constraints and not be achieved. Also includes the planning followed during the first and second semester.

Chapter 4 contains all the information related to the Internal Control Plan, which is part of the global Cybersecurity Continuous Improvement Plan. As controls are fundamental to any company, whatever its size, it was decided to also include the experience obtained during this internship. Therefore, a set of recommendations are also included in this chapter which will certainly assist any organization in identifying threats as well as measures to be implemented to help reduce the impact of these threats.

Chapter 5 focus on the integration of security by design into projects. It means that, every project or minor change request with IT or OT involved will need to follow a methodology developed by SG. A selection of relevant projects opened during this internship will be presented in this chapter to better understand how we integrated the security into those projects. The principle is very simple, if we assess the risk at an early stage and consider the security by design on each project or major change request, the impact will be reduced in case of compromise.

Chapter 6 describes what has been done to develop and implement a Security Awareness Program with the goal to boost the user awareness for potential threats to our organisation and how be better prepared to avoid them. From sending newsletters, through awareness-raising sessions to regular phishing campaigns. As users are considered the weakest link from security stand point, this is probably one of the most important and challenging objective of this internship.

Finally, **chapter 7** addresses the final conclusions obtained from this interesting internship and the future work that will be continued. Securing information systems is a continuous process and we recognize that we cannot do everything during the time window of this internship. Therefore, for each objective, something will need to be improved or changed to better secure our Information Security Management System.

At the end of the report, in the appendix section, we can found more information related to the internal control plan, e.g. the list of controls implemented.

This page is intentionally left blank.

Chapter 2
Background and related work

Before diving into the subject of security controls and the methodology used by CIS CSC, it is absolutely important to understand the different existing alternatives as a way to also understand what may not be included in some and included in others. In fact, they all complement each other, although it is necessary to decide which to follow as a baseline, for this work, will be the CIS CSC. It was decided to explore during the 1st half of the internship the CIS itself and other methodologies; these being as follows:

- EN ISO/IEC 27001:2017: Information Security Management
- ISO/IEC 27002:2022: Information security controls
- NIST Special Publication 800-53 Revision 5
- NIST Cybersecurity Framework

Clearly, these methodologies are not exhaustive and enough to cover all needs, as no one size fits all. What is important to note is that there is not great deal of difference between these selected frameworks. For specific cases other than the SG case, which does not mean, however, that some controls cannot be useful for specific situations within SG, there are other different approaches more particular. One example is the Payment Card Industry Data Security Standard (PCI DSS) which applies to all entities involved in payment card processing that could be applied for some situations where SG has e-commerce platforms and need to process or transmit cardholder data [4]. Other example, is the SOC 2 Type 2 which help in define criteria for managing customer data based on five principles: availability, processing integrity, confidentiality and privacy.

During the intermediate defence of this internship, in February 2022, one interesting comment was raised by Professor Henrique Domingos: "Why have I not considered the ISO 27002, more precisely the last version of 2022"? One of the reasons explained was that when we started the analysis of the different frameworks and entering the ISO world, several doubts have arisen. The "ISO27k" suite is quite complex for those who are not familiar with ISO. Therefore, during the 2nd half of the internship, ISO 27002 version has been studied and what was found will be better explained in this chapter 2.

Nevertheless, we can anticipate that, clearly, version ISO 27002 have greater weight compared to ISO 27001 for this internship, as the internal control plan (ICP) orbit mainly around controls and ISO 27002 explains in more detail, each of the controls. On the other hand, without ISO 27001, more focused on management structure, ISO 27002 loses its strength if there is no support from the top management of the company. Getting the necessary top management commitment is not always straightforward, but due to the growing trend of cyberattacks, organisations are realising that cybersecurity is getting more visibility in their risk management strategy.

2.1 ISO 27001:2017

There is a very little difference between ISO 27001:2013 and 2017 standards except for a few minor cosmetic points and a small name change [6, 22]. In fact, ISO is already working on its new version ISO 27001:2022, but we decided to not include in this research, considering that, normally, the difference is mainly on the controls instead of the major changes on the core. What we should keep in mind is that this ISO version was developed to provide requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), which are a strategic decision for an organization [5].

Therefore, this standard can be used by all the stakeholders involved, to assess if the organization is well prepared to meet the established security requirements. This standard is designed to be implemented mainly for those organizations who want to get the ISO certification, nevertheless, it does not mean that the organization need to become certified if they follow and implement this standard. Honestly speaking, if the organization follows all the aspects defined in this standard, it is more than a reason for it to go ahead with the certification. Sometimes it is a requirement to provide services or sell products as it is a way to guarantee that the company that complies with the best practices in this field of information security.

After an analysis of this standard, I can conclude that this methodology should not be seen only as something to perform due to audits and corresponding certification but rather as a very useful process of identifying the main aspects to take into consideration to ensure a resilient ISMS.

The ISO 27001 defines a set of information security management requirements, which can be described in these seven sections, extracted from the standard [6]:

Context of organization

The organization shall understand the internal and external issues that are relevant to its purpose and could impact their objectives in terms of ISMS. Understand the needs and expectations of all the interested parties involved. Determine the scope by which the organization will have to deal with, thus defining the boundaries and applicability of its ISMS. Establish, maintain and continuously improve its ISMS in compliance with the requirements of this ISO 27001.

Leadership

This is a very important requirement, because without the support and commitment of the top management in the leadership and commitment to carry out this framework, the objectives of this standard would not be satisfactorily achieved. Not being exhaustive, at least the following important aspects should be taken into account:

- Information security policy and objectives are established and in line with the strategic direction of the organization;
- Integrate the ISMS requirements into the organization's processes;
- Resources needed for the ISMS are available;
- Promoting continual improvement.

The top management shall establish an information security policy that is appropriated to the purpose of the organization and be available to all the interested parties, hence they can find the information security objectives as a guideline to be followed.

Planning

When the organization is planning their ISMS, they need to take the necessary measures to address risks and opportunities to prevent, or reduce, undesired effects. Achieve continuous improvement to provide a resilient ISMS. While planning how to achieve the objectives defined by the leaders, the organization will have to determine:

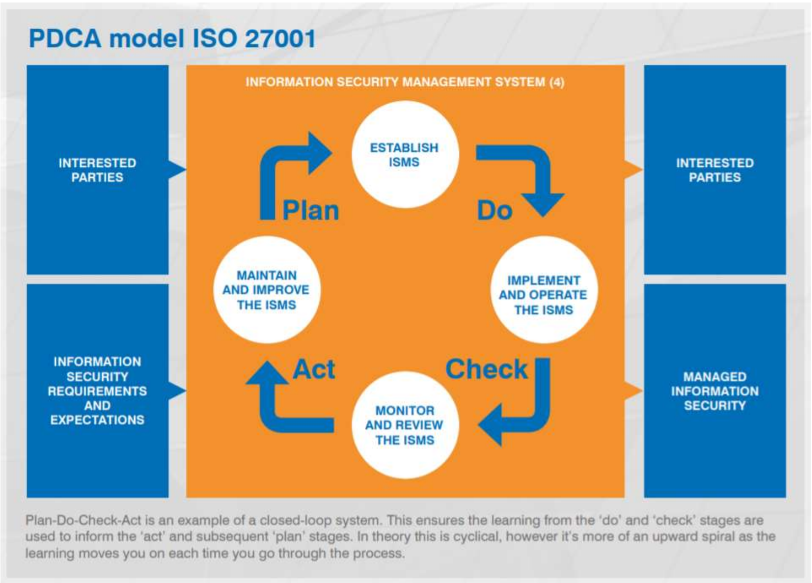
a) WHAT will be done?
b) WHAT resources will be required to accomplish those objectives?
c) WHO will be responsible for each one?
d) WHEN it will be completed?
e) HOW the results will be evaluated?

The ISO 27001 is based on the Plan-Do-Check-Act (PDCA) cycle, also well known as the Deming Wheel or Shewhart Cycle.

The plan-do-check-act cycle consists in [8]:

1. **Plan**: Recognize an opportunity and plan a change;
2. **Do**: Test the change. Carry out a small-scale study;
3. **Check**: Review the test, analyse the results, and identify what we have learned;
4. **Act**: Take action based on what we learned in the study step. If the change did not work, go through the cycle again with a different plan. If we were successful, incorporate what we learned from the test into wider changes. Use what we learned to plan new improvements, beginning the cycle again.

The following figure shows the PDCA model in the ISO 27001:


PDCA model ISO 27001
INFORMATION SECURITY MANAGEMENT SYSTEM (4)
INTERESTED PARTIES
INFORMATION SECURITY REQUIREMENTS AND EXPECTATIONS
ESTABLISH ISMS
Plan
Do
MAINTAIN AND IMPROVE THE ISMS
IMPLEMENT AND OPERATE THE ISMS
Act
Check
MONITOR AND REVIEW THE ISMS
INTERESTED PARTIES
MANAGED INFORMATION SECURITY

Plan-Do-Check-Act is an example of a closed-loop system. This ensures the learning from the 'do' and 'check' stages are used to inform the 'act' and subsequent 'plan' stages. In theory this is cyclical, however it's more of an upward spiral as the learning moves you on each time you go through the process.

Figure 1.1: PCDA model ISO 27001 (from [8]).

Support

To carry out this standard, the organization need to identify and provide the necessary resources to establish, implement, maintain and continuously improve its ISMS.

The following aspects should be taken into consideration [5]:

- **Competence**: Determine the necessary competence of person(s) that will be involved in the ISMS performance, promoting the necessary training;

- **Awareness**: All the persons who contribute to the implementation of this standard, shall be familiar with the security policies defined by the organization;

- **Communication**: The communication relevant to the ISMS, whether internal or external, shall be well defined (what, when, whom, who);

- **Documented information**: Depending of the complexity of the organization, the lifecycle of the documentation generated shall be well managed to ensure proper integrity and availability;

Operation

At the operational level, the organization should take into consideration at least these three aspects [5]:

- **Operational planning and control**: To plan, implement and control the processes to meet the information security requirements and implement the necessary actions defined in the planning phase. All change management shall be taken into account;

- **Information security risk assessment**: In a regular basis or when significant changes occur, the organization shall perform information security risk assessments;

- **Information security treatment**: Implement an action plan for the treatment of the risks identified, prioritizing those who could affect critical/sensitive assets.

Performance Evaluation

The organization shall evaluate the information security performance and the effectiveness of the ISMS, therefore, the following three aspects shall be taken into consideration [5]:

- **Monitoring, measurement, analysis and evaluation**: Define what needs to be monitored and measured, the methodology to monitor, measure, analyse and evaluate, for instance, processes and controls;

- **Internal audit**: In a regular basis, internal audits shall be conducted to understand if the objectives are correctly followed, performing the gap analysis to improve the ISMS. Is important to document and inform the relevant management;

- **Management review**: Top management shall review the organization's ISMS in a regular basis to ensure its continuing suitability, adequacy and effectiveness.

Improvement

Last but not least, this is also a relevant aspect in the lifecycle of this standard. This standard is not a black box and much less a one size fits all, therefore, there is always room for continuous improvement of processes and controls. Important to find the non-conformity to put in place the necessary corrective actions that shall be appropriate to mitigate them.

Annex A – 14 controls

The controls defined in the annex A of the ISO 27001:2017 help the organizations in the identification of security risks and in the selection of the appropriate controls to tackle them. There are 114 controls divided into the following 14 categories [5]:

Control	Category	Description
A.5	Information Security Policies	How the policies are written and reviewed
A.6	Organization of Information Security	How the responsibilities are assigned
A.7	Human Resources Security	Controls prior to employment, during, and after the employment
A.8	Asset Management	Controls related to inventory of assets and acceptable use; also for information classification and media handling
A.9	Access Control	Management of access rights of users, systems and applications, and for the management of user responsibilities
A.10	Cryptography	Related to encryption and key management
A.11	Physical and Environment Security	Defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.
A.12	Operations Security	To ensure correct and secure operations of information processing facilities, such as: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc
A.13	Communications Security	To ensure the protection of information in networks and its supporting information processing facilities
A.14	System Acquisition and Maintenance	Definition of security requirements, and security in development and support processes
A.15	Supplier Relationships	To ensure protection of the organization's assets that is accessible by suppliers
A.16	Information Security Incident Management	Reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

A.17	Business Continuity Management	Planning of business continuity, procedures, verification and reviewing, and IT redundancy
A.18	Compliance	Identification of applicable laws and regulations, intellectual property protection, personal data protection (very important, mainly in EU with the GDPR), and reviews of information security

Table 1: ISO 27001:2017 - Control categories (from [6])

It is not the aim to describe, in detail, each of them in this report, but it is relevant to mention that all of these domains and corresponding controls are correlated, in general, with what will be developed in this internship on the basis of the CIS CSC.

According to the ISO 27001:2017 standard, it's not mandatory for the organizations to implement all the 114 controls. In fact, they are a simple list of possibilities that shall be considered based on the requirements defined. All of these controls shall be used while conducting a gap analysis and risk assessment [7]. While this standard is a highly respected framework in the field of controls, its adoption has been quite modest, justified by the fact that the documentation costs approx. 200 EUR. Unlike other control frameworks, mentioned in this state-of-the-art analysis, which are free of charge. It could be irrelevant for a company, but expensive for students or other professionals. The justification for being a company certified with ISO 27001 is more than enough to justify the initial cost of documentation, for sure.

2.2 ISO 27002:2022

The ISO 27002 standard is directly related to the ISO 27001, is a companion standard. Essentially, ISO 27002 includes additional information related to the implementation guidance for each of the controls listed before This standard help us to better understand the goal of each control, as well as indications on how they can be implemented. This standard does not have its own certification criteria [31], as in the case of the ISO 27001.

The key differences between ISO 27001 and ISO 27002 are essentially three, including the following:

- **Detail**: ISO 27001 is not so detailed when compared to ISO 27002 regarding controls and guidelines. To go more in depth with ISMS's components is necessary to go with other ISO standards, such as ISO 27002 or ISO 27003 for ISMS implementation advice and with ISO 27004 if we want to go with more in depth regarding evaluation monitoring and measurement
- **Certification**: To be certified, we should go with the ISO 27001 as this standard provides complete criteria list that allows the alignment with a compliance state. In the case of ISO 27002, it only addresses one piece of an ISMS
- **Applicability**: The ISO 27002 standard does not specific which controls we should apply to our organisation as ISO 27001 do.

In sum, the ISO 27002 provides the necessary details needed to implement the controls mentioned in the Annex A of ISO 27001. The management framework provided by ISO

27001 and with the support of the organisation's top management, is essential to allow the successful implementation of those controls.

In terms of controls, the difference between the latest version ISO/IEC 27002:2022 and the previous ISO/IEC 27002:2013, is the introduction of 11 new controls, grouped into the following security categories or themes [33]:

Organisational Controls

- Threat Intelligence: Is a process that allows the gathering of information about actual and potential future cyberattacks, by analysing and contextualising them. Is very useful to better prepare the organisations with deeper knowledge of threats.
- Information Security for use of cloud services: With the trend to use more and more cloud services, is important to implement the necessary controls to better secure the use of cloud services.
- Information and Communication Technology readiness for business continuity: *"outlines how ICT services interact with various key metrics and supporting controls, including an organisation's recovery time objective (RTO) and the overall business impact analysis (BIA) [33]"*

Physical Controls

- Physical Security Monitoring: Essential for the detection and prevention of internal and external intruders who try to get access to restricted physical areas without the necessary permission. Detain surveillance tools are important.

Technological Controls

- Configuration Management: Establish the necessary governance policies for a better management of configurations of systems.
- Information Deletion: *"is a preventative control that modifies risk by outlining an approach to data deletion that complements an organisation's existing data retention policies, and keeps them compliant with any prevailing laws or regulatory guidelines [33]".*
- Data Masking: Use of techniques (e.g. Data Privacy Models) to protect sensitive data, such as Personally Identifiable Information (PII).
- Data Leakage Prevention: Preventive and detective control that automatically detect and prevent the disclosure of information without authorization.
- Monitoring Activities: Detective and corrective control by improving monitoring activities to identify abnormal behaviours.
- Web Filtering: Reduce the risk of suffering malware infections while accessing to external websites with malicious content.
- Secure Coding: Improve the software development by following best practices during the software development lifecycle.

The following table shows the total number of controls present in this ISO/IEC 27002:2022 standard [32], grouped by 4 security categories or themes instead of 14 control domains in the previous version as we can see in the section 2.1 (control domains from A.5 to A.18), where the highlighted ones are new:

Organizational controls
5.1 Policies for information security
5.2 Information security roles and responsibilities
5.3 Segregation of duties
5.4 Management responsibilities
5.5 Contact with authorities
5.6 Contact with special interest groups
5.7 Threat intelligence
5.8 Information security in project management
5.9 Inventory of information and other associated assets
5.10 Acceptable use of information and other associated assets
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the ICT supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services
5.24 Information security incident management planning and preparation
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during disruption
5.30 ICT readiness for business continuity
5.31 Legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights
5.33 Protection of records
5.34 Privacy and protection of PII
5.35 Independent review of information security
5.36 Compliance with policies, rules and standards for information security
5.37 Documented operating procedures
People controls
6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Remote working
6.8 Information security event reporting
Physical controls
7.1 Physical security perimeters

7.2 Physical entry
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring
7.5 Protecting against physical and environmental threats
7.6 Working in secure areas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media
7.11 Supporting utilities
7.12 Cabling security
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment
Technological controls
8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering
8.24 Use of cryptography
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.28 Secure coding
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit testing

Table 2: ISO/IEC 27002:2022 controls (from [32])

2.3 NIST Special Publication 800-53 Revision 5

The NIST Special Publication (SP) 800-53 in its fifth revision have the same principle described in the ISO 27001:2017 – the need to protect the information system of a given organization. Again, the security controls are the safeguards employed to protect Confidentiality, Integrity and Availability, also known as the CIA triad, within an organization. According to the NIST SP 800-53, the controls can be implemented within any organization or system that processes, stores, or transmits information [9].

The chapter three of the NIST SP 800-53, provides twenty controls and multiple sub-controls, focusing on the fundamental measures necessary to protect information and the privacy of individuals across the information life cycle [9], being them:

ID	Control Name	Examples of controls
AC	Access Control	Account management and monitoring, least privilege, separation of duties
AT	Awareness and Training	User training on security threats, technical training for privileged users
AU	Audit and Accountability	Content of audit records, analysis and reporting, record retention
CA	Assessment, Authorization and Monitoring	Connections to public networks and external systems, penetration testing
CM	Configuration Management	Configuration change control, authorized software policies
CP	Contingency Planning	Business continuity strategies, testing, alternate processing and storage sites
IA	Identification and Authentication	Authentication policies for users, devices and services, credential management
IR	Incident Response	Incident response training, monitoring and reporting
MA	Maintenance	System, personnel and tool maintenance
MP	Media Protection	Access, storage, transport, sanitization, and use of media
PE	Physical and Environment Protection	Physical access, emergency power, fire protection and temperature control
PL	Planning	Policy and procedures, system security and privacy plans, central management
PM	Program Management	Risk management strategy, insider threat program, enterprise architecture
PS	Personnel Security	Personnel screening, termination and transfer, external personnel, sanctions
PT	Personally Identifiable Information Processing and Transparency	Authority to Process Personally Identifiable Information
RA	Risk Assessment	Risk assessment; vulnerability scanning, privacy impact assessment
SA	System and Services Acquisition	Risk assessment; vulnerability scanning, privacy impact assessment
SC	System and Communications Protection	Application partitioning, boundary protection, cryptographic key management
SI	System and Information Integrity	Flaw remediation, system monitoring and alerting
SR	Supply Chain Risk Management	Acquisitions and divestiture strategy, supply chain risk management plan

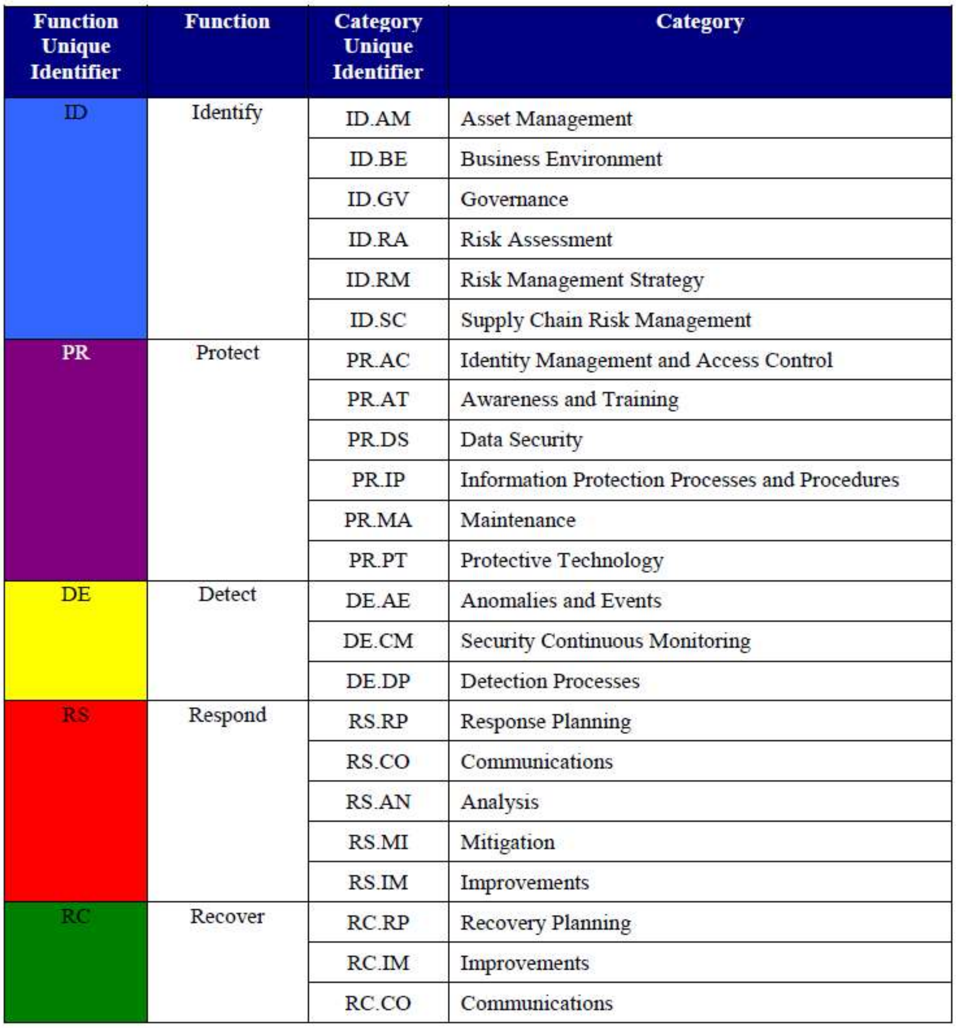
Table 3: NIST SP 800-53 Rev.5 - Control families (from [9])

Although this framework applies only to federal agencies and their information systems in the United States, it has been used and adopted by a range of organisations apart of the federal government. As a regulatory guideline, improves the link between the cybersecurity teams and organisational objectives.

2.4 NIST Cybersecurity Framework

The National Institute of Standards and Technology in response to the Executive Order 13636 [13], created the Cybersecurity Framework with the aim to improve the security of the United States of America critical infrastructures from cyber-attacks. While created to protect “critical infrastructures”, the framework can be used by every organization that would like to improve their cybersecurity posture. Is a risk-based approach for the management of cybersecurity risks and is composed of three parts [11]:

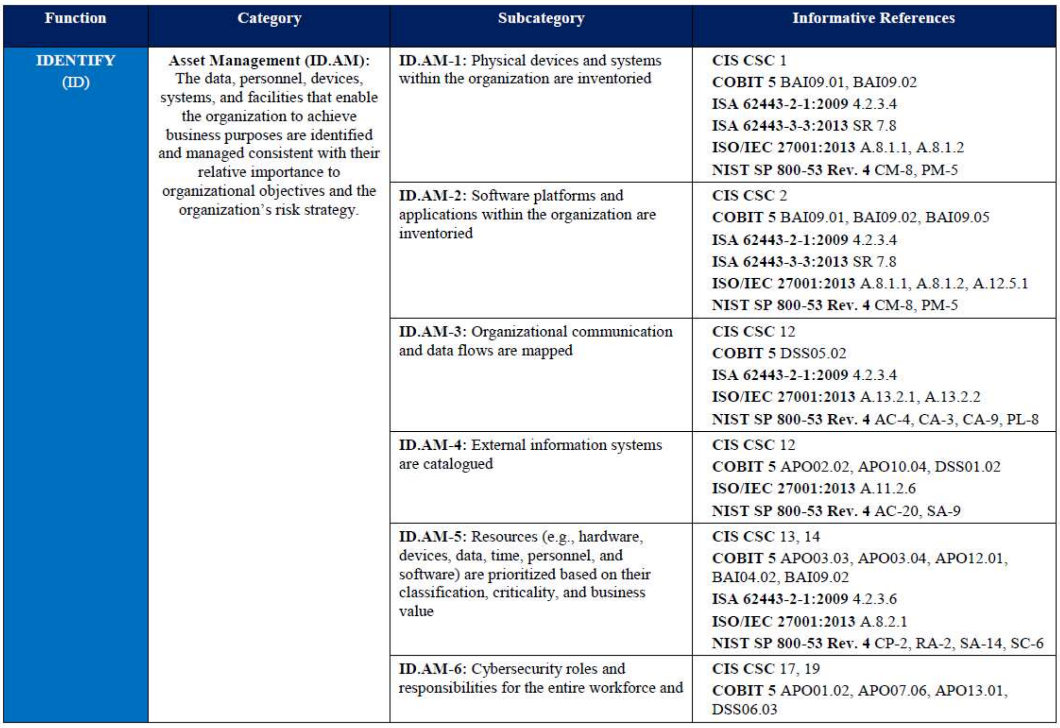
1. **Framework Core**: is a set of cybersecurity activities, targeted outcomes, and applicable references that are in general common across these critical sectors. It presents industry standards, guidelines and best practices that allows the communication of cybersecurity activities across the organizations from the executive level to the implementation/operations level. As stated by NIST, the core consists of concurrent and continuous functions:



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 4: NIST Cybersecurity Framework Core Outcome (from [13])

According to NIST, when considered together, these functions provide a high-level and strategic view of the lifecycle of an organization's management of cybersecurity risk. For each one, there is a set of categories, subcategories and informative references. As an example, for the Identify function, the first category is the Asset Management, with their corresponding subcategories and informative references:

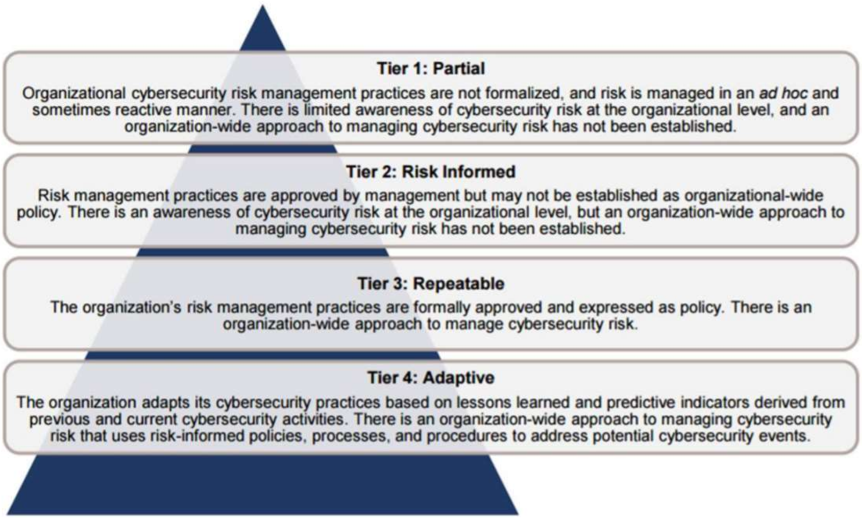


Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Table 5: NIST Cybersecurity Framework Core – Identify example (from [13])

It's very similar with the controls present in the annex A of the ISO 27001 and with CIS CSC in the sense that, it follows the principle of covering each category through controls. In the case of this framework, it's not so exhaustive such as the ISO and the CIS, because it only gives the references to be used as a guideline. If we look for the example of the ID.AM-1 it's the same of control 1 in the CIS and ISO.

2. **Framework Implementation Tiers**: provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. There are four different tiers:



Tier 1: Partial

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk Informed

Risk management practices are approved by management but may not be established as organizational-wide policy. There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.

Tier 3: Repeatable

The organization's risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.

Tier 4: Adaptive

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

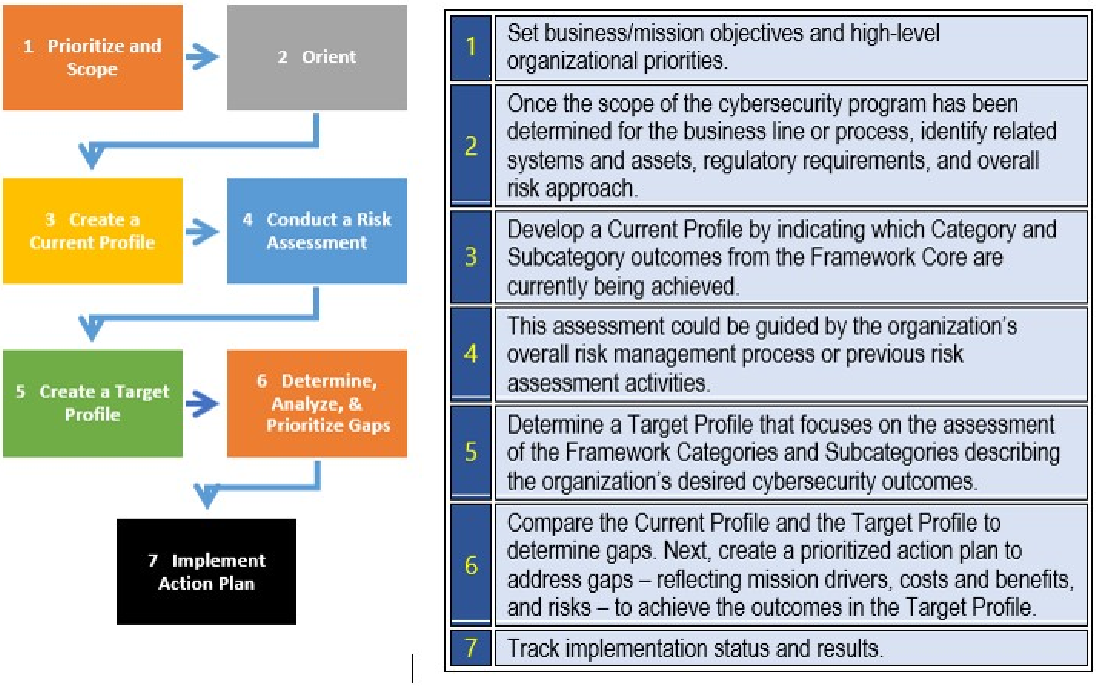
Figure 2.1: NIST CSF - Tiers (source: ESS Implementation Guide, 2015).

As stated by NIST, the tiers: "*help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices*" [13]. They are not meant to be seen as a maturity model. Instead, we should look at tiers as benchmarking tools that will give clear directions to improve the cybersecurity level of any organization that follows this approach.

3. **Framework Profile**: "*represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. A profile enables organizations to establish a roadmap for reducing the cybersecurity risks that they face, aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities*". It allows the definition and comparison of "current" profile with "target" profile, identifying opportunities for improving cybersecurity posture, thus revealing gaps to be addressed to achieve cybersecurity risk management objectives.

It's important to note that this framework is voluntary and so there is no "right" or "wrong" in its implementation. The subcategories and the priority for each one will help in the creation of a prioritized implementation plan, by analysing the gaps, defining the budget necessary to carry out the plan that could have different implementations over the years (high priority with small gaps could be implemented after the high priority with large gaps).

With the understanding of the core, the tiers and the profiles, organisations could use the following steps to establish or improve their cybersecurity program:


1 Prioritize and Scope
2 Orient
3 Create a Current Profile
4 Conduct a Risk Assessment
5 Create a Target Profile
6 Determine, Analyze, & Prioritize Gaps
7 Implement Action Plan

1	Set business/mission objectives and high-level organizational priorities.
2	Once the scope of the cybersecurity program has been determined for the business line or process, identify related systems and assets, regulatory requirements, and overall risk approach.
3	Develop a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.
4	This assessment could be guided by the organization's overall risk management process or previous risk assessment activities.
5	Determine a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.
6	Compare the Current Profile and the Target Profile to determine gaps. Next, create a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile.
7	Track implementation status and results.

Figure 3.1: NIST Cybersecurity Framework – the 7 steps (from [14]).

The NIST Cybersecurity Framework is designed to be easily personalized, suitable for organizations of any size and industry. It documents the organization functions and processes by allowing that security disciplines are formalized, sustainable, and scalable. In terms of security controls and their importance in this internship, this framework is very useful as for each control there are a set informative references from others frameworks.

2.5 CIS Critical Security Controls

CIS Critical Security Controls, developed by the Center for Internet Security® (CIS), are a set of prioritized of best practices to defend against the most pervasive and harmful attacks to the information systems. Currently led by the CIS, these critical controls have become an international community of volunteers (Individuals and Institutions).

According to CIS [1], this translates into:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Create and share tools, working aids, and stories of adoption and problem-solving;
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them;
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community.

It is relevant to mention that all this set of good practices and guidelines, reflect the combined expertise from a wide range of experts. Public, private sectors and individuals, with different roles, from threat responders and analysts, passing through policy-makers and auditors, and across many sectors (government, power, defence, finance, transportation, academia, consulting, security, IT, etc.), who came together to create, adopt, and support the CIS CSC.

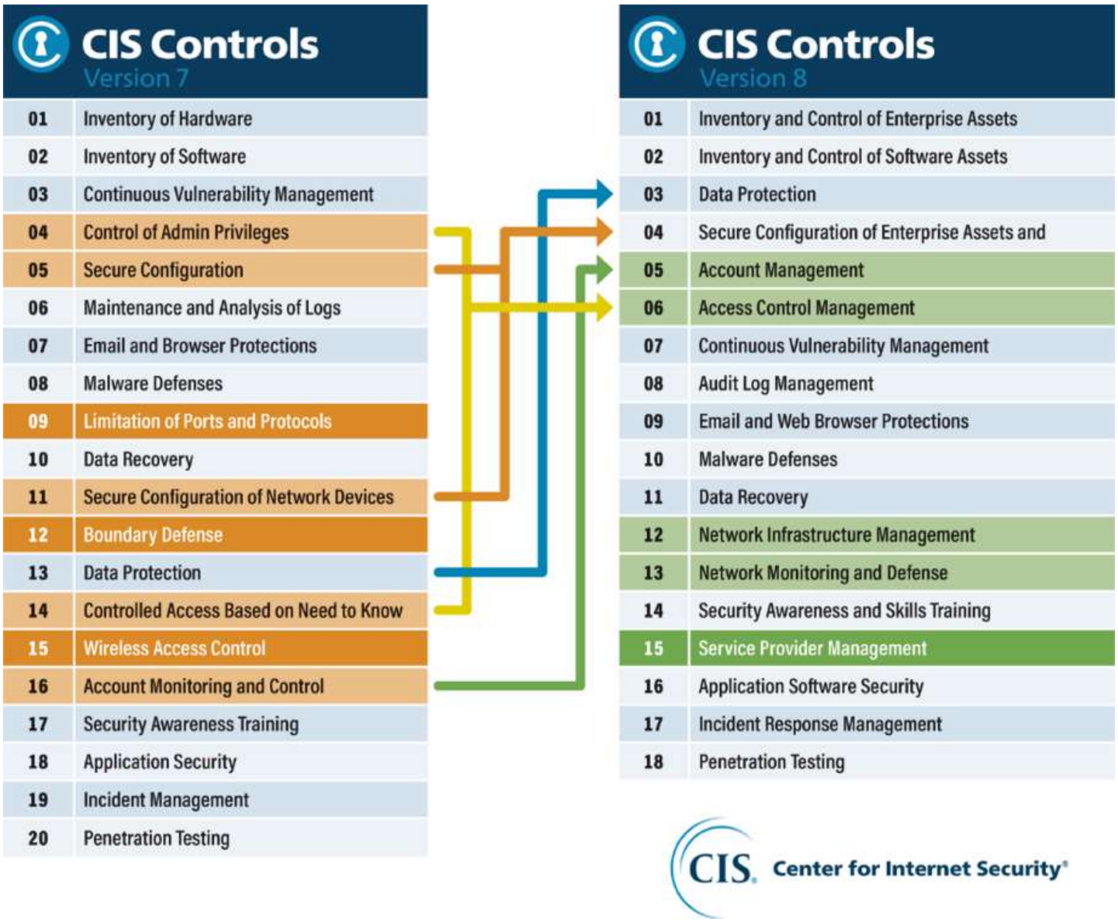
Indeed, we can conclude that CIS CSC is not a replacement for any other framework or regulation. In fact, it’s available on the official webpage of CIS a mapping between CISC CSC and other frameworks. Some of the controls includes also a reference to other guidelines, mainly from NIST and others from OWASP, PCI Security Standards Council, SANS and even from other guidelines of CIS itself.

2.5.1 The version 8 of CIS Critical Controls

With the dynamism that exists in information technology and cybersecurity ecosystem, CIS decided to create a new version 8 to improve the old version 7.1 of the critical controls. There is a growing trend to migrate from the typical on premise environment to cloud-based computing, elastic virtualization, mobility and outsourcing, work-from-home, and of course, the constant evolution of the tactics used by the attackers to deceive security measures. The result is a decrease in controls and safeguards to 18 controls instead of 20, these made up of 153 safeguards, down from 171 previously.

According to CIS, those 18 controls highly contribute to reduce the risk exposure or even stop the majority of the attacks well known nowadays.

The next figure shows the changes that have occurred between versions:



CIS Controls Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Figure 4.1: CIS Critical Controls - changes between v7.1 and v8 (from [10]).

2.5.2 CIS Controls Implementation Groups

Starting with version 7.1, CIS created the Implementation Groups (IGs) as a guidance to prioritize the implementation of these controls. The IGs are self-assessed categories for enterprises which identifies a subset of the CIS Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement [1]. There are 3 IGs:

- **IG1**: It's the entry point. From small to medium-sized enterprise with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The main objective of these enterprises is to keep the business operational and without sensitive data to be protected. The "mandatory" controls present in IG1 are considered as basic cyber hygiene.

- **IG2 (includes IG1)**: For enterprises that support multiple departments with differing risk profiles based on job function and mission. They often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

- **IG3 (includes IG1 and IG2)**: Enterprise with assets and data that contain sensitive information or functions that are subject to regulatory and compliance oversight. An enterprise that belong to this group must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Controls designed to protect against sophisticated adversary, such as advanced persistent threat (APT), a stealthy threat actor, typically a nation state or state-sponsored group.

To better understand the universe of controls and their applicability, the following table shows the breakdown of controls by IGs to understand how many controls are applicable for each group.

#	***Controls***	***Total Safeguards***	***IG1***	***IG2***	***IG3***
01	Inventory and Control of Enterprise Assets	5	2	4	5
02	Inventory and Control of Software Assets	7	3	6	7
03	Data Protection	14	6	12	14
04	Secure config. of Enterprise Assets & Software	12	7	11	12
05	Account Management	6	4	6	6
06	Access Control Management	8	5	7	8
07	Continuous Vulnerability Management	7	4	7	7
08	Audit Log Management	12	3	11	12
09	Email and Web Browser Protections	7	2	6	7
10	Malware Defences	7	3	7	7
11	Data Recovery	5	4	5	5
12	Network Infrastructure Management	8	1	7	8
13	Network Monitoring and Defence	11	0	6	11
14	Security Awareness and Skills Training	9	8	9	9
15	Service Provider Management	7	1	4	7
16	Application Software Security	14	0	11	14
17	Incident Response Management	9	3	8	9
18	Penetration Testing	5	0	3	5
	Total	153	56	130 (+74)	153 (+23)

Table 6: CIS Critical Controls and Implementation Groups

For each safeguard, CIS use the same principle of the NIST Cybersecurity Framework to define the security function: Identify, Protect, Detect, Respond and Recover.

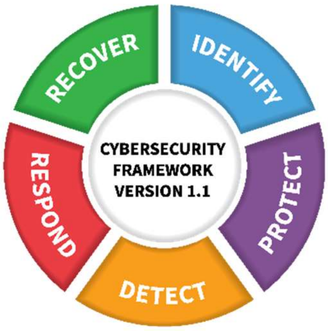
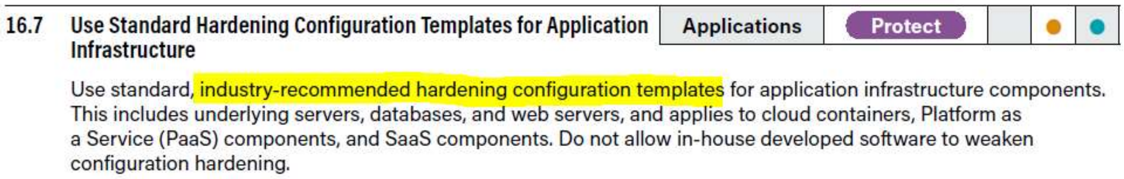


Figure 5.1 - NIST Cybersecurity Framework - Security Functions (from [11]).

The CIS CSC also has cross-compatibility and direct mapping to major compliance frameworks and standards, many of which are industry specific, as mentioned before, with NIST 800-53, ISO 27001, NIST Cybersecurity Framework, among others, and regulations such as PCI DSS and also the GDPR. This means that organisations that must follow these regulations can use CIS Controls as a compliance aid. To help this relationship between CIS CSC and the different frameworks, CIS provides a mapping for each of the controls.

Also important to mention that CIS developed the CIS Benchmarks. Consisting of configuration baselines and best practices for hardening specific operating systems, middleware, software applications, and network devices [12]. We can found on their website more than 100 configuration guidelines across 25+ vendor product families, from Operating Systems, Server Software, passing through Cloud Providers until Multi-Function Printers. Nevertheless, is not an exhaustive and complete list of hardening guides, therefore, we should also look for other sources, such as other communities and even from official materials from different vendors.

Each of the guidance recommendations are also referred in the CIS CSC. For example, in control 16 (Application Software Security) the safeguard 16.7 refers to:



16.7	**Use Standard Hardening Configuration Templates for Application Infrastructure**	Applications	Protect		●	●

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Figure 6.1 - Safeguard 16.7 from Control 16 – hardening configuration (from [1]).

This safeguard belongs to the security function “Protect” and applies to IG2 and IG3 but not for IG1.

As mentioned in the introduction, the CCIP developed by SG is inspired by this recommended set of actions from the CIS CSC version 8, adapted with more safeguards as no one size fits all. The safeguards introduced by SG will be better explained in the chapter 4 with all the step by step followed during this internship.

2.5.3 CIS CSC mapping

The characteristics of each selected control framework was described in this chapter 2, nevertheless, in this section, the aim is to compare some of the controls defined in the CIS CSC with NIST Cybersecurity Framework (CSF), ISO 27001:2018 and NIST Special Publication 800-53 revision 5.

Some examples, that should not be considered as an exhaustive analysis, for the mapping between CIS CSC version 8 and the researched control frameworks:

CIS CSC v8 and CSF	
CIS Sub-Control	CSF subcategory
1.1 Establish and Maintain Detailed Asset Inventory	ID.AM-1: Physical devices and systems within the organization are inventoried
2.1 Establish and Maintain a Software Inventory	ID.AM-2: Software platforms and applications within the organization are inventoried
2.3 Address Unauthorized Software	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

Table 7: CIS mapping with NIST Cybersecurity Framework

CIS CSC v8 and ISO 27001:2018	
CIS Sub-Control	ISO 27001 Controls
14.1 Establish and Maintain a Security Awareness Program	A.7.2.2: Information security awareness, education and training
6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems	A.8.1.1: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained
5.2 Use Unique Passwords	A.9.4.3: Password management systems shall be interactive and shall ensure quality passwords

Table 8: CIS mapping with ISO 27001

CIS CSC v8 and NIST SP 800-53 Revision 5	
CIS Sub-Control	ISO Control
2.1 Establish and Maintain a Software Inventory	CM-8: Reviews and updates the information system component inventory CM-11: Establishes governing the installation of software by users & Enforces software installation policies through
2.3 Address Unauthorized Software	DE-CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
11.2 Perform Automated Backups	CP-9: Conducts backups of user-level information contained in the information system & Conducts backups of system-level information contained in the information system

Table 9: CIS mapping with NIST SP 800-53 Revision 5

As we can see, there are many similarities between these frameworks, some have more, others have less or different controls. CIS has a very interesting tool, the CIS Critical Security Controls Navigator [16] to see how CIS controls is mapped to other security standards. In terms of controls, we could say that sky is the limit. For example, the specific third control of CIS, related to Data Protection, in its sub-control 3.10 (not necessary to implement on Implementation Group 1), which consists of: "*Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security and OpenSSH" [10]*, have quite a lot of mappings with other frameworks [23], such as:

Frameworks / Standards	Controls
CSA Cloud Controls Matrix v4 Groups	CEK-03 and IVS-03
CMMC Groups	SC.3.185 and SC.3.190
ISACA COBIT 19 Groups	DSS05
MITRE Enterprise ATT&CK v8.2 Groups	T1020.001, T1602, T1602.001, …
NIST CSF Groups	PR.DS-2
NIST SP 800-171 Groups	3.1.13, 3.5.10 and 3.13.8
PCI v3.2.1 Groups	2.1.1, 4.1, 4.1.1 and 8.2.1

Table 10: Data Protection – Examples of Frameworks and Controls

As stated in [15], we are in the era of multi-framework where organizations small and large, public and private, need to be compliant with a multiplicity of cybersecurity policies, regulatory and legal frameworks. Each organisation will need to implement and follow the framework/guideline adapted to their needs. If there is no specific obligation to use a specific framework, from this research we conclude that CIS Critical Controls in its version 8 is the most suitable. Of course that, no one size fits all, therefore, each case is unique.

The analysis of these different frameworks allows us to better understand each of the controls defined in the Internal Control Plan developed by Saint-Gobain and correlate them to the different frameworks available, as some of them could have more details. During the second semester is not expected to continue the research, nevertheless, these frameworks will be consulted as a reference for the implementation of the control plan.

Chapter 3
Approach towards each objective

This chapter details the approach followed to achieve each of the following objectives during this internship:

1. State-of-the-art research on a set of frameworks mainly focused on security controls;
2. Internal Control Plan: implement, monitor and improve the security controls;
3. Integration of Security into Projects following the principle of security by design;
4. Develop and implement a Security Awareness Program.

3.1 Approach

In the chapter 1, a set of objectives was defined for this internship. The approach to accomplish all of them, are based on the following steps, with a brief contextualization in each of them:

3.1.1 Control frameworks analysis

Research a set of cybersecurity frameworks that use the principle of security controls and understand the particularities of each one. It was decided, in the 1st half of the internship, to analyse the ISO 27001, the NIST Special Publication 800-53 revision 5 and the NIST CSF by comparing them with the CIS CSC version 8. The latter, have a good comparative between the controls with other frameworks, which help us to complement each control with complementary information from others. The curricular unit of Security Auditing taught by Professor Edmundo Monteiro, in the second semester of the course, gave the necessary information and guidelines in this research and analysis. We learned these frameworks mentioned in the *state-of-the-art* and others more specific, such as, financial (PCI DSS), health (HIPAA), customer data oriented (SOC 2) or even more related to governance, like COBIT.

In February, during the intermediate defence, Professor Henrique Domingos, mentioned the ISO 27002 as important but missing in the research. Therefore, during the 2nd half of the internship, it was analysed and concluded that each of those controls are better explained in this version of ISO, as explained in the chapter 2.

3.1.2 Implementation of the Internal Control Plan

The internal control plan is part of the Cybersecurity Continuous Improvement Plan developed by SG. It's highly inspired by the CIS CSC and is constantly evolving. SG use an excel file where each Cyber Security Officers implement the corresponding controls in their scope. In our case, the controls will be followed according to our scope of Spain, Portugal and Morocco, filtering all the controls that applies. It was not defined by our managers the order in which we should implement the controls. Controls are ordered by priority (low, medium, high). Starting with highest priority, one or two controls are reviewed in a weekly basis, depending on complexity. Finally, an internal meeting is arranged to check and validate all gathered information. The chapter 4 has the list of all category controls that has been followed during this internship. The organisational structure is based on a geographical distribution with their corresponding IT structure that could give support for more than one country. For example, in the context of this internship, we belong to the perimeter of Spain, Portugal and Morocco. Therefore, in terms of cybersecurity context, all these three countries are under our responsibility for a set of subjects, others more transversal are managed centrally by the central team based in France. This means that not all the controls defined in the control plan will be under our responsibility, nevertheless, all of us have the responsibility to support and improve the overall security level of the group.

Controls are safeguards that are in place to ensure that the implemented security measures are effective and appropriate to the risks, and therefore are in place to highly reduce the impact in case of cyberattacks.

For each control, there is a need to define, implement and monitor them. The following table clarify how we will perform this:

Definition	Scope definition	Understand what will be controlled (servers, switches, workstations, firewalls, …)
	Priority	Implement and control those that have the highest priority defined by the group
	Frequency of execution	Define the frequency of the execution of each control (daily, weekly, monthly, yearly, …)
	Control owner	Define the owner (person or department) who will take care of the necessary actions to implement the control
	Source of information	Understand where the information comes from. It could be from hardware/software inventory, scanning tools, logs, other sources
	Operating procedure	Description of the control implementation details to clarify how the control will be implemented
	Evidences	Description of the evidences of the implementation of each control
Implementation	Remediation actions	Define the necessary actions to remediate the non-compliant devices. In some cases, a procedure must be defined
	Remediation Date	Define a deadline to the remediation of the non-compliant situations
	Compliance monitor	Define metrics to monitor the % of non-compliant devices

Table 11: Control Plan – Definition and Implementation

Basically, these will be the guidelines to implement the control plan. A weekly meeting is held with the department managers to follow-up general subjects related to aspects included in the security controls, mainly, those with highest priority. In parallel, a dedicated meeting with each control owner are held to clarify all the objectives for each or to the set of controls to allow that everyone is in the same page and aligned with the strategy. The chapter four explains more clearly the results of the controls followed during this internship. As some of the members of the Cybersecurity Policies & Controls Team, left the SG group during the 1st semester of 2022, the way we do the internal control plan (based on an extensive excel file) has been put on hold during the 2nd half of this internship. It doesn't mean that we stopped the control plan follow-up. However, it's clear that the new methodology will be more agile and more motivating, not only for Security Officers, but also for the control owners and the central team that consolidate all the information from all perimeters.

3.1.3 Integration of Security by Design into Projects

In the context of SG, for each new process or solution and in the event of major evolution or change, there is a need to follow the principle of Security by Design. For any of these needs, at SG, it is necessary to formalize the opening of a project in order to prepare the necessary follow up actions. Mainly and the most important point, the risk assessment. The process consists in the Integration of Security into Projects (ISP), through the Project Security Assessment Tool (PSAT). This tool is explained in more detail in the fifth chapter. The goal of this document is to centralize the ISP methodology that shall be completed partially or totally for all projects, depending on their sensitivity.

This allows the identification of two types of risks:

- **IT risks**: Risks with impact not only for the business (subsidiary), but also, more importantly, to the whole group. For example, those risks who can impact central services or even by lateral movement, can spread to other systems within and across borders;

- **Business risks**: Risks with impact only to the business, limited to its scope. Generally, those risks are mainly with impact to them. For example, impact on the availability of a certain service that only serves the need of that business.

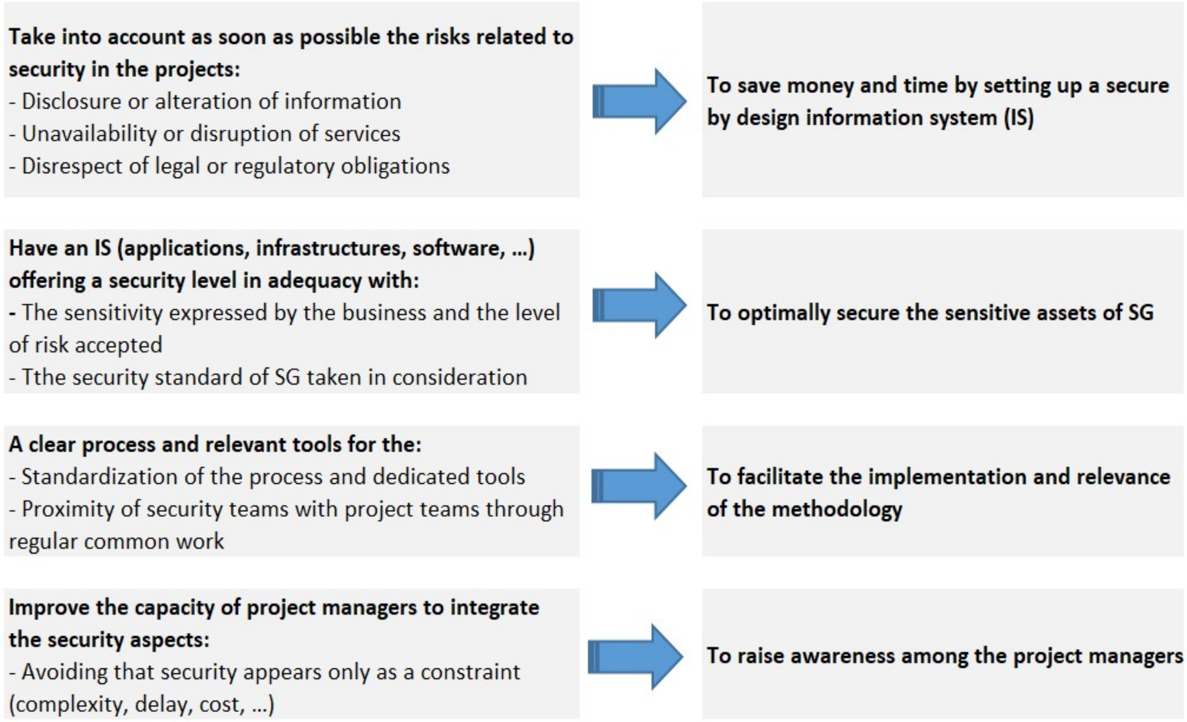
To support us with the risk assessment, we followed some of the most relevant risk management frameworks, precisely the ISO 27005, to better understand how should we do this analysis, including the following:

Framework	Brief Description
EN ISO/IEC 27001:2017	"Information technology. Security techniques. Information security management systems. Requirements"
ISO/IEC 27005:2018	"Information technology — Security techniques — Information security risk management"
IEC 31010:2019	"Risk management — Risk assessment techniques"
NIST SP 800-37	"NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
NIST SP 800-39	"Managing Information Security Risk: Organization, Mission, and Information System View"

Table 12: Risk Management Frameworks

The risk management will be better explained bellow where Business risks and IT risks are differentiated and handled accordingly.

Getting back to the ISP methodology, we raised the following question: Why is Integration of Security into Projects so relevant? To answer this, we created the following table with four, not exhaustive, examples, where the first two are related to risk management and the last two with project management:



Take into account as soon as possible the risks related to security in the projects:
- Disclosure or alteration of information
- Unavailability or disruption of services
- Disrespect of legal or regulatory obligations

To save money and time by setting up a secure by design information system (IS)

Have an IS (applications, infrastructures, software, …) offering a security level in adequacy with:
- The sensitivity expressed by the business and the level of risk accepted
- Tthe security standard of SG taken in consideration

To optimally secure the sensitive assets of SG

A clear process and relevant tools for the:
- Standardization of the process and dedicated tools
- Proximity of security teams with project teams through regular common work

To facilitate the implementation and relevance of the methodology

Improve the capacity of project managers to integrate the security aspects:
- Avoiding that security appears only as a constraint (complexity, delay, cost, …)

To raise awareness among the project managers

Figure 7.1: Importance of Security by Design into projects

During the analysis phase of this methodology used by SG for the ISP, the following aspects were identified to avoid a project blockage due to a lack or late consideration of the security into the projects:

Definition of a clear process

- Integrate as much as possible, methods and common practices, in many cases through experience gained from other projects, in the lifecycle of any project;
- Evaluate from the beginning the workload for each stakeholder;
- Define clearly the security path and the stakeholders;
- Adapt the requirements to the sensitivity of the project, based on the CIA triad (Confidentiality, Integrity and Availability).

Although SG has set as one of its priorities for 2022, develop a clear process for the integration of security by design into projects, it was well identified by all the security teams involved, that there is a clear need to improve the process in order to simplify and better adapt to each case, as no one size fits all. SG organisation is quite complex with its particularities, whether due to its size, either the economic activities covered or even their geographical dispersion. The other point to improve is that, a significant number of projects, when the business owner manifests their need and formalises the project opening, unfortunately, in some cases, the business has already made the necessary investment (CAPEX). Therefore, in some cases, vendor and the product/service is already purchased. If there is a security and/or privacy constraint or the product doesn't follow the principle of security by design, probably, to turn the project compliant, it become much more difficult.

Standardized tools:

The perception is that there is also a clear opportunity for improvement in the context of SG. Therefore, we identified three aspects to be improved in the upcoming months, mainly by the central security team:

- Define standardized tools adapted to the different steps of the ISP
- Adapt the tools for a simple use by the different stakeholders
- Develop a central repository where every security team can see other projects

The project security assessment tool (PSAT) developed and used by SG is based on an excel file, which is not at all, clear to all stakeholders. Each time a project is created, the business owner need the necessary support from the project manager to fill the file with all the necessary information to be evaluated by the security team. Otherwise, it will not be clear for them to assess correctly the security risks that the project rise. However, until a new methodology are in place, we followed during this internship the current PSAT excel file.

As a result, within our scope, each time there is a need from the different businesses to open a new Information Technology (IT) or Operational Technology (OT) project, it is mandatory to follow this methodology defined by the group. Therefore, as a Local Security Officer for Spain, Portugal and Morocco, we have the following responsibilities:

	Business Representative	**Project Manager**	**Local Security Officer**	**Central Security Team**
Ensuring that the ISP methodology has been taken into account	Consulted	Responsible	Accountable	Consulted
Accepting the business residual risk	Accountable	Informed	Responsible	Informed
Accepting the IT residual risk	Informed	Informed	Responsible	Accountable

Table 13: ISP Methodology – RACI

As we can see, the business owner will be accountable for business residual risks and we will act as responsible for both: business and IT risks (those who could affect other and not related business systems).

In terms of project phases' definition, the following figure describes the different phases from the very begin to the Go-Live phase:

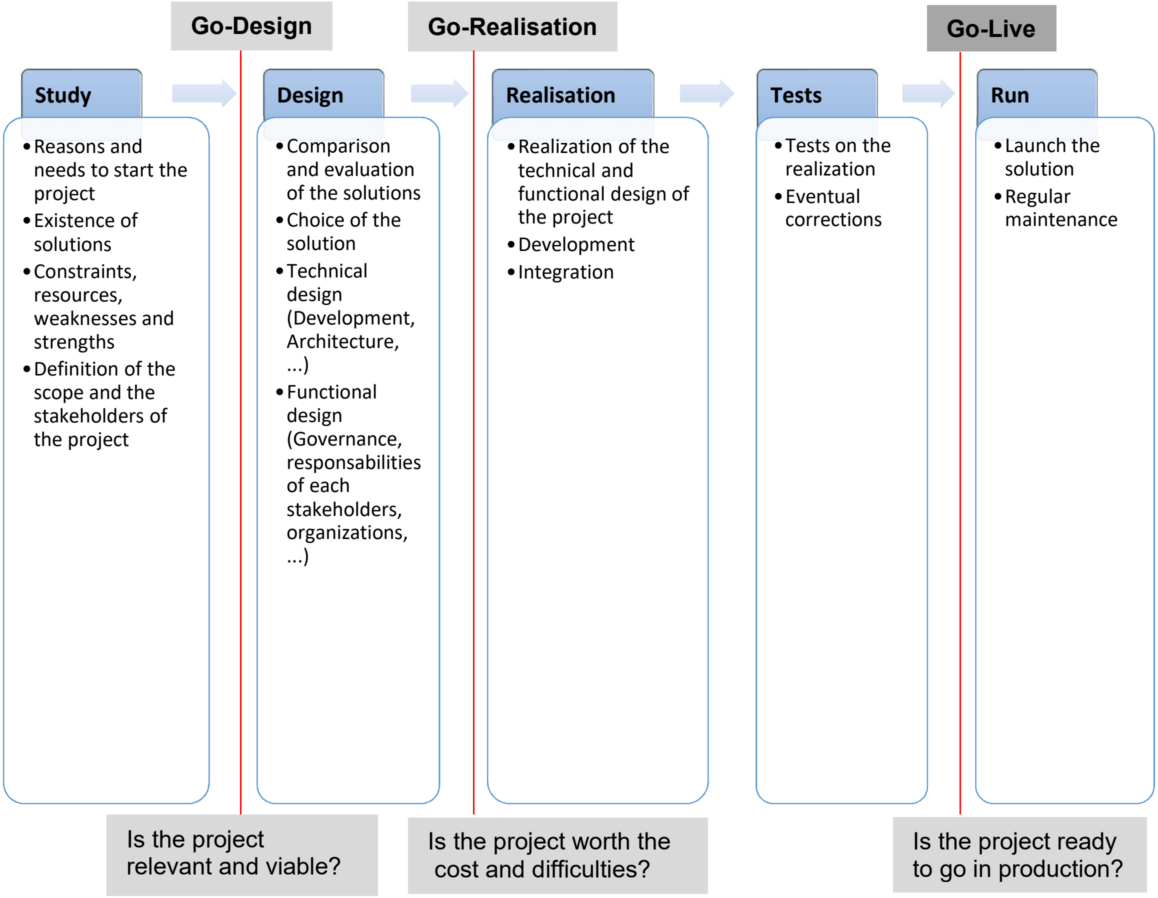

Go-Design
Go-Realisation
Go-Live
Study
• Reasons and needs to start the project
• Existence of solutions
• Constraints, resources, weaknesses and strengths
• Definition of the scope and the stakeholders of the project
Design
• Comparison and evaluation of the solutions
• Choice of the solution
• Technical design (Development, Architecture, ...)
• Functional design (Governance, responsabilities of each stakeholders, organizations, ...)
Realisation
• Realization of the technical and functional design of the project
• Development
• Integration
Tests
• Tests on the realization
• Eventual corrections
Run
• Launch the solution
• Regular maintenance
Is the project relevant and viable?
Is the project worth the cost and difficulties?
Is the project ready to go in production?

Figure 8.1: ISP: Project phases' definition

Depending on the complexity of the project the study and design phases could be merged into a single one before the go to realisation (sometimes referred as Implementation phase). For example, in some cases, when the project is opened the product/service/solution is already purchased or selected, therefore some of the points mentioned in the previous figure doesn't make sense. As a Security Officer, the main objective on those cases is to identify, analyse and treat the risks by challenging the stakeholders to go with security by design in mind. The business residual risks need to be accepted by the business owner and the IT residual risks, depending on the risk level, will be assessed and accepted (if so) by us or by the central team (in some cases, the risk acceptance need to be discussed in an exception committee).

In terms of risk assessment, the study and design phases are the most relevant ones, mainly for the risk identification on a very early phase, performing the corresponding risk analysis and treatment.

The following aspects are taken in consideration during the study/design phase, before Go-realisation:

- A questionnaire of data privacy is held, to understand if the project has personal data or not;

- A security insurance plan (SIP) assessed with external partners (if exists) to understand the level of maturity and if they are compliant with SG security requirements. The objective is to reduce the exposure of SG systems to third parties when there is a need to interconnect our network with them, reducing the risk of supply-chain attacks;
- Fill of specific hardening guides (inspired by CIS Benchmarks) for non-standard devices;
- Architecture and flows of the solution need to be also evaluated and discussed to check if they are compliant with the standard of SG. The project manager and the security officer helps the business to understand and apply the necessary security measures. At the end of the design phase, the security officer validates the document if compliant with the security rules of the group.

In the **realization and testing** phase, it's the moment to implement the solution (install the operating system, middleware, configure the network and firewall rules, etc.), evaluate the secure development and realisation of the project. It's the moment to perform the necessary tests and adjustments (change firewall rules, get approval for new components) by reflecting them in the PSAT file. If there is a need to perform software development, a code review (static analysis - SAST) should be performed to find potential vulnerabilities. If servers are present, there is a need to perform a vulnerability scan to find and mitigate those vulnerabilities found, if there are web applications, there is a need to perform specific scanning (ideally, a dynamic scan with authentication - DAST). All of the servers will be added to a regular scanning to find any new vulnerability found during their lifecycle. In some situations, due to the urgency of the implementation in production, some of the requirements mentioned as prerequisite for go-realisation, will only be implemented before go-live. Of course, analysing case by case, without jeopardising security, as in some situations, the project could be blocked until the risk is mitigated. The idea is to follow an agile project management approach but without increasing the actual risk.

For any identified risk associated to the project, and not evaluated during the design/study phase, a risk treatment process must be put in place through a risk analysis and treatment. For example, if the data transmission between a server and client are not encrypted in transit, as a Security Officer we should analyse it and challenge the business owner to find alternative and secure solutions. If it's an HTTP communication, we challenge them to configure HTTPS, if it's MQTT with tcp_1883 it must be changed to encrypted connection through tcp_8883 (TLS). The problem could appear when there is a limitation to configure secure protocols. In some cases, the application or even the hardware was not designed with security in mind. In those situations, if it's a business risk, a formal risk acceptance letter should be signed by the business owner accepting the risk associated with the probability of man-in-the-middle attacks.

The last phase, is the **Go-Live**, the moment to close the project if all the requirements have been met and the project are now ready to go in production. The main functional tests are done and major vulnerabilities are solved. All the remaining high and critical business risks are accepted by business, high and critical vulnerabilities are corrected, data privacy questionnaire (if applicable) are completed, the Security Insurance Plan (if 3rd parties are involved) is validated by the security officer and, the architecture and flows validated. Residual risks, for example, security improvements like Single Sign On (SSO) if there is a web application with authentication or even activation of multi factor authentication if the application is exposed on Internet, etc., are included in a regular follow-up process, reviewed every year, at least, by security officers.

In terms of business risk, the analysis is based on the following flowchart:

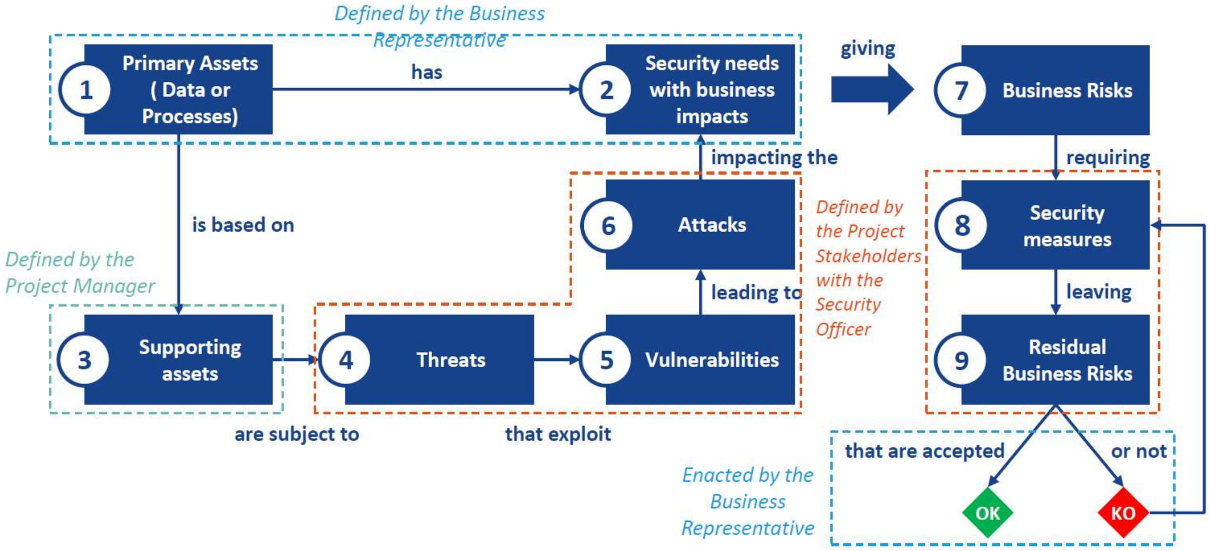

Defined by the Business Representative
1 Primary Assets (Data or Processes)
has
2 Security needs with business impacts
giving
7 Business Risks
requiring
is based on
Defined by the Project Manager
6 Attacks
impacting the
leading to
Defined by the Project Stakeholders with the Security Officer
8 Security measures
leaving
3 Supporting assets
4 Threats
5 Vulnerabilities
9 Residual Business Risks
are subject to
that exploit
that are accepted
or not
Enacted by the Business Representative
OK
KO

Figure 9.1: Main principles of business risk analysis

All the business risks identified during the study and design phase need to be accepted for the Go-Design. These risks are those who affect the business itself and not company in general.

For those IT risks that could have impact on other systems, we could analyse them based on the following flowchart:

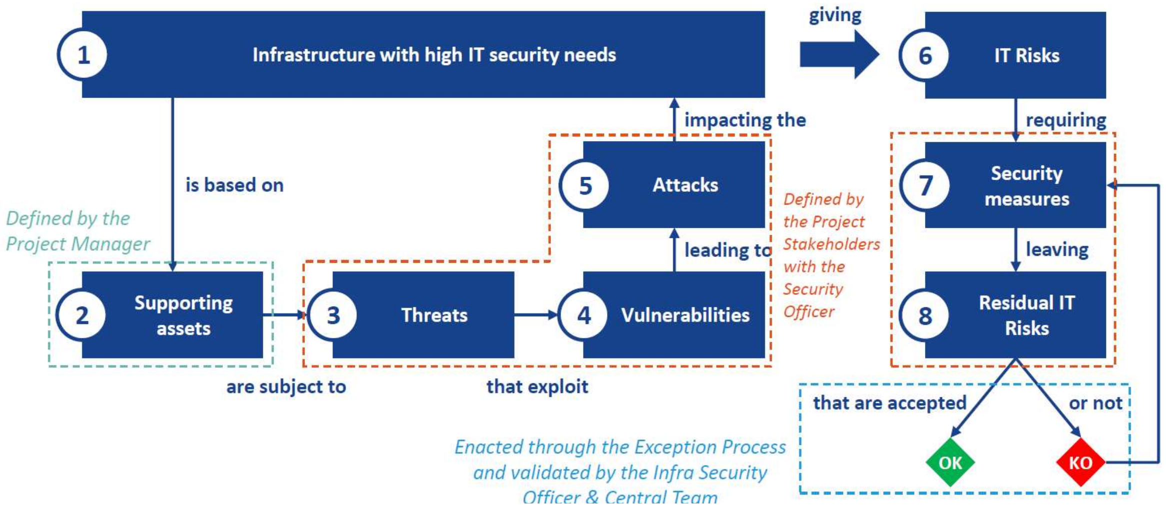

1 Infrastructure with high IT security needs
giving
6 IT Risks
impacting the
requiring
is based on
5 Attacks
7 Security measures
Defined by the Project Manager
leading to
Defined by the Project Stakeholders with the Security Officer
leaving
2 Supporting assets
3 Threats
4 Vulnerabilities
8 Residual IT Risks
are subject to
that exploit
that are accepted
or not
Enacted through the Exception Process and validated by the Infra Security Officer & Central Team
OK
KO

Figure 10.1: Main principles of IT risk analysis

In this case, in case of compromise / cyberattack, it could impact the overall infrastructure of the group, therefore a specific risk analysis must be performed as reflected in the previous figure.

All the steps mentioned on the previous figure 8.1, in some cases, such as complex projects, could request specific meetings with the different stakeholders to better understand the scope of the project, to perform a risk assessment, to clarify the architecture and flows. Almost of the cases, the email exchange or clarifications by call are enough. Monthly, there is a specific meeting within the IT organization of our perimeter to follow-up all the projects. It's where blocking points are discussed and moved forward.

In the fifth chapter some examples of relevant projects implemented during this internship will be better described to understand the challenge behind the integration of security into projects.

3.1.4 Security Awareness Program

While technology is often predictable, people are not. Usually, as humans, we are considered the weakest link in the security chain. We think by ourselves (free will) and make our own decisions – not always the right decisions. As no clear solutions exists for all the problems, people are error prone. Peter H. Gregory mention in his book [23] that "*This is mainly because of lapses in judgment, inattentiveness, fatigue, work pressure, or a shortage of skills. Personnel are generally considered the largest and most vulnerable portion of an organisation's attack surface*" (p. 297). Indeed, we also concluded this evidence during the internship and also during the research paper done in the 1st semester of the master with the title "*The Art of Mind Deception – a practical social engineering exercise*". An investigation that allowed a better understanding of physiological principles which facilitate the life of social engineers.

To improve the user awareness and as a consequence, improve the security of the organization, the strategy/approach to accomplish this was based on one of the security controls defined in the Internal Control Plan. Specifically, the control 17.3, which main objective consists in the creation of a security awareness program for all users to complete on a regular basis to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organization. The organization's security awareness program should be carried out in a continuous and engaging manner.

It's important to understand that security awareness training requires the support from the top management, human resources and from each department manager. Employees need the necessary permission to spend time on learning during their working hours. From the employee standpoint, they need to understand the importance and priority of these contents for them and for the organisation. If executives and managers understands how cyberattacks happen and what could be the potential impact in case of password theft from a user, information disclosure to competitors or even ransomware infections that completely disrupt the business continuity, they will motivate their employees.

Therefore, it will be necessary to create a program that includes the following groups of users:

- New hires (Preferable they should have training before having access to systems)
- Blue Collar (Shop floor Operators)
- Industrial (Maintenance, Automation)
- General users (everyone that have a user account in the Active Directory)
- Generic Accounts (A pool of users behind one single account)

- IT personnel (System/Network Administrators, Helpdesk, Project Managers)
- Software Developers
- Sensitive profiles (CEO's, Financial, Treasury, Management Committee Members)
- Third Parties (partners and customers)

In general, and also for each group, whether in-person or online, has at its base a genuine interest that our users understand how to identify the risks and be part of the security of the company. In fact, the most important objective of this security awareness program is, after all, that at the end we could reduce the risk exposure.

In terms of creating and selecting contents to be included in the program, we have decided that they should have the following characteristics:

- **Understandable** The content shouldn't be technical and difficult to understand, as most of the audience are nontechnical users. Otherwise, users will ignore and not understand the message that we want to transmit. As in our perimeter we have three countries and three languages, we need to create contents in their native language.

- **Relevant** The content need to be adjusted for the concerned audience, if it's necessary to send user awareness for developers, the content will be related to secure development, if it's related to financial department, it will be the same principle. The objective is that content is focused on their role and responsibilities.

- **Actionable** Important that the content ensure that users know what to do (and not do) in general contents transversal to all audience.

- **Memorable** in the sense that users could learn in an intuitive way allowing that contents be well understood, practised and internalised for future situations. For example, how to create strong passwords, how to identify malicious emails and report them, how to avoid unsafe behaviour in daily work.

With the audience and the characteristics defined, considering the current trend for remote work, mainly during the 1st half of this internship, due to the COVID-19 pandemic, we decided to focus on the following topics:

- Privacy and password best practices (2FA/MFA, password complexity, …)
- Social Engineering (Phishing, Vishing, Smishing, …)
- Confidentiality (Privacy vs Security)
- Protecting your computer (Keep it updated)
- Smartphone and mobile device security (Apps installed, lock screen, …)
- Working remotely and securely (VPN, Web surfing
- Reporting suspicious activities
- Wi-Fi security (Hotels, Airports, Home, Coffee shops, …)
- Unsecure behaviours (Unauthorized software installation, connection of personal computers to the corporate network, use of external USB storage devices, …)

The security awareness program is a continuous process which must be enhanced over time and adapted to the new trends and threats.

To carry out the awareness on these topics, the following communication and techniques was used:

- **Phishing** campaigns for each group identified before. Example: for specific departments (sales, logistics, human resources, marketing), for new hires, for generic accounts, per country, before and after a user awareness session. At the end of each campaign an email is sent to all the users deceived (clicked on a link, clicked on a link and introduced credentials, opened an attachment) by the phishing email.

- Monthly **newsletters** informing users about current threats and best practices. Each month a specific topic is launched with nontechnical contents as everyone receives the newsletter.

- **Training sessions** for IT users, Industrial, Marketing, Top Management, users from acquisitions, specific per country.

- **Awareness emails** or direct contact, each time a security incident is generated by a user, to make them understand the risk and the potential consequences to the user and the company.

- **Intranet web portal** dedicated to cybersecurity which include material such as posters, videos, best practices, tips, how to perform backups, keep the workstation updated, how to store passwords in a secure way, how to detect malicious emails, etc.

With all the steps described before concluded we moved forward with the creation of a formal document where all this information is reflected. The organization's security awareness program should be communicated in a continuous and engaging manner. The main objective is to have a documented program that should be followed during the year, collecting the necessary evidences of its applicability and updating with new ways to reach the end users, more assertively. Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.

The phishing campaigns were created and sent using a specific tool from a specialized vendor in this subject. This tool allows the creation of specific scenarios with landing pages, attachments, and educational content for those who are deceived by the scam. Scenarios could be customized or using recommended ones based on current active threats, industry relevance, and even on our previous used scenarios. The results of those phishing campaigns were shared, preserving anonymity, with the correspondent IT managers in the monthly reports, in the quarterly IT committee and whenever an awareness session is held. The main objective is to understand if users are well prepared to identify phishing emails and for those who were deceived, to improve their security awareness to be better prepared.

The training sessions are prepared and presented demonstrating actual cyber threats, not only for the organisation but also for others, including non-professional activities, such as actions they take in their personal life (personal email, social networks, smartphones, …). We also included contents related to social engineering, to let them understand the psychological principles behind our weakness as human beings, being better prepared against attacks.

Also important to refer that this objective (Security Awareness Program) is linked to the internal control plan, which in turn is linked to the CIS CSC. The control #17 refers to the security function "Protect" whose control category is: "Implement a Security Awareness and Training Program", subdivided into 7 sub-controls:

Control Title	**Short Description**
17.3: Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
17.4: Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
17.5: Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
17.6: Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
17.7: Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.
17.8: Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
17.9: Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

Table 14: Security Awareness Program - Controls

To support the development of this program we followed the recommendations from Peter H. Gregory [23], an interesting article from Terranova Security [24] where we could find some ideas for the contents. Finally, the book [25] from B. Gardner and V. Thomas with interesting information for defending against social engineering and technical threats. It's a dedicated book for those who are interested in the development of a robust security awareness program.

3.2 Risks and Schedule Plan

The objective of this section is to describe the risk analysis done for this internship. To understand what could happen and impact or even change the objectives outlined. Also the planning, reflected on a Gantt diagram of what has been done during the first and second half of this internship.

3.2.1 Risk analysis

This internship is oriented towards objectives involving a whole range of stakeholders, hence, the normal flow of things does not depend only on our pace and decision-making. The objective of Integration of Security into Projects, has the budget constraint in some of the different projects. Objectives although related, have their own particularities. The methodology followed for the Security into Projects, the Internal Control Plan and some actions in the Security Awareness Program is defined centrally, by the SG group. It means that we do not have much freedom to change the strategy or the tools used. Therefore, there is always a risk to adapt the objectives initially foreseen in case of deviations during the internship. SG has established a specific risk analysis methodology for the integration of Security into Projects and other for the internal control plan, thereby helping in the risk assessment for each of these objectives.

In the first half of the internship we did a risk identification to understand what kind of risks could come from one of several sources, taking in consideration our environment. After the identification of the risk we moved forward with the analysis to determine the different characteristics, such as: the likelihood that a certain event associated with that risk could occur. In this case, limited by the short time of this internship. Understand the impact or consequence of the event associated to the identified risk is fundamental. Finally, the risk treatment, accepting or not the risk and try to find solutions to mitigate and continue with the internship without impacting the overall objective of implementing a framework for continuous improvement in cybersecurity.

Generally, the risks identified, in case of a specific condition occur and the corresponding consequence are the following:

CONDITION	CONSEQUENCE
IT/OT projects under the responsibility of our perimeter could be cancelled or delayed.	The time dedicated in the analysis of the cybersecurity risks may have been wasted if the project is cancelled. If delayed, the overall progress of integration of security into project could not be explained during this internship.
A cybersecurity attack could affect our information systems.	The objectives may not be achieved as efforts will need to be redirected to mitigate the impact of the cyberattack. All the teams will have their responsibilities in the resolution.
SG decide to change the methodology used for the Cybersecurity Continuous Improvement Plan and the approach for the controls implementation changes.	All the methodology followed and explained in this report will need to be adapted since they may no longer make sense in some of them.
SG organisation changes and the scope of this internship also changes.	Objectives will need to be adapted during the internship if the organization changes and the objectives could not be achieved if the group decide to reorganize the teams where the trainee is based.

Table 15: Internship Risk Analysis

One of the risks identified that could highly impact this internship is clearly a cyberattack. In case of all the teams and the different stakeholders involving in our proposed objectives will be mobilized, to mitigate the impact and restore the normality as soon as possible with less impact to the organisation. The probability that the methodology for the control plan could change is high because is something that the group is already working since some time ago.

Nevertheless, from our humble point of view, as we learnt in the state-of-the-art section is clear that controls are an essential measure to reduce risks and therefore are extremely important to reduce the impact in case of cyberattacks. Something we must understand: It's not when but how.

In terms of risks identified, only one affected somehow one of our proposed objectives. The methodology used for the internal control plan will be changed. It's not yet clear what will be the new process, but as explained before, it's clear for everyone that it's not the best way to perform the internal control plan. The methodology consists in the filling of an excel file where for each control the necessary information is collected. The central team, at least twice per year consolidate all the information into a single database. At this moment, the group is working with a better approach in terms of what information should be collected from each perimeter, some of them to be automatic instead of manual collection. But, as we still don't have the final methodology announced and in production, we continued by filling the excel file, arranging the necessary meetings with the different control owners. On the other hand, the organisation is changing, the organisational structure is currently being adjusted. Nevertheless, without any impact in our approach towards each objective.

3.2.2 Planning

In terms of planning, the Gantt chart is based on the main activities carried out to successfully achieve the proposed objectives. The following table briefly reflects a rough estimation of the workload for each one:

Objective	Workload %
State-of-the-art control frameworks	5%
Internal Control Plan	50%
Integration of Security into Projects	30%
Security Awareness Program	15%

Table 16: Objectives - Workload

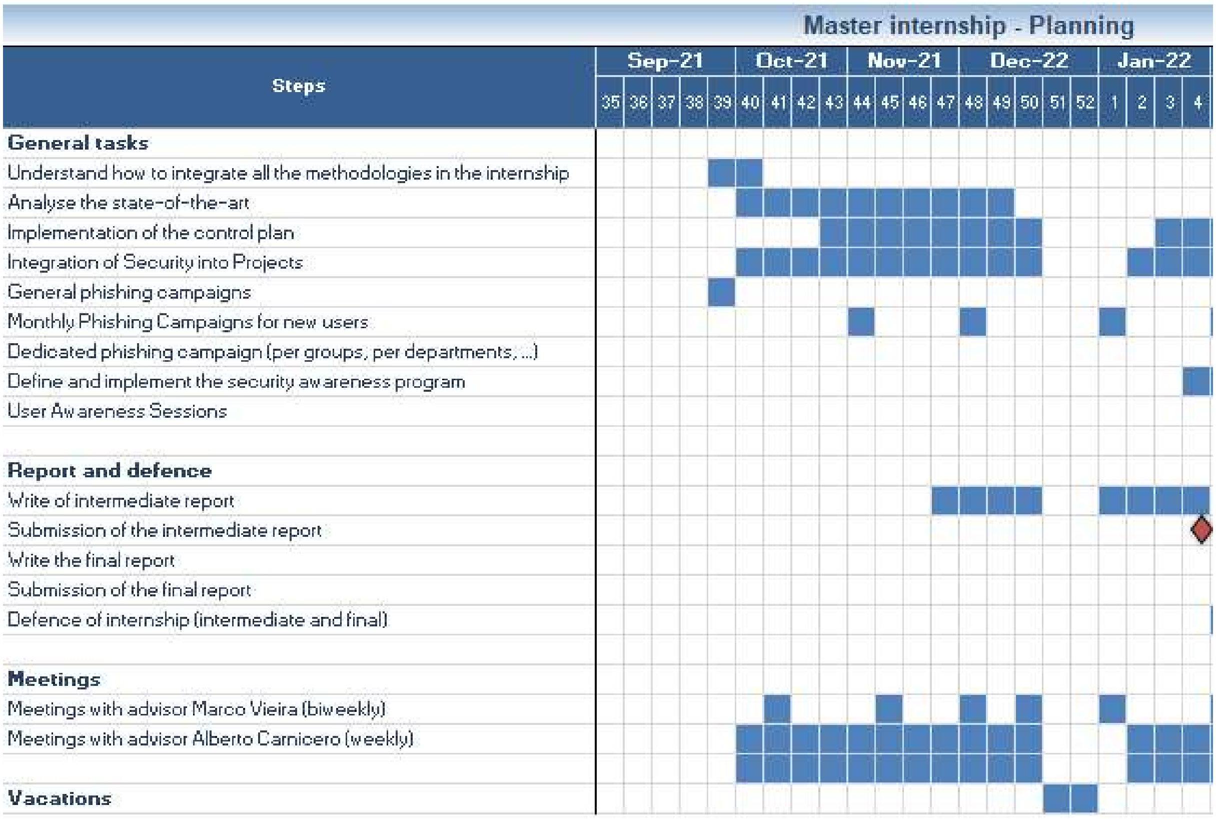
The controls defined, let's say, in the second objective are mainly created to ensure desired outcomes and also to avoid unwanted outcomes. Some are more complex than others, therefore, the initial plan changed in the 2nd half of this internship.

From a security perspective, we are dedicated to ensure that the necessary measures are in place. But each person in charge has their own priorities distinct from those related to security. Therefore, we need to balance the priority of each control with the workload. If we do not see that in some weeks we do not hold a follow-up meeting for the control plan, it does not mean that nothing was done on that week or weeks.

Almost of our daily tasks as a Cybersecurity Officer are based on controls. Just as an example: to monitor the number of devices without Endpoint protection, without Operating System (OS) updated with latest patches, vulnerability monitoring of OS or applications, by defining the corresponding action plan to mitigate all of them, mainly those with high CVE (score >8).

Therefore, the planning could change, that's why we defined that objectives such as the internal control plan, the integration of security into projects and the security awareness program are continuous. The integration of security into projects is a live task that depend mainly in the number of projects opened during this internship by the different business units. Is something that we can't control or predict. Some months could have more some less. Specifics tasks related to each objective are well defined as they are more static.

The tasks done during the first half of the internship:



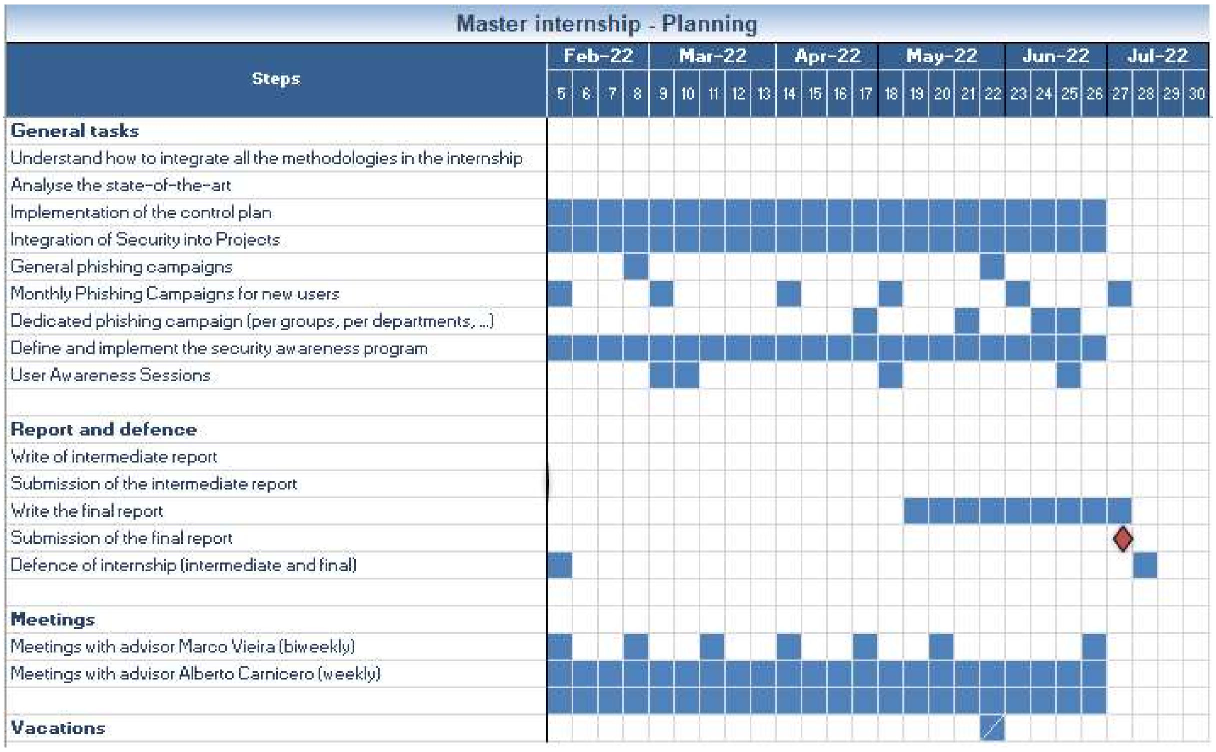
Master internship - Planning

Steps	Sep-21					Oct-21				Nov-21				Dec-22					Jan-22			
	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	1	2	3	4
General tasks																						
Understand how to integrate all the methodologies in the internship					■	■																
Analyse the state-of-the-art						■	■	■	■	■	■	■	■	■	■							
Implementation of the control plan									■	■	■	■	■	■	■	■					■	■
Integration of Security into Projects						■	■	■	■	■	■	■	■	■	■	■				■	■	■
General phishing campaigns					■																	
Monthly Phishing Campaigns for new users										■				■					■			
Dedicated phishing campaign (per groups, per departments, ...)																						
Define and implement the security awareness program																						■
User Awareness Sessions																						
Report and defence																						
Write of intermediate report													■	■	■	■			■	■	■	■
Submission of the intermediate report																						◆
Write the final report																						
Submission of the final report																						
Defence of internship (intermediate and final)																						
Meetings																						
Meetings with advisor Marco Vieira (biweekly)							■				■			■		■			■			
Meetings with advisor Alberto Carnicero (weekly)						■	■	■	■	■	■	■	■	■	■	■				■	■	■
Vacations																	■	■				

Figure 11.1: 1st semester planning

The 1st half was mostly focused on the first three objectives, leaving the development of a Security Awareness Program to the 2nd half. Although the phishing campaigns and the monthly newsletters included in the program, were performed. The contact was more regular with Professor Marco Vieira compared to the 2nd half, as there were more questions and doubts in the air about how to organise ideas and define priorities.

And for the 2nd half these were the tasks performed:



Master internship - Planning

Steps	Feb-22				Mar-22					Apr-22				May-22					Jun-22				Jul-22			
	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
General tasks																										
Understand how to integrate all the methodologies in the internship																										
Analyse the state-of-the-art																										
Implementation of the control plan	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
Integration of Security into Projects	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
General phishing campaigns				■														■								
Monthly Phishing Campaigns for new users	■				■					■				■					■				■			
Dedicated phishing campaign (per groups, per departments, ...)													■				■			■	■					
Define and implement the security awareness program	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
User Awareness Sessions					■	■								■							■					
Report and defence																										
Write of intermediate report																										
Submission of the intermediate report																										
Write the final report															■	■	■	■	■	■	■	■	■			
Submission of the final report																							◆			
Defence of internship (intermediate and final)	■																							■		
Meetings																										
Meetings with advisor Marco Vieira (biweekly)	■			■			■			■			■			■						■				
Meetings with advisor Alberto Carnicero (weekly)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
Vacations																		▨								

Figure 12.1: 2nd semester planning

During this 2nd half it is relevant to highlight the introduction of the user awareness sessions that will be better explained during the sixth chapter. In May the content was changed to focus not only on threats related to our daily work life but also on our personal life. The feedback was very positive from the audience, therefore, we decided to perform two sessions in May and two sessions in June. Also, the increase of phishing campaigns for specific groups of users, during the months of April, May and June.

Chapter 4
Internal Control Plan

As mentioned in the introductory chapter, following the results of the 2021 cybersecurity external audit, the Cybersecurity Continuous Improvement Plan (CCIP) - replacing the Cyber Defence Plan – was published in October 2021 with the sponsorship of members of the executive management in order to gather their support to the plan. The cornerstone of the CCIP is the Internal Control Plan where the deployment of continuous & personalized controls is done. The main objective of this internship orbits around the implementation and monitoring of these controls.

This chapter describes what has been done during this internship regarding this objective with relevant details that were not described in the previous chapter. Also, includes a guidance with a set of recommendations collected from different advisories, mainly from CISA, that could be followed by any organisation, regardless their size. Some of them, driven by current global tension due to the conflict between Russia and Ukraine. That conflict became a hybrid war, therefore, not only with missiles, tanks and troops in the war field but also with cyberattacks. Ukraine is suffering a lot with the war, but on the other side of the coin, the allies in coordination with Ukrainian intelligence services, share important information that allows their allies to learn about the techniques used by the Russians. This exchange of information already takes place at least since the Russia's illegal annexation of Crimea in 2014.

These set of recommendation are included as a sub-section of this chapter. It's a continuous process as threats evolve, therefore, is not exhaustive. We strongly recommend that any organisation follow the guidance developed by CISA, which they call: "Shields UP" [26] and are updated on a regular basis.

4.1 Objectives

The main goal of the controls, in this case, within our organisation include the following:

- Protection of the IT assets (hardware, software, information), therefore is important to have an accurate inventory. It's one of the most important controls
- Keep an accurate traceability of actions performed in our Information Systems, to protect the information of unauthorized users and modifications
- Ensure Confidentiality and Privacy, mainly for sensitive information
- Ensure Availability for those assets, mainly those who's criticality is higher
- Compliance with the policies, standards and rules defined in the organisation
- Compliance with applicable regulations within Spain, Portugal and Morocco, for example the GDPR for European Union countries

Considering that the risk assessment and the control design phases were conducted by the central team of SG, the main responsibilities, as a Cybersecurity Officer for our perimeter, are focused on the following processes [23]:

1. **Control Implementation**: Since the controls has been designed by the central team and inspired by the CIS CSC v8, we "just" need to put into service. Involving each of the stakeholders from the different areas that each of the controls may affect.
2. **Control Monitoring**: Once in place, the control need to be monitored to understand if the necessary measures are in place to address risks which the control is intended to mitigate. The Gap Analysis is important in this process to understand if we are going astray. Some of those controls are not so easy to monitor, due to their complexity. This process is conducted on regular basis. Some of the most relevant (high priority) controls are monitored on a daily or weekly basis.
3. **Control Assessment**: Important to periodically assess the controls defined for our perimeter – to understand if they are working as intended and as designed. This process is conducted mainly by the central team with the help of external audits.

According to ISO/IEC 27002:2022, a control "*is defined as a measure that modifies or maintains risk*". Modifies or maintains essentially means that a given control reduces or eliminates the risk identified in a given IT asset. Getting back to the security functions identified by NIST CSF, the main goal of the controls is based on the following [28]:

- **Identify**: Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy to better understand the risks
- **Protect**: Access Control, Awareness and Training, Data Security, Protection Processes and procedures, Maintenance and Protective Technology to limit the impact of cybersecurity incidents
- **Detect**: Anomalies and Events, Security Continuous Monitoring and Detection Processes to ensure that any cybersecurity incident are detected as soon as possible
- **Respond**: Planning, Communications, Analysis, Mitigations and Improvements to carried out in case of cybersecurity incident detection
- **Recover**: Panning, Improvements and Communications to restore any capabilities or services in case of a cybersecurity incident.

4.2 Controls

At its core, this Internal Control Plan is based on the eighth version of the CIS Critical Security Controls. With a set of 22 control categories subdivided into 173 security controls:

Control categories:

1. Inventory and Control of Hardware Assets;
2. Inventory and Control of Software Assets;
3. Continuous Vulnerability Management;

4. Controlled Use of Administrative Privileges;
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers;
6. Maintenance, Monitoring and Analysis of Audit Logs;
7. Email and Web Browser Protections;
8. Malware Defences;
9. Limitation and Control of Network Ports, Protocols and Services;
10. Data Recovery Capabilities;
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches;
12. Boundary Defence;
13. Data Protection;
14. Controlled Access Based on the Need to Know;
15. Wireless Access Control;
16. Account Monitoring and Control;
17. Implement a Security Awareness and Training Program;
18. Application Software Security;
19. Incident Response and Management;
20. Penetration Tests Exercises;
21. Data Center Management;
22. Integration of Security into Projects.

The category 7: "Email and Web Browser Protections" is excluded from our scope, as it exclusively concerns to the central cybersecurity team. For each category, there is a set of sub-controls that was implemented and followed during internship. To assess the implementation of each one, there is an excel file where we, as cybersecurity officers for our perimeter, collect all the information related to inputs, control owners, evidences, frequency of execution, gap analysis, understand and describe design and operating effectiveness, etc. There is a regular weekly meeting where we (Cybersecurity Officers for our perimeter) discuss at least one control, filling the excel file with the corresponding information gathered, and whenever needed, a dedicated meeting with the control owner was held to clarify the scope, the controls in place, to collect the evidences, to analyse the gap (if so) and create the necessary action plan to mitigate them. The list of controls followed during this internship are included as appendix to this final internship report.

Since October 2021 we started with the implementation and monitoring of the 173 controls defined in the control plan, of which 95 (55%) are our responsibility, as Cyber Security Officers, within the perimeter of Spain, Portugal and Morocco. It means that, for each one, the relevant information and evidences was collected, the priorities for each was defined, the gap analysis was done and in case of non-compliant situation, the necessary remediation action plan is defined with the corresponding control owner(s).

The following chart shows the control distribution for each of the four (Recover is not included as is out of our scope) security functions defined by NIST CSF and the corresponding priority defined by the central team of SG:

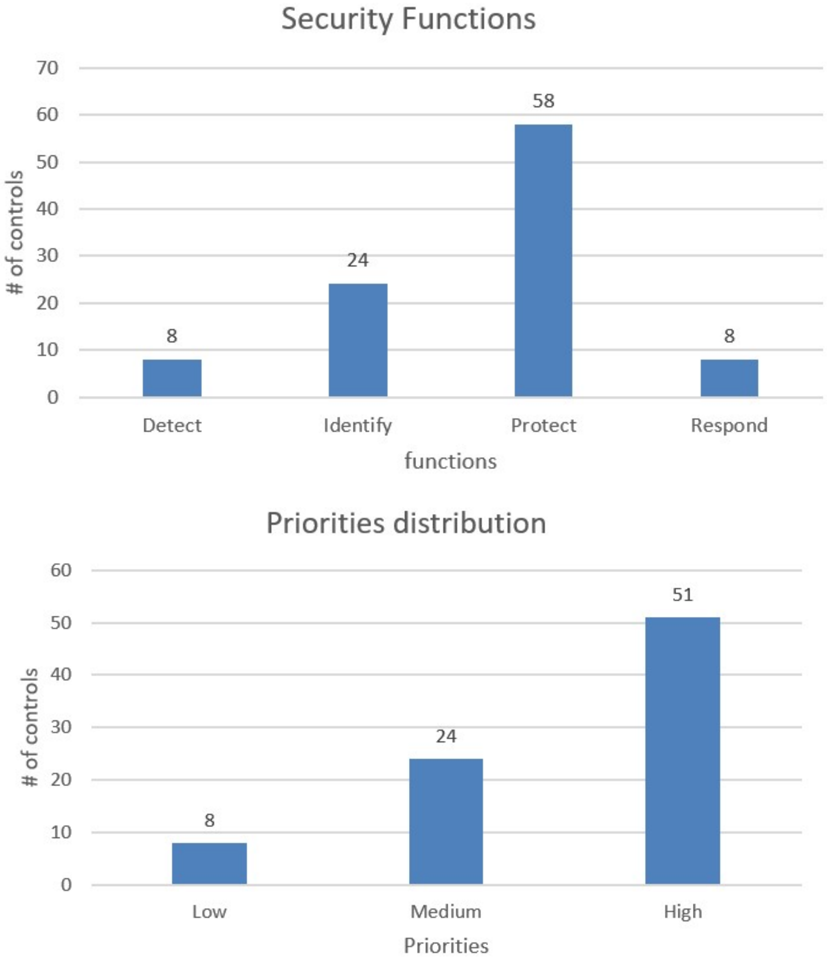


Figure 13.1: Distribution of the controls per security function and priority

Some controls are easy to implement than others. Due to the fact that they have their own particularities: dependency of some specific technologies not yet in place; controls that depend from the central team, applications or systems that doesn't support hardening configurations such as encryption in transit or at rest, lack of human resources to implement them.

The main goal will always be to have security in mind in all aspects, following the principle of zero-trust (NIST SP 800-207) [29], to guarantee that whenever possible we can guarantee Confidentiality, Integrity and Availability. One simple example is the least privileged principle to ensure that users have limited access to the resources and limited on their needs and, of course, assuming that there is always a risk everywhere, therefore, is necessary to minimize blast radius.

4.3 Implementation

Following the approach towards this objective described in the third chapter, we will go now into the description regarding the implementation of the controls that concern our perimeter. As we are talking about 95 controls, we decided to only select and describe the top five most important controls, based on their priority and relevance.

These are the selected top five controls:

Control Category	Control Title	Short Description
Inventory and Control of Hardware Assets	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets (focus on PCs and servers) with the potential to store or process information. This inventory shall include all Hardware assets (except removable devices), whether connected to the organization's network or not.
Malware Defences	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis (workstations and servers).
Data Recovery Capabilities	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.
Inventory and Control of Software Assets	Address Unapproved Software	Ensure that unauthorized software is removed
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized applications and software.

Table 17: Top five controls implemented

4.3.1 Maintain Detailed Asset Inventory

Indeed, this control is fundamental and is present in the most relevant control frameworks researched and described on the second chapter. It’s important, as we cannot protect what we do not know we have. An active and passive discovery tool is essential to automatically perform the inventory of our assets. Even those assets that aren’t connected to the network, for example, legacy devices or decommissioned but needed for historian, need to be inventoried.

For this control the following information was taken into consideration during the whole period of this internship:

Inputs

For this control we used an IT Service Management Software (ITSM) tool that allows the inventory management of assets. Also a tool used for software distribution where we can see what assets have specific software distributed through this tool and crosscheck the inventory of these two tools with the Active Directory. It’s important to have accurate inputs to crosscheck them and analyse the corresponding deviations.

Evidences

As this is a live and dynamic control, as assets are added and removed from the inventory on a regular basis, it’s necessary to maintain traceability at least monthly of the assets inventory in a database to be audited whenever needed.

Control Owner

The control owners in this case are the managers of the two relevant departments (Infrastructures and Support Services) that have under their duties the management of servers, switches, firewalls, workstations, printers, tablets, mobile phones, among others included in the inventory.

Remediate Actions

During the analysis of each input, if we found any deviation in the crosscheck with the different sources, we discuss our findings during the cybersecurity weekly meeting with the control owners. Using the Microsoft Planner, we create the corresponding task to be followed-up.

Conclusion

For this control, we consider that the design effectiveness is correctly established, implemented and operating as expected. The weak point here is the fact that this control is constantly changing, therefore, hard to keep a consistent inventory. The gap analysis is important when crosschecking the different sources with the total number of assets. This is clearly one of the most difficult controls to follow-up. Sometimes, we feel that we don’t know exactly how many devices we have at a certain moment in time.

4.3.2 Anti-Malware Software and Signatures

This control is essential because the endpoints are one of the most entry points for cyberattacks. If we consider that phishing is one of the most common types of cybersecurity techniques [30], it's important to protect the endpoint where the user will open their emails.

For this control the following information was taken into consideration during the whole period of this internship:

Inputs

The inputs of this control is based on a tool used by the group where we can see the current number of devices with or without endpoint protection, if their last seen is more than 15 days, if the policy applied is the correct one and if the version of the endpoint client is the last one. It's important to keep our assets as much as possible close to 99% protected considering the approx. scope of 4000 assets (servers and workstations). The central console of the endpoint solution is also used as input to crosscheck with the tool used by the group and Active Directory.

Evidences

The evidences for this control are based on the report from the tool used by the group and the inventory that we can see from the central console of the endpoint solution. We also weekly register the deviations, using Microsoft Planner, to see if the device is back to a compliant state again.

Control Owner

The same as the previous control. The managers of Infrastructure and Support Services are the control owners that will do what is necessary to regularise those irregular assets.

Remediate Actions

During the analysis of each input, if we found any deviation in the crosscheck with the different sources, we discuss our findings during the cybersecurity weekly meeting with the control owners. Using the Microsoft Planner, we create the corresponding task to be followed-up. If we found a sensitive device not protected, we will perform a strict follow-up with the corresponding control owner and if necessary we will ask to isolate the device from the network until it fulfils the requirements.

Conclusion

This controls are quite similar with the inventory control. Mainly, for workstations as they are dynamic (added and removed regularly – new users coming, users departing). This is one of the controls that we normally check on a regular basis, mainly to understand the reason why we see non-compliant devices because of not being protected with the endpoint software or without the corresponding policy applied.

4.3.3 Regular Backups

This control is also important to implement and monitor regularly, not only in case of accidental data deletion but essentially in the recovery phase in case of a cyberattack. The backup data need to be also protected, putting them offline to avoid data loss in case, for example, of ransomware attacks and encrypting backups whenever possible to avoid data theft.

For this control the following information was taken into consideration during the whole period of this internship:

Inputs

The inventory of assets to be protected with backups are based on the total number of servers and workstations controlled in the first control mentioned in this chapter. With this inventory we crosscheck with the reports from the different backups solutions in place. For example, by crosschecking the inventory of Active Directory and the Inventory Asset Management tool with the backup reports. These reports give us the assets under backup and in case of backup failures we can discuss with the corresponding control owners.

Evidences

The list of assets in the inventory and in the backup reports is used as an evidence of what are being protected or not. The Infrastructure manager developed a dashboard in Power BI where we can monitor the total number of devices under backup protection and also how many restore tests was done during the year.

Control Owner

The same as the previous control. The managers of Infrastructure and Support Services are the control owners that will do what is necessary to regularise those irregular assets.

Remediate Actions

In case we found devices without backup in place, an analysis is performed to understand the reason behind and to avoid that future deviations could occur. The critical assets for each business need to be protected and the necessary restore tests done.

Conclusion

This is also a difficult control to monitor. If we talk about workstations, due to the significant number of devices in our perimeter, it's normal that some of them could have failed the periodic backup. In terms of servers, the Infrastructure team analyse the reports on a regular basis by remediating as soon as possible those of failed the backup process.

4.3.4 Address Unapproved Software

Important control to monitor due to the fact that some applications can be installed without admin rights and be Potential Unwanted Programs (PUP) that could do Potential Unwanted Modifications (PUM) in the systems. Some users have admin rights on their machines due to their roles, but even knowing that, any software need to be previous analysed in a sandboxing before installing and they can only install authorized software from trusted vendors. That's why, in large environments like ours, with a significant number of devices, it's important to have this control well designed, implemented and monitored. For this control the following information was taken into consideration during the whole period of this internship:

Inputs

It's not yet in place a Configuration Management Database (CMDB) that could facilitate the lifecycle management of the software installed in our environment. Therefore, the input used for this control is based on our inventory discovery tool where we can see all the software installed on servers and workstations. All the software installed since 2-3 years ago are analysed in a sandboxing system to confirm if it's a non-malicious software or not. Each software that pass the sandboxing are added to a software catalogue. Each time there is a need to install additional software, the IT Technician will consult this file to see if the software is approved for installation, if not, they will request the corresponding sandboxing.

Evidences

The evidences for this control are based on the inventory done by the discovery tool and also with the software catalogue database. All the software presents in the inventory, except from vendors such as Microsoft, Autodesk and other relevant vendors, need to be in the software catalogue database.

Control Owner

In this control, Cyber Security Officers have the responsibility to implement and monitor this control.

Remediate Actions

On a regular basis, at least, once per week, using a specific report in the discovery tool, we can see all the software installed in the last 7 days. If we found software (except those mention in the evidences) not included in the software catalogue we launch the necessary actions to uninstall that software and to perform the necessary user awareness to avoid future behaviours like this.

Conclusion

This is an important control as in some situations during this internship, we found that some users, even without admin rights, can install PUP or PUM software, such as crypto miners, remote access tools (Anydesk and TeamViewer) that in these cases in addition to the removal we were able to blacklist those application on the endpoint protection solution.

4.3.5 Establish Secure Configurations

The last control was selected as top five of the controls implemented, because it's important to have our Operating Systems, Middleware, Software and devices configured following a set of best practices. The hardening guides from the vendors, from our experience and even from the CIS Benchmarks [12] is fundamental to establish secure configurations. For example, to only use secure protocols (HTTPS, SFTP/FTPS, SSH) instead of weak protocols (HTTP, FTP, Telnet), to change the default passwords, to reduce the available services to what is strictly necessary. For this control the following information was taken into consideration during the whole period of this internship:

Inputs

Following the previous control, the inputs used are based on the same principle. The software installed, mainly software that act as a server need to be configured using a hardening guide. Therefore, the inputs are mainly based on the inventory from the discovery tool.

Evidences

The evidences for this control are based on the hardening guides created for each application or Operating System. Each time an operating system is installed, the IT Technician need to follow the hardening guide. There is no automatic tool in place that will analyse the Operating System against a checklist used in the Hardening Guide. Therefore, the evidences need to be from collected case by case.

Control Owner

In this control, we focused on the servers and less on workstations. As mentioned in the inputs, the most important assets to apply the hardening guides is those who act as server instead of client. Therefore, at this moment, the control owner is the Infrastructure Manager and in some cases the application owner who will need to guarantee that the application is running with secure configurations.

Remediate Actions

Normally, we detect that a server (OS or application server side) have an unsecure configuration when we receive the results from vulnerability scanners. In those situations, we request the corresponding responsible to remediate them, according to the severity of the vulnerability.

Conclusion

As it is not yet in place any tool that allows an active analyses of the configuration of each Operating System and Application (server side), the control is not effectively implemented and operational.

4.4 Summary

When we started with the implementation and monitoring of the controls in our perimeter, we started by the first control in the list. After the implementation of some controls we decided to change the strategy, mainly due to the significant number (95) of controls to follow-up. That's when we decided to address first those whose priority is considered to be high. Is not described in the methodology followed by the group for the Internal Control Plan, but it seems they have set the priority for each control, based on the principle where:

Risk = Likelihood x Impact

The following figure is interesting to better understand the logic behind Impact & Probability, without using technical terms. Following figure shows the best practices mentioned in the different Risk Management Frameworks, such as ISO 27005. Therefore, the priority was already defined by the central team, so there is no intervention/change from our part.

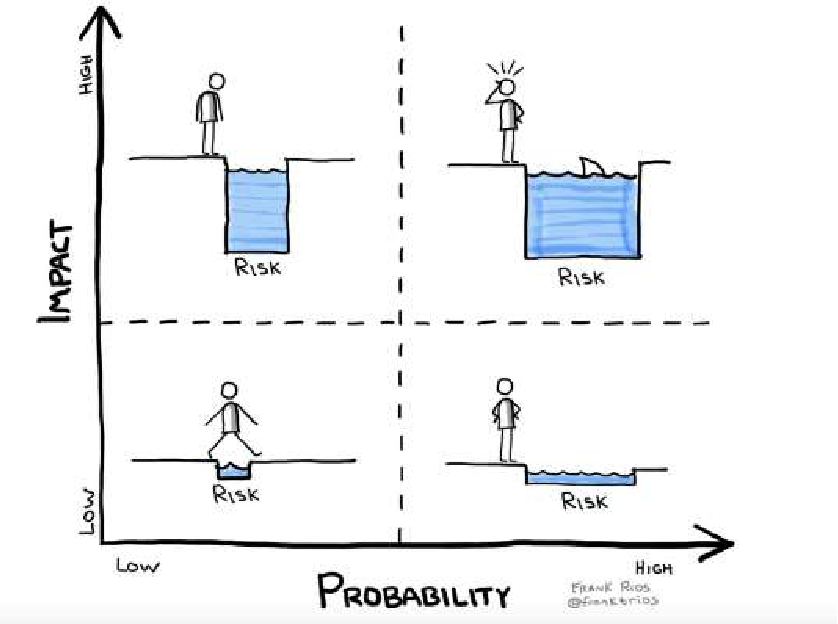


Figure 14.1: Impact vs Probability – (source: Frank Rios [34])

During the implementation of this Internal Control Plan, it has been understood that the most important thing is not only to obtain evidence to show in future audits. The most important thing is to keep in mind everything that should be monitored to minimise our exposure to risk. Each company should adapt the controls to its reality. For example, a financial institution will have different controls compared to a company dedicated to the construction market. It's a continuous process, that needs to be adjusted throughout its life cycle. Not all controls are properly implemented and properly monitored. It's an objective that will continue even after finishing this internship. The group is working in a way to improve our we follow-up each control, either by collecting evidences, perform gap analysis and implement remediation actions to mitigate the risks, either by centrally develop a database with all the KPI's from the different perimeters.

This internal control plan allowed us to significantly improve our level of security within our perimeter. With these controls, we were able, among others, to:

- Reduce the number of local admin accounts
- All users with admin rights signed the "Admin Charter" where they learned what they can and cannot do with those privileges
- Regular control of unapproved software installed by regular users or even by administrators without following the internal procedure to install software
- Reduce the attack surface regarding network access for partners, by reducing permitted protocols to the strictly necessary and only those who are secure (HTTPS, SSH, …)
- Improve the network segmentation, mainly between IT and OT
- Reduce the number of systems with high or critical vulnerabilities
- Keep as much as possible an expressive number of middleware components updated with their latest version available

In the following section there is a set of recommendations that had been collected during the implementation of the Internal Control Plan that could be used by any organisation – large and small. A set of recommendations that could help to respond to disruptive cyber incidents [26].

4.5 Guidance for All Organisations

Below we can find a set of recommendations as a way to encourage all organizations - regardless of size - to adopt a stronger posture when it comes to cybersecurity. Essentially, it's a compilation from the experience acquired during this internship, either through what the different standards/frameworks (ISO 27k, NIST SP 800-53 Rev5, NIST CSF, CIS Security Controls v8) have taught us, as well as advisories from Cybersecurity agencies such as: ANSSI, CNCS, CISA, ENISA [17, 18, 19, 20]. In fact, all related to each of the controls implemented, that's why it's included in this section.

The list of recommendations is not exhaustive; we just highlight the most relevant. In any case, the CIS Critical Controls is our main recommendation to be followed if we want to have strong security foundations. There was an idea of mapping the recommendations with the framework of ATT&CK [21] to better understand the correlation with the different tactics. It was not possible due to the planning, but it will be taken into consideration as future work.

Follows the following structure:

Recommendation	
Priority level	Context
	Complementary information

Table 18: Recommendation Structure

And in terms of priority it was decided to use three different levels that could be adjusted by anyone who would like to follow these recommendations:

P0 (high priority)
P1 (as soon as possible)
P2 (least important priority)

Table 19: Recommendation Priority

The following table provides a set of recommendations that we consider important to take into consideration (not ordered by priority):

Vulnerability Management Process	
P0	Establish a vulnerability management process to identify potential vulnerabilities either in systems and software running on the organisation. It's fundamental to have an accurate inventory to allow the identification, evaluation, treatment and reporting of security vulnerabilities. Prioritise the remediation of known exploited vulnerabilities as soon as possible, based on the severity (normally on CVE scores).

	Known Exploited Vulnerabilities Catalog from CISA: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Subscribe to Vulnerability Bulletins from Cybersecurity Agencies (CISA, CERT's) CISA: https://www.cisa.gov/uscert/ncas/bulletins CNCS: https://dyn.cncs.gov.pt/pt/alertas/
Implement an Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	
P 1	Identify and establish a baseline based on the normal network activity in the organisation. The main goal is to monitor the network and identify malicious behaviours. This kind of IDS/IPS should not only be network-based, it's also important to monitor the endpoints.
	What is IDS/IPS? https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html Learn about YARA rules. https://www.techrepublic.com/article/how-to-write-yara-rules-for-improving-your-security-and-malware-detection/ Open Source tools such as Snort could be a good choice.
Audit Log Management	
P 1	Develop a system (e.g. SIEM) that could analyse (aggregation and analysis) in real-time the huge number of logs from different systems/applications to find suspicious behaviours. Active Directory sign-in logs, logs from servers and workstations, switches, firewalls, honeypots, should be taken into consideration to this collection of logs. Important to have a central Syslog that should be protected against cyberattacks. The Syslog could be very useful in case of a cyberattack for *post-mortem* analysis.
	A Guide to CIS Control 8: Audit Log Management: https://blog.netwrix.com/2022/06/16/audit-log-management/
Protection against Credential Theft	
P 1	Enforce Multifactor Authentication whenever possible. Block any attempt of brute force attacks in authentication systems. The main goal is to detect the abuse of Authentication Mechanisms. Use strong authentication mechanisms and avoid legacy authentication protocols.
	What is Multifactor Authentication: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661 NSA | Cybersecurity Advisory: https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF
Email Protection	

P0	Block email forwarding to external email addresses. If needed, should be treated as an exception, properly documented. Implement strong filtering and detection products to avoid spam, phishing, malware on attachments and links. Link inspection before the user clicks is crucial. Next-Generation solutions with Machine-Learning based to find and detain malicious emails. Do not provide email web access. If it's really necessary, only allow the authentication with MFA. "Audit email rules with enforceable alerts via the Security and Compliance Center or other tools that use the Graph API to warn administrators to abnormal activity".
	Email protection: https://www.proofpoint.com/us/products/email-security-and-protection/email-protection
Control of connections by unauthorized devices	
P1	Develop and implement a policy which prohibits the connection of unauthorized devices by the employees in the network. If possible, implement a Network Access Control system (NAC) to only allow authorized devices to be connected to the corporate network. Awareness is essential to avoid this kind of unsecure behaviours.
	NAC Reviews and Ratings: https://www.gartner.com/reviews/market/network-access-control
Remote Access	
P0	Close any RDP port for servers accessible from Internet. Any access to those servers must be done from a secure connection (VPN) and well secure behind a firewall. Only allow the Remote Access from a specific set of sources and not from everywhere". Hardening guide for the RDP access. Blacklist any unapproved application that could be used to allow the remote access to the company network without authorization from the IT department. For example, block Anydesk, Teamviewer, PCAnywhere.
	Security Guidance for Remote Desktop adoption: https://www.microsoft.com/security/blog/2020/04/16/security-guidance-remote-desktop-adoption/
User Awareness and Training	

P 0	“Focus on awareness and training. Make employees aware of the threats—such as phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities”. Launch regular phishing campaigns to better prepare the users to this kind of threats. Do regular user awareness sessions not only focused on professional threats, but also related to their daily personal life. “Establish blame-free employee reporting and ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently”.
	Social Engineering: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/ Solution for Phishing Campaigns and user awareness: https://www.hoxhunt.com/
Secure the PowerShell usage	
P 2	Keep using PowerShell but implement the necessary security measures to reduce the risk of using this powerful tool.
	Security Measures to Use and Embrace: https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/1/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF PowerShell security: https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/learn-script-security Securing PowerShell in the enterprise: https://www.cyber.gov.au/acsc/view-all-content/publications/securing-powershell-enterprise
Account Management	
P 1	Identify and disable accounts that are no longer in use. Implement monitoring measures that could detect abnormal account management (creation and deletion within a short period of time)
	NSA | Cybersecurity Advisor: https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF
Patch Management	
P 0	Implement a patch management process to control the lifecycle of any application. Apply patches as soon as possible, based on criticality and exposure (Internal or External). Replace those systems/application with end-of-life, without any support from the vendor. Implement a centralized patch management system.

🟥	CISA alert AA22-158A: https://www.cisa.gov/uscert/ncas/alerts/aa22-158a Benefits and Best Practices: https://www.rapid7.com/fundamentals/patch-management/
Design and Development of Secure Software	
P 1	Define and implement an internal culture of design and development of secure software for internal developers but also for outsourced, following the best practices. The essential point here is to follow the principle of Security by Design.
	OWASP DevSecOps Guideline: https://owasp.org/www-project-devsecops-guideline/ Bibliography from the course unit of the MSI: - J. Viega and G. McGraw, Building secure software: how to avoid security problems the right way. Addison-Wesley, 2001. - M. Howard and D. E. Leblanc, Writing Secure Code, 2nd ed., Microsoft Press, 2002. - G. Hoglund and G. McGraw, Exploiting Software: How to Break Code. Pearson Education, 2004. - M. Howard, et al., 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, McGraw-Hill, 2005. - C. J. Berg, C. Berg, and P. G. Neumann, High-Assurance Design: Architecting Secure and Reliable Enterprise Applications, Addison-Wesley Professional, 2005. - M. Schumacher et al, Security Patterns: Integrating Security and Systems Engineering, Wiley, 2006. - G. McGraw, Software Security: Building Security In. Addison-Wesley Professional, 2006. - J. H. Allen et al, Software Security Engineering: A Guide for Project Managers, Addison-Wesley Professional, 2008. - M. Howard and S. Lipner, The security development lifecycle. O'Reilly Media, Incorporated, 2009.

Table 20: Recommendations learned during Internal Control Plan

We also strongly recommend the use of a knowledge base of adversary tactics and techniques at our disposal from MITRE ATT&CK® [21]. The interesting thing is that MITRE is working now also with cybersecurity countermeasures that they call D3FEND™ with a simplified relationship between Offensive and Defensive Techniques.

Chapter 5
Integration of Security into Projects

As mentioned in the chapter 3, the Integration of Security into Projects (ISP) is a methodology developed by Saint-Gobain to manage the lifecycle of a project in terms of security. Each project that is opened and formalised in our perimeter need to be incorporated into the Project Security Assessment Tool (PSAT) which is nothing more or less than an excel file with the goal to collect all the information related to security aspects of the project. It must be completed partially or totally by all IT/OT projects, depending of their sensitivity.

The central team is working on to improve this tool. The idea is to move to an agile approach, where all the steps for each project will be adjusted based on the criticality of the project. The risk assessment is essential to evaluate the criticality of the project. The requirements will vary according to the sensitivity assessed during the risk qualification phase (before Go-Realisation phase). If the sensitivity of the project is low or medium, the requirements will be less compared to high or critical sensitivity. Also, the tool that the central team is working will be web-based instead of an excel file. With this tool we will have visibility of the current status of the project, to define a workflow for approvals and to keep a better tracking during the lifecycle of the project. This chapter is based in the current excel file tool.

5.1 Project Security Assessment Tool

The PSAT have several sheets to be filled during the lifecycle of the project, from the study/design to the Go-live phase. These are the sheets presented in the document:

Sheet	Description	To be filled for
1 - Project overview	Project's stakeholders, description & planning	All projects
2 - Risk Qualification	Security needs, business sensitivity, and required security deliverables to be provided as part of the project	
3 - ASAT Architecture Assessment	Architecture diagram including internal and outsourced resources	All, except SaaS
4 - ASAT Flows Assessment	Flow Matrix with all in and outbound flows	
5 - Business Functions and Needs	Key functions brought by the project and for each the security needs and supporting assets	If project is sensitive (see sheet 2)
6 – Risks & Security measures	Main risks (both IT and Business) and the associated counter measures	
7a – Security Check-List D	Synthesis of the security actions needed and done for the Go-Design	All projects
7b – Security Check-List R	Synthesis of the security actions needed and done for the Go-Realisation	

7c – Security Check-List L	Synthesis of the security actions needed and done for the Go-Live	
8 – Security Exceptions	Tracking of exceptions accepted in the context of the project	All projects

Table 21: PSAT structure (source: PSAT file)

And in the following table, all the sheets that shall be used to support the filling of the PSAT:

Sheet	Description
Appendix 1a - Cloud Eligibility Matrix	To help you assess which kind of cloud can be used and give first requirements
Appendix 1b - PCMSR Compliance	To help you to secure the hosting of your application in Public Cloud
Appendix 2 - Flow Security Rules	To help you design your flow matrix in compliance with Saint-Gobain Rules
Appendix 3 - Threat Event Catalogue	To help you during your risk analysis
Appendix 4a - Data Classification	To help you to classify your Business Data & Processes
Appendix 4b - Data Protection	To help you to understand the security requirements that must be followed to protect assets based on their classification levels (AICT) and associated risk scenarios.
Appendix 5 - SHIA Rules	To help you to secure the hosting of your application in Internet DMZ
Appendix 6 - WASD Rules	To help you to secure the development of your web application
Appendix 7 - URL Inventory	To help you to inventory and secure your URL

Table 22: PSAT summary for contents and actions (source: PSAT file)

All business owners with the help of project managers and if necessary with our help, as Cyber Security Officers role, when they open a new project or a minor change request where there is a need of a PSAT, need to fill at least sheets 1 (Project Overview) and 2 (Risk Qualification).

In the previous table 20, we can see in the first column on the left side, the sheets present in the excel file. The tab "1 - Project overview" is where all the information about the project itself, such as, the definition of stakeholders, the project description, the planning and a questionnaire need to filled. As an example, the questionnaire has the following questions:

- Will there be any outsourcing in the project? (e.g. SaaS, PaaS or IaaS, hosting, service provided by a third party…)
- Will there be any personal data in relation with the EU (GDPR)?
- Will there be an IT infrastructure in the project?
- Will there be an OT (Industrial) infrastructure in the project?
- Will there be a web application?

Based on the answers, the tab “2 - Risk Qualification” will have more or less security requirements/deliverables that are expected before the Go-Live of the project, thus validated by the Cyber Security Officer and Industrial Cyber Security Officer, if industrial flows involved.

If, for example, the answer to one of the previous question “Will there be any outsourcing in the project?” is a yes, then the following deliverable is expected:

- **Security Insurance Plan (SIP)**: In order to secure SG systems, it is essential to assess and control the risks of third parties that will interact with Saint-Gobain IT environment.

Third parties may require access to SG sensitive resources; hence third-party security assessment is necessary to prevent cyber incidents on those resources with increasingly persistent attackers trying to exploit vulnerabilities to:

- Obtain information of users and the targeted SG entity Business
- Gain access to the SG information system
- Propagate and extend the attack scope on SG information system
- Damage or slow down the system and/or extract or modify data
- Obtaining intellectual property
- Among other malicious activities

Consequently, the purpose of the SIP will guarantee that the scope of the service is delivered under safe conditions ensuring SG data and systems are protected. An excel file is completed with all the information such as the type of access between the third party and SG network and on that basis, a set of security questions are generated to be filled by them. All the answers are analysed by the Cyber Security Officer and if they are compliant, a formal contract is generated from the excel to be signed by both parties. If not, a continuous challenge is made with third party until agreement is reached. In parallel, a Non-Disclosure Agreement (NDA) need to be also signed by them. Both, the SIP and the NDA are mandatory in order to be able to start the delivery of services by a third party.

For the question: “Will there be an IT infrastructure in the project?” if the answer is “Yes”, then the following deliverable is expected: ASAT - Architecture (PSAT – sheet 3) and flows (PSAT – sheet 4) to reflect the high-level diagram of the solution and the corresponding flows (TCP/UDP, from/to, hostnames) if the project has network flows or not. If there is a need to install new servers, it’s mandatory to also add them to a regular vulnerability scanning tool to analyse potential vulnerabilities and establish the necessary remediation action plan. If it’s necessary to connect to the network, non-standard devices (access control devices, CCTV, smart TV’s, others) it’s necessary to follow a specific hardening guide created by SG and in case it doesn’t exist, at least, to follow the vendor recommendations and if available to follow the CIS Benchmark guidelines.

Finally, for the question: “Will there be a web application?”, it’s necessary to add the web server to a regular web application scan (WAS) that could be based on static (SAST) or dynamic (DAST) analysis. It’s very useful the use of this kind of vulnerability scanning tools, as it gives on a regular basis, a vision of the current vulnerabilities in our servers and web servers.

Still in sheet 2 (Risk Qualification), we have four questions with the aim to evaluate the business security needs and thus the business sensitivity of the project. The description of each level of evaluation is available in the "AICT Matrix" tab. The association of these information's and the answers to the previous tab's questions ("1 - Project Overview") allow us to evaluate the expected security deliverables needed before the Go-Live. The AICT refers to Availability, Integrity, Confidentiality and Traceability, where business need to define the impact for each one. That could be low, medium, high or critical.

These are the questions for the assessment of **A**vailability, **I**ntegrity, **C**onfidentiality and **T**raceability (AICT):

- What would be the consequences if the need expressed regarding **availability** is not fulfilled?
- What would be the consequences if the need expressed regarding **integrity** is not fulfilled?
- What would be the consequences if the data **confidentiality** is not respected?
- What would be the consequences if the need expressed regarding **traceability** is not fulfilled?

At the end, based on the answers, the project business sensitivity could be low, medium, high or critical. If all the answers are low except one that could be high or critical, it's enough criteria to have sensitivity high or critical as a final result. In case, of high or critical, the sheet 5 (business functions & needs) and sheet 6 (risks & security measures) need to be completed with the aim to identify the business risks and IT risks. In the sheet 5 (in case of high or critical sensitive projects), business fill with the list of critical tasks identified and for each of them define the level (low until critical) for each ACIT and also the supporting assets (users, servers, switches, plc's, …).

The sheet 6 (Risks & Security Measures) will use the tasks identified before and ask for: threat & vulnerability (example: session hijacking, exploits, …), the security measures (in place to reduce/mitigate the identified risks), the residual risk and formal acceptance by the owner of the risk. The sheets 7a (for Design phase), 7b (for realisation phase) and 7c (for go-live) are filled, by the Cyber Security Officers, according to the different stage of the project. Is where the necessary comments are added to be accomplished before the next phase (realisation or go-live).

During this internship, for all the projects opened in our perimeter, we followed this methodology to Integrate Security into Projects (security by design).

5.2 Methodology Implementation

Following the same approach used for the Internal Control Plan, due to the significant number of projects managed during this internship, we decided to only mention a few of them. In total, we dealt with approx. 150 projects. Some of them opened before we started the internship and others opened during the internship.

Each project opened need to be validated by us, otherwise, the corresponding teams cannot start working on the project, for example, to purchase material (servers, storage, network devices) or even to create virtual machines. That's why in our perimeter, the IT services take project management as an important process, on the one hand, for its implementation to be a success and in line with the business expectations, and on the other, to follow the principle of security by design.

The type of projects opened were widely diversified, some more complex than others. Some projects related with the opening of subsidiaries, some with the migration of Operating System nearing the End-of-Life support. Mainly, projects related to new applications in the IT level and others related to OT (Industrial) level. Some of them with communications between IT and OT.

We have selected the following sample of projects from the total of 150, to demonstrate how they were analysed from a security standpoint:

1. Human Resources Web Application

We decided to include this project due to their sensitive as it will manage employee data and will be exposed on the Internet. It's an ongoing project that are currently under analysis (design phase) prior to Go-Realisation. Therefore, is still under scrutiny, hence is understandable that the security measures in place need to be strong.

Objective: Document management, Absence Management, submit suggestions and complains

Q&A:

Will there be any outsourcing in the project? (e.g. SaaS, PaaS or IaaS, hosting, service provided by a third party…)	YES
Will there be an IT infrastructure in the project?	YES
Will there be an OT (Industrial) infrastructure in the project?	NO
Will there be external development in the project?	YES
Will there be any personal data in relation with the EU?	YES
Will there be secret data?	NO
Will there be a web application?	YES
Will there be a component exposed to Internet in the project? (This question does not apply to SaaS applications project)	NO
Will there be a network link with the corporate network?	YES
Will it be hosted in the Cloud?	YES

In terms of AICT, business initially defined the project sensitive as MEDIUM, but based on the information (employee data) that will be used by the application, we challenged them to change to HIGH.

Requirements defined for this project **before Go-Realisation**:

- Considering the outsourcing in the project (Application Development), SIP & NDA need to signed. Otherwise, they are not allowed to access our systems without having those contractual agreements in place. If being strict, they are not even allowed to develop the application

- Segregation of duties (split between HR admins & employees)
- Flow matrix (tab 4) will all the flows between the different components (Frontend, Backend)
- Tab 5 (Business Functions & Needs) and Tab 6 (Risks & Security Measures) need to be filled as project sensitive is HIGH, in order to protect in particular Confidentiality
- Application is to be designed in Compliance with WASD (Appendix 6) and Data Privacy Requirements (Appendix 4b)
- Authentication Concept needs to be provided. Use of Single-Sign-On (SSO) for users in Active Directory, and for users without AD account, mainly for Blue Collar users, the local authentication should be done with Multi-Factor Authentication as the Web Application will be accessible from Internet
- Start the installation of components (Software, Middleware) with latest versions

These were the conditions imposed before the approval for Go-Design. At the time of writing this final report, the project is still waiting for fulfil of these requirements to give the corresponding approval to go to the next phase (Go-Realisation).

The following is to be ensured **prior to Go-Live** (End of Development) approval:

- All the requirements for Go-Realisation are completed
- Application is designed in compliance with GDPR law and registered in the central tool used by SG for the inventory of application that have PII, with the approval of the Data Privacy Correspondent
- Web Application Firewall implemented to protect the web application
- Data Protection Measures (Appendix 4b) must be taken into account
- The Servers are subscribed to the Vulnerability scanner and free of Vulnerabilities
- The URLs are subscribed to the Vulnerability Web Scanner and free of Vulnerabilities
- Supplier has delivered a Code Review Report free of Vulnerabilities and Security Hotspots
- A Grey Box Penetration test is conducted
- A Proper Change Management Process has to be formalized
- Reliable Patch Management Process in Place by the third party
- Application registered in the central tool used for the inventory of applications

2. Projects related with the migration of Windows Server 2012 R2

In this point we focus on the different aspects of projects opened during the internship for the migration of applications running on Windows Server 2012 R2 which End of Life is October 10, 2023. It can be perceived as so far away, with enough time to perform the migration, but we are talking about around 70 servers to be migrated with each one with their server side application running and particularities, it becomes a serious topic to be taken seriously.
In this kind of projects, each one has its own particularity and therefore no one size fits all. For each project regarding this migration (Win2012R2 EOL) we decided to define the following requirements at least before Go-Realisation or Go-Live. The idea is to not delay the global project of migration but taking the opportunity to have a better secure infrastructure:

- "Encryption by design" of all flows between the different servers/clients, for example, if they use SSL/TLS protocols, as a minimum the SSLv2, SSLv3, TLS 1.0 and TLS 1.1 are forbidden. Robust encryption algorithms shall be used, for instance, AES256 or stronger.
- Avoid the use of unsecure protocols such as HTTP, FTP, TELNET, MSSQL without encryption, among others. Use secure protocols: HTTPS, SFTP/FTPS, SSH, MSSQL Encrypted, OPC UA encrypted, among others.
- All components, such as Databases, Middleware and Firmware are making use of the latest version available from the corresponding vendor.
- Review of Users having Access to the System by Business Owner, segregation of duties.
- Configure the new server in a secure zone/vlan with strict filtering by the firewall. Adapt the current network flows with different assets following the segmentation (based on the Purdue model)

This kind of projects, in almost of the cases they have existing applications already in production, therefore, is more difficult to challenge the application owner to migrate to a different vlan (with different IP address), for a different firewall zone to perform the strict filtering between this new server and their dependencies (servers).

If we found legacy applications that cannot be upgraded, we need to analyse the corresponding project with the different stakeholders to try change the application with a new supported one, or by isolating the application with very strict filtering until the application owner find a solution (in some cases with the need of budget).

Chapter 6
Security Awareness Program

The main objective of the Security Awareness and Training Program is to ensure that all users in our perimeter understand and exhibit the necessary behaviours and skills to help ensure the security of our organization. This program is essentially focused on the following methods:

- **Phishing campaigns** for each group identified in the chapter 3. Examples: for specific departments (sales, logistics, human resources, marketing), for new hires, for generic accounts, per country, before and after a user awareness session. At the end of each campaign an email is sent to all the users deceived (clicked on a link, clicked on a link and introduced credentials, opened an attachment) by the phishing email.

- Monthly **newsletters** informing users about current threats and best practices. Each month a specific topic is launched with nontechnical contents as everyone receives the newsletter.

- **Training sessions** for IT users, Industrial, Marketing, Top Management, users from acquisitions, specific per country.

- **User Awareness** emails or direct contact, each time a security incident is generated by a user, to make them understand the risk and the potential consequences to the user and the company.

- **Intranet web portal** dedicated to cybersecurity which include material such as posters, videos, best practices, tips, how to perform backups, keep the workstation updated, how to store passwords in a secure way, how to detect malicious emails, etc.

6.3 Phishing Campaigns

During this internship, were carried out the following phishing campaigns:

- 2 campaigns for all users (Spain, Portugal and Morocco)
- 10 campaigns for all the new comers (monthly)
- 6 campaigns for specific departments
- 1 campaign for Generic Accounts (a pool of users behind)
- 4 campaigns with specific subjects and limited recipients

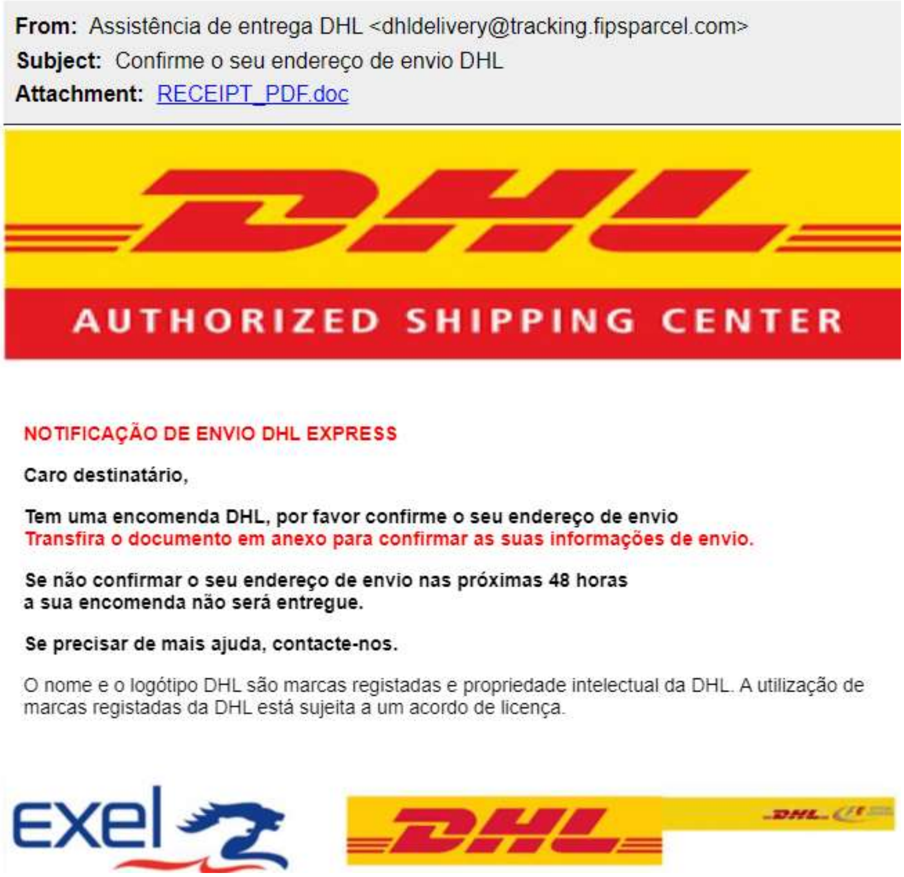
In our perimeter, we have different cultures and languages, therefore, different approaches or at least to try to have one single approach that covers all the countries. For example, in Morocco it doesn’t make too much sense to send Christmas phishing emails because it won’t have the same impact as in Portugal or Spain. A phishing campaign with the subject of “El Gordo” (lottery in Spain) will not have also the same impact in Portugal or “Correios de Portugal” (Portuguese Mail), “Via Verde” (Portuguese Tolls service) or “Autoridade Tributária”

(Portuguese Tax Authority) will not also have the same impact in Spain or Morocco. So, to select and perform effective phishing attack it was decided to use a common approach.

The phishing attacks are bypassing the traditional perimeter defences that secure the email system, normally called as secure email gateways and reaching the people's mailboxes. Human being are considered as the weakness link, error prone where each one has its own way of thinking and acting, therefore, we can't blame them (us). Even if the cybersecurity awareness has increased in recent years and users are getting better at spotting phishing emails, if there is at least one user that click on the link or open the attachment could be enough to compromise all the organization.

To improve the user awareness in our scope, all the users are informed that we perform regular phishing campaigns, with this in mind we think that users will be more aware when opening emails. Next we will demonstrate some examples of phishing campaigns that we sent during this internship:

Following the same principle in the Internal Control Plan and Integration of Security into Projects, due to the significant number of phishing campaigns we will just mention a few as example. The DHL phishing email sent in November 2021 during the week of black Friday, for Portuguese audience (558 users):


From: Assistência de entrega DHL <dhldelivery@tracking.fipsparcel.com>
Subject: Confirme o seu endereço de envio DHL
Attachment: RECEIPT_PDF.doc

AUTHORIZED SHIPPING CENTER

NOTIFICAÇÃO DE ENVIO DHL EXPRESS

Caro destinatário,

Tem uma encomenda DHL, por favor confirme o seu endereço de envio
Transfira o documento em anexo para confirmar as suas informações de envio.

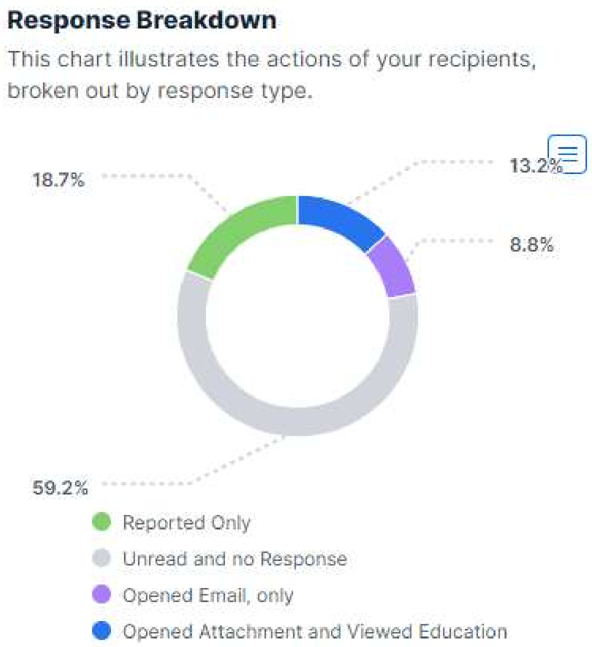
Se não confirmar o seu endereço de envio nas próximas 48 horas
a sua encomenda não será entregue.

Se precisar de mais ajuda, contacte-nos.

O nome e o logótipo DHL são marcas registadas e propriedade intelectual da DHL. A utilização de marcas registadas da DHL está sujeita a um acordo de licença.

Figure 15.1: DHL Phishing – Portuguese version

And the results speak for themselves, for the 558 Portuguese users:



Response Breakdown

This chart illustrates the actions of your recipients, broken out by response type.

Figure 16.1: DHL Phishing Campaign – Portugal results

As we can see, a significant number of users (13%) opened the attachment. Now, let's imagine that in that moment our systems are vulnerable to the recent CVE-2022-30190 [35] where attackers could execute malicious PowerShell commands through Microsoft Diagnostic Tool (MSDT) by simply open a Word document. It's clearly demonstrated in these results that we need to boost the user awareness making them aware of the importance to report suspicious e-mails. An expressive number of users (59%) did nothing. Even if it was a real phishing email, it means that probably a lot of users just deleted the email considering it suspicious before reporting it. This simple act of reporting is enough to the background teams, block the propagation of this kind of emails to other mailboxes, to analyse the content of the e-mail and add the corresponding Indicators of Attacks in our SIEM tools.

If we look to the following timeline, we can see at least something good – the first user that interacted with the e-mail was to report instead of opening it. Approx. 26 min after, the first user opened the attachment. This 26 min could be decisive in a real situation. If the team, in less than 26 minutes have the capability to analyse the e-mail, remove it from other mailboxes and add the Indicator of Attack (IoA) to the security systems (e.g. Endpoint protection), probability the potential cyberattack could be mitigated.

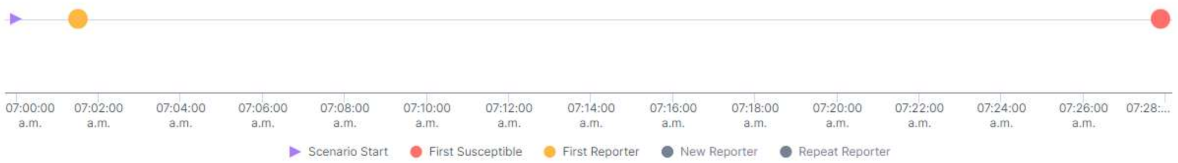
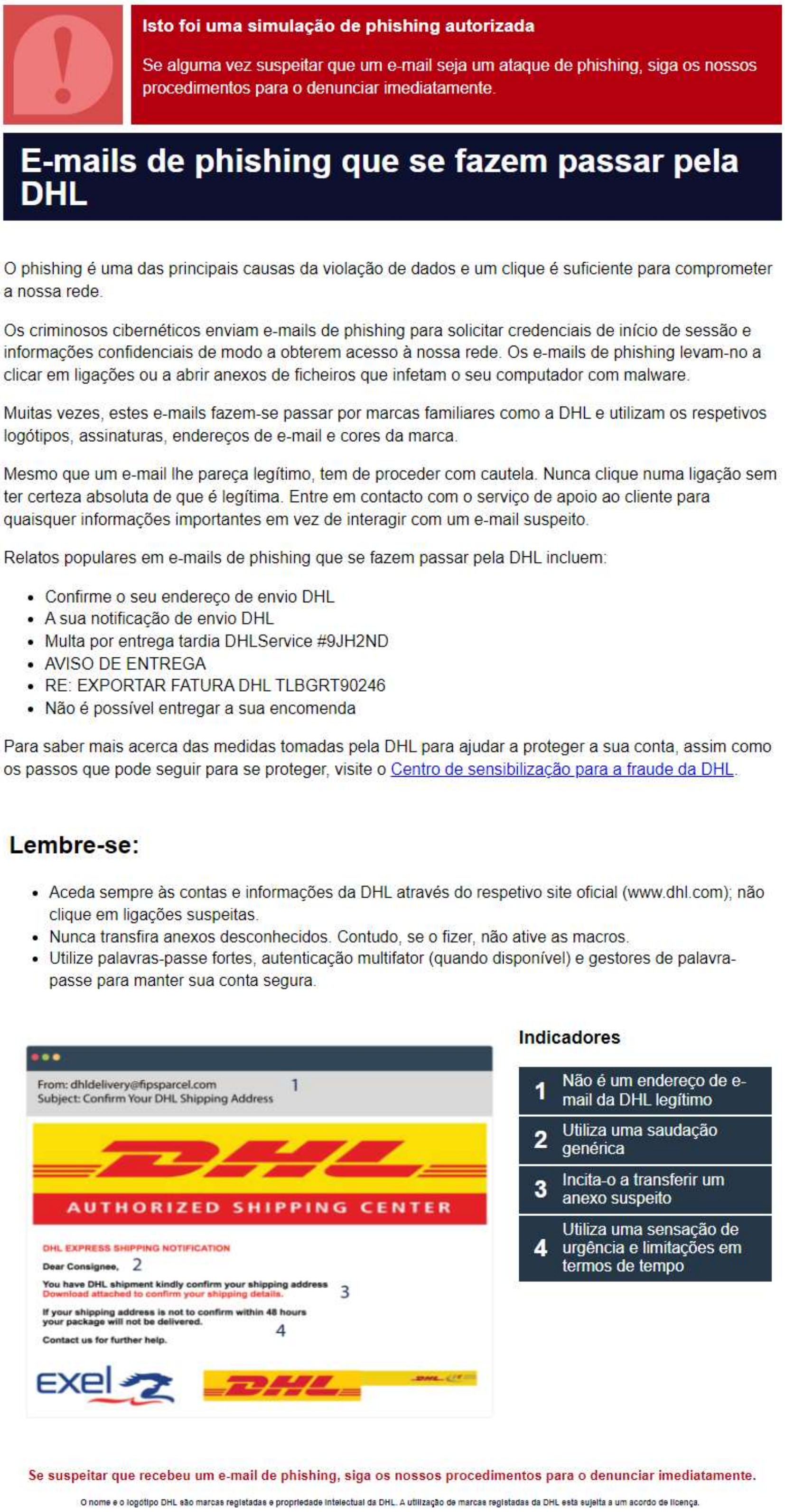


Figure 17.1: DHL Phishing Campaign Portugal – Timeline

When the user opened the attachment, they will see a document indicating that it was a phishing campaign, demonstrating the best practices to detect this kind of malicious emails. This is the content of the attachment:



Isto foi uma simulação de phishing autorizada

Se alguma vez suspeitar que um e-mail seja um ataque de phishing, siga os nossos procedimentos para o denunciar imediatamente.

E-mails de phishing que se fazem passar pela DHL

O phishing é uma das principais causas da violação de dados e um clique é suficiente para comprometer a nossa rede.

Os criminosos cibernéticos enviam e-mails de phishing para solicitar credenciais de início de sessão e informações confidenciais de modo a obterem acesso à nossa rede. Os e-mails de phishing levam-no a clicar em ligações ou a abrir anexos de ficheiros que infetam o seu computador com malware.

Muitas vezes, estes e-mails fazem-se passar por marcas familiares como a DHL e utilizam os respetivos logótipos, assinaturas, endereços de e-mail e cores da marca.

Mesmo que um e-mail lhe pareça legítimo, tem de proceder com cautela. Nunca clique numa ligação sem ter certeza absoluta de que é legítima. Entre em contacto com o serviço de apoio ao cliente para quaisquer informações importantes em vez de interagir com um e-mail suspeito.

Relatos populares em e-mails de phishing que se fazem passar pela DHL incluem:

- Confirme o seu endereço de envio DHL
- A sua notificação de envio DHL
- Multa por entrega tardia DHLService #9JH2ND
- AVISO DE ENTREGA
- RE: EXPORTAR FATURA DHL TLBGRT90246
- Não é possível entregar a sua encomenda

Para saber mais acerca das medidas tomadas pela DHL para ajudar a proteger a sua conta, assim como os passos que pode seguir para se proteger, visite o Centro de sensibilização para a fraude da DHL.

Lembre-se:

- Aceda sempre às contas e informações da DHL através do respetivo site oficial (www.dhl.com); não clique em ligações suspeitas.
- Nunca transfira anexos desconhecidos. Contudo, se o fizer, não ative as macros.
- Utilize palavras-passe fortes, autenticação multifator (quando disponível) e gestores de palavra-passe para manter sua conta segura.

From: dhldelivery@fipsparcel.com
Subject: Confirm Your DHL Shipping Address

DHL EXPRESS SHIPPING NOTIFICATION

Dear Consignee,

You have DHL shipment kindly confirm your shipping address
Download attached to confirm your shipping details.

If your shipping address is not to confirm within 48 hours
your package will not be delivered.

Contact us for further help.

Indicadores

1 Não é um endereço de e-mail da DHL legítimo

2 Utiliza uma saudação genérica

3 Incita-o a transferir um anexo suspeito

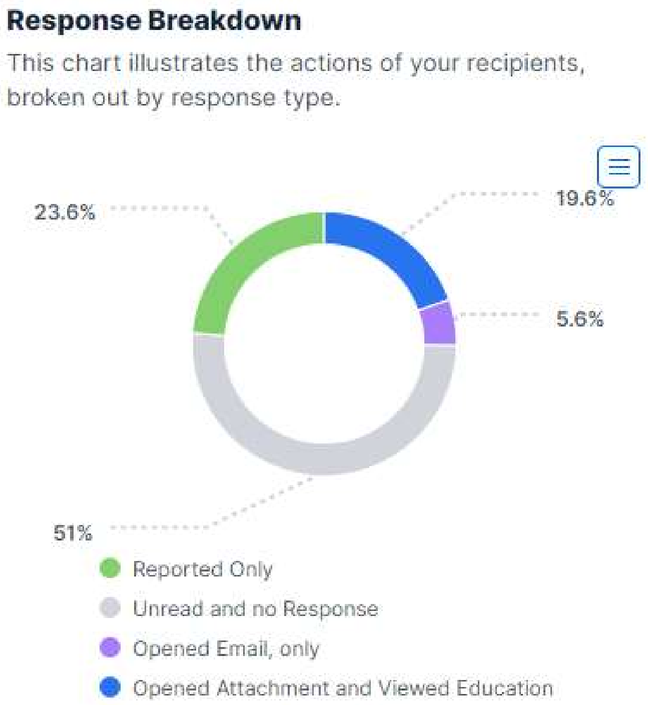
4 Utiliza uma sensação de urgência e limitações em termos de tempo

Se suspeitar que recebeu um e-mail de phishing, siga os nossos procedimentos para o denunciar imediatamente.

O nome e o logótipo DHL são marcas registadas e propriedade intelectual da DHL. A utilização de marcas registadas da DHL está sujeita a um acordo de licença.

Figure 18.1: DHL Phishing Campaign – Portugal user awareness

And the same campaign, in this case, with the language translated for Spanish audience (2973 users):



Response Breakdown

This chart illustrates the actions of your recipients, broken out by response type.

Figure 19.1: DHL Phishing Campaign – Spain results

Once again, we see a significant number of users (20%) that opened the attachment. The margin is shorter between those who opened and those who reported. Compared to the Portuguese audience who see that they are better prepared or at least they are more on alert as 24% reported compared to the 19% from Portugal.

Let’s see again the timeline, that in this scenario the distance between the first reporter and the first susceptible could be not enough for the CyberSOC team to react:

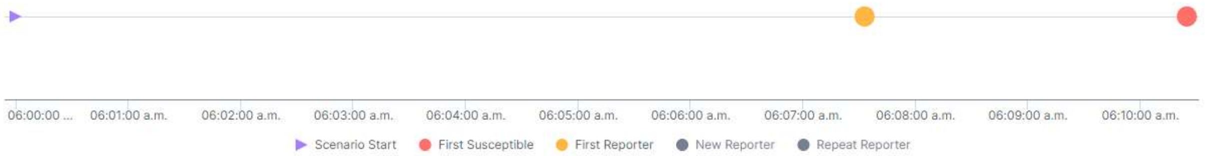
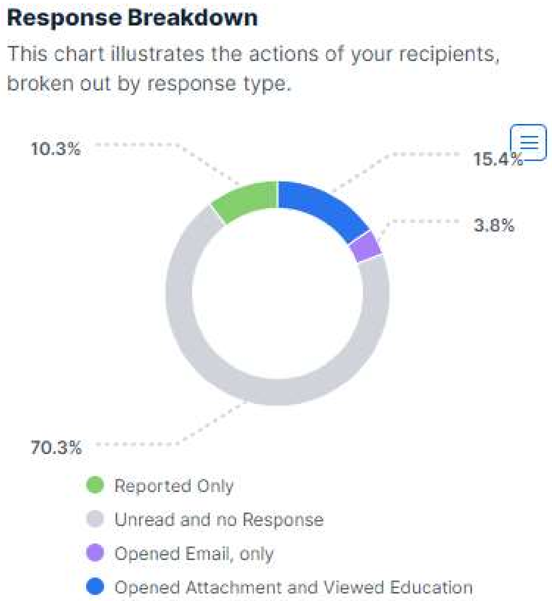


Figure 20.1: DHL Phishing Campaign Spain – Timeline

And the same campaign, with the language adapted for Moroccan audience (233 users):


Response Breakdown

This chart illustrates the actions of your recipients, broken out by response type.

Figure 21.1: DHL Phishing Campaign – Morocco results

In this campaign the behaviour regarding reporting and opening the attachment is different. The first interaction, unfortunately, was opening the attachment instead of reporting.

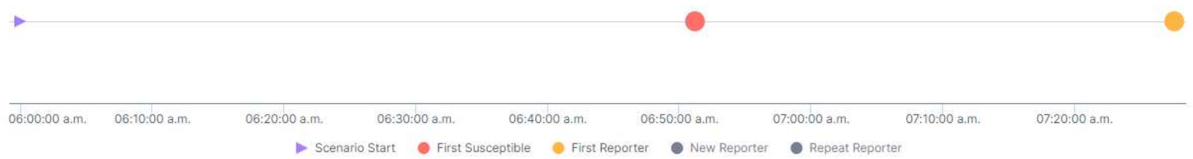


Figure 22.1: DHL Phishing Campaign Spain – Timeline

Regarding the monthly campaigns sent to new users who joined the company last month, we created a specific campaign, where the body of the email says that due to a password policy change, the user need to verify if the user password is compliant, to do so, the user need to click on a link. Once again, when the user clicks on that link, it will be forwarded to a user awareness page confirming that it's a phishing exercise and sharing the best practices to avoid this behaviour. These are the results for the 10 phishing campaigns for new users (new comers) in our perimeter:

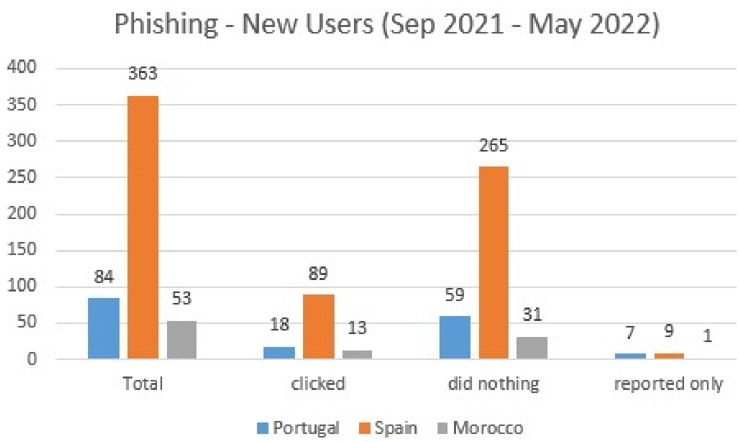


Figure 23.1: Phishing for new users - results

The main conclusions that we extract from this kind of campaigns is that new users either do nothing with the email, which on the one hand is good but on the other hand we consider that the % of users reporting the email as suspicious should be higher. It's necessary to improve the on boarding of these new users by each Human Resources department. Probably, these new users don't receive the necessary user awareness before starting working with their computer or they do but don't understand how to identify and report a malicious e-mail.

The last two campaigns we launched were on 14 June and then on 21 June, 2022. The first one before a user awareness session about Cybersecurity for the Portuguese audience, for both professional and personal. The aim was to launch the campaign and shortly afterwards, during the user awareness session, show the results and explain which indicators we should be aware of when we receive emails with that type of content. The second campaign, just one day after the user awareness session, to see if the message about phishing got through and was understood by the audience. Once again, the results were surprising.

The first campaign consisted of sending an e-mail, once again about a notification from DHL to 578 users, asking the user to confirm the address for an order delivery, and once the user click on the link the user awareness information is shared to the victim. These were the results:

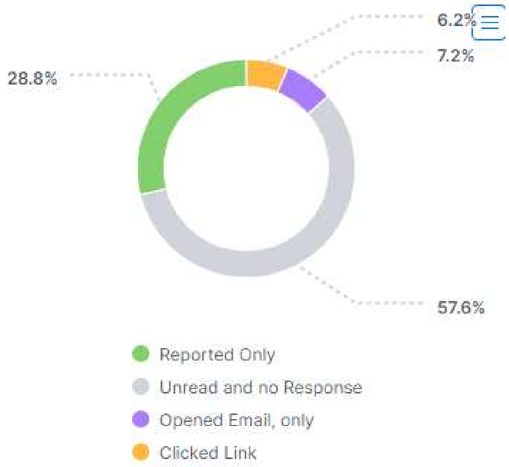
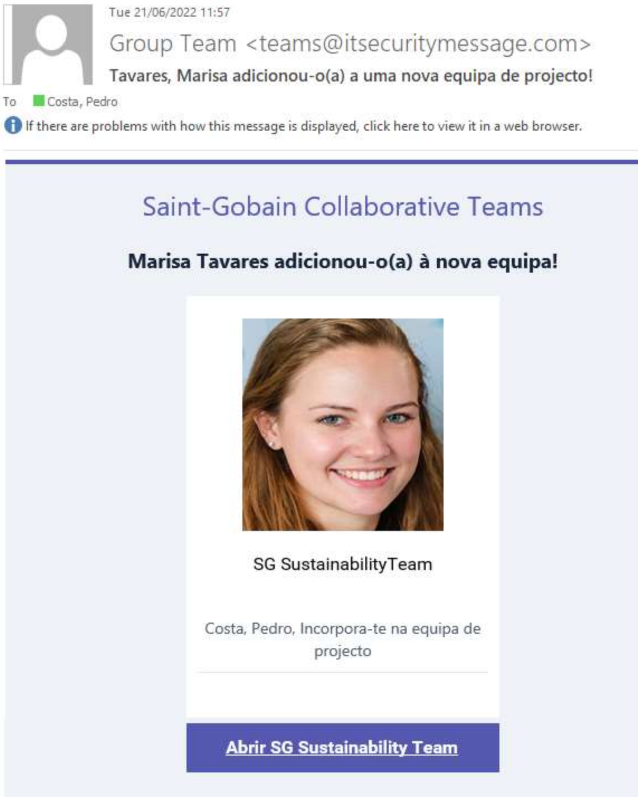


Figure 24.1: Phishing before User Awareness – Portuguese audience

We can see now a progressive improvement in the percentage of users that reported and a decrease in the number of users who clicked on the malicious link. Nevertheless, even for a context (DHL) already used before, we still have 6% of users to think about. After the user awareness session, where we reinforced once again the importance of checking first whether the email is legitimate or not, before clicking on or opening attachments, we launched the second campaign just one day after. Taking advantage of one of the subjects that has been very popular: "The Sustainability", we launched the following phishing email where the photo is from a person that does not exist (using the website: https://this-person-does-not-exist.com/en):



Tue 21/06/2022 11:57

Group Team <teams@itsecuritymessage.com>

Tavares, Marisa adicionou-o(a) a uma nova equipa de projecto!

To 🟩 Costa, Pedro

If there are problems with how this message is displayed, click here to view it in a web browser.

Saint-Gobain Collaborative Teams

Marisa Tavares adicionou-o(a) à nova equipa!

SG SustainabilityTeam

Costa, Pedro, Incorpora-te na equipa de projecto

Figure 25.1: Phishing after User Awareness – Portuguese audience

For the same audience (578 users) these were the results of the campaign:

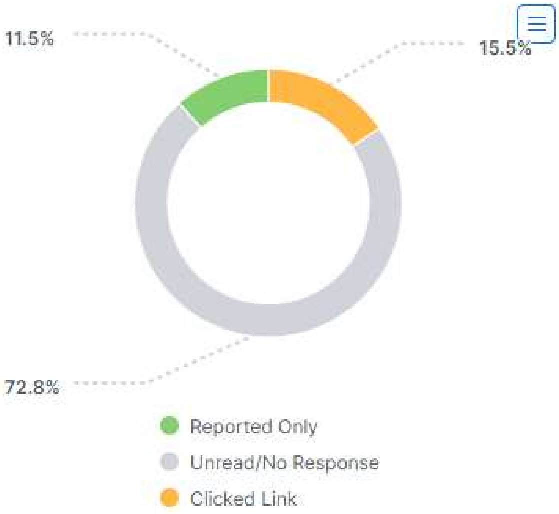


Figure 26.1: Phishing after User Awareness – Portuguese results

Even after a very recent phishing campaign launched, the necessary user awareness with a dedicated webinar for Cybersecurity aspects, we can still see these results. A worrying number (16%) of users clicked on the link. Once again, it’s clear that something need to be done regarding phishing awareness. We have not yet found the formula to enable users to become “Experts” on how to identify malicious e-mails.

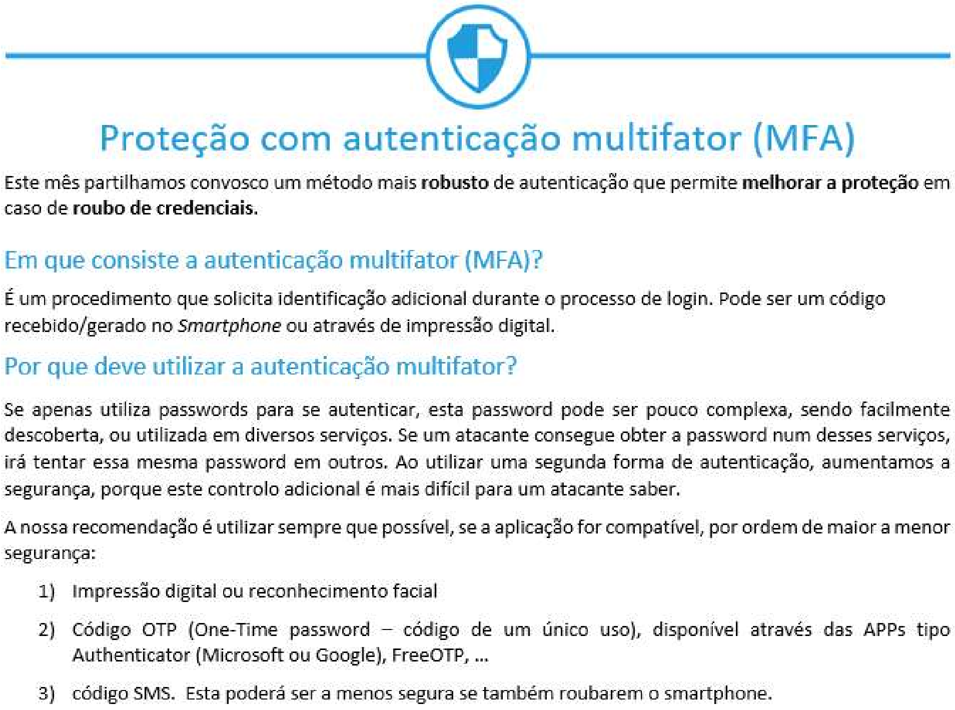
6.4 Monthly Newsletters

In terms of general user awareness, each month, a newsletter is sent with recommendations about cybersecurity aspects, for example, informing users to not connect non-standard or personal devices to the network, to not connect external drives without scanning them before, to not install any kind of software without approval, etc. The problem identified, is that, there is no tracking of who open and read these newsletters, then, it’s not possible to measure the effectiveness. Is something to be considered as a future work to send the emails through a platform that allows traceability (example of Mailchimp).

It was sent 10 newsletters during this internship, mainly about:

- Phishing, Smishing, Vishing awareness
- What is being done to protect how systems
- The conflict between Russia and Ukraine and Cyberattacks
- Best practices and recommendations (Professional and personal)
- Backup solutions at our disposal
- Enhancing security at special moments (Holidays, Vacations, Weekends, overnight)
- Configure robust authentication with strong passwords and MFA/2FA

As explained before, the newsletters are not enough for user awareness. It’s not measured yet, but probably a significant number of newsletters go “directly” to the recycle bin without being read first. Users receive a lot of emails during their working day, the pressure and stress regarding their daily tasks, all these factors do not convey the message through this channel (email). Nevertheless, we keep this strategy as the IT support team for our perimeter send a global newsletter talking about other subjects and is where we include the Cybersecurity subject. This is one excerpt of the last newsletter sent on June with the MFA/2FA subject:



Proteção com autenticação multifator (MFA)

Este mês partilhamos convosco um método mais **robusto** de autenticação que permite **melhorar a proteção** em caso de **roubo de credenciais**.

Em que consiste a autenticação multifator (MFA)?

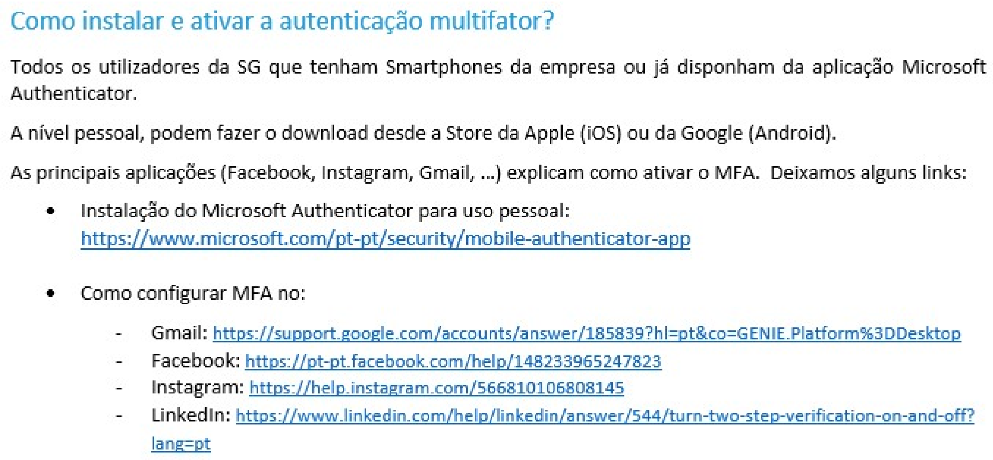
É um procedimento que solicita identificação adicional durante o processo de login. Pode ser um código recebido/gerado no *Smartphone* ou através de impressão digital.

Por que deve utilizar a autenticação multifator?

Se apenas utiliza passwords para se autenticar, esta password pode ser pouco complexa, sendo facilmente descoberta, ou utilizada em diversos serviços. Se um atacante consegue obter a password num desses serviços, irá tentar essa mesma password em outros. Ao utilizar uma segunda forma de autenticação, aumentamos a segurança, porque este controlo adicional é mais difícil para um atacante saber.

A nossa recomendação é utilizar sempre que possível, se a aplicação for compatível, por ordem de maior a menor segurança:

1) Impressão digital ou reconhecimento facial
2) Código OTP (One-Time password – código de um único uso), disponível através das APPs tipo Authenticator (Microsoft ou Google), FreeOTP, …
3) código SMS. Esta poderá ser a menos segura se também roubarem o smartphone.



Como instalar e ativar a autenticação multifator?

Todos os utilizadores da SG que tenham Smartphones da empresa ou já disponham da aplicação Microsoft Authenticator.

A nível pessoal, podem fazer o download desde a Store da Apple (iOS) ou da Google (Android).

As principais aplicações (Facebook, Instagram, Gmail, ...) explicam como ativar o MFA. Deixamos alguns links:

- Instalação do Microsoft Authenticator para uso pessoal: https://www.microsoft.com/pt-pt/security/mobile-authenticator-app

- Como configurar MFA no:
  - Gmail: https://support.google.com/accounts/answer/185839?hl=pt&co=GENIE.Platform%3DDesktop
  - Facebook: https://pt-pt.facebook.com/help/148233965247823
  - Instagram: https://help.instagram.com/566810106808145
  - LinkedIn: https://www.linkedin.com/help/linkedin/answer/544/turn-two-step-verification-on-and-off?lang=pt

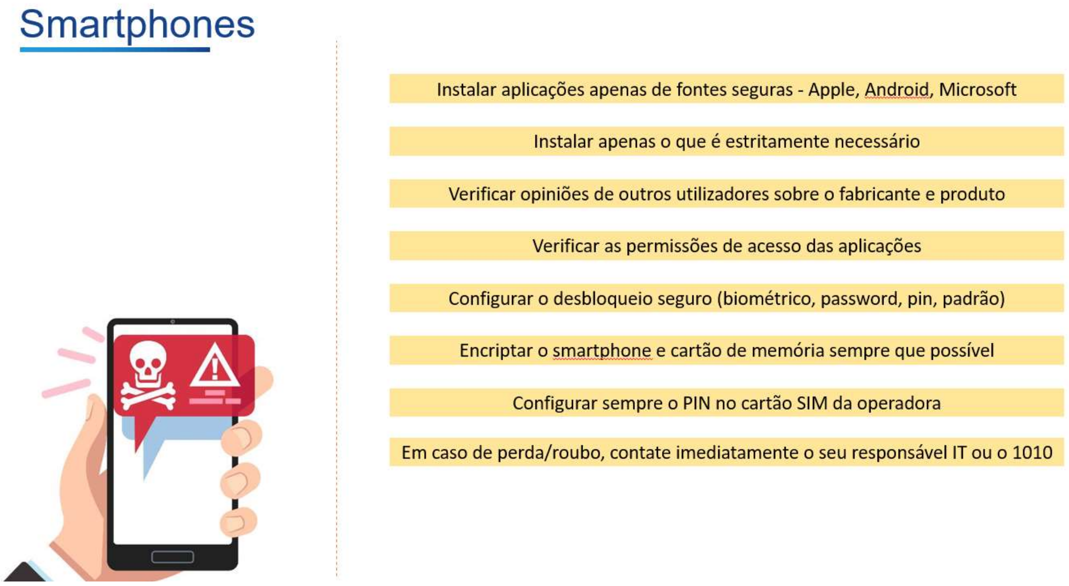
Figure 27.1: June Newsletter – Portuguese version

6.5 Training Sessions and User Awareness

During this internship we did around 6 user awareness sessions and the intention is to increase in the upcoming months. As we are just two persons within our perimeter for Cybersecurity matters, we don’t have enough human resources to perform more awareness sessions as we would like to. It’s our intention to extend the user awareness also to customers and partners, if they know how to protect their environment they will also help us by improving our systems as there are commercial relationships between these parties. In this section we will just highlight the last 4 sessions made for internal users:

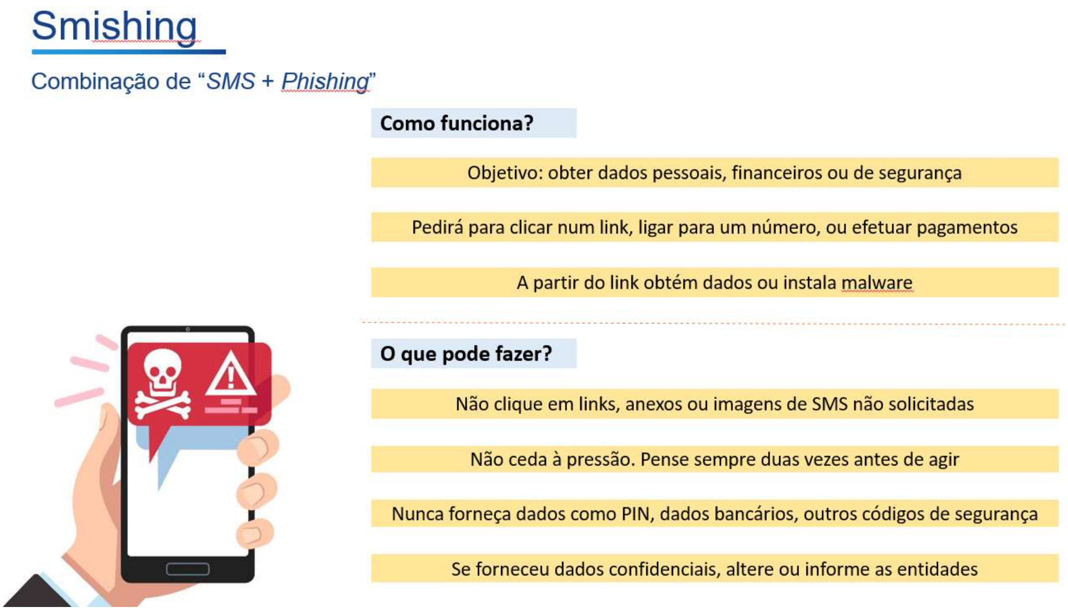
- 21 & 23 June 2022: A user awareness session for all users in Portugal
- May 6, 2022: A user awareness session for users of a newly acquired company
- May 3, 2022: A user awareness session for all users in Portugal

Some examples of the contents included during the user awareness sessions (in Portuguese):



Smartphones

- Instalar aplicações apenas de fontes seguras - Apple, Android, Microsoft
- Instalar apenas o que é estritamente necessário
- Verificar opiniões de outros utilizadores sobre o fabricante e produto
- Verificar as permissões de acesso das aplicações
- Configurar o desbloqueio seguro (biométrico, password, pin, padrão)
- Encriptar o smartphone e cartão de memória sempre que possível
- Configurar sempre o PIN no cartão SIM da operadora
- Em caso de perda/roubo, contate imediatamente o seu responsável IT ou o 1010



Smishing

Combinação de "*SMS* + *Phishing*"

Como funciona?

Objetivo: obter dados pessoais, financeiros ou de segurança

Pedirá para clicar num link, ligar para um número, ou efetuar pagamentos

A partir do link obtém dados ou instala malware

O que pode fazer?

Não clique em links, anexos ou imagens de SMS não solicitadas

Não ceda à pressão. Pense sempre duas vezes antes de agir

Nunca forneça dados como PIN, dados bancários, outros códigos de segurança

Se forneceu dados confidenciais, altere ou informe as entidades

Figure 28.1: User Awareness Session – Portuguese version

After the last user awareness session done in June, a sales and marketing director of one of the subsidiaries of SG in Portugal, invited us to perform a dedicated user awareness during a webinar with architects and civil engineers as target audience. Will be held on 14 July, 2022 in a remote session with users connected from different locations.

In parallel, and somehow related with this internship, we took advantage of some of the contents used on these user awareness sessions with a paper wrote for the seminar of the Master in Informatics Security, under the title: "The Art of Mind Deception – A practical Social Engineering Exercise" and submitted it to the Call for presentations (C-DAYS 2022) organised by the Portuguese Centro Nacional de Cibersegurança (CNCS) and it was accepted. Therefore, the subject of Social Engineering and some of the results of the phishing campaigns carried out within scope of this internship were presented on 7 June, 2022, in Estoril during the C-DAYS 2022 edition [36]. The topic was around Social Engineering, focused on physiological principles that influence us to be the weakest link in this cybersecurity chain. The techniques used by social engineers to exploit our weakness, the lifecycle of a social engineering attack, to better understand the four classic phases:

1. **Information Gathering** (Contacts, network contacts and the relationship between them, Personal and Professional information)
2. **Establish Relationship** based on the information gathered, gain confidence through rapport
3. **Execute / Explore** using specialized techniques such as phishing, smishing, vishing to extract information, access to resources, destroy data, among others
4. **Leave** without being discovered and without leaving a trace

There are different approaches for the life cycle of a Social Engineering attack, but typically converge in four or five phases. The important thing in conveying this information for users is that they understand the risks they are facing in the different phases. Also explained future (current) threats with the Depp Fake, where attackers are taking advantage to develop cleaver techniques. At the end of the presentation the feedback from the audience was positive, which also motivated us to participate in other events where these themes can be discussed. We consider fundamental to understand human behaviour in order to improve the user awareness raising by reducing this recognised risk, the human (user) behaviour.

Back to the June sessions, in each one (2 at total), we asked users to fill a short questionnaire in order to evaluate the session and also to understand their perception about phishing and the confidence they have or not have about the security of the SG group's information systems. Other questions such as the age range, the gender and their qualifications were also collected but will be used for future work. The idea here is to try to correlate the users that was deceived by phishing campaigns with their profile (male/female, age, qualifications).

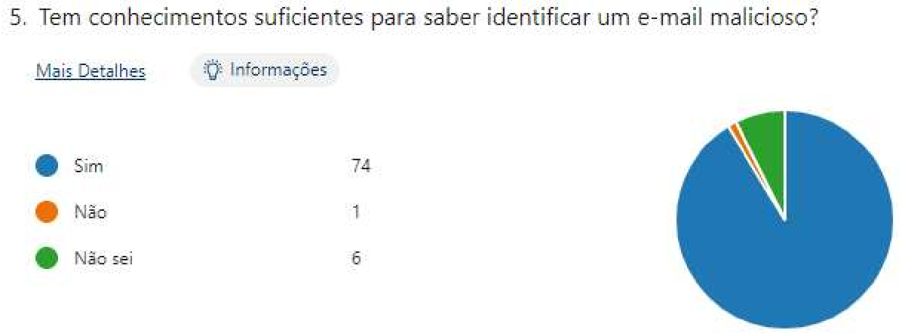
We were able to collect 81 answers, where 74 of them answered the optional question: *How would you rate this Cybersecurity awareness session?* And the result was very satisfying and motivating:

74
Respostas

★★★★★
Classificação Média de 4.74

Figure 29.1: User Awareness Questionnaire – Rating

This is for sure a good feedback and a boost to continue with this kind of awareness. We also asked if the user have enough knowledge to identify a malicious email, with this result:

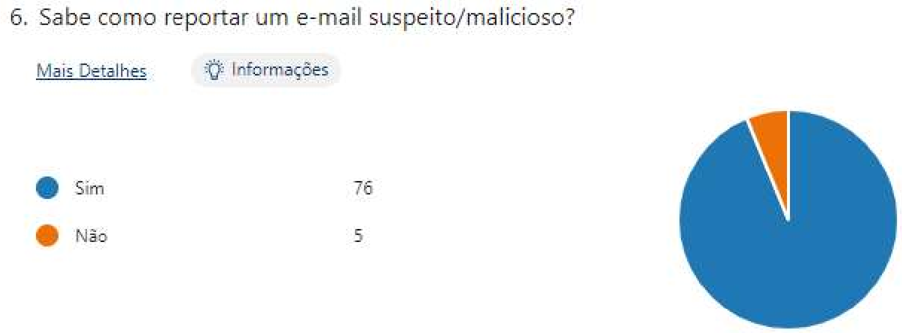


5. Tem conhecimentos suficientes para saber identificar um e-mail malicioso?

● Sim	74
● Não	1
● Não sei	6

Figure 30.1: User Awareness Questionnaire – identify malicious email

There is a significant number of users who indicate that they are able to identify a malicious email (despite the results of the last campaigns). During the user awareness session, we explained how should we report a suspicious e-mail, therefore, we did the following question: Do you know how to report a suspicious e-mail? And the result was:

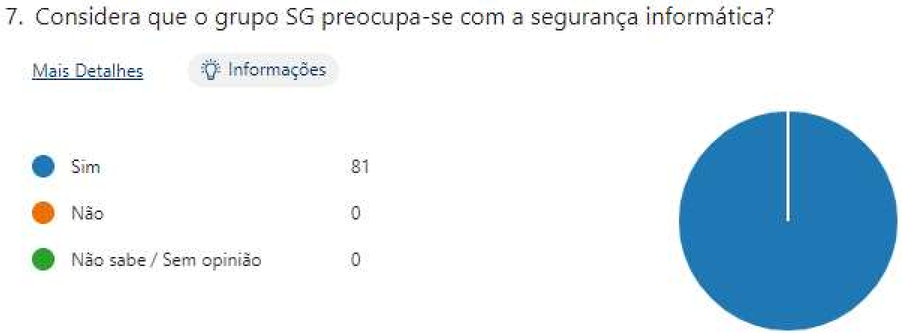


6. Sabe como reportar um e-mail suspeito/malicioso?

● Sim	76
● Não	5

Figure 31.1: User Awareness Questionnaire – Report malicious email

Once again, an expressive number of users answered positively that they know how to report (despite the results about reporting on the last phishing campaigns). We also asked if they consider that the SG group is concerned about Cybersecurity, and the feedback was also interesting and motivate our continuous improvement:

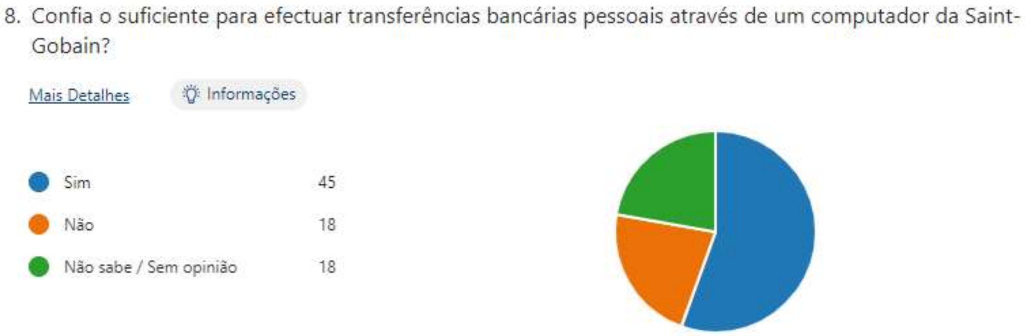


7. Considera que o grupo SG preocupa-se com a segurança informática?

● Sim	81
● Não	0
● Não sabe / Sem opinião	0

Figure 32.1: User Awareness Questionnaire – SG security perception

And the last question was to understand if based on the previous question, users feel enough confidence to perform personal banking transfers using the corporate network, these were the results:



8. Confia o suficiente para efectuar transferências bancárias pessoais através de um computador da Saint-Gobain?

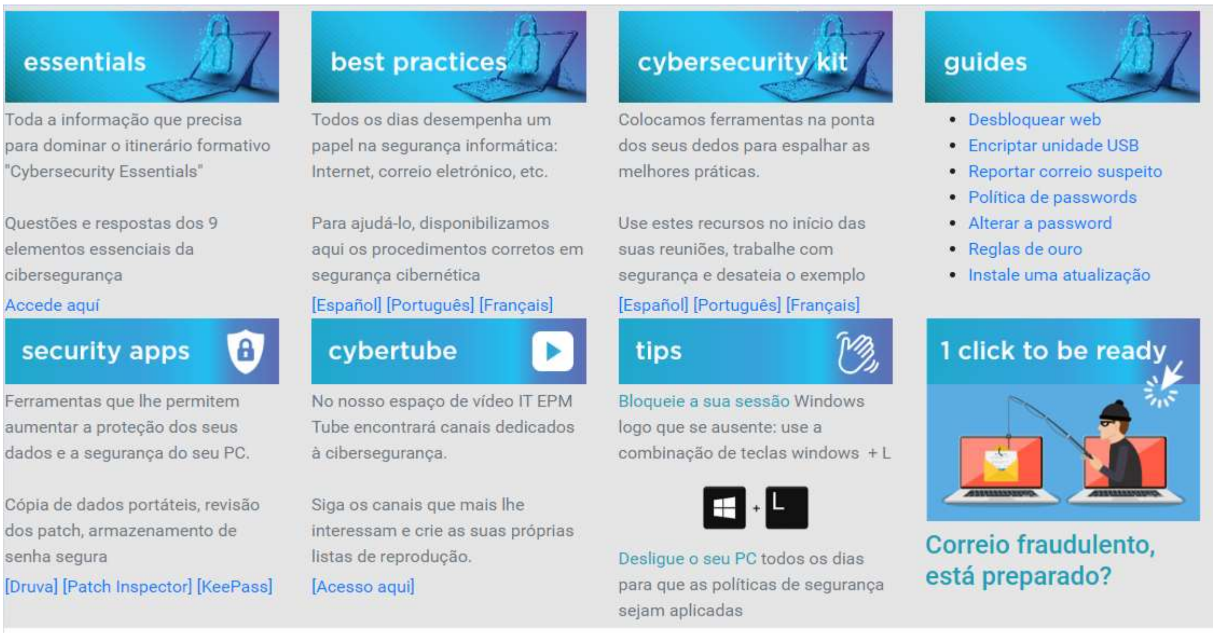
● Sim	45
● Não	18
● Não sabe / Sem opinião	18

Figure 33.1: User Awareness Questionnaire – Personal bank transfers

Furthermore, the user awareness is also extended for specific situations. For example, each time a user generates a security incident, either because they connected an infected USB storage device, or tried to download a malicious software. The idea behind is to make the user aware of the risk of such behaviour, not only for the compromise of their data, but also, and most importantly for the entire organisation. Therefore, for each incident generated we sent a user awareness email with a set of recommendations regarding cybersecurity, putting in copy their IT responsible.

In the phishing awareness, in the newsletters, in the dedicated awareness for users that generated an incident and also during the user awareness sessions, we share the link to our Intranet portal dedicated to Cybersecurity. There is a dedicated section for Q&A, best practices, how to keep the workstation updated, how to create strong passwords and how to protect them by using a secure password vault instead of papers, word or excel files. A set of images that users could use in their presentation, mainly for managers where they have the opportunity to share this contents before they start a meeting with their collaborators.

A short example of the content at user disposal in the Intranet:



essentials

Toda a informação que precisa para dominar o itinerário formativo "Cybersecurity Essentials"

Questões e respostas dos 9 elementos essenciais da cibersegurança

Accede aquí

best practices

Todos os dias desempenha um papel na segurança informática: Internet, correio eletrónico, etc.

Para ajudá-lo, disponibilizamos aqui os procedimentos corretos em segurança cibernética

[Español] [Português] [Français]

cybersecurity kit

Colocamos ferramentas na ponta dos seus dedos para espalhar as melhores práticas.

Use estes recursos no inicio das suas reuniões, trabalhe com segurança e desateia o exemplo

[Español] [Português] [Français]

guides

- Desbloquear web
- Encriptar unidade USB
- Reportar correio suspeito
- Política de passwords
- Alterar a password
- Reglas de ouro
- Instale uma atualização

security apps

Ferramentas que lhe permitem aumentar a proteção dos seus dados e a segurança do seu PC.

Cópia de dados portáteis, revisão dos patch, armazenamento de senha segura

[Druva] [Patch Inspector] [KeePass]

cybertube

No nosso espaço de vídeo IT EPM Tube encontrará canais dedicados à cibersegurança.

Siga os canais que mais lhe interessam e crie as suas próprias listas de reprodução.

[Acesso aqui]

tips

Bloqueie a sua sessão Windows logo que se ausente: use a combinação de teclas windows + L

+ L

Desligue o seu PC todos os dias para que as políticas de segurança sejam aplicadas

1 click to be ready

Correio fraudulento, está preparado?

Figure 34.1: Cybersecurity Intranet – Example of contents available

In general, it was clear that we (and organisations as a whole) must invest not only in Next-Generation defence software, but also, understand that defence technologies are becoming increasingly sophisticated, leading the attackers to also leverage the use of more sophisticated social engineering techniques to exploit the human weakness. To better secure an organisation in this digital field, it is vital that all employees understand the risks, not only for them but essentially for the whole organisation.

The Security Awareness Escape room

Our understanding, during the research about User Awareness is that a gamified approach could be the "solution" to improve the way we do cyber security awareness training today. The learning experience of this kind of approach with the use of Team Building, could help raising the awareness that is missing nowadays.

The concept is based on taking advantage of what has already been done with the well-known Escape Room concept. The employees are dared to solve a set of challenges with a certain time to complete the game. For example, the employees could be challenged to unlock a workstation infected by a malware that within a certain period of time will be infected with a Ransomware. This will allow that employees could test their cybersecurity knowledge and in parallel learn secure best practices in their daily life. Different subjects could be explored such as:

- Identify Phishing emails
- Understand how they should protect sensitive/confidential data
- Understand and defend against Social Engineering Attacks
- How to create strong passwords and where they shall be stored
- How to use public Wi-Fi (e.g. Hotels, Airports, Coffee shops)
- Among others

The consultant Deloitte has a very interesting article [37] about Escape Room as an effective cybersecurity learning approach to be taken into account to better understand the effectiveness, systematised by them as follows:

Effective Learning Model	4 Learning Styles	A.G.E.S model for change
70/20/10 principle 70% on the job learning, learning by doing 20% learning and developing through interaction 10% learning through structured courses and training (Lombardo & Eichinger, 1996)	**Activists**: learn by doing. **Theorists**: seek to understand the theory behind the action **Pragmatists**: want to know how to put what they're learning into practice in the real world **Reflectors**: learn best by watching people and thinking about what is happening (Honey & Mumford, 1982)	**Attention**: sufficient attention to the learning, brain tends to lose focus after 20 minutes **Generation**: process of creating your own connections to new ideas. **Emotion**: positive emotional arousal activates our brain and accelerates the formation of new memories. **Spacing**: memories grow over time, people remember best when learning is spaced out over time (and includes one or more nights of sleep). (Neuroscience Institute)

Table 23: Escape Room as an effective learning approach (Source: Deloitte [35])

And it seems to be a cost effective learning approach as demonstrated by Deloitte:

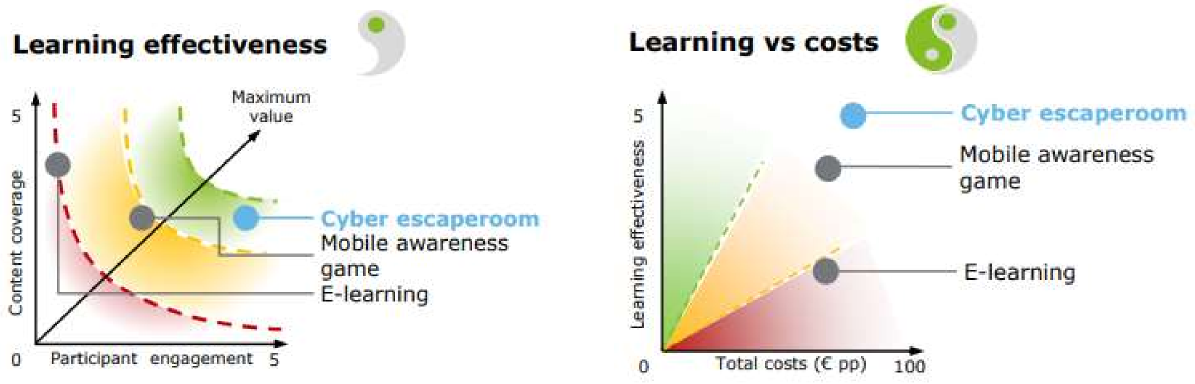


Figure 35.1: Escape Room – Learning effectiveness (source: Deloitte [37])

Another possibility we discussed, although not further explored during this internship, would be to create a "War Room", with two teams of employees: The Red and Blue Teams. The employees are challenged to be part of the Red Team (who attack) and Blue Team (who protect). This could be also a tempting challenge by having users compete against each other and learning at the same time the risks they face on their daily life and how to protect against them.

Chapter 7
Conclusions and Future Work

The increasing number of devices connected to the network has brought new challenges, especially in terms of security. Either because Internet of Things has driven this evolution, where almost everything can be connected to the network, or even due to the fourth Industrial Revolution where the industry to be competitive need to follow this revolutionary era. For many years we have been hearing about “Technological unemployment” as a consequence of the evolution of technology towards human being. Every day we have more tasks, processes and services used to be done by the human being and which today are done by a “Machine” – digitalisation of processes, the Robots on production lines, toll payments systems, among others.

Nowadays the wars are not only made with troops, aircrafts, cruise missiles, tanks or even nuclear weapons. The Cyber War is another concern for us and all the great powers and nations who aim to be, are investing heavily in this area. The recent conflict between Russia and Ukraine follows this pattern. The Russian military entered the Ukrainian border on February 24, 2022, nevertheless, the first “shots” were fired days or even hours before with destructive cyberattacks against Ukraine. Since the cyberspace is quite extensive, the collateral damage didn’t take long to be felt by other countries, nations and organisations. In fact, as explained at the very beginning of this report, Saint-Gobain suffered the collateral damage of the NotPetya Ransomware attack of Russia against Ukraine.

All these factors lead to a redefinition of the strategy to guarantee the security in the cyberspace. A big challenge ahead of us, but here we are, better prepared. As defenders, we have more and more assets to protect under our umbrella. But for those acting as attackers, this is something positive that can and should be exploited. We mean “should be” in the sense, that as defenders we also get our lessons learned from their attacks on how to improve the security of the cyberspace. However, they are clearly in advantage since it is easier to attack than to defend in an environment where it is almost impossible to control everything that is connected.

In this internship we proposed an approach based on the best practices that fundamentally are under the umbrella of control and risk management frameworks. For this, the controls are essential to build a resilient Information Security Management System, therefore, the ISO/IEC 27002 for controls, the ISO/IEC 27005 for risk management, the CIS CSC version 8 and also the NIST Cybersecurity Framework were crucial. All these standards/frameworks cover the objectives that this internship has set out to achieve, that’s the reason why the choice of title: “Implementing a Framework for Continuous Improvement in Cybersecurity”. The CIS Critical Security Controls in its eighth version was the source of inspiration which served as a basis to support the achievement of each objective.

We consider that the results obtained during this internship, allowed us to perceive the weak points that exist in our perimeter, thus improving their protection and even for those out of our scope we escalated whenever possible to the central cybersecurity team. We can say with conviction that our perimeter is certainly one of the most protected perimeter, following the policies, guidelines, standards of the group. In fact, the feedback received from our correspondents in the central team is very positive encouraging us to continue.

Even knowing that the Integration of Security into Projects is a difficult process for all stakeholders, we feel that they now better understand the relevance of the process. The early we can identify flaws or vulnerabilities in the project, the less the issue will cost and of course the easier it will be to remedy. In the case of the Security Awareness Program, the actions made during this internship are showing, especially in this final phase, that users are increasingly interested in cybersecurity, with more regular contacts with the IT Teams whenever they see a suspicious activity. The recent cyberattacks against recognized organisations, such as the case of Vodafone Portugal, Hospital Garcia de Orta, the clinical laboratories of Germano de Sousa, among others, came to alert people that we are all subject to suffer a cybersecurity incident with greater or lesser impact on our daily lives.

For future work it's necessary to improve the way in which the Internal Control Plan is currently managed. For that we need to wait for the new tool which is currently under development by the central team that will be used to implement, monitor and remediate the controls. For instance, following an agile approach, allowing the central team to have continuous access to the KPI's of each perimeter. At this moment this is done manually, at least, once per year. If we want to have a resilient cybersecurity posture every perimeter need to follow the same pace and it's also important to have the executive management support

In addition, regarding the Integration of Security into Projects, there is room to improve the methodology in use. For instance, the central team is also working to improve the tool to be more web-based on the actual PSAT excel file which slows down the life cycle of a project. The way we control the current status of a project is through the use of Microsoft OneNote and weekly meetings with the Infrastructure manager who in almost of the projects need to be involved. If we have a central tool, web-based, we can define workflows, reduce the number of deliverables based on an initial checklist that will define the corresponding workflow. Every stakeholder can access the tool and see the current status and directly contact them to speed up the progression to the next stage (Go-Design/Study ➔ Go-Realisation ➔ Go-live).

Furthermore, this work could also be improved with respect to the Security Awareness Program as we found that there is still a long way to go and improve. The Escape Room concept could be one of the next methodologies to challenge the central team to implement in the organisation or at least to allow within our perimeter. Probably, there might be budget constraints that could delay the implementation of this kind of learning.

As already mentioned during this report, the human being is considered the weakest link in cybersecurity landscape. Are we doing enough to improve users' awareness about the risks?

This page is intentionally left blank.

References

[1] Center for Internet Security. *CIS Critical Security Controls*, version 8. May 2021

[2] Petya Ransomware, Alert (TA17-181A). https://www.cisa.gov/uscert/ncas/alerts/TA17-181A, July 2017. Accessed: 2021-10-03.

[3] New Variant of Petya Ransomware Spreading Like Wildfire. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/ Accessed: 2021-10-04.

[4] PCI Security Standards Council. PCI DSS, Requirements and Security Assessment Procedures, version 3.2.1. Page 5, May 2018.

[5] International Standard. ISO/IEC 27001:2013 (SE), Page 5, October 2010

[6] Julia Heron. ISO 27001:2013 and ISO 27001:2017 what's the difference? https://www.isms.online/iso-27001/iso-27001-2013-iso-27001-2017-whats-the-difference/ Accessed: 2021-11-20.

[7] Luke Irwin. ISO 27001 Annex A controls explained. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained Accessed: 2021-11-21.

[8] ISO 27001:2013 Information Security Implementation Guide. https://www.sans.org/blog/cis-controls-v8/ Accessed: 2021-12-21.

[9] NIST SP 800:53 Revision 5. September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf Accessed: 2021-12-20.

[10] CIS Critical Controls - Implementation of CIS Controls V8. https://www.gat.digital/blog/implementacao-de-controles-cis/ Accessed: 2021-12-22.

[11] NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. April 2018 Accessed: 2021-10-03.

[12] CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/. Accessed: 2021-12-23.

[13] Executive order 13636 – Improving Critical Infrastructure Cybersecurity. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity Accessed on 2021-12-27 Accessed: 2022-01-03.

[14] "The seven performance steps to managing risk, the NIST way". https://www.doublechecksoftware.com/the-seven-performance-steps-to-managing-risk-the-nist-way/ Accessed: 2022-01-03.

[15] "CIS Critical Controls: Industry Frameworks Recognition". https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/ Accessed: 2022-01-08.

[16] CIS Critical Security Controls Navigator. https://www.cisecurity.org/controls/cis-controls-navigator/ Accessed: 2022-01-08.

[17] ANSSI – Agence Nationale de la sécurité des systèmes d'information. https://www.ssi.gouv.fr/en/publications/. Accessed: 2022-02-03.

[18] CNCS – Centro Nacional de Cibersegurança. https://dyn.cncs.gov.pt/pt/boaspraticas/. Accessed: 2022-02-04.

[19] CISA – Cybersecurity & Infrastructure Security Agency. Shields Up. https://www.cisa.gov/shields-up Accessed: 2022-03-01.

[20] ENISA – European Union Agency for Cybersecurity. https://www.enisa.europa.eu/. Accessed: 2022-03-02.

[21] MITRE ATT&CK. https://attack.mitre.org/ Accessed: 2022-05-08.

[22] "What's the difference between ISO 27001:2013 and ISO27001:2017?" https://qcsl.co.uk/whats-the-difference-between-iso-270012013-and-iso270012017/ Accessed: 2022-06-11.

[23] Gregory, Peter H. (2018). CISM: Certified Information Security Manager. McGraw-Hill Education

[24] Terranova Security. "How to Build a Strong Security Awareness Program in 2021". https://terranovasecurity.com/how-to-build-a-strong-security-awareness-program-in-2021/ Accessed: 2022-04-23

[25] Bill Gardner, Valerie Thomas. Building an Information Security Awareness Program. Syngress, 2014

[26] CISA. Shields UP – Guidance for all organisations. https://www.cisa.gov/shields-up Accessed: 2022-03-29

[27] NIST CSF. The Five Functions, https://www.nist.gov/cyberframework/online-learning/five-functions Accessed: 2021-10-22

[28] Security Affairs. Introduction to the NIST CSF for a Landscape of Cyber Menaces. https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html Accessed: 2022-05-12

[29] NIST SP 800-207. Zero Trust Architecture. https://csrc.nist.gov/publications/detail/sp/800-207/final Accessed: 2021-12-08

[30] Top 20 Most Common Types of Cybersecurity Attacks. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks, Accessed: 2022-06-28

[31] Data Guard. ISO 27001 vs. ISO 27002 - How are they different? https://www.dataguard.co.uk/blog/iso-27001-vs-iso-27002/ Accessed: 2022-06-12

[32] ISO/IEC 27002 Third Edition. Information security, cybersecurity and privacy protection — Information security controls. ISO/IEC, 2022

[33] isms.online. ISO 27002 Ultimate Guide. https://www.isms.online/iso-27002/ Accessed: 2022-06-13

[34] Impact vs Probability. https://twitter.com/xsfera/status/1139080973533044736?lang=ar-x-fm Accessed: 2022-07-01

[35] Bleeping Computer. New Microsoft Office zero-day used in attacks to execute PowerShell. https://www.bleepingcomputer.com/news/security/new-microsoft-office-zero-day-used-in-attacks-to-execute-powershell/ Accessed: 2022-07-01

[36] C-DAYS 2022. Call for Presentations. “The Art of Mind Deception: A Practical Social Engineering Exercise”. https://www.c-days.cncs.gov.pt/schedule/ Accessed: 2022-07-02

[37] Deloitte. Cybersecurity Awareness Escape Room. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cyber-risk-the-security-awareness-escape-room.pdf Accessed: 2022-07-03

[38] C. Hadnagy and S. Schulman, “Human Hacking”, Harper Business, 2021

[39] K. Mitnick and N. Sullivan, “The Art of Deception”, Wiley Publishing, Inc, 2002

[40] P. Carpenter and K. Roer, “The Security Culture Playbook”, WILEY, 2022

This page is intentionally left blank.

Appendix A
The 95 Controls Implemented

Below we list the 95 (ninety-five) controls implemented and monitored during this internship:

Control Category	Title	Short Description
1: Inventory and Control of Hardware Assets	1.1: Utilize an Active Asset Discovery Tool	Utilize an active asset discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
	1.2: Use a Passive Asset Discovery Tool	Utilize a passive discovery tool (e.g. Agent on servers , …) to identify devices connected to the organization's network and automatically update the organization's Hardware asset inventory.
	1.4: Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets (focus PCs) with the potential to store or process information. This inventory shall include all Hardware assets (except removable devices), whether connected to the organization's network or not.
	1.5: Maintain Asset Inventory Information	Ensure that the Hardware asset inventory records the network address, Hardware address, machine name, data asset owner, and entity related to each asset and whether the Hardware asset has been approved to connect to the network.
	1.6: Address Unauthorized Assets	Ensure that unauthorized assets are decommissioned according to a defined procedure or the inventory is updated in a timely manner.
2: Inventory and Control of Software Assets	2.1: Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software(with associated Business Owner) that is required in the enterprise for any business purpose on any business system.
	2.2: Ensure Software Is Supported by Vendor	Ensure that only software on which rely the applications (and currently supported by the software's vendor) are added to the organization's authorized software

		inventory. Unsupported software should be tagged as unsupported in the inventory system.
	2.3: Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
	2.4: Track Software Inventory Changes	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
	2.5: Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the Hardware asset inventory so all devices and associated software are tracked from a single location.
	2.6: Address Unapproved Software	Ensure that unauthorized software is removed
3: Continuous Vulnerability Management	3.4: Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
	3.5: Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
	3.6: Compare Back-to-Back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
4: Controlled Use of Administrative Privileges	4.1: Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts on PCs, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
	4.2: Change Default Passwords	Before deploying any new PC asset, change all default passwords to have values consistent with administrative level accounts.
	4.3: Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

	4.6: Use Dedicated Workstations for All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
	4.7: Limit Access to Scripting Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
	4.8: Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	5.1: Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized applications and software.
	5.2: Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates (PCs).
	5.3: Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
6: Maintenance, Monitoring and Analysis of Audit Logs	6.1: Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
	6.2: Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
	6.3: Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
	6.4: Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.

8: Malware Defences	8.2: Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis (workstation).
	8.4: Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
	8.5: Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.
9: Limitation and Control of Network Ports, Protocols and Services	9.1: Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.
	9.2: Ensure Only Approved Ports, Protocols and Services are Running	Ensure that only network ports, protocols, and services listening on a system (PC) with validated business needs, are running on each system (e.g. Operating System,…).
	9.4: Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
	9.5: Implement Application Firewalls (e.g. Palo Alto, …)	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.
10: Data Recovery Capabilities	10.1: Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.
	10.2: Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system (server Standard systems).
	10.3: Test Data on Backup Media	Test data integrity on backup media at least once a year, by performing a data restoration process to ensure that the backup is properly working (Server Standard).

	10.4: Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
	10.5: Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.
11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	11.2: Document Traffic Configuration Rules	Document Traffic Configuration Rules
	11.3: Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.
	11.4: Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.
	11.5: Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.
	11.6: Use Dedicated Workstations for All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
	11.7: Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

12: Boundary Defence	12.1: Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries. (VLAN Segmentation)
13: Data Protection	13.1: Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.
	13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
	13.4: Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.
14: Controlled Access Based on the Need to Know	14.2: Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfil their specific responsibilities.
	14.4: Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.
	14.6: Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
	14.7: Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.
	14.8: Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

15: Wireless Access Control	15.1: Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.
	15.4: Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.
	15.5: Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.
	15.6: Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.
	15.9: Disable Wireless Peripheral Access to Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
16: Account Monitoring and Control	16.1: Maintain an Inventory of Authentication Systems	Automatically lock workstation sessions after a standard period of inactivity.
	16.10: Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.
	16.11: Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.
	16.2: Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud applications.
	16.3: Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.
	16.6: Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.

	16.7: Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.
	16.8: Disable Any Disassociated Accounts	Disable any account that cannot be associated with a business process or business owner.
	16.9: Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.
17: Implement a Security Awareness and Training Program	17.3: Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
	17.4: Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
	17.5: Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
	17.6: Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
	17.7: Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.
	17.8: Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
	17.9: Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

18: Application Software Security	18.1: Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.
	18.10: Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
	18.11: Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.
	18.2: Ensure That Explicit Error Checking Is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
	18.3: Verify That Acquired Software Is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.
	18.4: Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.
	18.5: Use only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.
	18.6: Ensure Software Development Personnel Are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

	18.7: Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.
	18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a tools for communicating with Group Cybersecurity
	18.9: Separate Production and Non-Production Systems	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.
19: Incident Response and Management	19.5: Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.
	19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
	19.7: Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response Exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.
20: Penetration Tests Exercises	20.2: Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
	20.8: Control and Monitor Accounts Associated With Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
21.Data Center Management	21.1: Data Center Compliance Status	"Review and validate the compliancy of the different rules that should be followed in every Data Center room.

22.Third Party - Security Management	22.1 : Integration of security in contract	Maintain an inventory of Security Insurance Plan integrated on each contract with Services Providers or suppliers .The Security Insurance Plan must be periodically reviewed with the Service Provider to identify way of improvements ..
23.Integration of Security into Projects	23.1 : Integration of security in project	Maintain the list of upcoming projects to be studied. This list must make it possible to ensure that each project for global business and for the dedicated business site has its PSAT.