ONE INFORMATION ARCHITECTURE FOR THE NATIONAL REFERENCE FRAMEWORK FOR CYBERSECURITY

Edna Stella Batista Quaresma
Master Thesis Extended Summary

Instituto Superior Técnico

Outubro 2021

Abstract

In the Portuguese context, the transposition of European directives for this purpose led the National Cybersecurity Center to gather a set of measures for information security risk mitigation in the National Reference Framework for Cybersecurity (NRFCS). This dissertation focus is to look for a method supporting the implementation of the measures described in this document, or to simplify the implementation validation. Based on the analysis of the set of implementation evidences foreseen by the document, and through techniques covered by enterprise architecture discipline, these evidences were verified and treated as information entities, in order to translate the structure of the documentation designed by NRFCS.A tool based on information entities was developed aiming to support an organization to assess its level of compliance with the measures determined by NRFCS. A case study was carried out reflecting the reality of AMA, which provided satisfactory demonstration of results
Keywords: Cybersecurity, Information Security, QNRCS, CNCS, Information Architecture.

1. Introduction

After listing the implementation evidences of the NRFCS security measures, raised the need of finding a different name for each evidence, in order to uniquely identify them in the context of the document under study. With a strong sense of enterprise architecture, these documents are treated as information entities, and form the basis of the developed tool. This tool offers to an organization, the possibility to assess the status of implementation of security processes required for by NRFCS, facilitating the determination of the AS-IS status of the organization, regarding cybersecurity or information security. For organizations who intend to start implementing the measures, the tool contributes to the construction of a TO-BE vision, showing the failures or lacks in their implementation of the processes suggested in accordance with European regulations, within the scope of ISO 27001, da Directive (UE) 2016/1148, and similar norms. This study intends to offer an objective contribution, through the integration of the knowledge expressed in NRFCS with concepts of enterprise architecture, offering as a result a list of information entities that make up the information architecture here proposed, faithful to the context of the document under study. Presenting an information architecture of the information security processes referred to by NRFCS, based on information entities, is a concept clearly expressed in the TOGAF meta-model, which allows to unequivocally demonstrate which information structure is to be implemented or being implemented, clarify how it approaches to the information architecture designed by the Information Security Strategy defined in the NRFCS. This research is intended to complement the NRFCS and support organizations that intend to initiate or to assess the current state of its security measures implementation. This listing is intended to be used as checklist, to validate an organization's documentation, with the purpose of verifying the existence of the documents required by NRFCS. This information will allow us to conclude on the state of preparation or possible gaps, in the documentation that makes up the information architecture or in the information security processes. Given the relationship expressed in the NRFCS, between these information entities and the COBIT 5 processes, the developed tool allows the possibility to offer a view of the processes implemented, through the existence of referred information entities.

2. Motivation

The implementation of a business architecture including cybersecurity in Portugal, has NRFCS as a reference. This document transposes the European cybersecurity directives to the national scope, contemplating the implementation of risk mitigation measures. These measures are grouped by the objectives of identifying, protecting, detecting, responding and recovering.

It is increasingly evident for organizations, the need for an enterprise reference architecture, which favors the implementation of requirements, in accordance with regulations and legislation. According to NRFCS, risk management is strongly supported by incident management, which depends on the existence and constant analysis of security events records. These records, are part of the set of documents representing information entities, which along with other structural documents such as strategies, plans or policies, form the information architecture defined by NRFCS. Despite the recognition that the management of information security incidents is increasingly considered by organizations, there is little certainty about which model to implement to ensure efficient information management.

The main motivation of this investigation is to contribute so that organizations can review their information architecture, ensuring compliance with the main requirements of NRFCS. A case study will be presented, with the target organization being the Administrative Modernization Agency (AMA), a public institute responsible for the promotion and development of administrative modernization in Portugal.

3. Basic Concepts and Related Work

In defense of Cybersecurity and the concern with protecting systems against threats that can compromise business continuity, and in the commitment to sharing knowledge, normative and regulatory measures were born and grew, with the purpose of conducting the implementation of architectures aimed at include these security objectives. In Europe, the measures adopted are strongly driven by standards such as ISO/IEC 27001, ISO/IEC 27032 and ISO 22301 which guide systems to achieve these security goals, integrating risk management and information security management plans for data and for critical assets. Directive (EU) No. 2016/1148, of the European Parliament and of the Council, of 6 July was released public and it was determined that each member state of the EU has the responsibility to define a national strategy for the security of networks and information systems, as well as the creation of bodies for strategic cooperation and exchange of information. In Portugal, National Security Office/National Cybersecurity Center (CNCS) would lead the process of transposing the SRI Directive into the national legal system. In the Resolution of the Council of Ministers 92/2019 (RCM 92/2019) and Resolution of the Council of Ministers 41/2018 (RCM 41/2018), technical guidelines for the Public Administration are defined regarding the security architecture of networks and systems of information, and the National Framework of Reference for Cybersecurity (NFRCS) is presented as a transposition of European regulations, in particular Directive (EU) 2016/1148, and in accordance with ISO 27001 standards. The document allows organizations to reduce the risk associated with cyber threats, providing the bases for implementing the minimum security requirements of networks and information systems, reflecting the Portuguese organizational reality and responding to the need to implement measures for the Identification, Protection, Detection, Response and Recovery of threats to the security of the cyberspace [7][2][5].

3.1. World wide

All over the world, governments have created new security systems or improved existing systems, regulated by international guidelines and cooperating internationally for the common purpose of cybersecurity. BSI presents a juxtaposition of both, concluding that there is a clear conceptual overlap. Although NCSC CAF presents an objective-based assessment, the overlap is very evident when comparing ”Objective A” (*Managing security risk*) with ”Segment Identify”. Similar to these *frameworks* the NRFCS is distributed over five objectives, in a very direct relationship with the NIST CSF illustrated in figure 1.

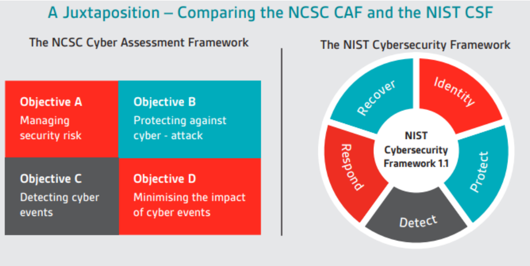

A Juxtaposition – Comparing the NCSC CAF and the NIST CSF
The NCSC Cyber Assessment Framework
Objective A
Managing security risk
Objective B
Protecting against cyber - attack
Objective C
Detecting cyber events
Objective D
Minimising the impact of cyber events
The NIST Cybersecurity Framework
Recover
Identity
Protect
Detect
Respond
NIST Cybersecurity Framework 1.1

Figure 1: UK frameworks comparison.

Although the aforementioned or similar strategies have been adopted by several countries, some studies are dedicated to the analysis of gaps in these documents, such as the article *Cybersecurity management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK , France, Estonia and Lithuania* [8], which analyzes the solutions adopted by these countries, arguing that the strategies that transpose the NIS Directive are generally inefficient in protecting critical infrastructures. The strategy adopted by France placed the country in third place in the *ranking* of cybersecurity in 2019, with a security strategy aimed more at the international level than at the national level. In the case of Lithuania, it is clear that cybersecurity is not just about technical aspects, having been enacted the *Lithuanian Cybersecurity Law*, which defines a set of legal, information disclosure, organizational and technical measures necessary to prevent, detect , analyze and respond to incidents. The strategies adopted by the various countries are often accompanied by guides, which are intended to support their implementation. Validating an existing implementation often falls within the scope of certification, oriented to existing standards or norms such as the ISO27001 Certification.

4. Context and Problem Analysis

The National Framework of Reference for Cybersecurity defines information security measures that generate documents when implemented. These documents represent evidence of the risk mitigation measures implementation required by NRFCS. Such evidence is also referred to in the Cybersecurity Capabilities Assessment Framework (QACC), a complementary document to the NRFCS for cybersecurity, where three levels of capability are defined for each cybersecurity measure defined by the NRFCS [4]. The evidences are thus distributed over the three defined levels, allowing the verification of the effective state of implementation of the security measures. When preparing the list of evidence contained in the NRFCS, from the subcategory (measure)/implementation evidence relationship, it's higlighted tha some evidence name are the same, but due to the context, it doesn't represent the same measure. For example, in the subcategory ”ID-AR-3 - Internal and external threats must be identified and documented in the risk management methodology”, it requires as evidence of implementation the document with the description ”Document that supports the management methodology of risk”, exactly the same description as the evidence of implementation of the measure ”ID.GR-2 - The organization shall determine and identify its tolerance to risk”. By analyzing the reference information indicated in the NRFCS, it is possible to verify that it is not the same document. The first problem to be solved is precisely the presentation of a list of the referred documentation, which allows to identify the documents designated by evidence, in a clear and unambiguous way.

This study intends to offer an objective contribution, drawing up a clear list of evidences and treat them as information entities.Bringing to NRFCS a concept clearly expressed in the TOGAF meta-model, it will be possible to present an information architecture of the information security processes referred to by NRFCS. In other words, demonstrate unequivocally which information structure to implement or being implemented, clarify how it approaches the information architecture designed by the **Information Security Strategy** defined in the NRFCS. This research is intended to complement the NRFCS and support organizations to initiate (or assess the current status of) the implementation of the measures in that document. This support or complementarity is delivered through the integration of the knowledge expressed in the NRFCS with concepts of business architecture, offering as a result a list of information entities that make up the information architecture proposed here, faithful to the context of the document under study. This list is intended to be used as a form of validation of an organization's documentation, in order to check the existence of the documents required by the NRFCS, whose results allow us to conclude on the status of preparation or possible gaps, both in the documentation that makes up the architecture information and the processes it relates to. Given the relationship expressed in the NRFCS, between these information entities and the COBIT 5 processes, the possibility of offering organizations a view of the processes implemented. CNCS provides *online* a self-diagnosis tool, with the purpose of an organization assessing cybersecurity status. This tool is complementary to the NRFCS and considers the levels defined by the Minimum Capabilities Assessment Framework in Cybersecurity [3].

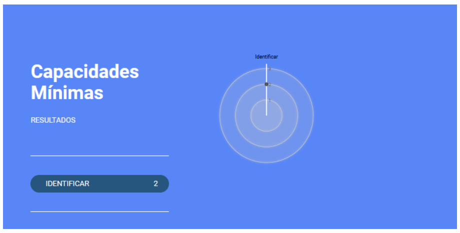


Figure 2: Results of a Cybercheckup.

Throughout this work, we seek to answer the following questions:

1. Considering that the implementation evidences required by NRFCS are documents, what name uniquely identifies them?

2. If we treat this evidence as information entities, we know from the outset that there is a relationship with processes to be implemented. So, what processes to implement, according to the NRFCS, and what is its relationship with the information entities?

3. Is it possible to integrate notions of enterprise architecture following the TOGAF ADM method in order to favor the implementation/understanding of NRFCS?

4. What is the contribution of the developed method, in the analysis of the state of implementation

of the NRFCS in an organization?

From the developed tool, an objective contribution is expected, which responds to concrete problems and clarifies the criteria used. By creating a solution that encompasses both the knowledge expressed in NRFCS with aspects of enterprise architecture, it is expected to achieve a tool that is ready to guide organizations in different stages of the implementation of security measures, offering the results in a simplified way.

5. Methodology description and case study

The incongruity in the name of the evidence raises the need to propose a change, in order to avoid interpretation error in the security measures implementation. The work is developed essentially in an Excel file named Information Entities [1], which has grown iteratively according to the raised possibilities, following the steps demonstrated on figure 3 and described below.

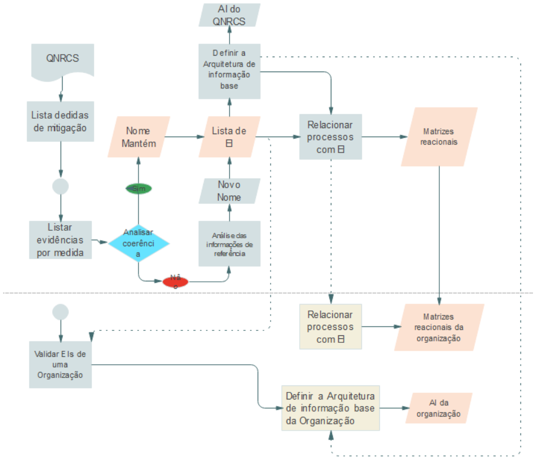

AI do QNRCS
QNRCS
Definir a Arquitetura de informação base
Lista dedidas de mitigação
Nome Mantém
Lista de EI
Relacionar processos com EI
Matrizes reacionais
Sim
Novo Nome
Listar evidências por medida
Analisar coerência
Análise das informações de referência
Não
Relacionar processos com EI
Matrizes reacionais da organização
Validar EIs de uma Organização
Definir a Arquitetura de informação base da Organização
AI da organização

Figure 3: Methodology mind map.

By carefully analyzing all the documentation indicated in the NRFCS as reference information, a name was reached up for each evidence, which, in addition to identifying it uniquely, is in line with the standard or regulation that drives the measure related to it. The standard or reference that justifies the change was indicated in the list of evidences.

The aforementioned evidences are then treated with information entities. The relationships between these information entities, identified by both NRFCS and reference documents (CIS Controls; COBIT 5; ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4) enables the design of a possible information architecture, offering a structure for the context defined by QNRCS information. Throughout the investigation, it was possible to validate the relationship between the information entities and the information security processes, having presented matrices with this relationship[6][1].

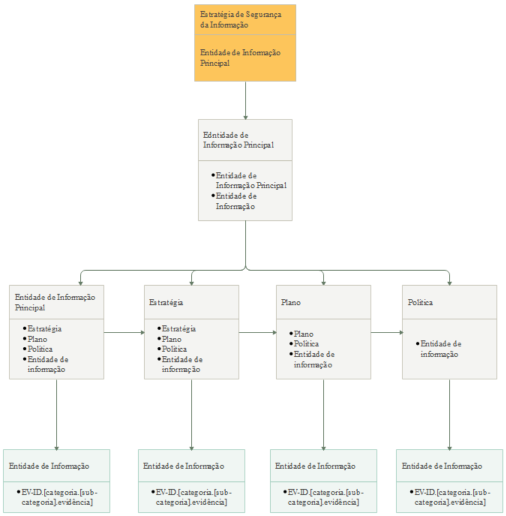
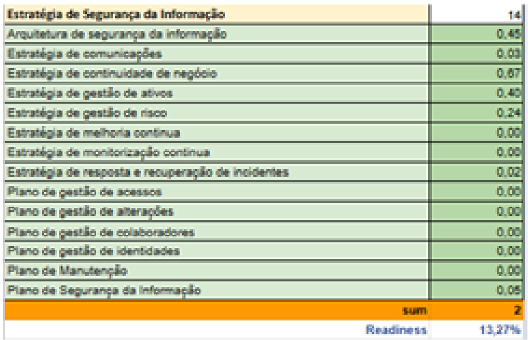

Estratégia de Segurança da Informação
Entidade de Informação Principal
Edntidade de Informação Principal
•Entidade de Informação Principal
•Entidade de Informação
Entidade de Informação Principal
•Estratégia
•Plano
•Politica
•Entidade de informação
Estratégia
•Estratégia
•Plano
•Politica
•Entidade de informação
Plano
•Plano
•Politica
•Entidade de informação
Politica
•Entidade de informação
Entidade de Informação
•EV-ID.[categoria.[sub-categoria].evidência]
Entidade de Informação
•EV-ID.[categoria.[sub-categoria].evidência]
Entidade de Informação
•EV-ID.[categoria.[sub-categoria].evidência]
Entidade de Informação
•EV-ID.[categoria.[sub-categoria].evidência]

Figure 4: Structure of the information architecture for NRFCS.

From the information entities list, a check list tool was developed, through which the organization AMA confirmed the existence of the evidences, allowing the analysis of applicability and demonstration of results in a case study.

This data collection allows to present results for the 'Identify' objective of the NRFCS, and to present an information architecture, which represents the reality of the organization in question. On the left table of figure 5 we can see the base architecture defined by NRFCS, if an entity is signed as 1 means that AMA confirmed existence of all its components while incomplete entities are signed with decimal numbers.



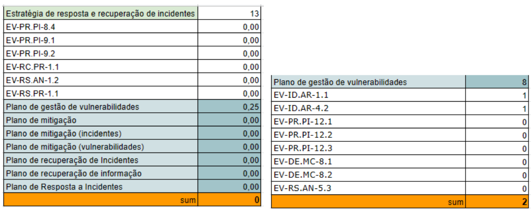
Estratégia de Segurança da Informação	14
Arquitetura de segurança da informação	0,45
Estratégia de comunicações	0,03
Estratégia de continuidade de negócio	0,67
Estratégia de gestão de ativos	0,40
Estratégia de gestão de risco	0,24
Estratégia de melhoria contínua	0,00
Estratégia de monitorização contínua	0,00
Estratégia de resposta e recuperação de incidentes	0,02
Plano de gestão de acessos	0,00
Plano de gestão de alterações	0,00
Plano de gestão de colaboradores	0,00
Plano de gestão de identidades	0,00
Plano de Manutenção	0,00
Plano de Segurança da Informação	0,05
sum	2
Readiness	13,27%

Figure 5: Information architecture for AMA.

The presented table shows the main information entities of the information architecture, in which information entities, plans, strategies and policies that are grouped as part of the security strategy under study. For each main information entity, the developed tool is prepared to present how the base architecture is affected by the entities validation. In order to exemplify the results, figure 6 shows the

[1] https://tinyurl.com/entidadesdeinformacao

13 components of Incident Response and Recovery Strategy, from where AMA has confirmed the existence of 2 information entities that specifically belong to Vulnerability Management Plan. With this information, it is possible to say that referred plan is composed by entities EV-ID.AR-1.1 and EV-ID.AR-4.2, representing 2 of the 8 documents in it composition.



Estratégia de resposta e recuperação de incidentes	13
EV-PR.PI-8.4	0,00
EV-PR.PI-9.1	0,00
EV-PR.PI-9.2	0,00
EV-RC.PR-1.1	0,00
EV-RS.AN-1.2	0,00
EV-RS.PR-1.1	0,00
Plano de gestão de vulnerabilidades	0,25
Plano de mitigação	0,00
Plano de mitigação (incidentes)	0,00
Plano de mitigação (vulnerabilidades)	0,00
Plano de recuperação de Incidentes	0,00
Plano de recuperação de informação	0,00
Plano de Resposta a Incidentes	0,00
sum	0

Plano de gestão de vulnerabilidades	8
EV-ID.AR-1.1	1
EV-ID.AR-4.2	1
EV-PR.PI-12.1	0
EV-PR.PI-12.2	0
EV-PR.PI-12.3	0
EV-DE.MC-8.1	0
EV-DE.MC-8.2	0
EV-RS.AN-5.3	0
sum	2

Figure 6: Incident Response and Recovery Strategy - AMA.

Knowing that 'Vulnerability Management Plan' is the only document represents 1 in a set of 13 information entities composing 'Incident Response and Recovery Strategy', it appropriate to say that this strategy is 1.92 % complete. The investigation referred to in this article, presents similar information results for all entities.

The presentation of results, includes a summary of the implementation status for COBIT 5 processes foreseen by NRFCS, grouped in the macro-processes APO, BAI, DSS, EDM and MEA, and in accordance to the validation carried out in the case study. For the observed resultes only EDM domain processes are near from 50% of completion. If consider that each macro process referred represents 1/5 of the total of foreseen processes, then we can say that 22.41% of the processes are probably implemented in this organization. The developed tool allows to generate matrices relating the information entities with the processes, allowing the visualization of an implemented panorama. This information guides the creation of diagram in figure 9, showing the processes affected by the lack of evidence, as validated by AMA organization. This feature offers to the organization the possibility to proceed with improvement actions, related to the implementation of the mitigation measures itself, or with the documentation required by NRFCS.

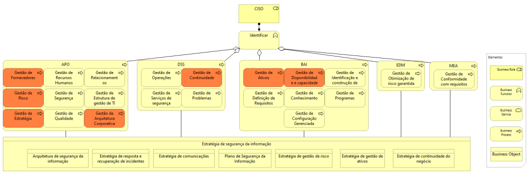
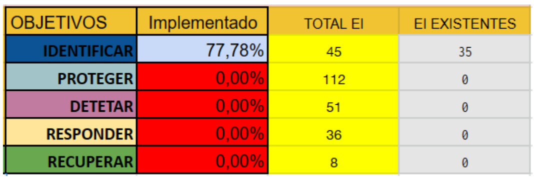

CISO
Identificar
APO
Gestão de Fornecedores
Gestão de Recursos Humanos
Gestão de Relacionamentos
Gestão de Risco
Gestão de Segurança
Gestão de Estrutura de gestão de TI
Gestão de Estratégia
Gestão de Qualidade
Gestão de Arquitetura Corporativa
DSS
Gestão de Operações
Gestão de Continuidade
Gestão de Serviços de segurança
Gestão de Problemas
BAI
Gestão de Ativos
Gestão de Disponibilidade e e capacidade
Gestão de Identificação e construção de
Gestão de Definição de Requisitos
Gestão de Conhecimento
Gestão de Programas
Gestão de Configuração Gerenciada
EDM
Gestão de Otimização de risco garantida
MEA
Gestão de Conformidade com requisitos
Elementos
Business Role
Business Function
Business Service
Business Process
Business Object
Estratégia de segurança da informação
Arquitetura de segurança da informação
Estratégia de resposta e recuperação de incidentes
Estratégia de comunicações
Plano de Segurança da Informação
Estratégia de gestão de risco
Estratégia de gestão de ativos
Estratégia de continuidade do negócio

Figure 7: Category 'Identify' - Processes Diagram.

The table in Figure 8, allows to conclude that, from the 252 existent information entities, only the first 38 were validated. Outcome considerations are limited to the 'Identify' objective, as the first 45 EI refer to this objective only. In any case, it can be said that around 78% of the information entities that prove the implementation of risk mitigation measures, related to the Identify objective, were validated as existent. Which means that AMA organization confirms the existence of 35 of the 45 EI that make up this objective.



OBJETIVOS	Implementado	TOTAL EI	EI EXISTENTES
IDENTIFICAR	77,78%	45	35
PROTEGER	0,00%	112	0
DETETAR	0,00%	51	0
RESPONDER	0,00%	36	0
RECUPERAR	0,00%	8	0

Figure 8: Incident Response and Recovery Strategy - AMA.

6. Case study summary

From the information entities list validation, AMA has validated as existent the first 38, reffering to 'Identify' category. This allowed the presentation of results including the information architecture summarized in Figure 1, which represents the reality of the organization in question.

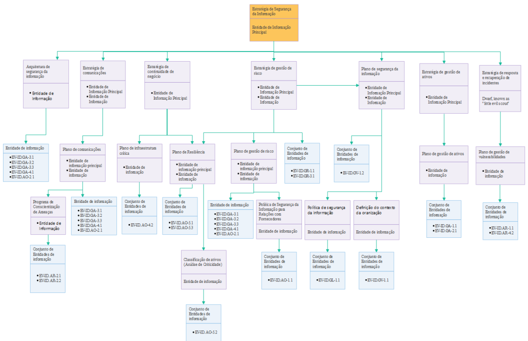

Estratégia de Segurança da Informação
Entidade de Informação Principal
Arquitetura de segurança da informação
Estratégia de comunicações
Estratégia de continuidade de negócio
Estratégia de gestão de risco
Plano de segurança da informação
Estratégia de gestão de ativos
Estratégia de resposta e recuperação de incidentes
Dwarf, known as "little evil scout"
Entidade de informação
Plano de comunicações
Plano de infraestrutura crítica
Plano de Resiliência
Plano de gestão de risco
Conjunto de Entidades de informação
Plano de gestão de ativos
Plano de gestão de vulnerabilidades
Programa de Consciencialização de Ameaças
Política de Segurança da Informação para Relações com Fornecedores
Política de segurança da informação
Definição do contexto da oranização
Classificação de ativos (Análise de Criticidade)
EV-ID.GA-3.1
EV-ID.GA-3.2
EV-ID.GA-3.3
EV-ID.GA-4.1
EV-ID.AO-2.1
EV-ID.GR-1.1
EV-ID.GR-3.1
EV-ID.GV-1.2
EV-ID.AO-4.2
EV-ID.AO-5.1
EV-ID.AO-5.3
EV-ID.GA-1.1
EV-ID.GA-2.1
EV-ID.AR-1.1
EV-ID.AR-4.2
EV-ID.AR-2.1
EV-ID.AR-2.2
EV-ID.AO-1.1
EV-ID.GL-1.1
EV-ID.GV-1.1
EV-ID.AO-5.2

Figure 9: Structure of Ama's information Architecture

According to AMA collected data, Ama's Information security strategy is 13.27% complete with the readiness of its main information entities expressed on table 1 .

EIP	(%)
Information security architecture	45,45%
Communications strategy	3,33%
Business continuity strategy	66.67%
Asset Management Strategy	40.00%
Risk management strategy	23.61%

Table 1: Confirmed entities readiness table

7. Contributions

The study carried out offers an objective contribution with regard to the documentation required by the NRFCS. The implementation of risk mitigation measures generate documents, for which a change to the name is suggested. The suggested name is unique and clear as proposed.

The integration business architecture knowledge, using strategies present in the TOGAF ADM method, allows treating these documents as information entities, and consequently, bringing a vision of information architecture to the scope of NRFCS. This vision makes it possible to structure the documentation and demonstrate its relationship with the COBIT 5 processes, provided for in the national strategy for information protection.

The tool developed based on these information entities allows an organization to assess the status of implementation of the security processes provided for by the NRFCS, that is, the determination of the *AS-IS* status of the organization regarding to cybersecurity or information security. From the results obtained, implementation status of COBIT 5 processes suggested by NRFCS is given, allowing improvements to be considered, indicating the implementation gaps. From the way the results are presented, it's clear that gaps may exist in the documentation that serves as evidence of the implementation of these processes, allowing improvements to occur in an assertive and efficient manner.

Organizations intending to start implementing the measures, the tool contributes to the construction of a *TO-BE* vision, showing the failures or shortcomings in the actual implementation of the NRFCS suggested processes which follows the European regulation, within the scope of ISO 27001 measures, of Directive (EU) no. 2016/1148, among with other norms and standards. The tool developed can guide an organization towards information security and in compliance with the NRFCS, efficiently.

8. Further Work

Predicting the continuity of this study, as well improvements in the developed tool, an active review of the proposed names for the information entities should be considered as a priority. The attribution of the evidence names must chase an approval by the CNSC. Furthermore, the development of an interface or application integrating all features developed, with automation mechanisms of crossing information and better output, to offer greater usability and make the tool more appealing. As Cybercheckup is a cybersecurity self-assessment tool integrating the notion of levels, defined by the Capacity Assessment Framework. Knowing that it retrieves undetailed results ofr allowing 'de facto' improvement actions, there is a clear possibility of integrating both tools, for better results in the context of information security in Portugal.

9. Limitations

No relevant studies were found based on the documentation generated by the strategies measures implementation, in particular, the NRFCS, which made the investigation difficult in terms of the precision of the considerations about the results.

References

[1] C. C. S. R. Center. Nist risk management framework. https://csrc.nist.gov/projects/risk-management/sp800-53-controls/release-search!/control?version=4.0number=SC-17. Accessed: 2021-10-28.

[2] Council of European Union. Council regulation (EU) no 1148/2016. http://data.europa.eu/eli/dir/2016/1148/oj. Accessed: 2021-10-28.

[3] C. C. N. de Cibersegurança. Cybercheckup. https://cibercheckup.cncs.gov.pt/. Accessed: 2021-10-28.

[4] C. C. N. de Cibersegurança. Quadro de avaliaÇÃo de capacidades de ciberseguranÇa. https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf. Accessed: 2021-10-28.

[5] P. D. C. De Ministros. Resolução do conselho de ministros 49/23018. *Diário da República*, 2018.

[6] ISMS.Online. Iso 27001 annex a controls. https://www.isms.online/search/ISO+27001+Annex+A+Controls Accessed: 2021-10-28.

[7] ISO Central Secretary. Information security management. Standard ISO/IEC TR 27001:2013, International Organization for Standardization, Geneva, CH, 2013.

[8] M. Tvaronavičienė, T. Plėta, S. Casa, and J. Latvys. Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of usa, uk, france, estonia and lithuania. *Insights into Regional Development*, 2(4):802–813, 2020.