QNRCS Implementation on a SME (2021)

finalista student João Costa, teacher coordinator Pedro Adão

Abstract – This paper resumes the IST MSIDC master thesis in which the author proposes to the implement the Portuguese security framework QNRCS – Quadro Nacional de Referência para a Cibersegurança on SME. This implementations follows the framework action points step by step, identifying gaps among the way and proposing solutions based on a risk approach methodology.

Keywords – QNRCS, SME, Cybersecurity framework, CNCS.

I. INTRODUCTION

Cybercrime and cyberwar have proven to be a rising major concern for Nation States and authorities. In fact, the rising interdependence of services and goods with the information technology has been exposing critical infrastructure beyond traditional security limits. Decades ago, it was simple to identify critical assets, since most of them were identifiable within the material world. However, this is not true nowadays. Furthermore, traditional security and defense infrastructures were design to protect nation state infrastructures and their citizens at large, but today many of the assets and goods, which societies need to protect, are not material and they are exposed to malicious actors as never before. In Portugal, the interdependence of companies and the State with information and communication technologies is increasingly an undeniable and irreversible reality. This phenomenon is a result of the digital transformation that the country has been going through, either on the initiative of the companies themselves to reduce costs and optimize processes and resources, or on the initiative of the State to encourage such measures.

As already mentioned, computer crime is a phenomenon that did not exist 50 years ago and that has grown in recent years. According to the 2018 Annual Internal Security Report [1], there is a clear growing trend of reported computer crime, despite the slight decrease from 2017 to 2018, with "illegitimate access/interception" being the most reported computer crime, followed by the crime of “computer sabotage” and “computer fraud”.

Thus, in an effort to face the new information security challenges posed by globalization and the geopolitical situation derived from it, the European Union and Portugal in particular, took several measures aimed at increasing the resilience of civil society against security threats external and internal. These measures are materialized in the elaboration of a set of laws and regulations, as well as in the creation of bodies responsible for the control of those same regulations. It is in this context that, in order to facilitate the implementation of a culture of information security - namely cybersecurity - in member states, the European Union created ENISA (European Union Agency for Cyber Security), which aims to create synergies between competent cybersecurity bodies of the various member states, as well as helping them in the design and implementation of common security policies, among other activities that involve the articulation of the various competent bodies for a more efficient common security. Meanwhile, the Portuguese State took its own measures. An important measure put forward by the Portuguese State was the creation of the National Cybersecurity Center (CNCS), which is an organization that "acts as operational coordinator and national authority specializing in cybersecurity with State entities, national critical infrastructure operators, operators of essential services and digital service providers, ensuring that cyberspace is used as a space of freedom, security and justice, to protect the sectors of society that materialize national sovereignty and the Democratic Rule of Law.” Indeed, the CNCS has taken several initiatives to raise awareness of the topic of cybersecurity, as well as promoting Regulations, such as the QNRCS [2] – Quadro Nacional de Referência para a Cibersegurança, which is not binding at the moment, among other measures resulting from the synergies created by the organization.

Since the Portuguese private sector is mainly made up of micro and small companies (99,5%) [3], and security implementation and solutions represent a hefty cost in the budget of any micro and small business, this master thesis proposes to present a generic IT solution – architecture, applications and processes – oriented to small organizations, which allows to respond to the requirements of the norms in force in the national territory, as well as with some of the main international norms, at the lowest possible cost. In this sense, it was decided to use the National Framework of Reference for Cybersecurity as a starting point for this analysis. The QNRCS is a set of cybersecurity recommendations of Portuguese origin, which is based on the best practices of international and national information security standards, which will be applied to an SME. The thesis will make use of supporting documents to QNRCS, and in case of omission, it will use and justify its assumptions for the implementation of the framework in the organization. The final hope is that this thesis will serve as a guide for implementing the QNRCS to SMEs.

II. LITERATURE REVIEW

The National Cybersecurity Framework, hereinafter called QNRCS, is intended to be a tool available to society to support this systematic response. In 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July, was approved, on measures to ensure a high common level of security of networks and information systems across the Union (Directive SRI). With the SRI Directive, it was intended to create the legal framework for the legislation of Member States in the field of cybersecurity and to provide a basis for developing a culture of cybersecurity in vital sectors for the economy of the Member States and for the correct functioning of the society, sectors that depend heavily on information networks and systems. This answer is also in line with Law no. 46/2018, which establishes the legal framework for cyberspace security, transposing the SRI Directive. It is structured in a set of security measures that translate five specific objectives: Identify, Protect, Detect, Respond and Recover.

- **Identify** – Knowing, in an organizational context, the resources that support its important functions and the respective associated risks, allows the organization to prioritize its efforts consistently.
- **Protect** – This capability is supported, among others, in the management of electronic identity and respective authorizations, in carrying out training and awareness-raising actions and in the definition and implementation of procedures, processes and information protection technologies.
- **Detect** – In the context of the “Detect” objective, the aim is to develop adequate and timely practices for detecting the occurrence of cybersecurity events, through the continuous monitoring of information networks and systems and the implementation of detection processes.
- **Respond** – It is intended, as a result of the objective “Respond”, to develop and implement practices that carry out response actions to a cybersecurity incident that has been detected.
- **Recover** – Within the scope of the “Recover” objective, it is intended to develop and implement practices and maintain resilience plans to restore any capacity and/or service that has been compromised following a cybersecurity event.

O Quadro de Avaliação das Capacidades Mínimas de Cibersegurança (The Minimum Cybersecurity Capabilities Assessment Framework) [4] is a complementary product to the National Cybersecurity Reference Framework (QNRCS), following the strategy of the National Cybersecurity Center (CNCS) to support organizations with their capacity, through the provision of references and tools. As a complement to the QNRCS, it presents, for each of the cybersecurity measures, the definition of three levels of capacity so that it is possible for organizations to fulfill the five objectives of the framework, taking into account their context and dimension.

The cumulative application of the defined measures is proposed, that is, for an organization to be positioned at the “3 – Advanced” capability level, it will have to implement the “1 – Initial[1]” and “2 – Intermediate” level measures.

[1] In this master thesis, the “Initial” nomenclature has been replaced by “Basic”

Security measures have their levels of sophistication distributed according to the classification presented and are organized according to the proposed structure of security objectives, described in QNRCS. Capability levels can be applied independently to each objective. As a result, an organization can position itself at different levels of capability for the same security objective. The capacity levels applicable to a given organization depend on its specific characteristics, such as size and services provided. Knowing that organizations can be at different levels of maturity and have different dimensions (from micro and small organizations to large companies or public institutions), and that some recommendations may be disproportionately demanding for the size of the organization or not be sufficiently demanding, he suggests It is necessary that the document is internalized with a critical spirit by each organization and adapted to its needs.

For this reason, it is recommended that the organization that implements the QNRCS adapt its proportionality to its Information Security Risk analysis, and for that, it will be necessary for the organization to articulate the implementation of its controls with the Process of Management of Information Security Risk. This strategy aims to approach the Information Security Management process recommended by the ISO/IEC 27001 standard. As there is no defined criterion at the time of this on which level of maturity the organization should indicate its implementation of the QNRCS, the same is defined by the target organization.

The methodology used in this thesis follows the set of steps recommended by the QNRCS. These steps allow for the systematization and continuous improvement of processes, and are:

- Step 1 – Priority and scope: The organization identifies its high-level objectives and priorities. With this information, the organization defines its strategic options regarding the implementation of cybersecurity measures and defines the universe of systems and assets that support the organization's critical activity.
- Step 2 – Guidelines: once the scope of the cybersecurity program has been defined, the organization identifies and defines the information networks and systems and respective assets related to the activity, regulatory requirements and the risk management strategy.
- Step 3 – Creation of Current Profile: The organization creates what is its “Current Profile”, indicating for each category and subcategory which security objectives it currently meets.
- Step 4 – Risk Assessment: The Risk Analysis can be guided according to the risk management process in place in the organization, or based on previous actions. The organization analyzes its operating environment to assess the degree of probability of occurrence of a cybersecurity event or incident and the impact it may have on the organization.
- Step 5 – Creation of Target Profile: The organization creates its “Target Profile” based on the categories and subcategories described in the QNRCS, reflecting those that are the intended results.
- Step 6 – Identify, analyze and prioritize gaps: The organization compares the “Current Profile” with the “Target Profile” and identifies gaps that must be addressed.
- Step 7 – Implementation of the action plan: The organization determines what actions to take in order to address the gaps identified in the previous step and adjusts the cybersecurity practices it currently has in place in order to achieve its “Profile Target".

Organizations must repeat this process whenever necessary and even with a planned and systematized cadence.

III. DATA COLLECTION

In short, the QNRCS provides guidelines for implementing cybersecurity measures. However, the lack of specificity regarding risk assessment, the relationship between risk management and the implementation of QNRCS measures or lack of criteria that indicate what would constitute a form of "compliance" with QNRCS, are assumed as gaps that this dissertation aims to complete.

As a test of the implementation of the QNRCS, this thesis uses a real SME, whose activity is based on technology and whose services provided fall under the categories of digital services, described in law 46/2018. According to table 2, this organization fits into the Micro Enterprise category, comprising a universe of no more than 10 people. The Assessment Framework classifications (Basic, Intermediate and Advanced) do not contemplate cases where the organization does not have any measure that meets a certain objective, nor cases for which the measure does not apply. Thus, for each objective, one of the following objectives will apply:

Basic – the Basic level applies when the description of the objective and respective evidence are verified.

Intermediate – the Intermediate Level applies when the descriptions of the objective and respective evidence are verified for the Basic and Intermediate levels.

Advanced – the Advanced Level applies when the descriptions of the objective and respective evidence are verified for the Basic, Intermediate and Advanced levels.

<Blank> - Applies the absence of any ranking if none of the above criteria are met.

N/A – applies to cases where the objective in question does not apply.

Additionally, a scoring system will be adopted that will be shaped according to the classification given to each objective. Thus, the following values will be assumed:

- <Blank> - 0 points.
- Basic – 1 point.
- Intermediate – 2 points.
- Advanced – 3 points.
- N/A – 3 points.

Note that the classification of N/A (“not applicable”) corresponds to the maximum score, because this is due to the fact that the evaluation concluded that the organization does not have an attack surface that justifies the achievement of the objective, and that it has no surface The exposure level is then considered to be minimal and therefore equivalent to the advanced rating scenario. As of the date of production of this document, none of the documents defines criteria for the full compliance of the framework. Compliance with a framework is essential for the organization not to lose focus of its implementation, ensuring the existence of an implementation objective beyond information security in the organization. The definition of this conformity should consider:

1. The organization's goals;

2. The objectives of the QNRCS, namely the ability to Identify, Protect, Detect, Respond and Recover.

In this sense, this thesis considers that the organization is in compliance with the QNRCS if the organization:

1. have a cybersecurity risk management process;

2. comply with all the objectives applicable to its scope, namely:

- Have 0 high non-conformities per objective;
- Ensure compliance with the 5 objectives and 23 categories;
- Possess a maximum of 20% average non-conformities per objective (eg 1 average non-conformity out of 5 possible in the 'Recover' objective).
- Possess a maximum of up to 25% low non-conformances per goal.

Regarding non-conformities, the following is considered:

- **major non-conformity:** total non-compliance with a process (eg risk management) or with an applicable sub-category (non-compliance with objective ID.GR1 when it is applicable) or a gap of 2 degrees of maturity or greater, if the risk of failure to do so is High or Critical and the treatment is Mitigate or Avoid.
- **medium non-conformity:** partial default of a sub-category whose gap corresponds to a degree of maturity and whose risk of non-compliance with that objective is High or Critical and the treatment is Mitigate or Avoid.
- **minor non-conformity:** any failure to meet an objective that does not meet the definitions of medium and high non-compliance.

The risk analysis methodology can be substantiated by an analytical approach of a qualitative or quantitative nature, or by a combination of both. In practice, qualitative analysis is mostly used, in a first approach, to obtain general indicators of the level of risk and to identify the most relevant risks. Thus, risk analysis is defined by assessing the impact of a given event (risk) and assessing the probability of that event occurring. In this sense, we can quantify the risk as being Risk = Impact x Probability.

IV. ANALYSIS

Bearing in mind the dimensions of SMEs and the time usually available to dedicate to risk assessment, this thesis presents a risk quantification solution based on 3 degrees of Impact and 3 degrees of Probability for the SMEs targeted in this work:

		Probability		
		1	2	3
Impact	1	1	2	3
	2	2	4	6
	3	3	6	9

Table 1- Risk Classification Matrix

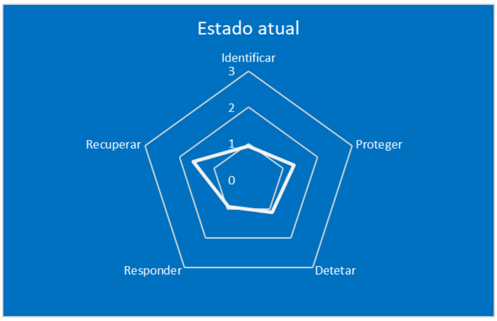
Risk	Description
1; 2	Low
3;4	Medium
6	High
9	Crítical

Table 2- Risk quantification

Step 1 – Scope: being a micro sized company, the scope of the implementation of this security framework will be the entire company, not only the operation process, but the support process as well. Risk strategy plan has been define at this stage too.

Step 2 – Assets: within the defined scope, all IT components and staff (who themselves are also considered information assets).

Step 3 - Current Security Profile: Within this step, the auditors take a snapshot onto the company's security profile within the framework's criteria. The company is audited per subcategory, according to the framework's maturity levels. The following graph shows the average maturity value aggregated by major objective.



Picture 1- Current security profile

Step 4 – Risk Assessment: from the risk criteria defined within the previous steps, the author proposes the evaluation of cyber risk by considering the risk (including impact and probability) of not implementing a subcategory. Therefore, the proposed risk exercise is calculated for each of the 102 QNRCS subcategories, in order to calculate the needed security maturity to engage the security needs.

Step 5 – After the risk evaluation, a target maturity is defined of each subcategory.

Step 6 – Gap Analysis: by knowing both current security maturity level and the target maturity level for each subcategory, the author is able to calculate the gap between current and target maturity levels. By doing so, it is possible to predict the actions needed to achieve compliance objectives (based on the framework's criteria).

Step 7 – By knowing the needed implementations, the author prioritizes implementation actions according to the risk assessment and risk plan.

The master thesis also refers to important topics to cybersecurity implementation, such as:

1. **Chief information security officer** and its role and responsibilities on implementing an information security framework, and the challenges for small and medium sized companies to train or hire such people for that role.
2. The importance of a **information security policy**, and how it fits on a SME.
3. The need of trusted **risk and threats feeds**, and how SME can acquire them.
4. **Vulnerability management** and how to apply it on a SME.
5. **Access Management** overview and low cost solutions.
6. The importance of a **Business Continuity Plan** and how does it fit with the QNRCS framework.
7. The importance of a Backup policy and how do make one.
8. The importance of a **Security Incident & Event Management** (SIEM) within the framework.
9. How to implement a **Security Operation Center** for SME given the framework's options and the company size and resources.
10. **Training, security awareness and communication** are probably the most effective weapon against cyber threats within a SME.

11. **Incident reporting** and how to fit it within a SME.

V. CONCLUSION

The QNRCS is an excellent initiative by the Portuguese State to establish computer security standards in the Portuguese business fabric (including the public sector). From a national sovereignty point of view, it is important that states guarantee the capacity to defend their citizens and their territory. But what happens when the territory ceases to be material and moves to the abstract plane? As Cyberspace is the realization of this new concept of abstract territory, it is up to the Portuguese State to take the most adequate measures to protect “its cyberspace”, and ultimately, its citizens. This protection is not only imposed against external agents, but also against internal agents. And it is in this context that QNRCS was born. Although the QNRCS is not assumed as "a cybersecurity norm, but as a reference that allows the identification of norms, standards and good practices in various domains of information security", the truth is that its implementation is increasingly relevant nowadays, and its certification is becoming more and more likely.

However, the law-decree 65/2021 that refers to possible certification reiterates its applicability to Public Administration, operators of critical infrastructure and operators of essential services, and at the time of writing this document there is still no clear definition of the latter. Thus, in the absence of QNRCS compliance and compliance criteria, the question may be asked: do you have to comply with all QNRCS subcategories? If yes, with what degree of maturity?

By placing the worst-case hypothesis (all subcategories with the maximum maturity degree), it is quickly concluded that the QNRCS would be too heavy a burden for national SMEs to bear, due to the costs of its implementation, thus preventing any large organization smaller to provide essential services to society. Thus, this thesis proposed to:

1. Test the QNRCS approach in an SME,

2. Establish QNRCS compliance criteria, and

3. Test the adequacy of the maturity grades of the Assessment Framework [2]

in order to assess how the QNRCS can adapt to smaller organizations, and in this way be more inclusive and comprehensive for the Portuguese business fabric.

The QNRCS states that it is based on the analysis and assessment of information security risk, which is especially true in the assessment of risks associated with information security incidents. However, if the QNRCS establishes the adoption of a set of controls, it is because these controls aim to mitigate risks, and are not just risks associated with incidents, but above all with business risks.

Thus, assuming the Risk Management process as the heart of the implementation and possible certification of the QNRCS, it is fair to say that the adequacy of controls (QNRCS sub-categories) and their degrees of maturity should not be the same for all organizations, but rather depending on their risk appetite, so there may be cases in which certain subcategories do not apply to some organizations, or where their risk does not justify an intermediate or advanced degree of maturity in a certain subcategory. However, it is important to keep in mind that the QNRCS has 5 objectives, and that if an organization intends to be certified in the QNRCS, it cannot omit to comply with all categories.

It should also be noted that, because smaller organizations have a smaller attack surface, the probability of being targeted by a cyber attack is also smaller, which may justify a requirement at lower maturity.

From the lessons learned from the implementation of the QNRCS in the organization, the following stand out:

1. Flexibility is key in a small business.

2. The most efficient process (cost/benefit ratio) of information security is the implementation of training and awareness actions. In fact, the most exploited attack vector is the human factor and this is also the one that, if trained, constitutes the best line of defense.

3. Forensic analysis processes prove to be the most difficult to implement due to their high level of specialization, a fact that will likely force SMEs to resort to external SOC services.

4. From a human effort perspective, the implementation of new processes and technologies inevitably translates into an increase in the workload of the organization's

employees, even if some new processes manage to simplify existing processes. Thus, it is very likely that a reinforcement of staff will be necessary to manage new processes or operate new tools, as well as operate them. However, the complexity of these processes in small and micro companies is less than in medium or large organizations. This can allow the requirement of knowledge necessary to not be so demanding and, therefore, it is possible to concentrate some processes from different areas on the same people (example: Risk Management with Change Management). However, some processes may not allow this simplification, such as system monitoring, which requires someone specialized in security and networks who can interpret the data presented by the system. The issue of demand still accumulates, since as we saw in the Introduction of this thesis, Portugal has many IT vacancies to fill (48% in 2018) and the implementation of these standards would further increase the demand for professionals in the field, taking into account that not all IT professionals are security.

5. The implementations suggested in this thesis are part of a scenario in which the organization has its own space (one or several offices or even dedicated facilities such as warehouses, buildings, etc.), but this is not always the case. Many small and micro-sized organizations ensure their activity from spaces shared with other organizations, so they lack the necessary autonomy to create access control processes as well as ensure installation of servers and other physical machines in safe places.

6. From a financial point of view, the acquisition of these resources – human and technical – could represent a great burden for micro and small companies. Typically, this type of organization tends to focus its investment on resources that have a direct impact on its turnover and its business.

Despite the identified constraints and considering the hypothetical principle that an organization can adapt its QNRCS implementation to its risk appetite, this thesis concluded that it is possible for an SME to position itself in accordance with the QNRCS. Through the adoption of efficient processes, institutional teaching materials, external services and open source technology, SMEs are able to assume a cybersecurity posture that allows them to reduce business risk, ensure compliance with QNRCS and ensure healthy and secure growth.

REFERENCE

[1] Governo de Portugal, (2018), Relatório anual de Segurança Interna 2018, disponível em: https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2018

[2] Centro Nacional de Cibersegurança, (2019), Quadro Nacional de Referência em Cibersegurança, disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[3] [9] Pordata (2021), Pequenas e médias empresas em % do total de empresas: total e por dimensão, disponível em: https://www.pordata.pt/Portugal/Pequenas+e+m%C3%A9dias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimens%C3%A3o-2859

[4] Centro Nacional de Cibersegurança, (2019), Quadro de Avaliação de Capacidades de Cibersegurança Disponível em https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf