Italian National Framework for Cybersecurity and Data Protection*

Marco Angelini[1,2], Claudio Ciccotelli[1,2], Luisa Franchina[2], Alberto Marchetti-Spaccamela[1,2], and Leonardo Querzoni[1,2]

[1] Dept. of Computer Control and Management Engineering - CIS Sapienza University of Rome
{angelini,ciccotelli,alberto,querzoni}@diag.uniroma1.it
[2] CINI Cybersecurity National Lab
blustarcacina@gmail.com

Abstract. Data breaches have been one of the most common source of concerns related to cybersecurity in the last few years for many organizations. The General Data Protection Regulation (GDPR) in Europe, strongly impacted this scenario, as organizations operating with EU citizens now have to comply with strict data protection rules.
In this paper we present the Italian National Framework for Cybersecurity and Data Protection, a framework derived from the NIST Cybersecurity Framework, that includes elements and tools to appropriately take into account data protection aspects in a way that is coherent and integrated with cybersecurity aspects. The goal of the proposed Framework is to provide organizations of different sizes and nature with a flexible and unified tool for the implementation of comprehensive cybersecurity and data protection programs.

Keywords: Cybersecurity · Data protection · GDPR.

1 Introduction

Organizations of all types are increasingly subject to data theft and loss, whether the asset is customer information, intellectual property, or sensitive company files. In fact, cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line: it can drive up costs and negatively impact revenues; it can harm an organization ability to innovate and to attract and maintain customers. As a consequence, average expenditures on cybercrime are increasing dramatically and, quite often, current spending priorities fail to deliver the expected levels of effectiveness (see for example [1]).

* Acknowledgements: the authors would like to thank Cosimo Comella, Marco Coppotelli and Dorotea Alessandra de Marco (representatives of the Italian Data Protection Authority) for their valuable feedback which helped improving the Framework and its relationship with data protection principles and requirements.

In fact, there are many organizations and companies with little or no experience in cyber protection; they may have security practices in place, but they are most likely not sure if those practices establish a comprehensive security program. They need to know the necessary requirements and actions (or at least the most important ones) from an information security perspective. This stimulated the development of documents, guidelines and tools to support companies and organizations in a cost effective way that takes into account specific characteristics of the organization. To answer this need, several proposals have been recently presented (see section 2). Among these proposals we focus on the Cybersecurity Framework originally proposed by the US National Institute of Standards and Technology (NIST) to support the development of a industry-led set of standards, guidelines, best practices, methodologies, and processes to cost-effectively reduce cyber risks of critical infrastructures. NIST released version 1.0 of the Cybersecurity Framework in 2014, describing it as a voluntary, risk-based approach to manage cybersecurity risk for organizations of all shapes and sizes. The Framework has been proposed for protecting critical infrastructures but its approach has a much broader applicability for industries and organizations and it has been widely adopted by non-critical infrastructure organizations [19]. Version 1.1 has been recently published [17]. In 2015, the Research Center for Cyber Intelligence and Information Security (CIS) at Sapienza University of Rome presented the Italian National Framework for Cybersecurity [4], the result of a collaboration between academy, public bodies, and private companies. The Italian National Framework for Cybersecurity is based on the NIST Cybersecurity Framework and provides an operational tool for organizing cybersecurity processes suitable for public and private organizations of any size; in particular, it has been customized and improved with a focus on the Italian economic system, mainly formed by small-to-micro manufacturing companies that have limited IT expertise.

The Italian National Framework for Cybersecurity provides organizations with a unified point of view from which other standards, guidelines, and best practices can be applied effectively. It does not provide a unique set of rules that should be applied by all organizations, but rather enables organizations, regardless of size, cybersecurity risk, or cybersecurity sophistication, to improve their security and resilience to cyber attacks.

As of May 2018, with the application of the General Data Protection Regulation [10] (GDPR), there is one single set of data protection rules to be enforced for all companies operating with EU citizens. The GDPR regulates the processing and circulation of personal data related to natural and legal persons, identifying roles and responsibilities. The GDPR explicitly requires organizations to demonstrate that they have embedded the principle of data protection by design and by default; for example, Article 8 requires that data controllers shall implement appropriate technical and organizational measures to ensure that processing of data is performed in accordance with the Regulation.

Security and data protection have complementary and mutually-reinforcing objectives with respect to managing the confidentiality, integrity, and availabil-

ity of personally identifiable information (PII). When applied to securing PII, security controls provide privacy protection and are, therefore, a mandatory requirement for the protection of data of individuals. Indeed, from an implementation perspective of identifying and selecting controls, these controls are generally classified as security controls. However, there are also data protection concerns with no direct implications for cybersecurity (and cybersecurity concerns without implications for data protection). Therefore, the privacy of individuals cannot be achieved solely by securing PII. We finally observe that there are cases where security approaches may pose at risk personal information (e.g. extensively logging information about user activities on a web application for security monitoring purposes), potentially creating conflicting goals between security and data protection that need to be carefully considered. We refer the interested reader to [16] for a thorough discussion that demonstrate various types of privacy concerns apart from data security breaches. These concerns relate to the ways in which systems process PII and the effects such processing can have on individuals.

We observe that there is a significant number of standards, guidelines that address specific privacy aspects and/or security requirements that should be followed. However the situation is not satisfactory. A recent report by ENISA [8] explores how the standards-developing world has been responding to the fast-changing and demanding realm of privacy. The study provides insights into the state-of-the-art of privacy standards in the information security context by mapping existing standards available and standardisation initiatives alike. Main findings of the study include that *"there is an increasing need to analyse the mapping of international standards and European regulatory requirements, as references to standards in the EU legislation are becoming recurrent and there are considerable differences from jurisdictions outside of the EU"*; additionally, *"proving compliance with privacy standards in information security is not as straightforward as expected. While there are some approaches for conformity assessment available in specific sectors others are still lacking appropriate mechanisms"*.

Clearly, SMEs are facing additional difficulties since they often lack the expertise needed to cope with such complexity. As an example, for this issue we refer to the position of SMEUnited (the association of crafts and SMEs in Europe) that points out significant difficulties in complying to the GDPR. Namely, it is pointed out that the main challenge is that the regulation is extremely complex while *"the guidelines published may help to understand the rules, but do not offer guidance on how to apply the theory in the real life"*[3].

The above issues suggest that organizations should put in place an appropriate framework that ensures they are implementing technical and organizational measures such that data processing is performed in line with the GDPR.

[3] https://smeunited.eu/news/smes-say-gdpr-needs-reality-check

1.1 Our contribution

The above discussion motivates the need for a security framework that considers both the protection of the organization from cyber attacks and the requirements established by the GDPR. This paper presents the Italian National Framework for Cybersecurity and Data Protection (hereinafter referred to as *Framework*) to support organizations that need strategies and processes aimed at the protection of personal data and cybersecurity[4]. The goal is *to provide a flexible and unified tool to support organizations in the implementation of cybersecurity* **and** *data protection programs toward standards and regulations.*

The proposed Framework, that extends the one presented in [4], includes specific prescriptions necessary for an organization to implement a full cybersecurity and data protection program; its adoption can help organizations define a path toward cyber protection that is consistent with current regulations and that can be adapted taking into account the specific needs and maturity of the company. For organizations that already implement measures consistent with GDPR, the Framework can be used for guiding the necessary continuous monitoring activities. According to the GDPR, data security is an important part of wider compliance with data protection obligations (mainly considered in articles 5 and 32 of GDPR). However we observe that these aspects are quite often those that represent technical challenges especially for SMEs. The adoption of a cybersecurity framework may represent a best practice and a way to demonstrate that the organization adopted a well-grounded duty of care, an important step to properly face fines and the legal liability of lawsuits.

2 Related Work

Several frameworks dedicated to cybersecurity and data protection have been proposed in the past. Most of them provide technical indications, while others propose a more high level approach. In this section we briefly discuss those among them that have the largest similarities with the Framework proposed in this paper. We refer to [19] for a detailed comparison and discussion.

ISO/IEC 27000. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publish the 27000 family of documents and standards to help organizations keep their information assets secure. In particular, organizations can be certified to respect the standard ISO/IEC 27001 published in 2013. We observe that certification is a plus that however comes at a cost that might be non negligible for small companies. ISO/IEC 27001 and ISO/IEC 27002 provide a comprehensive lists of security controls discussing how to accomplish each control statement; namely, it includes more that one hundred control measures that address the most common information security risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. ISO/IEC

[4] The Italian National Framework for Cybersecurity and Data Protection [5] is publicly available at http://www.cybersecurityframework.it/

27000 is a set of best practices with a focus on information security and provides practical advice on how to protect information and reduce cyber threats.

Recently, (August 2019) ISO/IEC published the document 27701 that complement the ISO/IEC 27000 family of standars by specifically addressing privacy issues and has the main goal of providing a unifying framework for implementing GDPR. The New ISO/IEC 27701 jointly with ISO/IEC 27001 proposes a consistent approach mixing information security and data protection (Privacy). ISO standards are well known and recognized in businesses worldwide and the market of auditors and certifiers is fully mature. This clearly sets an advantageous path for organizations that were already certified ISO/IEC 27001 compliant, to further embrace the new ISO standard and deploy startegies to protect personal identifiable information, in coherence with GDPR.

On the negative side, the ISO/IEC 27000 family of standard is known to be complex and expensive to implement and certify, limiting their general applicability to organizations with specific needs, or large size. This is particularly true for micro enterprises and SMEs, and in general for companies where IT is not the core business. For all these reasons accreditation with ISO/IEC 27001 is not widespread: in 2018 there were about 30,000 worldwide certifications, less than 9,000 in EU (including UK)[5]. Furthermore, an explicit adoption of ISO/IEC 27701 for GDPR certification by National supervisory authorities may pose problems in relation with Article 42/43 of the GDPR that state certification requirements must be made *"publicly accessible by the supervisory authorities in an easily accessible form"* and that authorities should take special care of *"specific needs of micro, small and medium-sized enterprises"*. Lauchad discusses these and further threats and opportunities on this topic in [7].

HITRUST CSF. The HITRUST Alliance is an independent organization based in the United States whose partners develop and maintain HITRUST CSF [11] a security framework that is based on ISO/IEC 27001 and 27002 that are integrated with other major information security standards, regulations, and requirements. Historically, they have focused on the healthcare industry but are also considering the financial services industry. Recent versions of the framework incorporate GDPR and privacy regulations in other countries. We note that HITRUST CSF targets heavily regulated markets and its implementation is rather complex. Organizations that are involved in healthcare delivery and payments would be well-suited to evaluate HITRUST for adoption since it covers many of the unique regulations of these industries; on the other side HITRUST CSF is not suited for organizations in other areas.

Other NIST Frameworks. The NIST Risk Management Framework (NIST RMF) [14] is a US federal government policy and standards to help secure information systems developed by National Institute of Standards and Technology. It provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle

[5] See ISO survey for details; available at `https://www.iso.org/the-iso-survey.html`

through six steps. During its life cycle, an information system will encounter many types of risk that affect the overall security posture of the system and the security controls that must be implemented. The RMF process supports early detection and resolution of risks. We note that this framework is more complex to implement than the NIST Cybersecurity Framework and that it could take external expertise to assist with implementation for most organizations.

NIST recently published the Privacy Framework [18] that specifically addresses compliance with privacy regulation though has not been designed to directly address GDPR requirements. The framework also provides cross references between the Privacy Framework and the Cybersecurity Framework; such references are directly applicable to our framework as well.

Finally, concerning technical proposals, ENISA reports a list of third-party tools tied to Risk Management and Risk Assessment, eventually encompassing Data Protection aspects [9]; After a review of these tools, we concluded that they mainly cope with technological aspects considered during policy implementation. Our proposal is positioned at a higher modeling level and can benefit from those tools in implementing the security controls. The above discussion motivates the relevance of the Cybersecurity Framework originally proposed in [17] for its generality and flexibility that makes it applicable to all organizations independent of the size, the cybersecurity maturity, the specific area etc.

3 Background on the Framework

This section introduces key elements of the first version of the Italian National Cybersecurity Framework referring to [4] for a more detailed presentation. The Framework inherits the three fundamental elements of the NIST Cybersecurity Framework, namely *Framework Core*, *Profiles* and *Implementation Tiers*, and introduces three additional concepts: *Priority Levels*, *Maturity Levels* and *Contextualization* (Fig. 1).

Framework Core. The Framework Core represents the life cycle structure of the cybersecurity management process, both from a technical and organizational point of view; it is hierarchically structured into functions, categories and subcategories. The five functions (*IDENTIFY*, *PROTECT*, *DETECT*, *RESPOND*, *RECOVER*) are concurrent and continuous and represent main security topics to be addressed; the cybersecurity enabling activities (e.g. processes and technologies) that should be executed are defined. Namely, for each subcategory the Core presents informative references that link the subcategory to known cybersecurity practices provided by industry standards (e.g. ISO/IEC 27000 [13], NIST SP 800-53 rev. 4 [15], COBIT 5 [12], CIS CSC [3]) or general legal regulations. The 5 functions group together categories and subcategories linked to the following themes:

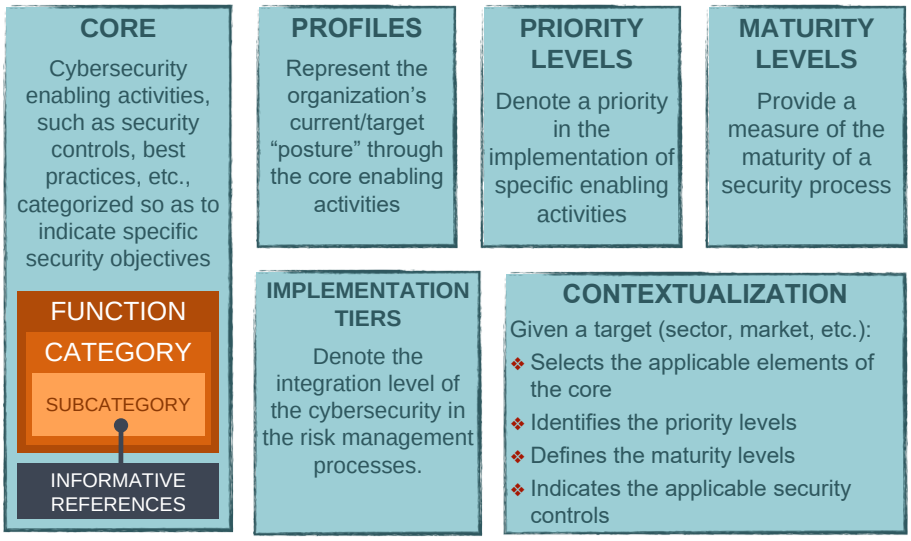

Fig. 1. Key elements of the Framework.

IDENTIFY - identification of business processes and associated risks with the goal of defining resources and investments coherent with risk management strategy and business objectives.
PROTECT - implementation of measures aimed at protecting business processes and corporate assets, regardless of their IT nature.
DETECT - definition and implementation of appropriate activities to promptly identify cybersecurity incidents.
RESPOND - definition and implementation of the appropriate activities to contain and mitigate impact when a computer security incident has been detected.
RECOVER - definition and implementation of activities for the recovery of processes and services impacted by an accident. The objective is to support the timely recovery of business operations.

Profiles. Profiles are the result of an organization's selection of specific subcategories based on several factors: the risk assessment, the business context, the applicability of the various subcategories. Profiles can be used to improve the security status by comparing the *current profile* with the desired (*target*) profile. The current profile can be used to define priorities and to measure progress towards the target. Profiles can be also used to communicate cyber risk posture within or outside the organization.

Implementation Tiers. Implementation Tiers provide context on the integration level of cyber risk management processes within the organization. There are four levels of evaluation, from the weakest to the strongest.

Partial The cyber risk management model does not systematically take into account cyber risk and it is managed with ad hoc processes and often reactively. The level of awareness of cyber risk is limited and there are no processes for sharing information related to cybersecurity with external entities.

Informed The cyber risk management model has processes that consider risk but they are not extended to the entire organization. The level of awareness of cyber risk is sufficient, but it does not involve all levels of the organization. The information exchange related to cybersecurity events is limited.

Repeatable The cyber risk management model is formally defined and the organization regularly updates its practices. Management of cyber risk is pervasive at all organizational levels and staff are trained to manage assigned roles. The organization regularly exchanges information on cybersecurity with other actors operating in the same ecosystem.

Adaptive The cyber risk management model regularly adapts its cybersecurity procedures through the use of past experience and risk indicators; moreover the organization adapts continuously to ever-changing threats and is able to respond effectively to sophisticated attacks. The exchange of information with other actors operating in the same ecosystem is continuous.

Priority levels. Priority levels allow organizations and companies to support the definition of an implementation program to reach a target profile that prioritize those actions that most reduce the risk level. There are three key factors:

1. exposure to threats, determining the actions that decrease the likelihood of the threat;
2. probability (i.e. frequency) of threat occurrence;
3. impact of the damage resulting from a cybersecurity incident.

The above classification is used to set priorities on the basis of two specific criteria:

- ability to reduce cyber risk by acting on one or more key factors for its determination;
- implementation costs and impact for specific actions.

The Framework suggests three simple priority levels: *High, Medium, Low.* High priority actions significantly reduce one of the three key factors of cyber risk that must be implemented independently of the complexity of the implementation. Medium (Low) interventions make it possible to achieve a reduction of one of the three key factors of cyber risk and are simple (complex and costly) to implement.

Maturity levels. Maturity levels provide a reference point by which each organization can evaluate its own subcategory implementation and set goals and priorities for its improvement. They measure the maturity of a security process, of a specific technology, of the amount of adequate resources used to implement a given subcategory. We observe that an organization may have different maturity

levels for different subcategories; moreover the maturity level of a subcategory requires that all specified security practices are implemented. This allows organizations to define their level of maturity and to identify the security actions necessary to achieve their desired goals.

Contextualization. Basic elements of the Framework are general and independent to the context characteristic (e.g. production sector, size or location of the organization). Contextualizing the Framework for an organization or an application area (e.g., a productive sector or a homogeneous category of organizations) requires specifying its core by selecting the relevant functions, categories and subcategories, and defining the desired priority and maturity levels for all the selected subcategories. A contextualization is defined through the following steps:

1. select the list of functions, categories and subcategories that are relevant to the organization on the basis of all or some of the previous elements (production sector, size and location of the organization, etc.);
2. define the priority levels for the implementation of the selected subcategories;
3. define guidelines at least for high priority subcategories;
4. specify maturity levels at least for high priority subcategories.

4 The Italian National Framework for Cybersecurity and Data Protection

The Framework presented in this paper introduces two main novelties:

- improves the Framework Core by introducing new categories and subcategories dedicated to data protection topics (Section 4.1);
- introduces *Contextualization Prototypes*, a new tool that support and facilitates the definition of contextualizations (Section 4.2)

4.1 Framework Core

As the original Italian National Cybersecurity Framework [4], the version presented in this document is also based on the Cybersecurity Framework developed by NIST [17]. In particular, changes made by NIST to the Framework Core with their recent v1.1 have been integrated: a new category has been added to manage security issues linked to supply chains; a category has been modified to strengthen the security of authentication and identity management processes by adding two subcategories; finally three new subcategories have been added to control the integrity of hardware devices, to meet resilience requirements and to manage information about vulnerabilities.

In addition to the modifications made by NIST, we introduced further categories and subcategories to integrate data protection elements in the Framework Core. To this end, nine new subcategories and a new category have been introduced which capture the following aspects related to data protection:

- data management processes, with particular reference to those applicable to personal data;
- methods for personal data processing;
- roles and responsibilities in the management of personal data;
- impact assessment on the protection of personal data;
- documentation and communication procedures following incidents that are considered a violation of personal data.

We observe that the proposed modifications extend the previous Framework Core and align it to the different standards that already deal with the problem of personal data protection and make it applicable even in contexts where general or sector regulations impose specific requirements on data processing.

4.2 Contextualization Prototypes

Contextualization prototypes are a new tool for simplifying and structuring the creation of a contextualization of the Framework. A contextualization, in general, requires to integrate several requirements, stemming from regulations, technical standards, best practices, etc. Prototypes can be defined such to embed these requirements in a general format that can be applied to independent contextualizations. Therefore, contextualization prototypes facilitate the definition of a contextualization by allowing to build it incrementally, coping with the different technical regulations, or legal regulations or best practices one at a time and then integrating them in the final result. Prototypes can be used, for example, to represent:

- general regulations that impose the implementation of specific practices of cybersecurity or data protection;
- technical standards or guidelines that indicate specific checks related to cybersecurity or data protection;
- industry best practices related to cybersecurity or data protection.

For each subcategory a prototype defines an implementation class among the following options:

- **MANDATORY:** the subcategory must be included in all contextualizations that implement the prototype;
- **RECOMMENDED:** the inclusion of the subcategory in all contextualizations that implement the prototype is suggested;
- **FREE:** the inclusion of the subcategory in the contextualization that implements the prototype is optional.

For each subcategory a contextualization prototype might define a priority level for its implementation. Furthermore, a prototype is accompanied by an implementation guide, a document that describes:

- the prototype's application context;

– additional constraints on the selection of subcategories and the definition of priority levels;
– an optional list of security checks, for the considered subcategories, which will be opportunely organized in the different maturity levels during the implementation of the prototype.

Therefore, contextualization prototypes do not replace contextualizations, but provide a support tool that facilitates the creation and update of a contextualization through their composition as illustrated in section 5.1. The contextualization prototypes maintain their compatibility with the form of a contextualization, and this feature allow their integration into tools that we already provided in the past for implementing the framework contextualizations, such as [6] and CRUMBS, a cybersecurity framework browser [2].

5 Implementation methodology

The use of the Framework is achieved through two fundamental activities described in the following sections: (i) contextualization of the Framework to a specific application context and (ii) implementation of the Framework by an organization.

5.1 Contextualizing the Framework

The process of defining a contextualization is usually delegated to the single organization that decides to adopt the Framework, but it can also be provided by an association, a regulator or, more generally, by any actor able to identify and apply to the contextualization a set of characteristics belonging to one or more organizations. The process, shown in Fig. 2, requires the selection of one or more prototypes, the integration of aspects that they model in the contextualization, (legal or technical regulations, industry best practices etc.) and the refinement of the resulting contextualization with respect to the organization's specific aspects.

For each prototype of interest the following steps are performed:

1. all subcategories indicated as mandatory in the prototype are selected in the contextualization;
2. the inclusion in the contextualization of the subcategories indicated as recommended in the prototype must be assessed, considering the specific characteristics of the application context;
3. any further restrictions on the selection of the subcategories documented in the prototype's implementation guide must be applied;
4. any further restriction on the definition of priority levels documented in the prototype's implementation guide must be taken into account when adapting prototype's priority levels to the application context;
5. any security checks documented in the prototype's implementation guide can be integrated into the contextualization application guidelines.

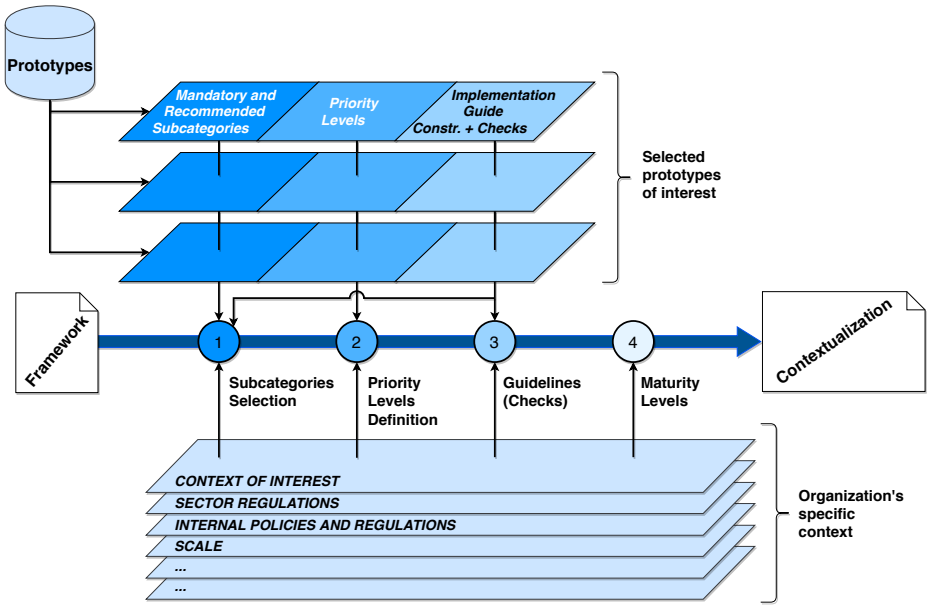

Fig. 2. Contextualization of the Framework through the implementation of prototypes.

At the end of this implementation process, repeated for all the contextualization prototypes of interest, the resulting contextualization can be further specialized where needed.

5.2 Implementing the Framework

Recall that the objective of the Framework is to provide a tool to support management of cyber risk management precesses. It is plausible that in many cases cybersecurity programs have already been implemented. In these cases the introduction of the Framework is to be intended not to replace what is already in place, but as further reference in order to:

- improve (or define, if not present) a cybersecurity and data protection program in a structured and integrated way, based on risk management, which can be implemented in the presence of pre-existing security governance models;
- determine the level of maturity of the cybersecurity and data protection activities, identifying appropriate improvements or rationalization of costs, in favor of a rational redistribution of resources;
- conduct benchmarking among companies and organizations operating in specific sectors or with similar characteristics that can favor the improvement of security levels, simultaneously enabling the cyber insurance market;
- facilitate communication with top management (e.g. directors and boards of directors, shareholders, etc.) and with external actors (e.g. rating agencies,

suppliers and partners), so that the cyber risk levels to which the organizations are exposed are clearly represented and to identify the investments and resources to be put in place for an adequate risk reduction.

The implementation of the Framework follows a set of essential steps. The identification/creation of a contextualization (step A) has been thoroughly described in the previous sections and is the part more impacted by the contextualization prototypes. In the following the essential steps are reported:

A. Identify a contextualization of the Framework. If the organization belongs to a regulated sector, it should use one of the contextualizations provided by its own sector regulator, or define its own contextualization by implementing any prototypes that collect the applicable regulations. In the case in which the organization does not belong to a regulated sector, it can identify the contextualization to be used among the available ones, or define a specific one;

B. Define priorities and scope. Periodically identify the organization's strategic objectives and business priorities to select key areas and functions that require specific focus;

C. Identify systems and assets. Identify information and systems that the organization considers vital and critical to guarantee the organization's operations. This step is especially important for the subsequent phases, since it allows for the proper assessment of the impacts during the analysis of the risks and thus facilitating the understanding of the actual needed level of protection;

D. Determining the current profile. The implementation status and maturity level for each subcategory of the Framework is expected to be assessed. This allows to define one or more current profiles in relation to the areas/functions envisaged for the implementation of the program;

E. Risk analysis. Determine and evaluate risks by adopting an appropriate methodology in relation to the specific organizational and market characteristics in which the organization operates. Some ideas regarding the process of analysis and risk management are provided in [4] (section 7.2);

F. Determine the target profile. Through the risk management process, the organization must be able to define a target profile that, unlike the current one, represents the level of implementation and maturity that it is intended to achieve for each subcategory of the Framework. It is desirable that the selection of these levels can be carried out having already integrated the cybersecurity risk management within the enterprise risk management program, so that the management of cyber risk can benefit from decisions taken at the higher organizational level (i.e., top management), using a comprehensive systemic view to support decision-making;

G. Determine the gap with respect to the target profile. Conduct a comparison between the target and the current profile to identify the gaps in the management of cybersecurity;

H. Define and implement a roadmap to reach the target profile. The application phase of the Framework implementation consists in defining the set

of activities necessary to reach the target profile determined in phase F. This means developing a specific plan to implement the individual security checks of the Framework, following a time schedule that will vary according to the actual risks and the specific conditions in which the organization operates;

I. Measuring performance. In order to review actions taken and improve them to efficiently reach the target profile, it is necessary to define monitoring metrics that can also highlight operational costs. Evaluation of the efficacy of the current profile must be used to define the new target profile.

6 A GDPR Contextualization Prototype

We now present a GDPR contextualization prototype (hereinafter referred to as the GDPR prototype). Recall that prototypes represent a starting point for creating contextualizations by adapting the prototype to the specific context of the sector, organization or company under consideration. This requires to select the subcategories of interest, the priority levels, and define appropriate maturity levels, according to the specificity of the application context. As we already pointed out, a contextualization for an organization can be obtained by combining more prototypes.

The GDPR prototype supports the integration of the fundamental elements of the regulation and, therefore, can be applied in many contextualizations.

Due to space constraints the entire specification of the contextualization prototype cannot be included in this document; we refer to [5] for a detailed presentation.

Selection of subcategories. The subcategory selection process is guided by the classification described in section 4.2. The GDPR contextualization prototype organizes the subcategories according to the following criteria:

MANDATORY: these subcategories express requirements that are explicitly stated in the Regulation, and that must therefore be included in any contextualization that adheres to this prototype. As an example, subcategory DP-ID.AM-8 captures a fundamental aspect of Art. 30 from GDPR by stating that "records of personal data processing activities must be identified and maintained".

RECOMMENDED: this class gathers those subcategories which, while unable to completely encompass fundamental aspects of the Regulation when considered singularly, allow to consider those aspects on which the Regulation waives more freedom regarding the modalities of implementation when combined together (e.g., artt. 25 and 32). On the other hand, the term RECOMMENDED should not suggest that their implementation is, to some extent, "optional" or "marginal". Conversely, these aspects must be implemented according to the modalities that best suit the specific context under consideration (as long as compliant with the Regulation) by coherently selecting the RECOMMENDED subcategories, and possibly integrating them

with additional FREE subcategories if necessary or appropriate for the specific context.

FREE: all the other subcategories. For these subcategories there is no motivation which definitely support their selection in relationship with the Regulation. Nevertheless, this does not mean that the selection of these subcategories is "not recommended"; it means that their selection is subordinate to the specific context under consideration.

Priority levels. The GDPR contextualization prototype specifies a "predefined" priority level for all MANDATORY and RECOMMENDED subcategories. During the creation of a contextualization these priority levels must be revised to appropriately fit the specificities of the context under consideration. Moreover, the priority levels for the selected FREE subcategories must be defined. The priority of each subcategory is defined on the three-level scale described in section 3 (*High, Medium, Low*).

Moreover, the GDPR prototype's implementation guide defines the following constraint: "all MANDATORY subcategories must be set to *High* priority". Namely, their default priority level is *High* and cannot be changed. Their implementation should be a priority regardless of complexity and cost. Refer to [5] for the details of the priority levels assigned to the MANDATORY and RECOMMENDED subcategories.

Implementation Guide. The GDPR prototype provides a guide for supporting the implementation of contextualizations based on it (see section 4.2). This defines for each MANDATORY subcategory a set of security and data protection *checks* that refer to one or more articles of the GDPR covering several fundamental areas of interests. The reader is encouraged to check the full details of the implementation guide on the supplementary material available at `http://www.cybersecurityframework.it/supplemental_material.pdf`.

7 Conclusions

In this paper we presented the Italian National Framework for Cybersecurity and Data Protection. Standing on top of the original Italian National Framework for Cybersecurity, this new proposal improves it by integrating elements linked to data protection and providing tools for its implementation in the current context where the General Data Protection Regulation (GDPR) provides a single source of data protection rules for all organizations that manage personal data from EU citizens. The framework has the goal of supporting organizations in the definition of a comprehensive cybersecurity and data protection program that is clearly structured, risk-based, goal-oriented and in line with current regulations and technical standards. The framework also supports the organization governance in monitoring the program implementation and assessing its evolution toward the intended targets.

References

1. Accenture and Ponemon Institute: Cost of cybercrime study. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017?src=SOMS (2017)
2. Angelini, M., Lenti, S., Santucci, G.: Crumbs: A cyber security framework browser. In: 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–8 (Oct 2017). https://doi.org/10.1109/VIZSEC.2017.8062194
3. Center for Internet Security: Critical Security Controls for Effective Cyber Defense (CIS Controls). https://www.cisecurity.org/
4. CIS Sapienza: 2015 Italian Cyber Security Report: Un Framework Nazionale per la Cybersecurity. https://www.cybersecurityframework.it (February 2016)
5. CIS Sapienza: Framework Nazionale per la Cybersecurity e la Data Protection. https://www.cybersecurityframework.it (February 2019)
6. CIS Sapienza: Tool for the implementation of Italian Cybersecurity Framework. http://tool.cybersecurityframework.it (2020)
7. E. Lachaud: ISO/IEC 27701: Threats and opportunities for GDPR certification. https://research.tilburguniversity.edu/en/publications/isoiec-27701-threats-and-opportunities-for-gdpr-certification (2020)
8. ENISA: Guidance and gaps analysis for european standardisation. https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation (2019)
9. ENISA: Inventory of risk management / risk assessment tools. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools (2020)
10. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC (May 2016)
11. HITRUST Alliance: HITRUST CSF. https://hitrustalliance.net/hitrust-csf/
12. ISACA: Cobit 5. ISA (2012)
13. ISO/IEC 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary (February 2018)
14. NIST: Risk management framework overview. http://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
15. NIST: SP 800-53 Rev. 4 – Security and Privacy Controls for Federal Information Systems and Organizations (April 2013)
16. NIST: An Introduction to Privacy Engineering and Risk Management in Federal Systems (NIST Interagency Report 8062). https://csrc.nist.gov/publications/detail/nistir/8062/final (January 2017)
17. NIST: Framework for improving critical infrastructure cybersecurity (version 1.1). https://www.nist.gov/cyberframework/framework (April 2018)
18. NIST: NIST Privacy Framework. https://www.nist.gov/privacy-framework (January 2020)
19. Zaras, D.: Information Security Frameworks and Controls Catalogue (Impact Makers Report) (2018)