NIST CyberSecurity Framework Compliance

A Generic Model for Dynamic Assessment and Predictive Requirements

Nuno Teodoro, Luís Gonçalves, Carlos Serrão

Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL
Ed. ISCTE, Av. das Forças Armadas, 1649-026 Lisboa, Portugal
nuno.filipe.teodoro@gmail.com, lcbsg@iscte-iul.pt, carlos.serrao@iscte.pt

***Abstract*— Organizations have become increasingly dependent on information systems to perform their business as usual activities. Moreover, organizations have registered an increase in the number of cyber-attacks, namely: industrial espionage, confidential information leakage, digital theft or pure damage to corporate image and reputation. In order to try to mitigate these issues, organizations like the National Institute of Standards and Technology (NIST) have made an effort to establish a cybersecurity protection guide. This paper presents a baseline for developing a generic and flexible model for manipulating key factors inside organizations: Processes, Human Resources and Technology, and extrapolate the percentage of compliance with the NIST cybersecurity framework, measure the current cybersecurity risk and allocate financial investments towards specific compliance objectives and reduce the overlapping of existing resources.**

Keywords*— *NIST, Compliance, Cybersecurity, Resources Optimization, Information Security, Generic Model, Privacy.

I. INTRODUCTION

Modern organizations are struggling to protect one of its most important assets - information. More than ever, information technology (IT) is a part of business, thus the prospect of IT compromise reflects on business compromise also. Therefore, electronic data must remain safe from criminal or unauthorized use. This ever-growing need as well as the methods to avoid such unwanted actions is commonly referred as cyber security (CS), which has been shaping the landscape of data and IT protection [1]. CS, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction [1].

More than ever, and progressively faster, daily lives, economic vitality and national security depend on a stable, safe, and resilient cyberspace. These vast arrays of networks support people and corporate communication, travelling, ensure power delivery to homes and companies, drive economies, and provide government services [2] [3].

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store large amounts of confidential information on computers and transmit them across networks to other computers. With the growing volume and sophistication, asynchronization and distribution of cyber-attacks, ongoing attention is required to protect sensitive businesses and personal information, as well as to safeguard national security [4]. Moreover, the majority of executives and business owners rarely possess the necessary CS expertise, turning decision making an even more daunting task. This lack of know-how, combined with the perceived "black box" nature of CS, creates additional challenges for executives on well-informed decision-making processes (which involve interdisciplinary dimensions, such as management, organization and technology) in this field [4].

By empowering the deployment of a robust and comprehensive CS strategy, top managers are driving revenue, by reducing exposure to cyber threats and increasing business continuity. From a strict economic perspective, such strategy deployment will result in capital expense (CAPEX) as well as operation expense (OPEX) reduction, *e.g.*, by minimizing technology overlapping and misfit [5].

Supporting the fact that CS is becoming a major focus for most organizations, chief information officers (CIOs) and chief security officers (CSOs) have elected it as one of their top priorities [6], especially when they are accountable for Information Security and Data Protection, responsible for securing strategic information assets on the organization. Although cyber security priorities have been changing over time from bottom to top, mostly due to economic recession, top managers are now aware and demand an effective cyber security strategy, but also require it to be accomplished on a lower budget, minimizing resources and in a short period of time.

All of these concerns have conducted to the development and deployment of some cyber security initiatives, conducted by some accredited international entities, such as ISO [7], SANS [8], NIST and ISACA [9]. Despite the fact that several frameworks have been developed and deployed by public and private organizations to address CS, the reality shows that there is no generic model embracing these initiatives. Such model would provide organizations with guidelines to manage and report on cybersecurity investments, as well as to enable progressive, continuous and learning approaches on organizational human resources (HR), processes and technology [10].

Huge focus has been placed on critical infrastructures, leading to the development and implementation of relevant cyber security frameworks (CSFs) to address them [11] [12].

When deploying a CSF and data protection strategies, one of the most usual steps is to survey all existing CSFs, misleading organizations into developing activities without proper guidance and the necessary management requirements that essential to succeed. Although current CSFs' applicability to organizations is not questionable, the reality is that it becomes impossible to achieve full compliance with all the frameworks' activities. Moreover, activities' complexity and implementation times greatly reduce the overall efficiency of the approach, and scatters the definition and deployment of a CS strategy.

The authors consider that the best way to address these problems is through the definition of a management system capable of supporting progressive deployment, and to implement a maturity model capable of preventing misplaced investments, aligning them with the organization's CS strategy and requirements. All of these should integrate a single and generic risk-based CSF that continuously assimilates new information and track the changing stakeholder priorities and adversarial capabilities, using decision-analysis tools to link technical data with expert judgment.

Moreover, modern organizations are dynamic environments influenced by internal and external factors, which can drastically impact HRs' capabilities and security teams' size and competences, thus making static CSFs and models inefficient and inadequate to adapt to these changes.

By focusing what we consider to be the three organizational pillars to CS (HR, processes and technology), a generic and flexible model is introduced allowing organizations to evaluate their compliance level with the NIST CSF, enabling identifying capital and operational investments, risk prediction and management (e.g. key HR leaving or phased out technology) as well as capacity planning. The model will be conceptually defined and, in order to provide a practical example, a specific scenario will be used to evaluate its applicability.

The remainder of the paper is organized as follows. In section II the motivation behind using NIST as single reference framework and the proposed model objectives are presented. Section III focuses on the NIST framework and corresponding activities, input information to the proposed model, presented in Section IV. Section V presents the scenario assumptions for section VI, where the model will be applied, and evaluations as well as the most relevant results are presented in Section VII. Finally, Section VIII concludes this paper.

II. MOTIVATION AND OBJECTIVES

The implementation of NIST's CSF in its full extent within an organization can become a complex and time-consuming task. Moreover, by not knowing if an organization is compliant with this framework at some level can lead to misplaced investments and processes reengineering especially in HR and technology, resulting in higher costs and an overall CS efficiency decrease.

A. Organizational Aspects

From an overall CS strategy standpoint, by not having a program capable of steering CS initiatives at the business level may cause adversities inside organizations, namely:

- Lack of measurable results through consistent metrics;
- Top management not allocating budget for CS initiatives;
- Lack of top management sponsorship within the organization's process and hierarchy for CS;
- Mislead strategic investments from CIOs and CSOs;
- Inadequate protection on clients and organization's data, leading to increased exposure to CS threats;
- Misaligned Governance Risk and Compliance strategies, by not considering Cyber Risk;
- Inadequate Business Continuity programs, by not considering CS requirements' changes over time;
- Improper response capability to CS incidents, both at the technical and process levels;
- CS activities misalignment with business objectives, leading to overspending and decreased efficiency.

From an operational point of view, the inexistence of a CS model addressing HR, processes and technology capabilities, driving CS initiatives, reveals some additional shortcomings, such as:

- Unqualified and ineffective HR developing CS activities;
- Conducting initiatives misaligned with the organization's CS maturity, leading to unnecessary effort and no way to take advantage of its results;
- Unsustainable CS investments on existing resources, both financial and human;
- Inexistent of a grading scale to justify investments to top management in order to achieve a continuous improvement state;
- Incapacity to assess risk levels to cyber-attacks and predict risk exposure variation by manipulating internal processes, human resources and technology.

B. NIST Framework Aspects

NIST CSF identifies a set of core activities [13], aiming to implement a complete CSF within organizations. If it focused on five core functions, each with a set of activities, in order to achieve CS strategic or operational goals.

However, NIST CSF fails to consider organizational key factors like processes, HR and technologies (already existing or that should be considered within an organization). Not considering those factors, there is not a clear relationship path or mapping between the NIST CSF's activities and outcomes and the organizational CS activities and strategy is missing. This leads to some important drawbacks:

- No standard reference for organizations to follow;
- Scattered and proprietary CS frameworks;

- No compliance assessment;
- Misleading strategic CS investments;
- Lack of visibility of CS maturity gaps on key vectors (processes, HR skills and technologies);
- Incapacity to create direct relationship between CS risk exposure and NIST CSF compliance.

Failing to bridge this gap makes compliance difficult to assess, KPIs hard to be drawn and implications of variations of organizational competences and capabilities cannot be assessed.

C. Bridging The Gap

In order to reduce the existing gap between the aspects from the last two subsections, a model is introduced to bridge the NIST framework's core activities and the three fundamental organizational CS pillars: Human Resources, Processes and Technology. Mapping both, along with the possibility to predict compliance with the framework and maturity levels variation with the inclusion and/or exclusion of additional vectors is the improvement proposed by the work described by this paper.

In order to achieve such goal, a model is introduced aiming to be as generic and flexible as possible, allowing it to be adapted to most organizations. Its final purpose is to be able to provide organizational guidance and steer CS strategies according to NIST CSF.

III. NIST Cybersecurity Framework Core Functions

The National Institute of Standards and Technology - NIST - is the federal technology agency that works with industry to develop and apply technology, measurements, and standards. NIST, together with several public and private entities, has created a CSF which focuses on using business drivers to guide CS activities and considering CS risks as part of the organization's risk management processes. There are five concurrent and continuous core functions to provide a high-level, strategic view of the lifecycle of an organization's management of CS risk. The five core functions (Identify, Protect, Detect, Respond and Recover) are presented and described in the following sections.

A. Identify

The activities within this core function aim to develop the organizational understanding and awareness to manage CS risk to organizational systems, assets, data, and capabilities. Understanding business contexts, the resources that support critical functions and the related CS risks enable an organization to focus and prioritize efforts, consistent with its risk management strategy and business needs.

B. Protect

The second core function aims to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential CS event or incident.

C. Detect

The third core functions focuses on developing and implementing the appropriate and necessary organizational activities in order to timely and proactively discovers and identify the occurrence of a CS event or incident.

D. Respond

The Respond function addresses the identification of the activities to take action regarding a detected CS event or incident. It is a post-event function, focusing on reactive activities, supporting the ability of impact containment.

E. Recover

Like the Respond function, Recover is a post event or incident reactive function. It focuses mainly on developing and putting to practice the appropriate set of activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a CS event or incident, supporting timely recovery to normal operation state, thus reducing the overall impact of event.

IV. Conceptual Proposed Model

The proposed model will be developed in such a way that it can be applicable to most organizations. In order to be flexible and generic enough to be applied to different organizational realities, this model will have into account the following assumptions:

- Different CS maturity levels across the organization;
- NIST CSF subcategories' relevance may differ between organizations;
- Technology agnostic, focusing on the functionality and objectives;
- Internal structure and organizations between teams and departments.

The model aims to be as generic as possible from an organization perspective (represented by the three pillars, HR, processes and technology) and to bridge each own reality with NIST CSF, providing as result a set of metrics which allow for a baseline analysis of compliance level to that standard.

A. Model Architecture

The model high-level architecture is presented in Figure 1. As stated, the model takes into account the three organizational vectors, which can vary. These vectors are the model inputs, namely organizational processes, human resources capabilities and existent technologies. The combinations of the several input levels also enables evaluating maturity levels and extrapolate results for the defined output *key performance indicators* (KPI).

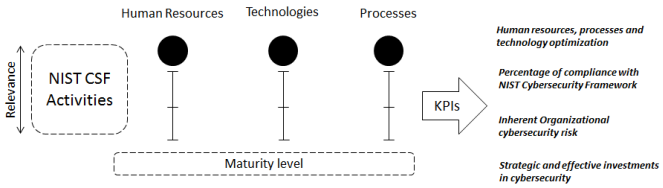

Figure 1 – Model Architecture.

By mapping these inputs with the NIST CSF activities, KPIs are derived as model outputs allowing a high level analysis and compliance levels establishment.

B. Model Outcome

The proposed model outputs will provide guidance and enable analysis on the different aspects that are presented next.

- *Optimizing HR, processes and technology*

Choosing and optimizing HR's capabilities according to core CS activities can result in cost reductions and increased efficiency, maximizing the return on investment. By having skilled and high spectrum knowledgeable personnel to address CS, organizations maximize technology usage and reduce function overlapping. By bridging with NIST core activities, organizations can assess their needs and plan HR capacities for CS, deciding on whether to hire or outsource functions, according to their business needs. As an example, an organization which is not targeted by specifically developed malicious software, might not need a dedicated reverse engineering skill, thus outsourcing that specific function. On the other hand, for a company that frequently suffers from those kinds of cyber-attacks, having specific in-house HR skills instead of outsourcing it may induce cost reductions. The proposed model enables this kind of analysis.

Technology wise, overspending, feature overlapping and usage minimization are the most common problems. By evaluating and choosing CS technologies' features according both to organizational needs and to the NIST cybersecurity framework requirements will enable an optimized CS set of activities, reduced maintenance and upgrade costs, as well as maximized usage and benefit extracted from technology.

HR and technology are connected through processes. By deploying the correct and optimized processes and procedures, overall CS efficiency will increase, minimizing cyber-incident response times, mitigation and post-incident recovery.

- *Assess the percentage of compliance with NIST CSF*

By assessing processes, HR and technology vectors regarding capabilities and completeness, the proposed model will provide a measurement of compliance with NIST CSF. The three vectors are inputs to the model and can vary, resulting in an estimated percentage of NIST CSF compliance, therefore allowing to fine tune required capabilities.

- *Evaluating inherent organizational Cyber Risk.*

The proposed model, by enabling the evaluation of the NIST CSF's compliance, can be used to perform dynamic cyber risk analysis, *e.g.*, when HR skills are no longer available or obsolete technology is used. Additionally, evaluating the risk of technology changes and performing risk-based capacity planning are enabled by the model, closely relating changes prediction within the organization with CS posture.

- *Performing strategic and effective investments in CS processes, HR and technology*

Budget allocation and investments in CS related activities can be difficult to justify without proper KPIs and consistent objectives. Additionally, in order to continuously evaluate the health level of the CS activities and maturity level of an organization, several checkpoints must be in place. These checkpoints enable a consistent increase of the CS posture, while evaluating the return on the investment. Moreover, those checkpoints allow for corrective measures, when needed, budget adaptations and may even justify budget or investment reinforcements.

The proposed model balances the interaction between processes, HR and technology, with compliance and KPIs as outcome, allowing management level analysis over long term investments and CS strategies, in order to reach a minimum NIST CSF compliance baseline and acceptable risk levels.

V. MODEL DEFINITION AND ASSUMPTIONS

To define the model and prove the underlying concept, only one function from the NIST CSF was considered for this work: Response. Nevertheless, the model can extent its supports to all the different functions due to its generic nature. The Response function has a total of $\tau_{S_C} = 15$ subcategories (S_C), which are addressed individually. Considering that not all subcategories have the same relevance for each organization, three $\sigma_{\{L,M,H\}}$ weight levels are defined, associated to each subcategory, where $\gamma_{\frac{\{L,M,H\}}{100}}$ represents the relevance percentage of each sub-category, according to (1). In this case we assume $\mathrm{L_i} = 0;\ \mathrm{L_s} = \mathrm{M_i} = 25;\ \mathrm{M_s} = \mathrm{H_i} = 50;\ \mathrm{H_s} = 100.$

$$\begin{aligned} \gamma_{\frac{L_i}{100}} \leq \sigma_L \leq \gamma_{\frac{L_s}{100}} \\ \gamma_{\frac{M_i}{100}} < \sigma_M \leq \gamma_{\frac{M_s}{100}} \\ \gamma_{\frac{H_i}{100}} < \sigma_H \leq \gamma_{\frac{H_s}{100}} \end{aligned} \quad (1)$$

For simplicity sake, we consider the highest value of each weight interval, *i.e.*, $\sigma_L = 0{,}25$, $\sigma_M = 0{,}5$ and $\sigma_H = 1$.

Regarding input variables, we consider $\varepsilon_{\{T,H,P\}}$ representing the three fundamental vectors previously stated, technology, HR and processes, respectively. To quantify each $\varepsilon_{\{T,H,P\}}$ the capability maturity model integration (CMMI) levels [14] are used, to characterize each input's performance value, as a reflex of organizations' processes, according to (2)

$$\varepsilon_{\{t,h,p\}} = \left[\varepsilon_{\{t,h,p\}.\mu_{\{I,M,D,Q,O\}}} \left(\boldsymbol{S_{C_1}}\right) \cdots \varepsilon_{\{t,h,p\}.\mu_{\{I,M,D,Q,O\}}} \left(\boldsymbol{S_{C_{\tau_{S_C}}}}\right)\right] \quad (2)$$

CMMI considers the existence of five maturity models, $\mu_{\{I,M,D,Q,O\}}$, related to internal process development: Initial, Managed, Defined, Quantitatively Managed and Optimizing. Each level has a numeric value associated, ranging from $\mu_I = 1$ to $\mu_O = 5$ respectively. For simplicity we consider the most improved level, Optimized, corresponding to μ_O.

These values are then applied to each input variable, where, *e.g.*, $\varepsilon_H(\mu_O)$ represents a HR input variable with a maturity level of 5, the maximum.

Finding a final value for each subcategory should be done by taking into account all input values and it's corresponding σ. By providing the capability to associate maturity levels to each subcategory and a weight, which directly demonstrates the relevance of that subcategory for the

organization, the model allows flexibility and adaptability to most organizations.

Table I represents a generic placeholder for the parameters described on the previous section and the input and output vectors of the preconized model.

TABLE I. SCENARIO SNAPSHOT PARAMETERS

Function	Category	Subc	Weight	Tech	HR	Proc	Result
Response	DE.AE	DE.AE -1	1 – 0.5 – 0.25	0-5	0-5	0-5	X

From [12] each S_C subcategory of the desired function is extracted and each individual weight level is considered, according to Table II, resulting in a W_{S_C} weight vector for all subcategories given by (3).

$$\mathbf{W}_{\boldsymbol{S_C}} = \left[\sigma_1(\boldsymbol{S_{C_1}}) \cdots \sigma_{\tau_{S_C}}\left(\boldsymbol{S_{C_{\tau_{S_C}}}}\right)\right] \tag{3}$$

By considering (4), the vector of maximum weights is given by (3), considering the maximum $\sigma_{\{L,M,H\}}$ value.

$$\mathbf{W}_{\boldsymbol{S_{C_{MAX}}}} = \left[\sigma_1(\boldsymbol{S_{C_1}}) \cdots \sigma_{\tau_{S_C}}\left(\boldsymbol{S_{C_{\tau_{S_C}}}}\right)\right] \tag{4}$$

In our case, the maximum weight vector is given by (5):

$$\mathbf{W}_{\boldsymbol{S_{C_{MAX}}}} = [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1\,] \tag{5}$$

The sum of all results for all subcategories represent the maximum compliance score, which later on, is used as reference for compliance fulfillment percentage calculations. The input variables are mapped to the CMMI levels and each function's subcategory, S_C has a corresponding ε_i vector, each by the sum of the three components, as given in (6):

$$\varepsilon_i = \varepsilon_T.\mu_{\{I,M,D,Q,O\}} + \varepsilon_H.\mu_{\{I,M,D,Q,O\}} + \varepsilon_P.\mu_{\{I,M,D,Q,O\}} \tag{6}$$

TABLE II. NIST RESPOND FUNCTION'S SUBCATEGORIES

Subcategory, S_C
RS.RP-1: Response plan is executed during or after an event
RS.CO-1: Personnel know their roles and order of operations when a response is needed
RS.CO-2: Events are reported consistent with established criteria
RS.CO-3: Information is shared consistent with response plans
RS.CO-4: Coordination with stakeholders occurs consistent with response plans
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
RS.AN-1: Notifications from detection systems are investigated
RS.AN-2: The impact of the incident is understood
RS.AN-3: Forensics are performed
RS.AN-4: Incidents are categorized consistent with response plans
RS.MI-1: Incidents are contained
RS.MI-2: Incidents are mitigated
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
RS.IM-1: Response plans incorporate lessons learned
RS.IM-2: Response strategies are updated

By considering all subcategories, and the corresponding ε_i value, a maturity vector is defined according to (7):

$$\mathbf{C}_{\boldsymbol{S_C}} = \left[\varepsilon_1(\boldsymbol{S_{C_1}}) \cdots \varepsilon_{\tau_{S_C}}\left(\boldsymbol{S_{C_{\tau_{S_C}}}}\right)\right] \tag{7}$$

Each subcategory contribution to absolute compliance, α_i occurs with $\mu_{\{I,M,D,Q,O\}} = \mu_O$ and $\varepsilon_{MAX} = \varepsilon_{\{T,H,P\}}(\mu_O)$. Assuming maximum CMMI levels, each ε_i becomes majored, resulting in:

$$\varepsilon_{i_{MAX}} = \varepsilon_T\mu_O \;+\; \varepsilon_H\mu_O + \varepsilon_P\mu_O = 5+5+5 = 15 \tag{8}$$

Conversely, each input parameter $\varepsilon_{\{T,H,P\}}$ has its own column vector for all $\tau_{S_C} = 15$ subcategories, given by (9).

$$\theta_{\{T,H,P\}} \;= \sum_{i=1}^{\tau_{SC}} \varepsilon_{\{T,H,P\}_i} \;.\mu_{\{I,M,D,Q,O\}} \tag{9}$$

Each is also majored when μ_O CMMI value is considered, given by (10):

$$\theta_{\{T,H,P\}_{MAX}} = \sum_{i=1}^{\tau_{SC}} \varepsilon_{\{T,H,P\}_i}.\mu_{\mathrm{O}} \tag{10}$$

In this case, majoring:

$$\theta_{T_{MAX}} = \theta_{H_{MAX}} = \theta_{P_{MAX}} = 75 \tag{11}$$

In the considered scenario, the maturity vector is the majored one, given by (12) and (13):

$$\mathbf{C}_{\boldsymbol{S_{C_{MAX}}}} = \left[\varepsilon_{1_{MAX}}(\boldsymbol{S_{C_1}}) \cdots \varepsilon_{\tau_{S_{C_{MAX}}}}\left(\boldsymbol{S_{C_{\tau_{S_C}}}}\right)\right] \tag{12}$$

$$\mathbf{C}_{\boldsymbol{S_{C_{MAX}}}} = [15,15,15,15,15,15,15,15,15,15,15,15,15,15,15\,] \tag{13}$$

The overall maximum score which represents absolute compliance with this subset of NIST CSF, is given by (14):

$$\theta_C = \sum_{i=1}^{\tau_{SC}} \mathbf{W}_{\boldsymbol{S_{C_i}}} \cdot \mathbf{C}_{\boldsymbol{S_{C_i}}} \tag{14}$$

In our case, given the assumptions, the maximum NIST CSF compliance score corresponds to $\theta_{Abs} = 157{,}48$, given by (15).

$$\theta_{C_{MAX}} = \sum_{i=1}^{\tau_{SC}} \mathbf{W}_{\boldsymbol{S_{C_{MAX_i}}}} . \mathbf{C}_{\boldsymbol{S_{C_{MAX_i}}}} \tag{15}$$

Finally, the model outputs the compliance percentage with NIST CSF framework, given per each input vector $\varepsilon_{\{T,H,P\}}$, is the following:

$$C = \frac{\theta_C}{\theta_{C_{MAX}}} \tag{16}$$

$$T = \frac{\theta_{\mathrm{T}}}{\theta_{T_{MAX}}} \tag{17}$$

$$H = \frac{\theta_H}{\theta_{H_{MAX}}} \tag{18}$$

$$P = \frac{\theta_P}{\theta_{P_{MAX}}} \tag{19}$$

where C, T, H and P represent the total compliance percentage and the compliance percentage for technology, HR and processes, respectively.

VI. Reference Scenario

In order to test the first approach designed for this model, a scenario was considered based an organization with a CS maturity level, with skilled HR, dedicated CS teams and well defined processes, all put in practice. It also features fully functional high-end CS technology.

TABLE III. Scenario's Technology.

CS Technology	ID
Perimeter Firewalls	P.FW
Perimeter IDS	P.IDS
SIEM	SIEM
Web Application Firewalls	WAF
Load Balancers	LB
Anti-DDoS Solution	A.DDoS
Ticketing Tool	Tk
Vulnerability Scanners	VS
Patch Management Systems	P.MS
Email	Email
Forensic Virtual Machines	F.VMs

Regarding the human resources, Table V presents the existing HR teams for the considered company:

TABLE IV. Scenario's HR Teams.

Team	#elements	ID
Technology Security	10	TechSec
Corporate Security	3	CorpSec
CSIRT	3	CSIRT
Firewall change Management	2	FwCM
User and Access Management	5	UAM

Table V presents the existing HR CS teams and the corresponding mapping with the existent technologies, key in detecting overlapping activities and optimizing human resources number and scope of action.

TABLE V. HR Teams and Technology Mapping

Subcategory	Technology	Human Resources
RS.RP-1	SIEM	CSIRT
RS.CO-1	Tk	TecSec and CSIRT
RS.CO-2	Tk and SIEM	TecSec and CSIRT
RS.CO-3	Tk	TecSec and CSIRT
RS.CO-4	Tk and SIEM	TecSec, CSIRT and CorpSec
RS.CO-5	Email	TecSec, CSIRT and CorpSec
RS.AN-1	SIEM	TecSec and CSIRT
RS.AN-2	SIEM and F.VMs	TecSec and CSIRT
RS.AN-3	F.VMs	TecSec and CSIRT
RS.AN-4	Tk	TecSec and CSIRT
RS.MI-1	A.DDoS, P.FW, P.IDS, WAF and LB	CSIRT, TecSec, CorpSec, FwCM and UAM
RS.MI-2	P.MS	CSIRT, TecSec, CorpSec, FwCM and UAM
RS.MI-3	VS and Tk	CorpSec and CSIRT
RS.IM-1	Tk	TecSec and CSIRT
RS.IM-2	Tk	TecSec and CSIRT

Based on the table above, it is possible to verify that most activities are performed by TecSec and CSIRT teams thus leading to the conclusion that probably teams like CorpSec could be deprecated or integrated within TecSec of CSIRT.

In the considered scenario, according to the developed CMMI program from the considered company, the weight vector ($\mathbf{W}_{S_C}$), the CMMI maturity levels and the resulting value ($\mathbf{C}_{S_C}$) are given by table VI:

TABLE VI. Scenario's Input Values and Results

Subcategory	ε_t	ε_h	ε_p	$\mathbf{W}_{S_C}$	$\mathbf{C}_{S_C}$
RS.RP-1	3	4	4	1	11
RS.CO-1	3	3	4	1	10
RS.CO-2	1	3	3	1	7
RS.CO-3	2	3	3	0.5	4
RS.CO-4	3	3	4	0.5	5
RS.CO-5	1	2	2	0.25	1.25
RS.AN-1	3	5	3	1	11
RS.AN-2	4	4	5	1	13
RS.AN-3	4	2	4	0.5	5
RS.AN-4	2	4	4	0.5	5
RS.MI-1	3	4	3	1	10
RS.MI-2	4	3	3	1	10
RS.MI-3	4	2	2	0.25	2
RS.IM-1	2	4	5	0.5	5.5
RS.IM-2	2	3	2	0.25	1.75
Model Output	θ_T	θ_H	θ_P	-	θ_C

The above tables present all the input data that is considered and afterwards fed to the model. The model outputs and results are shown in the following section.

VII. Results

This section presents the results of the proposed model. The first results are extracted from the application of the model to the considered scenario, and a baseline set of results is drawn. From that point on, having those results as baseline, input data and parameters are changed, and new results are generated.

A. Reference Scenario Results

The compliance level of the reference scenario is achieved by applying the analytical model from Section V to the reference scenario data from Section VI. Therefore, equations 20 to 25 present the proposed model's compliance results:

$$\begin{aligned} \theta_C &= 101.5 \\ \theta_T &= 29.25 \\ \theta_H &= 35.75 \\ \theta_P &= 36.50 \end{aligned} \tag{20}$$

$$C = \frac{\theta_C}{\theta_{C_{MAX}}} = \frac{101.5}{157.48} = 0.645 \tag{21}$$

$$T = \frac{\theta_T}{\theta_{T_{MAX}}} = \frac{29.5}{75} = 0.393 \tag{22}$$

$$H = \frac{\theta_H}{\theta_{H_{MAX}}} = \frac{35.75}{75} = 0.476 \quad (23)$$

$$P = \frac{\theta_P}{\theta_{P_{MAX}}} = \frac{36.50}{75} = 0.486 \quad (24)$$

Figure 2 presents the compliance levels of all vectors for the reference scenario.

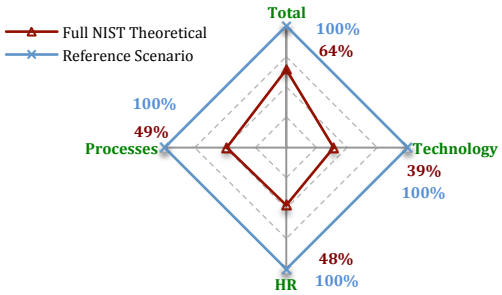

Figure 2 – Compliance Levels of reference scenario compared to NIST CSF theoretical maximum compliance levels.

The results show that the reference scenario is 64.5% compliant with the NIST CSF. Regarding the three input vectors, technology, HR and process wise, the considered scenario represents 39%, 47% and 48% of total compliance respectively.

Addressing the results from a strategic investment perspective, it is shown that technology is the input vector with the lowest compliance percentage and maturity level. Strategically, this conclusion might drive future investments, in order to increase technology and overall compliance levels, eventually leveling with the other two vectors at 47%.

The model not only allows concluding that the reference scenario can be optimized but also allows impact analysis on random events, as shown hereafter. The flexible nature of the model is shown as input data is changed and new results are generated.

B. NIST CSF Compliance Impact of process change

Extrapolating this result to the whole extension of NIST CSF can lead to several optimizations regarding teams that have small contributions to cybersecurity activities and may represent a financial waste on this matter. Additionally, several impact predictions can be made when varying input parameters.

In the use case bellow it is possible to see that the model can produce results predicting the impact of changes on Technology, HR and processes. Specifically in this case, it is possible to measure results and the difference on compliance with the framework when a response plan is not executed during an event. Clearly, the proposed scenario focuses on process changes.

We consider any inexistence of CMMI as zero. Table VII shows the different CMMI levels of both the baseline scenario and the scenario of not having a response plan executed. We consider that the response plan is not executed during an event, resulting in CMMI values equal to 0, reflected on RS.RP-1 subcategory changes.

TABLE VII. USE CASE ε_p CHANGES

Subcategory	ε_t	ε_h	ε_p	$\mathbf{W}_{S_C}$	$\mathbf{C}_{S_C}$
RS.RP-1: Response plan is executed during or after an event	3	4	4	1	11
RS.RP-1: Response plan is **not** executed during or after an event	3	3	0	1	6

Table VII (Figure 3) presents the results on compliance impact of not executing a response plan when a cybersecurity event occurs. It can be seen that overall compliance drops approximately 2.5% whilst technology and HR compliance remain the same. As expected, process is the only vector with compliance decrease, close to 5.3%.

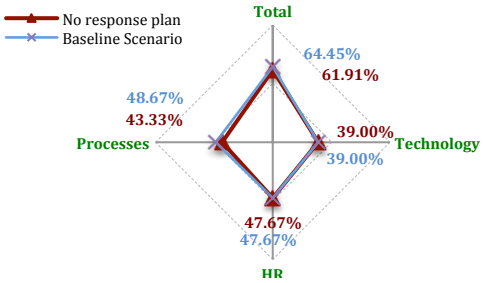

Figure 3 – Compliance Impact of NOT executing response plan RS.RP-1

C. NIST CSF Compliance Impact of HR changes

Another considered scenario focuses on HR changes. This hypothesis focuses in loosing operational capabilities due to outsourced CS functions. We consider that internal CS teams are composed of outsourced personnel, with clear allocated functions, but some of those resources cease working for the contractor company, thus leaving the reference company without knowledgeable personnel, regarding their roles and order of operation when facing a CS incident. The use cases changes are shown in Table IX.

TABLE VIII. USE CASE ε_p CHANGES

Subcategory	ε_t	ε_h	ε_p	$\mathbf{W}_{S_C}$	$\mathbf{C}_{S_C}$
RS.CO-1: Personnel know their roles and order of operations when a response is needed -	1	3	3	4	11
RS.CO-1: Personnel **do not** know their roles and order of operations when a response is needed due to outsourced leaving..	3	0	4	1	8

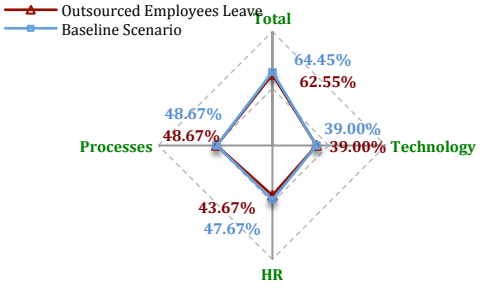

Figure 4 – Compliance Impact of NOT executing response plan RS.RP-1

Figure 4 presents the compliance impact of this scenario in overall compliance for the company. The results show that

overall NIST CSF compliance decreases by 1.9%, being the HR vector the one with the most impact, 4%. The other two vectors, as expected, are not affected by the HR changes considered regarding RS.CO-1. In practice, this result shows that the reference company will sustain relevant compliance decrease if this scenario ever becomes a reality.

The previous results are a non-extensive example of how flexible the model is. By creating random scenarios, where the several functions are changed, the overall compliance impact can be drawn, allowing impact predictions on the scenario.

VIII. CONCLUSIONS

In order for organizations to draw effective CS strategies it is of utmost importance to have references, not only from standards point of view, but also an integrated framework to follow. By having such framework as reference, companies have the ability to evaluate their compliance level, therefore having the necessary instruments to drive strategic decisions, *e.g.*, CS technological investments.

This work considered the NIST framework as the reference framework. Based on the NIST CSF, a generic model was proposed in order to allow for overall compliance evaluation. Three input key vectors were considered as the pillars: technology, human resources and processes on CS activities. The proposed model takes into consideration NIST CSF Functions, Categories and Subcategories, mapping them with the input vectors in order to establish a relationship resulting in compliance percentage levels.

A reference scenario was considered, with real company data and the model applied to it, in order to extract a compliance baseline. Model results show that compliance levels with NIST CSF are close to 64%, thus improvements may exist. From that baseline scenario, two random scenarios were derived in order to evaluate the corresponding compliance changes. The results show that the model is flexible enough for an analyst to create random impact scenarios, either simple (impact on one of the input vectors) or complex (impact on more than one input vector at the same time).

The results of the model show that by using it, organizations can gain visibility of the overall compliance with NIST CSF and assess the maturity level of key aspects on technology, human resources and processes within the organization regarding CS activities.

The proposed model is still in its early stages, and this work focuses on the model conception. The presented scenarios were not extensive. Nevertheless, we believe that the model as it is, can be of added value to organizations regarding NIST CSF activities assessment and inferring strategic optimizations and investments in technology, human resources and processes. We foresee the following model improvements, although not limited to:

- Key technologies already mapped with all NIST CSF subcategories;
- Inclusion of an experimental Cybersecurity Maturity Model [15] to map the percentage of compliance with a maturity scoring value;
- Inclusion of a risk management process to calculate the qualitative risk exposure for the organization based on the percentage of compliance and maturity level of NIST CSF subcategories;

The proposed model allows several scenarios and hypothesis to be drawn and to assess how compliance levels change accordingly, thus representing a real impact on the company.

We believe the proposed model can provide added support to strategic governance of CS projects by considering each company's existing maturity levels and can be used to drive CS investments, with the overall aim of reducing CS incidents probability and impact as well as global company exposure to CS threats.

REFERENCES

[1] Yang, Y.; Littler, T.; Sezer, S.; McLaughlin, K.; Wang, H.F., "Impact of cyber-security issues on Smart Grid," Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on , vol., no., pp.1,7, 5-7 Dec. 2011

[2] Zhu, Huafei, "Towards a Theory of Cyber Security Assessment in the Universal Composable Framework," Information Science and Engineering (ISISE), 2009 Second International Symposium on , vol., no., pp.203,207, 26-28 Dec. 2009

[3] Okimoto, T.; Ikegai, N.; Inoue, K.; Okada, H.; Ribeiro, T.; Maruyama, H., "Cyber security problem based on Multi-Objective Distributed Constraint Optimization technique," Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on , vol., no., pp.1,7, 24-27 June 2013

[4] Chmielecki, T.; Cholda, P.; Pacyna, P.; Potrawka, P.; Rapacz, N.; Stankiewicz, R.; Wydrych, P., "Enterprise-oriented cybersecurity management," Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on , vol., no., pp.863,870, 7-10 Sept. 2014

[5] Pal, R.; Golubchik, L.; Psounis, K.; Pan Hui, "Will cyber-insurance improve network security? A market analysis," INFOCOM, 2014 Proceedings IEEE , vol., no., pp.235,243, April 27 2014-May 2 2014

[6] Bodeau, D.J.; Graubart, R.; Fabius-Greene, J., "Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels," Social Computing (SocialCom), 2010 IEEE Second International Conference on , vol., no., pp.1147,1152, 20-22 Aug. 2010

[7] http://www.iso.org/iso/catalogue_detail?csnumber=44375

[8] https://www.sans.org/media/critical-security-controls/CSC-5.pdf

[9] http://www.isaca.org/cyber/Pages/default.aspx

[10] Sandhu, R.; Krishnan, R.; White, Gregory B., "Towards Secure Information Sharing models for community Cyber Security," Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on , vol., no., pp.1,6, 9-12 Oct. 2010

[11] Kozik, R.; Choras, M., "Current cyber security threats and challenges in critical infrastructures protection," Informatics and Applications (ICIA),2013 Second International Conference on , vol., no., pp.93,97, 23-25 Sept. 2013

[12] Holstein, D.K.; Stouffer, K., "Trust but Verify Critical Infrastructure Cyber Security Solutions," System Sciences (HICSS), 2010 43rd Hawaii International Conference on , vol., no., pp.1,8, 5-8 Jan. 2010

[13] http://www.nist.gov/cyberframework/

[14] M. K. Kulpa and K. A. Johnson, Interpreting the CMMI: A Process Improvement Approach, Second Edition. Boca Raton: Auerbach Publications, 2008

[15] http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Pilot%20version%20A.15.12.2014.pdf