IMPROVING HUMAN CAPITAL FOR SOCS AND CSIRTS:

A COLLECTIVE NEED FOR INDIVIDUAL COMPETENCIES

TNO innovation for life

Auteurs:
G.R. Jansen-Ferdinandus
E.F.T. Buiel
P.P. Meiler
T. Verburgh

Reviewers:
J.G.M van de Ven (TNO)
B. van der Kamp (NCSC)
A.C. Kernkamp (TNO)

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The increasing complexity of threats in the digital domain and the growing labour shortage of skilled cyber security personnel is forcing many Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) to prioritise the services they offer and rethink their workforce development strategies. However, given the complexity of the domain it is not straightforward to determine the required competencies of personnel based on the services a SOC/CSIRT offers. Over the years several renowned organisations have developed frameworks regarding the organisation of SOCs and CSIRTs, but these publications have different purposes or scopes and cannot be readily applied to the challenge of identifying personnel competencies.

To support SOC and CSIRT organisations in their workforce development, the Dutch National Cyber Security Centre (NCSC) has commissioned TNO to study existing frameworks regarding the competencies of SOC and CSIRT personnel and identify how they can be used in practice. This publication details the results of that study and introduces the Dutch Cyber Cube Method as a practical approach to combine selections of existing frameworks and leverage their strong points.

DUTCH CYBER CUBE METHOD

In this study the following frameworks relating to the competencies required for SOC/CSIRT personnel have been considered:

- Step-by-step approach on how to set up a CSIRT (ENISA)
- FIRST CSIRT Framework (FIRST)
- NICE Cybersecurity Workforce Framework (NIST)
- Job profiles for information security 2.0 (QIS)
- European e-Competence Framework 3.0 (CEN)
- CERT skill list (CMU SEI)
- Handbook CSIRT Effectiveness and Social Maturity (GMU)

From our review we conclude that none of the above frameworks by themselves provide a complete solution to identify the required competencies of SOC/CSIRT personnel based on the services offered by the organisation. However, combined these frameworks can provide a lot of the needed information. The Dutch Cyber Cube Method allows the combination of frameworks in a step-by-step approach while ensuring the link between the work that needs to be performed and the competencies required to do so. We use the Dutch Cyber Cube Method to combine three frameworks: the ENISA service list, the NIST framework and the GMU handbook. The resulting instantiation of the Dutch Cyber Cube Method is summarised below:

1. Services: Identify the services offered by the organisation using the ENISA service list.
2. Work roles: Specify who provides the services by selecting the appropriate work roles from the NIST framework.
3. Tasks: Determine the focus of the work role by specifying the core tasks based on the NIST framework.
4. Competencies: Select the required knowledge, skill and attitudes required to perform the main tasks from both the NIST framework (technical) and the GMU Framework (personal/team) and determine the required proficiency levels.
5. Education, Training, and Exercises: Use the competencies as a starting point to identify relevant education, training, and exercise options.

CONCLUSIONS

We summarise our work as follows:

- The increasing labour shortage of skilled ICT personnel forces SOC and CSIRT organisations to prioritize the services they offer and optimise their workforce development strategies.
- Our review of currently available frameworks shows that there is no single framework that provides a complete solution to identify the required competencies of SOC and CSIRT personnel based on the services an organisation offers.
- We therefore introduce the Dutch Cyber Cube Method to combine the strengths of three frameworks published by ENISA, NIST, and GMU.
- Combining these frameworks allows for a step-wise analysis to identify the services an organisation offers, the work roles contributing to those services, and the associated tasks and competencies.

We welcome any feedback on the approach we have described and aim to further refine it into a tool that can readily be used by SOC and CSIRTs.

1. INTRODUCTION

The complexity of the digital thread landscape has significantly increased over the past few years not only in the Netherlands, but worldwide. There are more attacks, more variety in attack types, and due to the high level of digitalisation and interconnectedness a successful attack can have far-reaching consequences. Private and national Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) all over the world guard the cyber security of organisations and governments. New technologies are constantly being developed to enable SOCs and CSIRTs to better prevent, detect, and respond to attacks. However, the labour shortage of skilled ICT professionals is increasing and recruiting new personnel has become a real challenge. The resent Cybersecurity Workforce Study of (ISC)^2 estimates the shortage close to three million globally [ISC2]. To cope with this shortage many SOC and CSIRT organisations have to revaluate their priorities, rethink their recruitment strategy, and find ways to keep current personnel and enhance their skills. However, given the complex and the fast-changing nature of the digital domain, it is not easy to define the required competencies of personnel.

In some branches collective SOC and CSIRT organisations have started to develop standardised approaches to describe the services they offer and the resulting competency requirements for personnel. The use of a standardised approach has two main benefits. It can offer a basis from where to start when analysing one's organisation and it can serve as a common vocabulary to build an understanding between organisations regarding the knowledge and skills of personnel. Such understanding can improve cooperation between different SOCs and CSIRTs and between SOCs and CSIRTs and other types of organisations such as educational institutions. Over the years several renowned organisations such as SEI, NIST, ENISA and FIRST have developed standards and frameworks assisting in setting-up and organising SOCs and CSIRTS. However, these standards are generally not focussed on analysing the required competencies of personnel based on the services offered by an organisation. As a result, the application of these frameworks to the problem at hand is not straightforward and no standardised approach for identifying competencies for SOC/CSIRT personnel has been widely accepted.

The Dutch National Cyber Security Centre (NCSC) wants to support SOC and CSIRT organisations in the recruitment of new personnel and at the same time facilitate cooperation between SOCs and CSIRTs. To this end NCSC commissioned TNO to study the existing frameworks and identify how they can be used in practice. This publication details the results of that study and introduces the Dutch Cyber Cube Method as a practical approach to combine selections of existing frameworks and leverage their strong points. This approach is beneficial for two reasons. First, it allows to align roles and tasks between organisations which facilitates cooperation. Secondly, it supports the identification of the competencies required by cyber security personnel to perform those roles and tasks. These competencies are required for both the selection of future personnel and to identify education and training for current personnel. In this study we use the definition of competencies as used by the European E-Competence framework: 'Competence is a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results'.

The primary target audience of this publication are collective SOC and CSIRTs working on a standardised approach within their sector, but also team leads/managers of individual SOC and CSIRT organisations who are looking for a structured approach to analyse the education and training needs of their teams. Secondary, it is also of interest to anyone working in a SOC or CSIRT, policy developers, decision makers, and cyber security education and training institutes. The guidelines provided are the result of a literature review, interviews with different organisations and hands on experience in using some of the discussed frameworks.

READING GUIDE

Chapter two provides a quick description of the different types of SOC and CSIRT organisations and how that influences the required competencies for personnel. Chapter three presents an overview of the currently available frameworks and an analysis of their strengths and weakness in regard to identifying competencies for SOC/CSIRT personal. Chapter 4 introduces the Dutch Cyber Cube Method as a way to structure the use of existing framework in practice. Chapter five describes a step-by-step example of how the method can be applied. Finally, we conclude with a summary.

2. TYPES OF SOC AND CSIRT ORGANISATIONS

There are no established definitions what a SOC or a CSIRT is and no clear distinction where the responsibilities of one end and the other begins[1]. In general, a SOC is focused on preventing an incident by continuously monitoring the environment and analysing abnormalities. The main business of a CSIRT is responding to the incident, analysing the cause and implementing recovery strategies. Confusingly, several alternate terms have been used over the years to describe incident response teams, for example: CERT (Computer Emergency Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) and SERT (Security Emergency Response Team).

Another aspect regarding the types of SOCs and CSIRTs is the way they are related to the systems they protect. Commonly the following types are discerned:

- **Dedicated/internal:** these organisations, departments or teams are dedicated to the (pro-active) protection of a specific (parent) organisation. Large organisations whose core business relies heavily on the digital domain such as banks or government institutions often have dedicated departments who provide SOC and CSIRT services. However, nowadays even small organisations have people that are tasked to guard cyber security and although they may not be organised as a typical SOC or CSIRT they have similar goals.
- **Product-oriented:** these departments are part of IT providers, tasked with the detection, analysis and mitigation of threats and incidents regarding the specific products or services offered by the parent company. For example, CISCO and Siemens have their own product incident response teams.
- **Business-oriented/commercial:** these companies provide paid SOC and/or CSIRT services to other organisations based on service level agreements or on an on-demand basis.
- **Collective/sectoral:** these organisations provide their services to a sector, branch or chain. The services they offer vary greatly depending on the agreements made by the participating/client organisations regarding the role and responsibilities of the collective SOC/CSIRT. In some branches a collective organisation may be an information sharing platform where lessons learned and threat intelligence are shared. In another setting the collective organisation may have a coordination and advising role in case of threats and incidents. Or the collective organisation may be tasked with the whole range of SOC/CSIRT responsibilities from awareness raising till on site incident response handling. Incident response handling may range from instantaneous support at a distance to coordination on site.
- **National/governmental:** these SOCs or CSIRTs provide their services to a whole nation or parts of its critical infrastructure. Usually their services are focussed on coordination, information sharing and advice.

The most important distinction between these different types of organisations is the services they offer and the responsibilities and rights associated with them. Here we use the term services as defined by FIRST: 'A service is a coherent, ready-to-use deliverable that is of value to the customer.' Generally speaking, the larger the constituents of the organisation, the more the services tend to go towards signalling, advising and coordination whereas the hands-on services such as incident handling and the development and installation of security tools are more common to organisations with fewer constituents. A second distinction can be found in the context wherein people work. The context might influence the required competencies of personnel even when considering the same services. E.g. people working in non-dedicated CSIRT organisations that offers on-site support might need to be able to switch to a new environment (both technically and socially) more often and more rapidly than people working in a dedicated CSIRT or SOC.

1 https://securityboulevard.com/2018/03/certs-csirts-and-socs-after-10-years-from-definitions/

3. FRAMEWORKS

Several institutes have published frameworks or guidelines regarding the required competencies of cyber security personnel. To build on this existing knowledge base we have performed a quick analysis of the strengths and weaknesses of these frameworks. This chapter provides a brief overview of this analysis.

OVERVIEW OF EXISTING FRAMEWORKS

The following international frameworks have been considered:

- European e-Competence Framework 3.0 (CEN)
- CERT skill list (CMU SEI)
- Step-by-step approach on how to set up a CSIRT (ENISA)
- FIRST CSIRT Framework (FIRST)
- Handbook CSIRT Effectiveness and Social Maturity (GMU)
- NICE Cybersecurity Workforce Framework (NIST)
- Job profiles for information security 2.0 (QIS)

The frameworks vary in structure, level of detail, scope, domain-focus, etc. For the purpose of this study the most important differences between the frameworks relate to the domain specificity (i.e. from ICT-wide to specifically focused on SOCs/CSIRTs) and the level of detail in which the required competencies of personnel are described. For example, the FIRST framework describes several services that can be provided by SOCs/CSIRTs but does not describe the required competencies of the personnel to perform the tasks underlying these services. Other frameworks provide an overview of the required competencies in general terms and NIST even provides an extensive list of over a thousand separate knowledge items, skills and abilities related to working in the cyber security domain. Table 1 presents an overview of the characteristics of the different frameworks.

Framework by author	SOC/CSIRT domain specificity	Level of detail of competencies	Completeness of technical competencies	Completeness of social competencies	Competencies based on standard	Last updated
CEN	Low	Medium	Medium	Low	Yes	2014
CMU SEI	High	Medium	Medium	Medium	No	Jan. 2017
ENISA	High	Low	Low	Low	No	Dec. 2006
FIRST	High	N/A	N/A	N/A	N/A	May 2017
GMU	High	High	N/A	High	No	2016
NIST	Medium	High	High	Low	No	Jan. 2018
QIS	Medium	Medium	Medium	Low	Yes	Jan. 2017

The studied frameworks are presented concisely below. A more elaborate analysis is provided in Appendix A.

EUROPEAN E-COMPETENCE FRAMEWORK (E-CF) FOR ICT PROFESSIONALS

The European e-Competence Framework [e-CF] is a reference framework of competencies applied within the ICT sector. It is published by CEN (European Committee for Standardization) and is an implementation of the the European Qualifications Framework [EQF] that offers a standardised approach to describe qualification. The e-CF foccusses on competences needed to develop, operate and manage ICT projects and processes; to exploit and use ICT; to make decisions, develop strategies, and to foresee new scenarios.

- **Domain specificity:** The e-CF is a generic ICT competence framework and as such considers the subject of cyber security at a very high level. It does not explicitely cover the SOC/CSIRT expertise domain.
- **Level of Detail:** The e-CF is structured using four dimensions: e-Competence areas, a set of high-level reference e-Competences for each area, proficiency levels on e-Competences, and samples of knowledge and skills that relate to the e-Competences.

CERT SKILL LIST

The document "What skills are needed when staffing your CSIRT?" [CERTSkillList] describes a set of skills that CSIRT staff members should have, based on experience at Carnegie-Mellon University (CMU). A set of 'basic' skills is described that each team member should have and additional 'specialist' skills are suggested that a few team mebers should posses or have acces to through their network. The basic skills are separated into personal skills and technical skills.

- **Domain specificity:** the CERT Skill list focuses on staff members of CSIRTs.
- **Level of Detail:** the CERT Skill list provides competencies at a medium level of detail. The competencies are described at high level with specific examples. The competencies are not directly related to to the services offered by the organisation but rather describe a default set.

ENISA STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

The step-by-step approach on how to set up a CSIRT, provided by the European Network and Information Security Agency (ENISA), discerns several CSIRT business models (each describing the organisation of a different CSIRT [ENISA]. It considers business- and process management and technical perspectives. The framework will henceforth be referred to simply as 'ENISA'.

- **Domain specificity:** specifically focuses at CSIRTs, covering 4 primary services (Reactive, Alerts and Warnings, Artefact Handling and Security Quality Management) which are each divided in sub-services.
- **Level of detail:** The ENISA framework describes different services that a CSIRT may offer. It provides some brief guidelines on the composition of the staff and lists the key competencies (personal and technical) the staff should posses at a very high level.

FIRST CSIRT SERVICES FRAMEWORK

The Computer Security Incident Response Team (CSIRT) framework is provided by the Forum of Incident Response and Security Teams [FIRST]. Its purpose is to facilitate CSIRT interoperability, global capability development activities, and education. The framework will henceforth be referred to simply as 'FIRST'.

- **Domain specificity:** FIRST focusses on three Incident Response Team types: National; Sector (critical infrastructure); and Enterprise (organisational).
- **Level of Detail:** The FIRST framework considers the services level only. The framework is a hierarchical model consisting of services, where each service is broken down into its primary functions and their sub-functions. Many of the functions and sub-functions can be part of the realisation of multiple services and can be interdependent

HANDBOOK 'IMPROVING SOCIAL MATURITY OF CYBERSECURITY INCIDENT RESPONSE TEAMS'

The handbook 'Improving Social Maturity of Cybersecurity Incident Response Teams' [GMU] responds to the growing sense among CSIRT professionals that technical knowledge and skills are increasingly not enough to properly respond to cyber threats. The handbook provides methods and strategies to build, staff, train, and foster a team that leverages both the latest cyber technologies and the social dynamics required to make the best use of them. One of the provided tools is an overview of non-technical knowledge, skills, abilities and other characteristics (KSOAs) relevant for CSIRTs.

- **Domain specificity:** the handbook focuses specifically at CSIRTs.
- **Level of Detail:** the handbook focuses on the social aspects that turn a CSIRT into a successful team; it does not describe technical aspects / competences. The provided overview of KSOAs is at a high level-of-detail. The list consists of three categories: social/team skills, cognitive skills, and personal character.

NICE CYBERSECURITY WORKFORCE FRAMEWORK

The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework [NICE] (also known as the NICE Framework), provided by the National Institute of Standards and Technology (NIST), provides a common, consistent lexicon that categorizes and describes cybersecurity work (processes), by covering a broad spectrum of cyber security functions.

- **Domain specificity:** covers a wide range of cyber security roles from high-level managers to specialists in digital forensics, including SOC and CSIRT related functions Some roles are described in a military context while they can also be relevant in non-military settings.
- **Level of detail:** Describes 52 roles within the field of cyber security and provides detailed lists of the tasks and competencies (in terms of knowledge, skills and abilities) associated with each role. For the technical roles the competencies focus mostly on the technical aspects with little attention to 'soft'-skills.

QUALIFICATION OF INFORMATION SECURITY (QIS) JOB PROFILES FOR INFORMATION SECURITY

To promote a clear and uniform system of qualifications for professionals in information security the Dutch Association of Information Security Professionals (PvIB) has published a description of 4 main information security job profiles (Chief Information Security Officer; Information Security Officer; ICT Security Manager; ICT Security Specialist) and the required competences. [QIS] provides a basis for a uniform system of qualifications for information security professionals. The framework will henceforth be referred to simply as 'QIS'.

- **Domain specificity:** the QIS job profiles are not specific to SOC or CSIRT organisations. The profile of the ICT Security Specialist contains aspects of the tasks associated with SOC/CSIRT staff members, but the focus is on the design and implementation of the organisation's ICT security policies.
- **Level of Detail:** for each job profile the QIS framework describes deliverables, tasks and competencies using the e-CF. It also describes the required education and experience.

FRAMEWORK REVIEW CONCLUSIONS

To assist SOC and CSIRT organisations in their workforce development we are looking for a standardised approach to identify the required competencies of personnel based on the services offered by the organisation. In reviewing the above-mentioned frameworks, we conclude that there is no single framework that can readily be used for this purpose. Figure 1 provides a visual overview of the frameworks according to their domain specificity and the level of detail of the competencies described. The framework we are looking for is also indicated in the figure below.

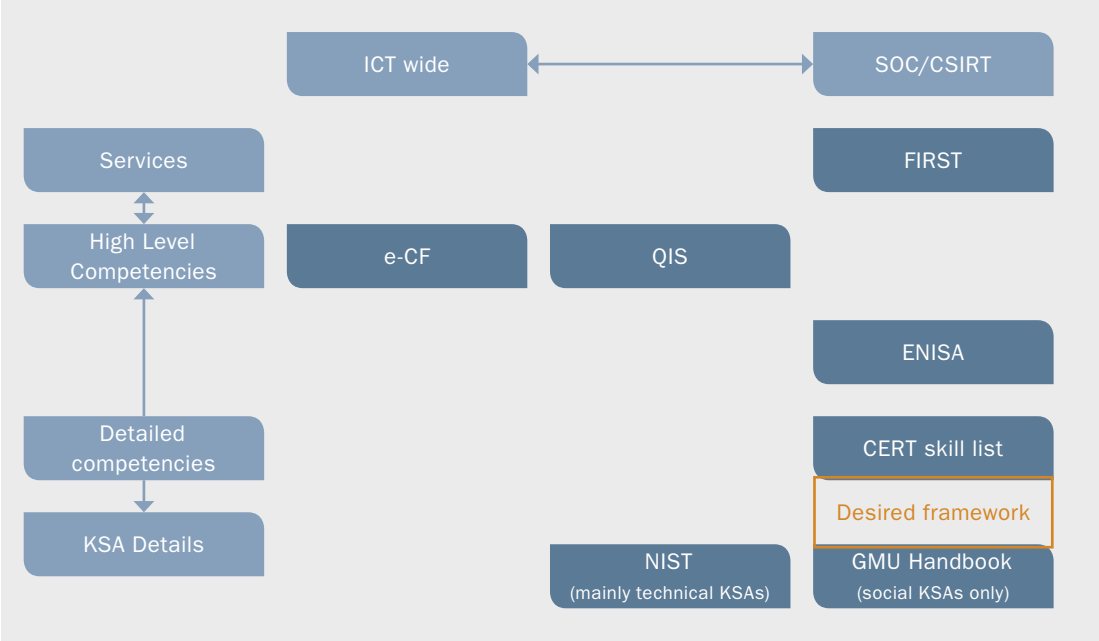

Figure 1: *Visual ranking of the studied frameworks with respect to domain focus and level of detail regarding competencies*

Based on the ranking in Figure 1 it might seem logical to conclude that a combination of the CERT skill list and the GMU handbook should be enough to achieve the desired result. However, both these frameworks describe a list of required competencies for a generic SOC/CSIRT team. They do not take into consideration the specific context of the organisation such as the services offered and the resulting work roles and associated tasks. ENISA and FIRST offer a way to describe the context of an organisation by provide an extensive overview of the services that an organisation can offer. Yet these frameworks do not describe the required competencies to deliver those services in detail. The NIST framework does offer a detailed list of knowledge, skills and abilities per role, but since it is not specific to SOC and CSIRT organisations it also includes a lot of competencies that are not applicable. Also, the NIST framework has little coverage of non-technical skills for technical oriented experts. The e-CF and QIS frameworks are not specific to SOC and CSIRT organisations and therefore do not offer the required level of detail.

As we see, none of the frameworks considered offers a 100% match for the need to identify individual competencies for SOCs and CSIRTs. However, combined these frameworks can offer a lot of the needed information. The next chapter will describe a method to combine the strengths of a selection of the frameworks described in this chapter.

4. DUTCH CYBER CUBE METHOD FOR SOC/CSIRT PERSONNEL

The Dutch Cyber Cube Method has first been used within the Dutch Ministry of Defence to identify the tasks and required knowledge and skills for professionals working in the cyber domain [CyberCubeOrg]. It offers a practical step-by-step approach ensuring the link between the work that has to be performed and the competencies required for this work.

Four sides of the cube are used to represent the who, why, what, and how questions:
- Who: who needs to be trained?
- Why: why does the trainee need to be trained, i.e. which tasks does the trainee need to be able to perform?
- What: what should the trainee know and be proficient in to perform these tasks?
- How: how should the trainee be educated and trained to perform these tasks?

Each side is described by two dimensions and by 'flipping' the cube to the next side one of the dimensions of the previous side will be coupled with a new dimension and so a path can be followed from the high level who-question to the low level how-question. This principle is illustrated in Figure 2.

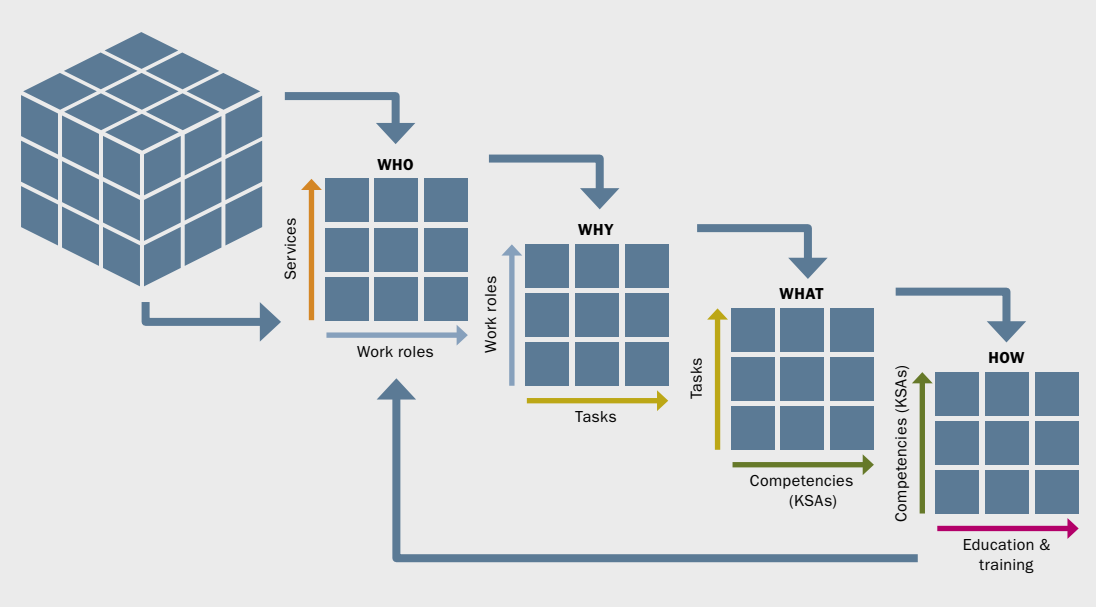

Figure 2: *Illustration of the steps taken in the Dutch Cyber Cube Method*

Our analysis of the existing frameworks shows that no single framework can easily be used to identify the required competencies for SOC/CSRIT personnel. The Dutch Cyber Cube Method offers a structured approach to combine several frameworks. This specification of the Dutch Cyber Cube Method is summarized below:

1. Services: Identify the services offered by the organisation using the ENISA service list.
2. Work roles: Specify who provides the services by selecting the appropriate work roles from the NIST framework.
3. Tasks: Determine the focus of the work role by specifying the core tasks based on the NIST framework.
4. Competencies: Select the required knowledge, skill and attitudes required to perform the main tasks from both the NIST framework (technical) and the GMU Framework (personal/team) and determine the required proficiency levels.
5. Education, Training, and Exercises: Use the competencies as a starting point to identify relevant education, training, and exercise options

This approach combines three frameworks, the ENISA service list, the NIST framework and the GMU Framework. Below we specify what we have selected these specific frameworks.

IDENTIFYING SERVICES

The purpose of the first step is to describe the core business of the organisation that is being analysed by a set of standardised services. By starting the analysis from the service level and not making any assumptions regarding the services an organisation offers, this method can be applied to all types of SOCs and CSIRTs (e.g. dedicated, collective, national, etc.). Many organisations already state the services they provide in their mission and this step usually comes down to finding the service descriptions that best describe the organisations goals and activities. Based on the literature review definitions of both the ENISA framework and the FIRST framework are suitable for this purpose. The FIRST framework provides a more detailed and structured overview of the services that a SOC or CSIRT can provide and the FIRST framework is still being updated. However, given our focus on collective SOC/CSIRT organisations, we prefer the use of the service definitions from the ENISA framework. It explicitly differentiates between 'coordination' and 'handling' services and on- and off-site support services. A collective SOC or CSIRT might have the role of coordinator during an incident while the analysis and mitigation activities might be performed by experts from the targeted organisation.

FROM SERVICES TO COMPETENCIES

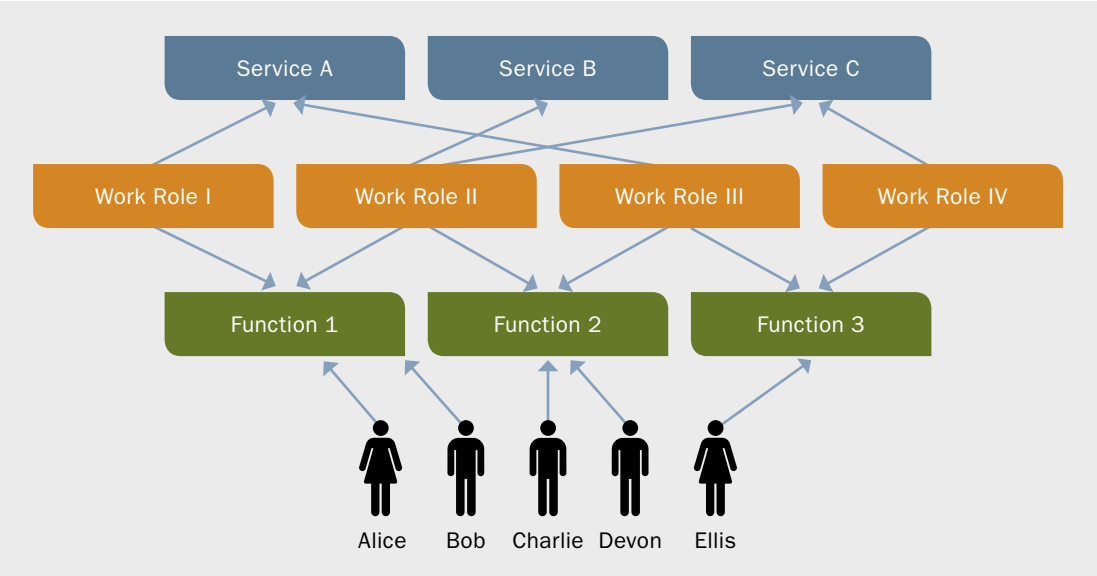

Figure 3: *illustrates the relation between services, work roles, functions and people*

The services provide the context for selecting the required competencies for SOC and CSIRT personnel. In steps 2 and 3 we focus on identifying work roles and tasks related to SOCs and CERTs as these will be the hook for identifying competencies for SOCs and CERT personnel in step 4.

Within an organisation a person has a specific job or function, this function is usually a combination of work roles. Work roles can be identified as primary and secondary, and sometimes also tertiary. An example is a project leader; his or her primary role is to lead projects, and 80-90% of the time is related to tasks regarding this work role. A secondary work role could be a coach for (junior) project leaders, this might take up 10% of the time, and once every month this person is the chairperson of a coordination group where other SOCs join. As such a function may consist of multiple work roles and different work roles performed by different people may be involved in delivering one service. Figure 3 illustrates the relations between these concepts.

The NIST framework defines a large number of cyber security work roles including the tasks that are commonly associated with such a role and the knowledge, skills and abilities required to perform that work role. This framework is therefore especially suited to be used within the Dutch Cyber Cube Method to determine the 'who' (work roles), 'why' (tasks), and 'what' (knowledge, skills, and attitudes). However, as noted in the framework review, the NIST framework does not associate the technically oriented roles (such as the "Cyber Incident Responder") with non-technical knowledge or skill aspects such as team skills or attitudes. SOC and CSIRT organisations often rely heavily upon their technical people to perform coordination, alignment and stakeholder management roles. As such non-technical skills are very important. In order to address these social KSAs we therefore included the Handbook 'Improving Social Maturity of Cybersecurity Incident Response Teams' [GMU] in our approach. This handbook includes an overview of non-technical KSAs highly relevant for SOCs and CSIRTs. The list consists of three KSA categories: social/team skills, cognitive skills, and personal character (attitudes). The [CERTSkillList] provides a similar overview of non-technical skills applicable to CSIRTs, but most of these skills are also represented in [GMU]. We prefer to use [GMU], since it provides concise but clear KSA descriptions in terms of observable human behaviour. [CERTSkillList] provides more prosaic descriptions.

5. STEP BY STEP EXAMPLE

This chapter will use a running example of a fictional collective SOC/CSIRT to describe the application of the Dutch Cyber Cube Method in more detail. For the purposes of the example the organisation being studied is greatly simplified, however the steps and considerations are the same when studying different (more complex) types of SOC/CSIRT organisations.

EXAMPLE: INTRODUCING TEAM LOCKDOWN
A group of detention centers in Cheese Land have identified the need to strengthen their cyber security. They feel that, to cope with the changing threat to their digital systems, they need to invest in strengthening their cyber security. For practical reasons such as costs, efficiency, and the opportunity to share knowledge, they have chosen to set up a collective CSIRT for detention centers in Cheese Land called Team Lockdown. Team Lockdown aims to provide support in handling cyber vulnerabilities and incidents. Their primary focus is on coordination and advising, rather than providing technical support. The technical support is provided by dedicated on-site experts from the different constituents.

STEP 1: IDENTIFY THE OFFERED SERVICES

The purpose of the first step is to describe the core business of the organisation by a set of standardised services. For this step we use the service list provided by ENISA. Table 1 shows the services listed in the ENISA framework[2].

Reactive Services	Proactive services	Security Quality Management	Artefact Handling
Alerts and Warnings	Announcements	Risk Analysis	Artefact Analysis
Incident Handling – Incident Analysis – Incident Response Support – Incident Response Coordination – Incident Response on Site	Technology Watch	Business Continuity and Disaster Recovery	Artefact Response
	Security Audits or Assessments	Security Consulting	Artefact Response Coordination
Vulnerability Handling – Vulnerability Analysis – Vulnerability Response – Vulnerability Response Coordination	Configuration and Maintenance of Security	Awareness Building	
	Development of Security Tools	Education/Training	
	Intrusion Detection Services	Product Evaluation or Certification	
	Security-Related Information Dissemination		

Table 1: *Overview of SOC/CSIRT services from the ENISA framework*

For some organisations the services they offer might not match exactly with one service from the list above: some services might be a combination of several ENISA services or some services might not be represented in the ENISA framework at all. In both cases additional services can be defined. For these new services any related ENISA services should be noted to adhere to the common vocabulary and enable interoperability.

2 As stated by ENISA these services are originally taken from the [CSIRTServices] published by the CERT/CC.

In the FIRST framework there is also a category of services regarding “Situational Awareness”, including services for advising on and execution of data collection, threat intelligence analysis, and security information knowledge management. This category is not explicitly represented by the ENISA services although the underlying activities can be recognised in the descriptions of the services “Incident Analysis”, “Intrusion Detection Services” and “Technology Watch”. If this service category represents an important aspect of the organisation being analysed the corresponding services from the FIRST framework can be used to complete the description.

EXAMPLE: SELECTING SERVICES FOR TEAM LOCKDOWN

The mission of Team Lockdown is to improve the cyber security resilience of their constituents and to offer assistance in case of incidents. The services they select reflect this mission by focusing on the coordination, proactive and security quality management services. To describe their coordination responsibilities Team Lockdown selects both the incident and vulnerability coordination services. To describe their responsibilities regarding the development and dissemination of cyber threat intelligence they select the announcements, technology watch and security-related information dissemination services. Finally, they select the services that describe their role as advisors and knowledge managers from the security quality management category.

The result of the first step is:
- Incident response coordination service
- Vulnerability response coordination service
- Announcements
- Technology Watch
- Security-Related Information Dissemination
- Security Consulting
- Awareness Building

Each service should be defined with a short description to specify the organisation’s interpretation of the service. The ENISA framework offers descriptions of each service, which can be adjusted where necessary to reflect the focus of the organisation.

In the remainder of this example we will focus on the incident coordination services. That is described as follows:
Team Lockdown assists with the coordination of the response effort among parties involved in the incident. These can include the detention centre that is the victim of the attack, other detention centres involved in the attack, and any other centres requiring assistance in the analysis of the attack. Team Lockdown also coordinates the dissemination of relevant information regarding the incident, possible consequences, and lessons learned to other constituents.

STEP 2: IDENTIFY ROLES THAT COVER THE RELEVANT SERVICES

The purpose of the second step in the Dutch Cyber Cube Method is to identify the work roles needed to perform the selected services. For this step we use the NIST framework.

When selecting the relevant work roles, it is often helpful to take into mind a specific person and select the work roles that together make up his or her work. The first step is to read the role descriptions that are included in the framework. Many work roles will immediately be crossed off because they don’t cover the duties and activities of the intended person. For the remaining work roles, a quick scan of the associated tasks can provide insight into whether this work role describes an essential part of the function being considered. As with the selection of the services it might be that the NIST roles do not completely cover the provided service. The NIST roles should be seen as a starting point, the descriptions and associated tasks can be adapted to better fit the organisation.

To simplify the selection of roles we have created a best practice list that couples the ENISA services to the roles of the NIST framework, see Appendix ⇑ B. However, every organisation is different, if the roles indicated by this list do not properly represent the organisation being analysed there might be other roles within the NIST framework that better describe the work being done.

It might be that the same role is selected for multiple services. If these services require a completely different part of the role and or different people perform those different aspects it is useful to consider these role-parts as separate roles when moving on to the associated tasks and competencies. If however the focus of the role is similar within multiple services, the role should be considered as a whole, keeping in mind the context of several services when proceeding with the analysis.

EXAMPLE: SELECTING A WORK ROLE FOR TEAM LOCKDOWN

Team Lockdown organises a meeting with a group of experts that will define the Incident Response Coordination service to identify the relevant work roles from the NIST framework. One of the relevant work roles identified in the best practices list in Appendix B for this service is the 'Partner Integration Planner'.

The NIST framework describes this role as:
Partner Integration Planner (CO-OPL-003): Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Although terms like 'cyber operations' are not generally used in the detention centre sector, the focus of the work role is on advancing cooperation and might therefore be suitable to describe the Incident Coordination Service when considering incident handling as a type of 'cyber operation'.
A quick look at the associated tasks shows that here too the terminology of the descriptions in unsuitable for the sector, but the underlying meaning of the tasks are highly relevant. The team therefore decides to use this work role as the basis for the service. For complex services it might be required to select several working roles, but for the purpose of this example we limit the selection to one work role.

STEP 3: IDENTIFY THE RELEVANT TASKS FOR THE SELECTED WORK ROLES.

The purpose of the third step is to further refine the selected work role by describing the main tasks. For this step we also use the NIST framework. The selected tasks should describe the essential activities of a person performing that role. It is advisable to have the selection checked by people with a clear understanding of the day to day activities that someone in this role performs. Selecting too many tasks will result in a generic work role that may not adequately represent the actual work performed. When developing education or training plans, the rule of thumb is to select a maximum of 5 tasks per work role to focus the required competencies that need to be trained.

The tasks defined in the framework might not seamlessly describe the essential activities for that role. For example, a task might specify a coordination aspect when in practice this should be an execution task. Where required tasks can be adapted.

EXAMPLE: SELECTING TASKS FOR TEAM LOCKDOWN

Having selected the Partner Integration Planner as the main work role for the Incident Response Coordination services, the project team of Team Lockdown discusses the associated tasks and selects those that together best describe the main responsibilities of this work role. Where necessary they keep track of adjustments/specifications to the task descriptions. The final selection is:

Id	Description	Comments
T0582	Provide expertise to course of action development.	course of action refers to the plan for handling the incident
T0795	Provide planning support between internal and external partners.	
T0817	Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.	
T0635	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	to do: identify specific partners
T0700	Facilitate the sharing of 'best practices' and 'lessons learned' throughout the cyber operations community.	'cyber operations community' should be replaced by Lockdown constituents

In the example above we have considered a generic instance of the work role Partner Integration Planner, without any attention to the level of experience of the person performing this role.

STEP 4: IDENTIFY THE RELEVANT COMPETENCIES

The fourth step selects the required competences for each work role. In the Dutch Cyber Cube Method a combination of knowledge, skills and attitudes (KSAs) is selected instead of higher level competencies. This allows for a more specific selection. For this step we use both the NIST Framework and the GMU Framework. The NIST Framework provides a list with knowledge, skill and abilities (KSA) items per work role whereas the GMU handbook provides a general list relevant to SOC/CSIRT personnel.

There is no best practice for the number of KSAs to be chosen. However, for the resulting overview to be usable in practice when creating job descriptions or education and training plans it is advisable to only select the most important KSAs. The selection of the core tasks performed in step 3 can be used to guide the selection of the most important KSAs. When required the description of a KSA item can be adapted to better fit the organisation. If the selected NIST work role does not provide all essential KSAs, elements from different work roles can be added as well.

EXAMPLE: SELECTING KNOWLEDGE, SKILLS AND ABILITIES FOR TEAM LOCKDOWN

In a follow-up session the experts of Lockdown discuss the required KSA for the Partner Integration Planner work role within the context of the Incident Response Coordination service. They start with the list of KSAs associated with the work role in the NIST framework. A few examples of relevant items are:

- K0400: Knowledge of crisis action planning for cyber operations.
- K0538: Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities
- S0218: Skill in evaluating information for reliability, validity, and relevance.
- S0185: Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.

Next they consider the GMU Framework, a few relevant examples are:

- 4: Skill of understanding others and being understood by others; this skill can include speaking, writing, listening, etc.
- 5: Ability to make timely and difficult decisions about which course of action to take
- 10: Ability to maintain an objective attitude despite uncertain or unclear instructions, situations, or problems
- 12: Tolerance adhering to rules and procedures despite personal opinion

Up to this point in the analysis we have considered a 'generic instance' of the work role Partner Integration Planner, without any attention to the level of experience of the person performing this role or any subdivisions/specialties that may exist within the work role. Depending on the reason for performing the analysis it can be helpful to identify different instances of a work role that have different requirements for the proficiency level at which the tasks are performed and the resulting competency requirements. For example, we could distinguish between a junior forensic analyst who performs his or her analysis following a set procedure and a senior analyst who considers the bigger picture and might choose to follow a different path based on his or her earlier experiences. Another example could be a specialty area within a work role, for example one analyst might specialise in Android devices where someone else focusses on Apple devices. When developing job descriptions making such distinctions can assist in identifying the competencies a person should already possess before he or she can perform the work role, and those that can be learned on the job. When developing education and training plans, the required proficiency level per competency is likely to dictate the manner in which knowledge and skills are taught.

STEP 5: EDUCATION, TRAINING, AND EXERCISES

The last step in the Dutch Cyber Cube Method is to identify the appropriate education, training, and exercises to achieve and maintain the required competencies to perform a work role. The details of this step are out of scope for this study. Many commercial companies offer a wide variety of courses that can be bought as-is or that can be customised to meet specific requirements. In some cases, the offered packages might not cover the entire set of to be-trained competences and custom courses might need to be developed.

6. CONCLUSIONS

In light of the growing need for skilled cyber security personnel and the shortage of such personnel on the labour market many SOC and CSIRT organisations are searching for ways to professionalise or reorganise their approach to workforce development. A standardised approach to identify the required competencies for SOC and CSIRT personnel can provide a practical tool for such analysis and promote cooperation by creating a shared understanding between organisations. The aim of this study was to describe such a standardised approach in a practical way, building on the existing knowledge and frameworks developed by other organisations. To this purpose several international frameworks to assist in analysing and organising SOC and CSIRT organisations have been reviewed. However, none of these frameworks are designed for the purpose of identifying the required competencies for SOC and CSRIT personnel, and as a result the application of these frameworks is not straightforward. In this publication we introduce the Dutch Cyber Cube Method as a way to combine the strengths of the ENISA step-by-step approach on how to set up a CSIRT, the NIST Cybersecurity Workforce Framework and the GMU Handbook CSIRT Effectiveness and Social Maturity. Combining these frameworks allows for a step-wise analysis based on the services an organisation offers, the work roles contributing to the services, and the tasks and competencies associated with the work role. We used a fictional use case to describes how the Dutch Cyber Cube Method can be applied to a practical situation.

The next step is to apply this approach on real SOC/CSIRT organisations to test its practicality in real life. We welcome any feedback on the approach we have described and aim to further refine it into a tool that can readily be used by SOC and CSIRTs.

7. REFERENCES

[CERTSkillList] What skills are needed when staffing your CSIRT?; Carnegie Mellon University, Software Engineering Institute; Pittsburgh, PA, USA; 2017. Retrieved March 12, 2018 from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485683.

[CSIRTServices] CSIRT SERVICES; Carnegie Mellon University, Software Engineering Institute; Pittsburgh, PA, USA; 2002, Rev-03-18.2016.0. Retrieved March 12, 2018 from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

[CyberCubeOrg] Cyber Cube: A structured approach towards cyber excellence; Josine van de Ven, Paul 't Hoen, Allard Kernkamp; Presented at The International Forum for the Military and Civil Simulation, Training and Education Community (ITEC), May 17, 2016. Retrieved November 19, 2018 from: https://www.researchgate.net/publication/329041058_Cyber_Cube_A_structured_approach_towards_cyber_excellence.

[e-CF] European e-Competence Framework (e-CF), A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework; version 3.0; Reference EN 16234-1:2016; Work Item Number 00428001. Retrieved February 27, 2018 from: www.ecompetences.eu.

[ENISA] A step-by-step approach on how to set up a CSIRT; H. Bronk, M. Thorbruegge, M. Hakkaja; ENISA, Deliverable WP2006/5.1(CERT-D1/D2); December 22, 2006. Retrieved January 24, 2018 from: www.enisa.europa.eu/publications/csirt-setting-up-guide.

[EQF] European qualifications framework. Retrieved February 27, 2018 from: www.cedefop.europa.eu/nl/events-and-projects/projects/european-qualifications-framework-eqf

[FIRST] Computer Security Incident Response Team (CSIRT) Services Framework; Forum of Incident Response and Security Teams, Inc. (FIRST); Version 1.1; May 19, 2017. Retrieved February 14, 2018 from: www.first.org/education/service-framework;

[GMU] Improving Social Maturity of Cybersecurity Incident Response Teams; George Mason University; 2016. Retrieved June 11, 2018 from: www.incidentresponse.com/wp-content/uploads/GMU-Cybersecurity-Incident-Response-Team_social_maturity_handbook-updated_10.20.16.pdf

[ISC2] Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens; (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018.

[NICE] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework; William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte; National Institute of Standards and Technology (NIST) Special Publication 800-181; Retrieved February 14, 2018 from: www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

[NICE CWF Sup] NICE Framework Specialty Areas and Work Role KSAs and Tasks. Reference Spreadsheet for the NICE Framework. Retrieved February 14, 2018 from: www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

[QIS] Job profiles for information security 2.0; M. Spruit and F. van Noord; PvIB Dutch Association of Information Security Professionals; Version: 2.0; 1 January 2017; ISBN: 978-90-78786-00-9. Retrieved February 14, 2018 from: www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging.

A. FRAMEWORK OVERVIEW

This appendix provides an overview of the frameworks that have been considered in this study. It is similar to the overview that is provided in the chapter 3, but it is more elaborate.

A.1 NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK

Specifications

Author organisation	National Institute of Standards and technology (NIST)
Compliancy with HR (e-CF) standards	Not compliant with E-CF. The knowledge, skills and abilities sets are not used in the same way as e-CF.
Reviewed version	NIST SP 800-181, 2017
Update rate	The framework is still under development new version can be found at www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Purpose
The NIST Framework is a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work, the roles, tasks and the knowledge, skills, and abilities (KSAs) needed to complete those roles and tasks. The NIST Framework aims to improves communication about how to identify, recruit, develop, and retain cybersecurity talent.

Target audience
The NIST Framework is intended for the public, private and academic sectors. It can be used both by employers and cyber security professionals to gain a better understanding of the work roles and tasks and the associated KSAs. It aids employers to inventory and track their cybersecurity workforce and gain a greater understanding of the strengths and gaps. The framework can also be used by education and training providers as a reference to compose curricula.

Framework dimensions
The NIST Framework is hierarchically structured, it describes 7 categories (high level groupings of common cybersecurity functions) such as Securely Provision (SP), Operate and Maintain (OM), et cetera. Each category is subdivided into about 2 to 8 specialty areas for a total of 33 speciality areas. Based on these specialty areas a total of 52 work roles are defined. Each work role consists of a description, a list of associated tasks and a list of required knowledge, skills, and abilities that are required to perform those tasks.

Considerations for using the framework
Suitability of the NIST framework for our research purposes:
- The framework was created in a bottom-up process, which implies that possible gaps are not identified from a higher-level view.
- The framework is still a work in progress.
- Some elements of the framework have been removed because of classification issues. The element that have been removed are not explicitly indicated but seem related to military roles and are therefore unlikely to influence the SOC/CSIRT domain.
- The framework uses the concepts of knowledge, skills and abilities and does not specify competencies which are often used in other frameworks.
- The framework is not compliant with the E-CF HR standard, because the knowledge, skills and abilities sets are not used in the same way as e-CF.
- Social skills and attitudes are not taken into account by the framework for the more technically oriented roles.
- The framework does not refer explicitly to competence levels.
- Roles are related to tasks and KSAs. There are no links among the tasks and the KSAs. As such it is not immediately clear how to create a tailored KSA list for a role where some tasks have been removed.
- The NIST framework is a very comprehensive document. It is best to actually work with it using the Excel tool as provided in the Reference Spreadsheet for the NICE Framework [NICE CWF Sup].

A.2 ENISA STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

Specifications

Author organisation	European Network and information Security Agency (ENISA)
Compliancy with HR (e-CF) standards	The framework discerns types of CSIRTs, business models (the organisation of a CSIRT) and roles. These are not at the same level as e-CF.
Reviewed version	2006
Update rate	This publication does not necessarily represent state-of the-art and it might be updated from time to time. www.enisa.europa.eu/publications/csirt-setting-up-guide

Purpose
The document describes the process of setting up a Computer Security and Incident Response Team (CSIRT) from several perspectives like business management, process management and technical perspective. Although not its main focus, the document does specify relevant roles and competences at a limited level of detail.

Target audience
The primary target audience for this guide are governmental and other institutions that decide to set up a CSIRT to protect their own IT infrastructure or that of their stakeholders. The document addresses the following types of CSIRTs and therefore the organisations that implement and manage them: Academic Sector; Commercial; CIP/CIIP Sector; Governmental Sector; Internal; Military Sector; National; Small & Medium Enterprises (SME) Sector; Vendor.

Framework dimensions
The guide describes several aspects relevant to determining the competencies for SOC/CSIRT personnel. It describes 4 role categories (general, staff, operational technical team and external consultants). They also define several different operational models to organise the CSIRT that influence the responsibilities of each roles:
– Independent business model
– Embedded model
– Campus model
– Voluntary model

Using a list published by the Software Engineering Institute of Carnegie Mellon University they identify 4 service categories that can be offered by a CSIRT (reactive services such as incident handling, proactive services such as security audits and assessments, artefact handling services and security quality management services such as risk analysis). Each service requires a (combination of) roles. The guide also discerns several high-level competences. Each competence is divided in several sub-competences (not shown here for brevity).
– Personal competences, e.g. Strong analytical skills.
– Technical competences, e.g. Knowledge of network infrastructure equipment.
– Additional competences, e.g. Level of education.

Considerations for using the framework
– This guide offers a very hands-on approach to setting up a CSIRT.
– The guide covers the organisational aspects by explicitly discerning different business models.
– Required competences are specified, but they are high level descriptions and do not adhere to any standards.
– The guide does not refer explicitly to competence levels.

A.3 FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST) CSIRT FRAMEWORK

Specifications

Author organisation	Forum of Incident Response and Security Teams (FIRST)
Compliancy with HR standards	The functions are not linked to the e-competence proficiency levels as defined in the European e-competence framework
Reviewed version	First CSIRT Framework, Version 1.1 2017
Update rate	The framework is still under development new version can be found at https://www.first.org/education/service-framework

Purpose
The FIRST CSIRT Framework provides a comprehensive list of services that CSIRTs may provide to assist these organisations in building, maintaining and growing their capabilities. The framework does not assume any specific organisation model and can be used by any organisation.

Target audience
The FIRST framework is intended for CSIRTs choosing their service portfolio.

Framework dimensions
The framework is a hierarchical model consisting of the following levels:
1. Service Area: a group of services related to a common aspect. They help to organise the services along a top-level categorization to facilitate understanding.
2. Service: a set of recognizable, coherent actions towards a specific result on behalf of or for the stakeholder of an incident response team. The list of functions used to implement the service.
3. Function: a means to fulfil the purpose or task of a specified service. The list of tasks that can be performed as part of the function

Next to these three levels, the framework defines internal activities. Internal activities designate supporting functions, which are needed to provide services, but are not specific to a CSIRT. Not all internal activities are defined, only those whose specification in this framework can bring value to CSIRT.

The following service areas are defined, for a complete overview see [FIRST]:
1. Incident Management
2. Analysis
3. Information Assurance
4. Situational Awareness
5. Outreach/Communications
6. Capability Development
7. Research and Development

Considerations for using the framework
- The framework does not provide insight into the competences required to fulfil the defined functions.
- The framework incorporates dedicated services for human factor aspects such as education and training (service 6.2) as well as conducting exercises (service 6.3).
- Relevant quotations regarding the update process of this framework:
  - "This Framework will likely develop: CSIRTs will continue to develop to face the everchanging challenges to keep their stakeholders secure against new threats emerging".
  - Regarding the definition of service areas: "This area will be further developed in Version 2.0."
- The framework definition requires a "purpose" and "outcomes" for every function that is part of the framework. However, not all functions are described by a purpose and an outcome (e.g. compare §1.2.1 and §1.2.2). The level of detail of purpose and outcome descriptions differ between functions.

Future version(s) will add:
- Services grouped by like services in a services area in future version.
- Description of the interdependences among functions.
- Two additional types: Product Security Incident Response Teams (PSIRT); and Regional / Multi-Party Incident Response Teams.
- List of specific tasks and sub-tasks as well as actions for the development of training modules.
- Examples for each CSIRT type and service areas, services, and functions.

A.4 JOB PROFILES FOR INFORMATION SECURITY PROFESSIONALS

Specifications

Author organisation	Dutch Association of Information Security Professionals (PvIB)
Compliancy with HR standards	Employs e-CF, CWA 16458, ISO guide 73, CWA 16234-1, ISO 27000, and others.
Reviewed version	2.0 English, 2017
Update rate	Unknown, www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging

Purpose
The Dutch Association of Information Security Professionals (PvIB) aims to increase the level of professionalism within the field of information security. To this purpose they suggest the establishment of a uniform system of qualifications for professionals. In this paper they have described standardised job profiles identifying the most important professions in the field with transparent and clear qualifications.

Target audience
The target audience are professionals in the field of information security and those that are involved in defining job profiles and education and training.

Framework dimensions
The paper describes 4 job profiles:
– Chief Information Security Officer
– Information Security Officer
– ICT Security Manager
– ICT Security Specialist at 3 levels

A profile can be part of a function description but is not necessarily the same. Every organisation can adapt and combine job profiles into functions as required for their organisation.

Considerations for using the framework
– The job profiles are too high level to directly apply to the SOC/CSIRT domain. It would not offer enough guidelines for determining the tasks and required competences.
– Competences per job are specified using the e-CF standard including the required proficiency level.

A.5 WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT?

Specifications

Author organisation	Software Engineering Institute – Carnegie Mellon University
Compliancy with HR standards	Not compliant with E-CF. The skills are not based on a standard.
Reviewed version	REV-03.18.2016.0
Update rate	Unknown, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485683

Purpose
The white paper describes a set of skills that CSIRT personnel should possess to provide basic incident-handling service.

Target audience
Unspecified, we assume CSIRT organisations and education and training providers.

Framework Dimensions
The whitepaper describes several personal skills (like communication and team skills) and technical skills subdivided in general technical skills and incident handling skills.

Considerations for using the framework
– The white paper lists both technical and non-technical skills, however no competency levels are indicated.
– The paper focusses on the basis skills required of CSIRT personnel, advanced or specialty skills are not discussed.
– The skills are not described as measurable behaviour.

A.6 EUROPEAN E-COMPETENCE FRAMEWORK (E-CF) FOR ICT PROFESSIONALS

Specifications

Author organisation	Software Engineering Institute – Carnegie Mellon University
Compliancy with HR standards	Not compliant with E-CF. The skills are not based on a standard.
Reviewed version	REV-03.18.2016.0
Update rate	Unknown, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485683

Purpose

The European e-Competence Framework (e-CF) was established as a tool to support mutual understanding and provide transparency of language through the articulation of competences at five proficiency levels required and deployed by ICT professionals (including both practitioners and managers).

Target audience

The e-CF was created for application by ICT service, user and supply companies, for managers and human resource (HR) departments, for education institutions and training bodies including higher education, for market watchers and policy makers, and other organisations in public and private sectors.

Framework dimensions

The European e-Competence Framework is structured from four dimensions. These dimensions reflect different levels of business and human resource planning requirements in addition to job / work proficiency guidelines and are specified as follows:

1. Dimension 1: **5 e-Competence areas**, derived from the ICT business processes PLAN – BUILD – RUN – ENABLE – MANAGE
2. Dimension 2: A set of **reference e-Competences for each area**, with a generic description for each competence. The framework defines 40 competences in total. The e-CF expresses ICT competence using the following definition: “Competence is a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results”. This is a holistic concept directly related to workplace activities and incorporating complex human behaviours expressed as embedded attitudes.
3. Dimension 3: **Proficiency levels of each e-Competence** provide European reference level specifications on e-Competence levels e-1 to e-5, which are related to the EQF levels 3 to 8.
4. Dimension 4: Samples of **knowledge and skills** relate to e-Competences in dimension 2. They are provided to add value and context and are not intended to be exhaustive.

Whilst competence definitions are explicitly assigned to dimension 2 and 3 and knowledge and skills samples appear in dimension 4 of the framework, attitude is embedded in all three dimensions.

Considerations for using the framework

– The introductory sections of the e-CF state that “to consider the changing priorities of existing issues (e.g. security) were addressed across the entire framework and incorporated within relevant dimensions”. Indeed, the security issue is referred to in many of the competence descriptions. Still, the document does not describe what specific security-related knowledge and skills are required to obtain the specific competence (e.g. competence C.2 Change support requires knowledge about the best practices and standards in information security management).

A.7 IMPROVING SOCIAL MATURITY OF CYBERSECURITY INCIDENT RESPONSE TEAMS

Specifications

Author organisation	Software Engineering Institute – Carnegie Mellon University
Compliancy with HR standards	Not compliant with E-CF. The skills are not based on a standard.
Reviewed version	REV-03.18.2016.0
Update rate	Unknown, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485683

Purpose

This handbook is written to support CSIRT managers to improve hiring decisions, training programs, and their abilities to design and develop effectivein teams for handling cyber incidents. It focusses not on the technical skills but on the required social dynamics within the team.

Target Audience

The handbook is written primarily for CSIRT managers, team leaders, and Human Resources (HR) staff but also serves to share the results of the research project with other applied researchers interested in cybersecurity.

Framework dimensions

The handbook provides several methods, strategies and tools to build, staff, train, and foster a team that leverages both the latest cyber technologies and the social dynamics required to make the best use of them. Relevant to our research is an overview of non-technical knowledge, skills, abilities and other characteristics (KSAOs) relevant for CSIRTs team members. These KSAO's are divided in three categories: teamwork, cognitive factors, and personal character.

Considerations for using the framework

- The handbook focusses on the team skills required by effective CSIRT teams but does not address the technical competencies.
- The KSAOs have been derived from interviews and surveys with CSIRT teams, study of existing frameworks such as the NIST framework and job advertisements.
- The KSAOs do not adhere to any standards.

B. OVERVIEW OF ENISA SERVICES COMBINED WITH NICE ROLES

ENISA services	NICE Framework roles
Reactive Services	
Alerts and warnings	Cyber Defence Incident Responder (PR-CIR-001)
Incident handling	
Incident analysis	Cyber Defence Analyst (PR-CDA-001) Cyber Defence Forensics Analyst (IN-FOR-002) Cyber Crime Investigator (IN-INV-001)
Incident response support Incident response on site	Cyber Defence Incident Responder (PR-CIR-001) Cyber Defence Infrastructure Support Specialist (PR-INF-001)
Incident response coordination	Partner Integration Planner (CO-OPL-003) Information Systems Security Manager (OV-MGT-001) Cyber Defence Incident Responder (PR-CIR-001) Information Technology (IT) Project Manager (OV-PMA-002)
Vulnerability handling	
Vulnerability analysis	Vulnerability Assessment Analyst (PR-VAM-001) Systems Security Analyst (OM-ANA-001)
Vulnerability response	Systems Security Analyst (OM-ANA-001) Technical Support Specialist (OM-STS-001) System Administrator (OM-ADM-001) Cyber Defence Infrastructure Support Specialist (PR-INF-001)
Vulnerability response coordination	Partner Integration Planner (CO-OPL-003) Information Systems Security Manager (OV-MGT-001) Systems Security Analyst (OM-ANA-001) Information Technology (IT) Project Manager (OV-PMA-002)
Proactive Services	
Announcements Technology watch	Warning Analyst (AN-TWA-001) Information Systems Security Manager (OV-MGT-001)
Security audits or assessments	Security Control Assessor (SP-RSK-002) Vulnerability Assessment Analyst (PR-VAM-001) Secure Software Assessor (SP-DEV-002)
Configuration and maintenance of security	Cyber Defence Infrastructure Support Specialist (PR-INF-001) Security Architect (SP-ARC-002) Technical Support Specialist (OM-STS-001) System Administrator (OM-ADM-001) Cyber Policy and Strategy Planner (OV-SPP-002)
Development of security tools	Cyber Defence Infrastructure Support Specialist (PR-INF-001) Systems Developer (SP-SYS-002)
Intrusion detection services	Cyber Defence Analyst (PR-CDA-001)
Security related information dissemination	Knowledge Manager (OM-KMG-001) Partner Integration Planner (CO-OPL-003)
Security and Quality Management	
Risk analysis	Security Control Assessor (SP-RSK-002)
Business Continuity and Disaster Recovery	Systems Security Analyst (OM-ANA-001)
Security Consulting	Partner Integration Planner (CO-OPL-003) Cyber Policy and Strategy Planner (OV-SPP-002) Information Systems Security Manager (OV-MGT-001) Systems Security Analyst (OM-ANA-001) Security Architect (SP-ARC-002) Systems Requirements Planner (SP-SRP-001)

ENISA services	NICE Framework roles
Awareness Building	Cyber Instructional Curriculum Developer (OV-TEA-001) Knowledge Manager (OM-KMG-001)
Education/Training	Cyber Instructional Curriculum Developer (OV-TEA-001) Cyber Instructor (OV-TEA-002)
Product Evaluation or Certification	Security Control Assessor (SP-RSK-002) Secure Software Assessor (SP-DEV-002)
Artefact Handling	
Artefact analysis	Cyber Defence Analyst (PR-CDA-001) Cyber Defence Forensics Analyst (IN-FOR-002)
Artefact response	Cyber Defence Infrastructure Support Specialist (PR-INF-001) Cyber Defence Analyst (PR-CDA-001)
Artefact response coordination	Partner Integration Planner (CO-OPL-003) Systems Security Analyst (OM-ANA-001) Information Technology (IT) Project Manager (OV-PMA-002)

Auteurs:
G.R. Jansen-Ferdinandus
E.F.T. Buiel
P.P. Meiler
T. Verburgh

Reviewers:
J.G.M van de Ven (TNO)
B. van der Kamp (NCSC)
A.C. Kernkamp (TNO)

18-10417