



# Getting started with a national CSIRT



Cybersecurity  
Capacity Building



# Colophon

## Authors

Hanneke Duijnhoven (TNO)

Bram Poppink (TNO)

Tom van Schie (TNO)

Don Stikvoort (m7)

## TNO

Oude Waalsdorperweg 163

2597 AK Den Haag

The Netherlands

info@tno.nl

TNO.NL



Editing and design: Waai Impact Agency

This guide has been developed in the context of the Global Forum on Cyber Expertise (GFCE), Working Group B, taskforce Cyber Incident Management. The GFCE is a global platform that aims to strengthen cyber capacity and expertise globally through international collaboration, through practical initiatives around relevant topics.

May 2021

The development of the guide is funded by the Dutch government.

©TNO 2021 This guide is for informational purposes only. The user is allowed to freely copy and/or distribute this guide within the aforementioned purposes and provided the guide and its contents remain in full and unchanged. Without prior written consent, it is prohibited to submit this guide for any registration or legal purposes, commercial use, advertising or negative publicity. Unauthorised or improper use of this guide or its content may breach intellectual property rights of TNO, for which you are responsible. Although TNO has exercised due care to ensure the correctness of the information as stated in the guide, TNO expressly disclaims any warranties on its contents. All content is provided 'as is' and 'as available'. Decisions which you take on the basis of this information will be at your own expense and risk. Translation of the full guide into another language is allowed, provided that the authors are notified and their written consent has been received.

# Getting started with a national CSIRT

**TNO**

Hanneke Duijnhoven, Bram Poppink, Tom van Schie

**m7**

Don Stikvoort

# Index

❖ **Introduction**

5

❖ **What is an nCSIRT?**

7

❖ **Gaining Political Support**

22

❖ **Community building**

13

❖ **Formulating a business case**

29

❖ **Resource guide**

57

❖ **Wisdom from the field**

42

❖ **Glossary**

62

❖ **Authors and contributing experts**

64

# Introduction

Why does your country need a national CSIRT? What does it take to build one? And where do you begin? If you are asking yourself these types of questions, we have got some good news for you.

Many people before you, in countries all over the world, have once found themselves in the same situation. They were looking for support in the early stages of policy formation. Some got help from experts, while others had to work through a lot of resources by themselves. Taking those first steps in setting up an nCSIRT can be quite challenging and time-consuming. Even though there is a lot of information available, it can be difficult to assess which sources are the most valuable. Let alone finding those bits and pieces of information that will help you take specific actions towards setting up an nCSIRT.

## Resource guide

*In this guide we refer to several valuable resources, some of which provide more in-depth information. We have selected the most important insights and will reference some of the underlying resources for you to further inform yourself. Some of these will also be addressed in other sections of this guide. An overview of annotated references can be found in the [resource guide](#) on page 57.*

## How to use this guide

*This guide is structured in such a way that you can easily navigate between sections in no particular order. The next section 'What is an nCSIRT?' is a good starting point to get a quick overview of the key aspects of an nCSIRT. From there on, you can pick any topic that may be of interest to you. In this guide, we cover the following topics: The value of community building and important stakeholders, the importance of political support for nCSIRT capacity building, key ingredients to help formulate a business case, lessons learned from experts and nCSIRTs across the globe. Finally, the resource guide highlights the relevance of some key resources available, and the glossary provides an overview and explanation of key terminology.*



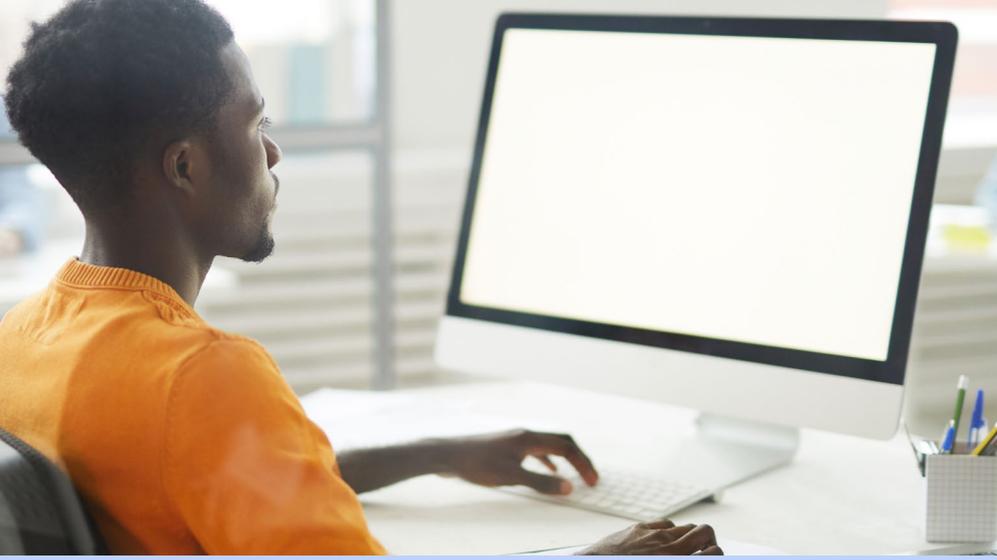


In this guide, we have documented experiences from both experts and your peers across the world. This guide draws from their experiences and aims to guide you through the planning, development and initial stages of nCSIRT capacity building. This guide is meant for anyone who wants to learn more about setting up an nCSIRT. Whether you are:

- A policymaker who wants to define the appropriate cybersecurity capacity for your country's needs
- Part of an organisation that wants to convince your government of the necessity of collaboration for building cybersecurity capacities, or
- Looking for guidance on specific topics such as where to embed the nCSIRT or how to coordinate responsibilities.

This guide will offer you hands-on information and useful examples on any nCSIRT- related topic you are looking for.

- [What is an nCSIRT?](#)
- [Community building](#)
- [Political support](#)
- [Business case](#)
- [Wisdom from the field](#)
- [Resource guide](#)
- [Glossary](#)



# What is an nCSIRT?

Before we take you through the nuts and bolts of setting up an nCSIRT, we would like to give you a quick understanding of the basics and explain why every country should have its own nCSIRT. If you are already familiar with nCSIRTs, we suggest you skip right ahead to a topic that is of interest to you.

## What is an nCSIRT?

In this guide, we focus on CSIRTs that take on national responsibility, usually called a national CSIRT or nCSIRT. An nCSIRT's primary goal is to enhance the country's digital safety, security and protection. An nCSIRT can be seen as a capacity that provides a wide range of cyber activities and services (both technical and non-technical) to relevant stakeholders in order to fulfil this goal. Although in practice many nCSIRTs are part of their respective government, nCSIRTs may also be operated by an independent third party. What makes an nCSIRT national is that it has a formal mandate to fulfil a national responsibility.

## Where it all started

The emergence of CSIRTs – and thus, the emergence of nCSIRTs – as an effective approach to fight against computer security incidents can be linked directly to one of the first large scale incidents that has spread over the Internet, the Internet Worm in 1988. In 1990, the Forum of Incident Response and Security Teams (FIRST) was launched to coordinate and ease collaboration

between different teams that had emerged as a response to the Internet Worm and subsequent incidents<sup>1</sup>. From that moment on, CSIRTs started to emerge in all areas of society, forming a global community. Among these teams were also the first government teams, focussing on government networks and systems.

Some countries had a 'team of last resort' that functioned as a national team but without an official mandate. An example is CERT-NL that was later renamed SURFcert. It is not entirely clear when and where the first officially mandated national CSIRTs emerged. However, around 2005 governments started to increasingly realise that focussing on the government networks alone was not enough. Furthermore, large cyber-attacks in Estonia (2007)<sup>2</sup> and Georgia (2008)<sup>3</sup> played an important role in making nations aware of the need to respond to such attacks in a more coordinated fashion. Over the years, nCSIRTs have become an essential part of cyber security management. Today, the majority of countries worldwide have established a national CSIRT.



## Different types of CSIRTs

A CSIRT (Computer Security Incident Response Team) supports a particular target audience (i.e. the CSIRT's constituency) in preventing as well as responding to computer security incidents. There are different types of CSIRTs, often defined by the type of constituency they serve, such as<sup>4</sup>:

- parent entity (e.g. company, government or any other kind of organisation)
- geographical region (e.g. city, state, country, region, or entire continent)
- sector (e.g. telecom, financial or academic)
- customers (e.g. an individual company or customers using a product from a specific vendor)

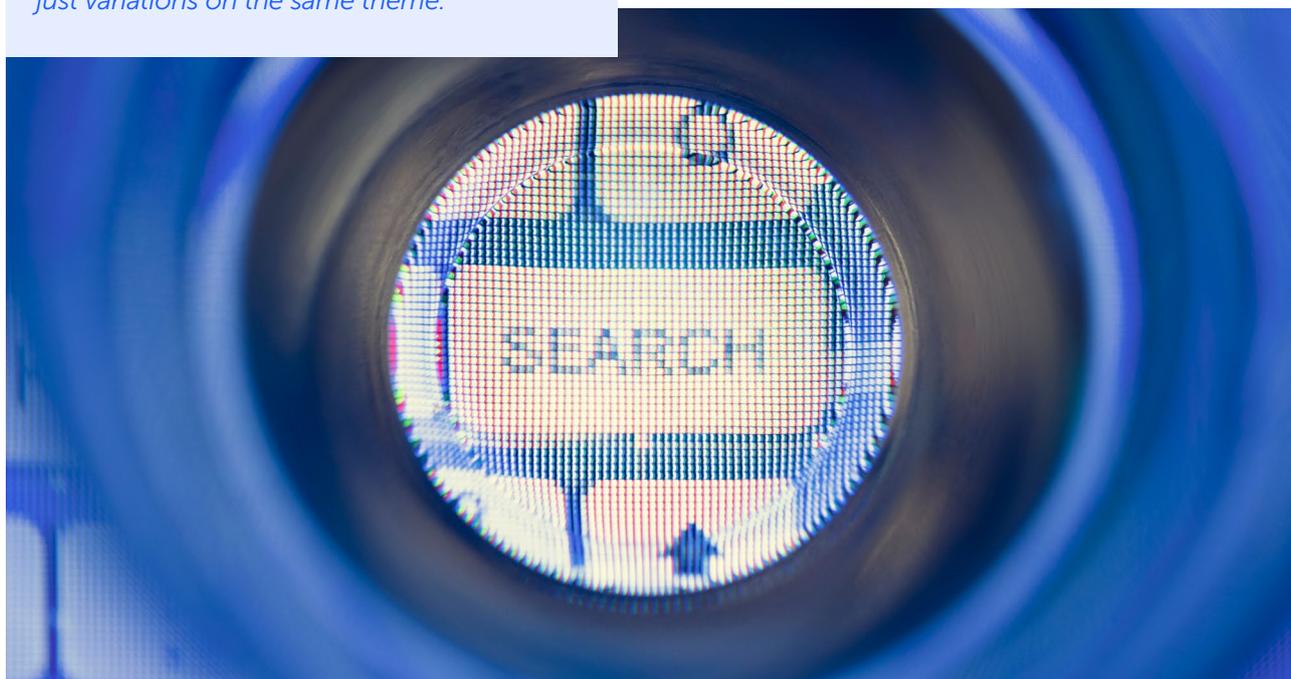
In the CSIRT community, a lot of acronyms are used for naming teams. CERT (Computer Emergency Response Team) is the oldest one, but that name is the intellectual property of the Carnegie Mellon University. CSIRT is the most common acronym and has no licensing restrictions. Other names in use are National Cyber Security Centre (NCSC), Cyber Defence Centre (CDC) and Cyber Incident Response Team (CIRT). Although each team has its own particular focus, in reality, all these names are just variations on the same theme.

## The importance of nCSIRTs

Over the last few decades, there has been a significant increase in the establishment of nCSIRTs. This is a good indication that a growing number of countries recognise the added value of such a national CSIRT capacity.

It is difficult to list the exact benefits of having an nCSIRT, as it varies per country and depends on local aspects. However, all societies are nowadays highly reliant on computer networks and Critical Information Infrastructure. Therefore, protecting both of these is of vital importance to improve national cyber resilience and national security. nCSIRTs play a crucial role in ensuring the protection of these critical national assets against cyber threats. How, why, for whom, and within what legal bounds an nCSIRT capacity operates, differs per country.

There is an increasing awareness that the establishment of nCSIRTs is an essential step in building cyber capacity across nations. Because cyber threats are not limited by country borders, an effective response requires collaboration between countries. Therefore, international organisations such as the UN GGE<sup>5</sup>, as well as regional organisations like the African Union, the Association of Southeast Asian Nations (ASEAN), and the Organization of American States (OAS), encourage the establishment of nCSIRT capacities in the global fight against cyber threats.



## Activities and services an nCSIRT provides

Although the term 'incident response' may suggest otherwise, most nCSIRTs spend significant time on prevention activities such as:

- Awareness campaigns
- Education and training
- Threat analysis
- Organising information sharing
- Collaborating with relevant stakeholders

When an incident does occur, an nCSIRT should facilitate a nationally orchestrated response by alerting relevant stakeholders, facilitating information exchange, and coordinating actions. An nCSIRT may also be involved in the actual incident resolution for some part of its constituency, depending on the mandate it has. In the aftermath of an incident, an nCSIRT should also be involved in the evaluation and make sure the lessons learned will reach relevant stakeholders. Due to the broad scope of nCSIRT activities, terms such as 'incident management' or 'incident readiness' are increasingly used as alternatives to the term 'incident response'.

## To whom does an nCSIRT provide its services?

The target audience or constituency of an nCSIRT differs per country and depends on what type of organisation the nCSIRT capacity is (e.g. government branch, independent organisation, etc.). In many countries the nCSIRT constituency includes government organisations and critical infrastructure providers. In some cases, it also includes large businesses and specific sectors. Although the name 'national CSIRT' suggests it represents the entire country, this is not always true. There are also countries with a number of different nCSIRTs that each serve their own constituencies. For instance, in New Zealand, the National Cyber Security Centre (NCSC) supports the government and critical infrastructure providers, while CERT NZ services the rest of the country (such as small and medium businesses and the general population). In turn, tunCERT in Tunisia considers the entire country as its constituency.

## The importance of transnational cooperation among nCSIRTs

*Cyber threats spread across organisational boundaries, sectors, national borders and even continents. They permeate every aspect of society. Therefore, for a national team to be effective inside its country, it should establish and maintain good relations with national and transnational stakeholders, including other national teams and CSIRT cooperations – both in its geographical region and worldwide.*

## Key aspects of an nCSIRT capacity

*If you consider setting up an nCSIRT capacity, you should keep in mind that the choices you make will depend on your country's specific context, the challenges you face, and the ambitions you have. An essential range of key aspects is listed in the Global CSIRT Maturity Framework, in particular the 'organisational' aspects. The Global CSIRT Maturity Framework is a widely accepted maturity development model for nCSIRTs.*



### **A multi-stakeholder approach is key**

In the other sections of this guide, we will provide information that will help you develop a concept and a plan for your country's nCSIRT capacity. Be aware that setting up an nCSIRT is not something you can or should do all by yourself. A crucial element for success, according to experts, is that an nCSIRT capacity should always be established in collaboration with a wide variety of stakeholders. When establishing an nCSIRT, adopting a multi-stakeholder approach right from the start is quintessential for success. Go out and get to know the relevant stakeholders in your country, so you can involve them right from the start. Together, you should be able to answer the what, for whom, how, and why questions of your nCSIRT capacity. Get the stakeholders on board, and keep them on board.

### **Useful resource**

*The Forum of Incident Response and Security Teams (FIRST) has created an extensive document on what kind of services a CSIRT can provide. This [FIRST CSIRT Services Framework](#) is a widely accepted resource for selecting which set of services will work best for a specific CSIRT, including national teams.*

---

<sup>1</sup> <https://www.first.org/about/history>

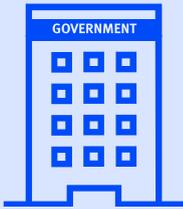
<sup>2</sup> [https://en.wikipedia.org/wiki/2007\\_cyberattacks\\_on\\_Estonia](https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia)

<sup>3</sup> [https://en.wikipedia.org/wiki/Cyberattacks\\_during\\_the\\_Russo-Georgian\\_War](https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War)

<sup>4</sup> This list is not exhaustive and there currently is no universally agreed taxonomy of CSIRTs.

<sup>5</sup> UN GGE: The United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.

# Myths



**An nCSIRT is a government-led organisation/institution.**

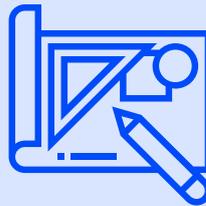
# FACTS



**An nCSIRT can be a government-led organisation, but it can also be an independent (not-for-profit) organisation or part of a national network information centre or domain registrar. The defining feature of an nCSIRT is its national responsibility for cybersecurity incident prevention and response.**



**We can just copy another nCSIRT's strategy, structure and institutional embedding.**



**There is no one-size-fits-all model for an nCSIRT capacity because legislative and cultural contexts differ across countries. However, good practices from other countries can provide a valuable source of inspiration.**



**An nCSIRT is all about responding to incidents.**



**Responding to incidents usually accounts for only 20% of an nCSIRT's activities, the remaining 80% is dedicated to prevention, detection, implementing lessons learned, information sharing and outreach activities.**



# Community Building

How do you determine which stakeholders are relevant? How do you build a relationship with them? What are the important lessons we can learn from the experiences of other nCSIRTs? These questions, and more, will be addressed in this section.

## The importance of a multi-stakeholder approach

Setting up and growing a national CSIRT capacity is not a task that can or should be done in isolation. Because an nCSIRT cannot properly function without (in)formal relationships with national and international stakeholders, including the global CSIRT community. Therefore, effort should be put into identifying and engaging with relevant national and international stakeholders. Experts agree that the single best advice for an nCSIRT is to go out and start building a strong community right from the start.

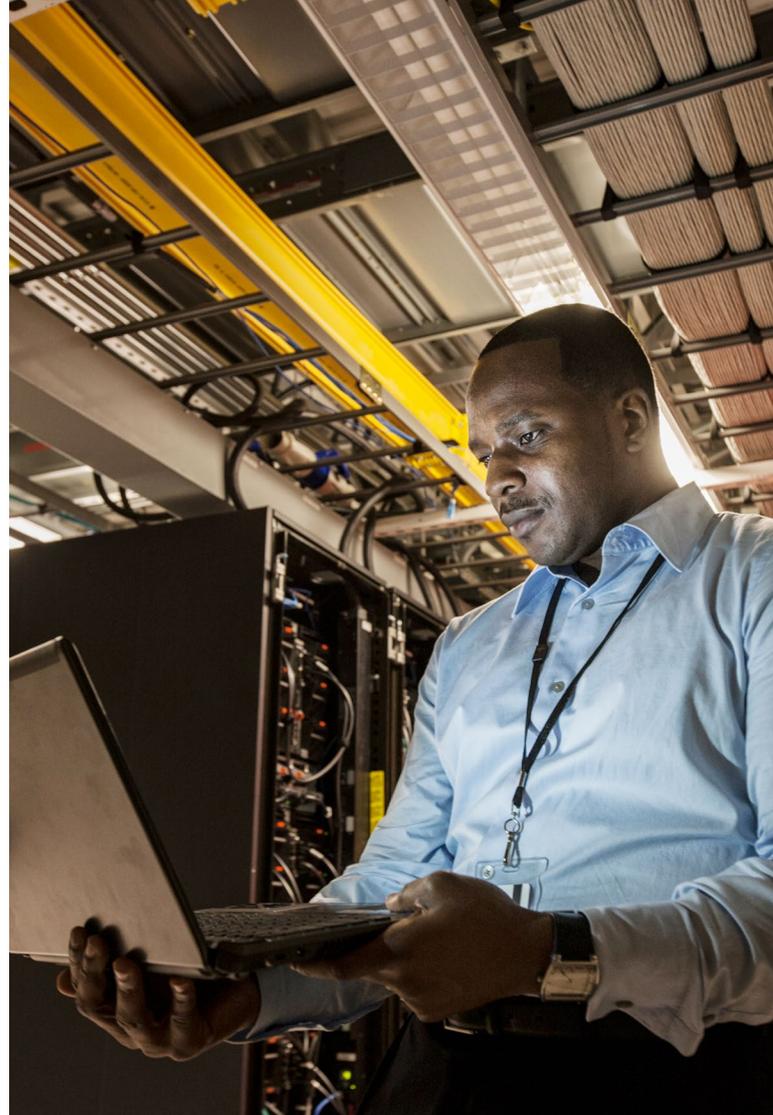
Investing in building strong relationships with stakeholders will prove to be very valuable later on. Collaboration and trust are built in the 'cold phase' (when there is no crisis) and capitalised on during crises.

## Trust is key

An nCSIRT must become a trusted entity within the cybersecurity community. Trust is primarily built by recruiting nCSIRT staff members who are well-known for their expertise and by sharing information in a reliable and discrete manner. The nCSIRT should also be able to handle confidential information securely, for instance, when it receives reports about incidents from one of its stakeholders.

Becoming a trusted entity requires building relationships with different types of stakeholders and actively contributing to a cybersecurity community that spans different domains and sectors, including the private sector. Building trust, both nationally and internationally, may take several years. Once built, trust needs to be carefully maintained. Always keep in mind that trust is established between people (experts) and not between entities.

An nCSIRT must be aware of how cybersecurity intersects with the different critical infrastructure domains as well as other relevant sectors of the economy. A good approach is to form collaborative groups to share information and develop relationships to increase awareness



building, technical expertise and analysis, and incident response. A first step is to figure out which people or organisations in your country are already involved in cybersecurity and incident response. Reach out to them and listen to their ideas and concerns. This will not only contribute to building a trusted relationship, it will also help you determine what the most urgent needs are within your country and subsequently improve your strategy.

A newly established national CSIRT capacity must become known to the public and its constituents. One successful way to let the world know who you are and what you do is by organising events. In [Cyprus](#), CSIRT-CY organised both technical as well as awareness-raising events about cybersecurity. As a result, CSIRT-CY was known and trusted by its stakeholders and constituents right from the start.

## Communicate with stakeholders

In order to build a community around your nCSIRT, you have to go out and communicate about your initiative as soon as you can. You should not wait until you are fully established. Instead, use the interactions with stakeholders to spark collaboration. Proactive communication to the outside world is key.

Make sure your communication activities connect with the target audience, even if this involves creating different versions of the same content piece for different audiences – which is what CERT NZ in [New Zealand](#) does. Cybersecurity is an important but also a quite difficult topic. Many people have a hard time to understand it in its entirety. However, if you can successfully help them and make their lives easier by providing real value, you will receive trust and support in return. This will result in people and businesses being more likely to report incidents, providing you with the necessary data for analyses and reports, thereby enabling the nCSIRT to provide even better support. It is all about growing together.

Use different styles and media for your communication activities. This is important during the planning and establishing stages, and also later on. nCSIRTs are often involved in national

awareness campaigns; they exchange information with different interest and stakeholder groups; they publish reports; and they communicate with a range of different stakeholders from private companies, technical communities, civil servants and politicians. Each of these tasks and each audience requires a different approach to get the information across in a meaningful way. Having a communication professional in your team is one way to ensure your communication strategy is most effective. Moreover, it is recommended that you invest in the communication skills of all your [nCSIRT staff](#), as human communication is a vital ingredient of the nCSIRT work. So do make sure to invest not only in your team's technical abilities but also in their soft skills, with communication being the crucial one.

As a national CSIRT, it is essential to get information across to a wide range of audiences, especially when it comes to awareness campaigns. It is emphasised by tunCERT in [Tunisia](#) that having a specialised communication professional and press liaison in your team can be very effective to translate technical information for the general public.



## Identifying relevant stakeholders

Who are the relevant stakeholders for your nCSIRT? It largely depends on your national context. That is why it is crucial to familiarise yourself with the existing cybersecurity community. Go out and talk to people in this community. What do they do? Who do they engage with? What do they need? What would they expect from an nCSIRT?

A multi-stakeholder approach is essential in building a strong and sustainable community in a country, as shown by CERT.br. in [Brazil](#). Their team consists of experts that were already active in the industry and knew one another, which helped them build and extend the community. For new teams, the important lesson to learn from this is to connect to the people and organisations that are already active in the cybersecurity field. They are the consistent factor, especially when an nCSIRT is a government organisation, because such organisations tend to have a high rotation of staff.

### Existing CSIRTs in your country

A good place to start with community building is by looking for existing CSIRTs in your country, for example, sectoral CSIRTs or CSIRTs at national educational research networks, universities, telecom providers, Internet Service Providers, Information Technology (IT) vendors and other (large) private sector organisations. During the initial stages of your nCSIRT, these stakeholders can provide valuable input for and feedback on the goal and strategy of your nCSIRT. These teams often have a good overview of the cybersecurity community in your country and an in-depth understanding of the threat landscape. They probably also have experience with incident response and extensive technical knowledge. Their experience and knowledge will prove useful to you when building a community around your nCSIRT.

## Resource

*In their "[Best Practices for Establishing a national CSIRT](#)", the Organization of American States (OAS) provides an extensive overview of the types of relevant stakeholders and the different types of relationships they may have towards the nCSIRT (a member of the constituency, strategic partner, sponsor, service provider, etc.). The OAS document also offers practical suggestions for identifying and engaging with stakeholders.*

## Bring experts and stakeholders together

*DDoS (distributed denial of service) attacks are quite common. They can disrupt or black out whole companies, universities, government IT networks, or even worse. Your country's educational research network and ISPs will have experience in handling these types of incidents. You, as an nCSIRT, will rarely have to deal with a DDoS attack hands-on, but you are the one with the unique ability to bring experts and stakeholders together and advise on a response strategy, especially in the case of a very big attack.*

*As you can see, it is crucial to bring the various experts in your country together. No one will expect an nCSIRT to have all the answers. Rather, they will expect an nCSIRT to leverage and support the community in such a way that they can come to a solution together and implement effective strategies to fight off a DDoS attack or any other serious threats.*

### Critical infrastructure

A particular group of stakeholders are critical infrastructure providers. They can provide information and are a strategic partner, as well as often part of the constituency. Developing relationships with critical infrastructure providers requires a dedicated staff. It is necessary to invest in these relationships as they are very valuable to an nCSIRT.

### Government organisations

Another relevant group of stakeholders consists of government organisations that have a specific role in cybersecurity. Building a strong cybersecurity community within the national government is important, as many government organisations are active in cyberspace – including law enforcement, the military, the intelligence community, and regulators. As the nCSIRT, responsible for cybersecurity nationwide, you should reach out to these organisations to map their specific role to ensure that each organisation knows what role to play and how to work together effectively – and that the approach will support the nCSIRT's cybersecurity mission. We especially encourage you to invest in building a good working relationship with law enforcement and the intelligence community. By the nature of their work, collaboration will not always be easy. Still, it is in the interest of your country to make sure that all these complementary approaches towards national security work well together. The specifics of your collaboration will need to be determined with your peers. Some of the bigger nCSIRTs opt to have a standing member from law enforcement in their team and also one from the intel forces, to optimise and streamline cooperation.

### Research and education sector

Establishing a good relationship with research and educational institutions is beneficial in many ways. Your country most likely has an educational research network that runs a network for the educational sector. The experts of the educational research network are often very accomplished in cybersecurity and experienced in (inter)national cooperation. Besides, research institutes can become trusted, long-term partners of an nCSIRT

to ensure a solid knowledge base for the nCSIRT to draw from. For smaller nCSIRTs, such research institutes can also provide a flexible workforce to outsource specific analyses and research projects, aided by the fact that there is already a level of trust (and screening if necessary) that enables exchanging sensitive data and information.

Having long-term, trusted relationships with (academic) research institutions is very valuable for nCSIRTs. It ensures that you can acquire the technical expertise and innovation that is needed to keep up with technological developments. Take, for example, the relationship between the [US government](#) of the and research institutes such as [SEI with its CERT/CC](#).

Academic institutions and other educational organisations provide an essential source of knowledge to draw from. But collaborating with the educational sector can also take place in other ways. By setting up specific IT or cybersecurity programmes at all levels of education, the level of awareness and knowledge within the country can increase significantly. Having strong educational programmes may also attract IT businesses to the country.

Collaborations between nCSIRTs and educational institutions, as the example of [Tunisia](#) shows, can be an effective strategy to strengthen the maturity of the IT security sector in a country. Educational programmes yield professionals with higher levels of expertise and relevant skills who will find employment that contributes to the nation's cybersecurity.

### IT sector and Internet Service Providers

The nCSIRT is essentially the guardian of the security of your country's cyberspace. Your country's IT sector operates in this cyberspace. The argument for close cooperation with that sector could not be expressed more clearly. A few parties in the IT sector play a unique role, and cooperation with them is of vital importance.

- First of all, there are the (private) parties that operate the Internet exchange points that

## Civil society

*It may be less obvious, but it is also worthwhile to investigate if there are civil society organisations that are relevant to reach out to. There is a growing number of associations, NGOs and not-for-profit organisations that have an interest in cyber.*

*International examples are Amnesty International who actively pursue the protection of human rights on the Internet; the Internet Society who work to sustain an open, globally connected, secure, and trustworthy Internet; and AccessNow who defend the digital rights of users at risk around the world.*

## Get connected

*Even if your ability to contribute to the international community is limited in the beginning, it is still relevant to connect and start building an international network and learn from international experts and peers. International collaboration takes time and may require some cultural adjustment. Gradually, as your nCSIRT matures, you will be able to contribute and add value to the international community by collaborating and sharing your experiences.*

connect your country to the global cyberspace – together with the top-level domain operators, they are the lungs of your cyberspace.

- Secondly, there are the large telecom operators who run most of the connections inside your country – they are the arteries.
- Thirdly, there are the leading Internet Service Providers (ISPs) that provide access – they are the skin.

Your team needs to connect with the lungs, arteries and skin of your country's cyberspace. Additional providers, such as big hosting providers, IT service companies, vendors, and cybersecurity firms, can also play a valuable role.

## International collaboration

In addition to national partnerships and collaborations, make sure that you also start engaging with relevant stakeholders at the international level as early as possible. The transnational nature of cyber threats makes it inevitable to collaborate across nations to build cyber capacities and protect the safety and security of the cyber realm. This can be a challenge because adverse cyber acts definitely play a role in international relations, often rooted in geopolitical tensions. When you are taking the first steps towards setting up an nCSIRT, building international relations may not be the first thing on your mind. Nevertheless, it is of vital importance to reach out and engage with international stakeholders.

### Important examples of regional collaborations (non-exhaustive list)

⇨ [Africa: AfricaCERT](#)

⇨ [Asia-Pacific: APCERT](#)

⇨ [Europe: TF-CSIRT](#)

⇨ [Europe: Trusted Introducer](#)

⇨ [The Americas: OAS-CICTE](#)

⇨ [Latin-America: LACNIC CSIRT](#)

## Regional collaborations

The first step in building international relations is to reach out to existing collaboration platforms in your region. In most regions of the world, there are one or more organisations that serve as a contact point for nCSIRTs. These regional organisations cannot only offer information and support to you, but they can also provide a platform for communicating and collaborating with other nCSIRTs in your region. For instance, through joint training and exercises, information sharing, or by assisting each other in case of incidents. An advantage of regional collaboration between national teams is that oftentimes there already is at least a basic level of understanding of each other's culture and history. Lessons and insights from peer nCSIRTs in your region can therefore be very valuable for you as a starting team.



There are many examples of regional cooperation between nCSIRTs, where the support of a more mature nCSIRT has significantly contributed to the development of new nCSIRTs. In South-East Asia, Japan has helped ThaiCERT during its early stages, which was very valuable. In turn, [Thailand](#) has been involved in the establishment of APCERT, a partnership in the Asia and Pacific region.

Tunisia was the first country in Africa to establish a national CSIRT, and ever since, it has played an important role in Africa, assisting other countries in the region. [Tunisia](#) also played an important role in the launch of AfricaCERT, a regional collaboration forum for African CSIRTs.

## Global collaborations

Several global organisations advocate transnational collaboration between nCSIRTs (as well as other cybersecurity stakeholders), primarily to improve digital security on a global level. Engaging with these organisations can open new doors and introduce you to an extensive network of peers.

### Global collaboration platforms

- *The Forum of Incident Response and Security Teams (FIRST): FIRST brings together a wide variety of security and incident response teams across the world (<https://www.first.org/>)*
- *NatCSIRT: Annual Technical Meeting for CSIRTs with National Responsibility hosted by Carnegie Mellon University's CERT Coordination Centre (CERT/CC) bringing together national CSIRTs worldwide. NatCSIRT meetings usually co-locate with FIRST conferences (<https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm>)*
- *The International Telecommunication Union (ITU): the United Nations specialised agency for information and communication technologies. (<https://www.itu.int/en/Pages/default.aspx>)*
- *The focus of the GFCE is much broader than cyber incident management or CSIRTs, but they do bring together key players from that community, including FIRST and the ITU, with representatives of governments (including cyber diplomacy), big companies and NGOs (<https://thegfce.org/>)*

A new nCSIRT can significantly increase its national and international trustworthiness by obtaining membership and accreditation from well-established organisations in the international incident response community, such as Trusted Introducer and FIRST. Obtaining such memberships and accreditations was an important goal for CSIRT-CY in [Cyprus](#). The requirements for membership and accreditation can quickly be met when policy and procedures are written down right from the start, and when they are based on existing standards.

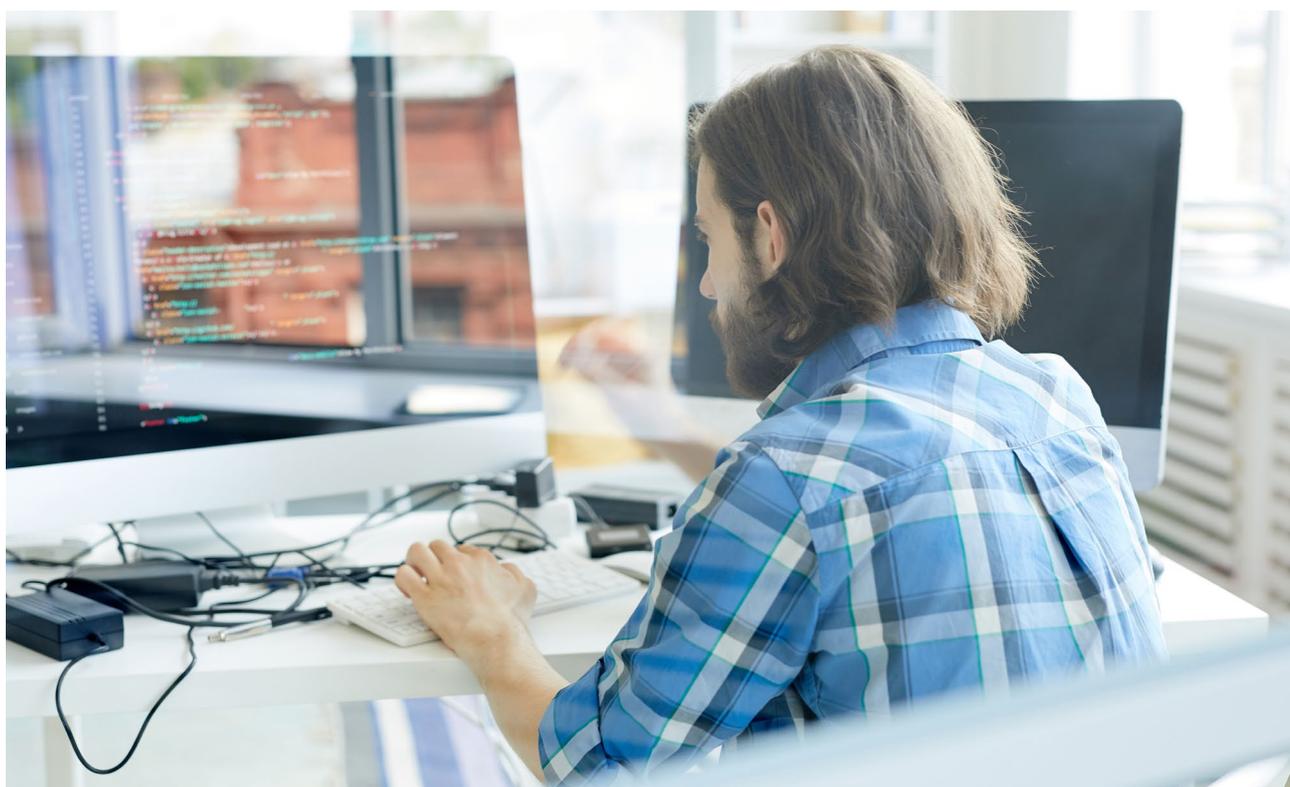
### **Engaging with peers and experts in the international CSIRT community**

Most of these international organisations have an events calendar with meetings and conferences on different topics in various locations – and increasingly, also remote, virtual events. Such events offer great opportunities to meet peers and exchange ideas. At these events, you can build lasting relationships of trust with experts and other nCSIRTs who have a strong track record within the community or who are, like you, new to the community. In general, the international CSIRT community is characterised by an inviting and open atmosphere. People are always willing to help each other, as long as you are also willing to

share your knowledge and experiences. Meeting with and talking to peers is valuable, even if they are from a different region or have opted for a set-up that is different from yours. Such interactions often lead to strong bonds between people and the trust built between people is the foundation on which trust between CSIRTs is built.

#### **Get in touch with other nCSIRT teams**

*At an early stage, it may seem logical and practical to focus on the organisational form and aspects of your nCSIRT, especially when time and budget are limited. But it pays off to look outward and engage with existing teams to learn from their experiences. Not only will this help you create a path to maturity, it is essential for building trust, which is key to international cooperation and also critical to the success of your nCSIRT. This trust will help you get access to reliable sources of information and contacts worldwide. Additionally, this exchange of information will provide your team with the necessary knowledge to build a strong business case for your nCSIRT.*



It is always valuable for both new and existing teams to learn from each other's practices, procedures and tooling when they meet during conferences, events and training. In [Cyprus](#), the CSIRT-CY team members were encouraged by their upper management to travel abroad, because all agreed that it was important for the team to participate in the culture of sharing right from the start. One of the benefits of learning from other national teams is that duplication of efforts can be avoided.

Especially for new nCSIRTs, building relationships with peers, experts and other stakeholders is invaluable. These interactions can inspire you and may help with difficult decisions about your nCSIRT while under construction. Although it takes time and effort, it is wise to have at least all your senior team members involved in the community and to also introduce the less experienced ones. This will ensure that you will not have to rely on one representative's contacts but that you are truly part of the CSIRT community. The value of the input and inspiration you will get from these

relationships will prove to be well worth the investment, because it provides you with crucial trusted relationships, reliable information sources and worldwide contacts. It will also help you make the right choices based on the lessons learned by other nCSIRTs before you. Being a member or part of international organisations may also help you strengthen the political support for your nCSIRT.

A member of the establishing team of CERT NZ in [New Zealand](#) always asks peers what the single most valuable thing is that they do as an nCSIRT. This question can be answered in many different ways and has led to a variety of different conversations. Sometimes the conversation is about something very technical, sometimes it is about a particular intervention they did, and sometimes it is about a successful institutional arrangement. In the same way, it can also be insightful to ask about initiatives that turned out to be useless or not worth the effort. Answers to both these questions can give you invaluable insights that will help you structure policies and processes.





# Gaining Political Support

An nCSIRT can only be a national CSIRT if it has the formal (government-issued) mandate to take that responsibility. This means that political support for a national CSIRT initiative is essential. This section focusses on how to obtain and maintain political support for your nCSIRT initiative right from the start.

## Gaining political support

Political support is needed to reach a decision and get the green light to establish an nCSIRT. But the need for political support does not end there. After establishment, the mandate, activities and position of the nCSIRT have to be continuously backed by formal political support, as the national responsibility of the nCSIRT has to be recognised and legitimised across the country – as well as internationally.

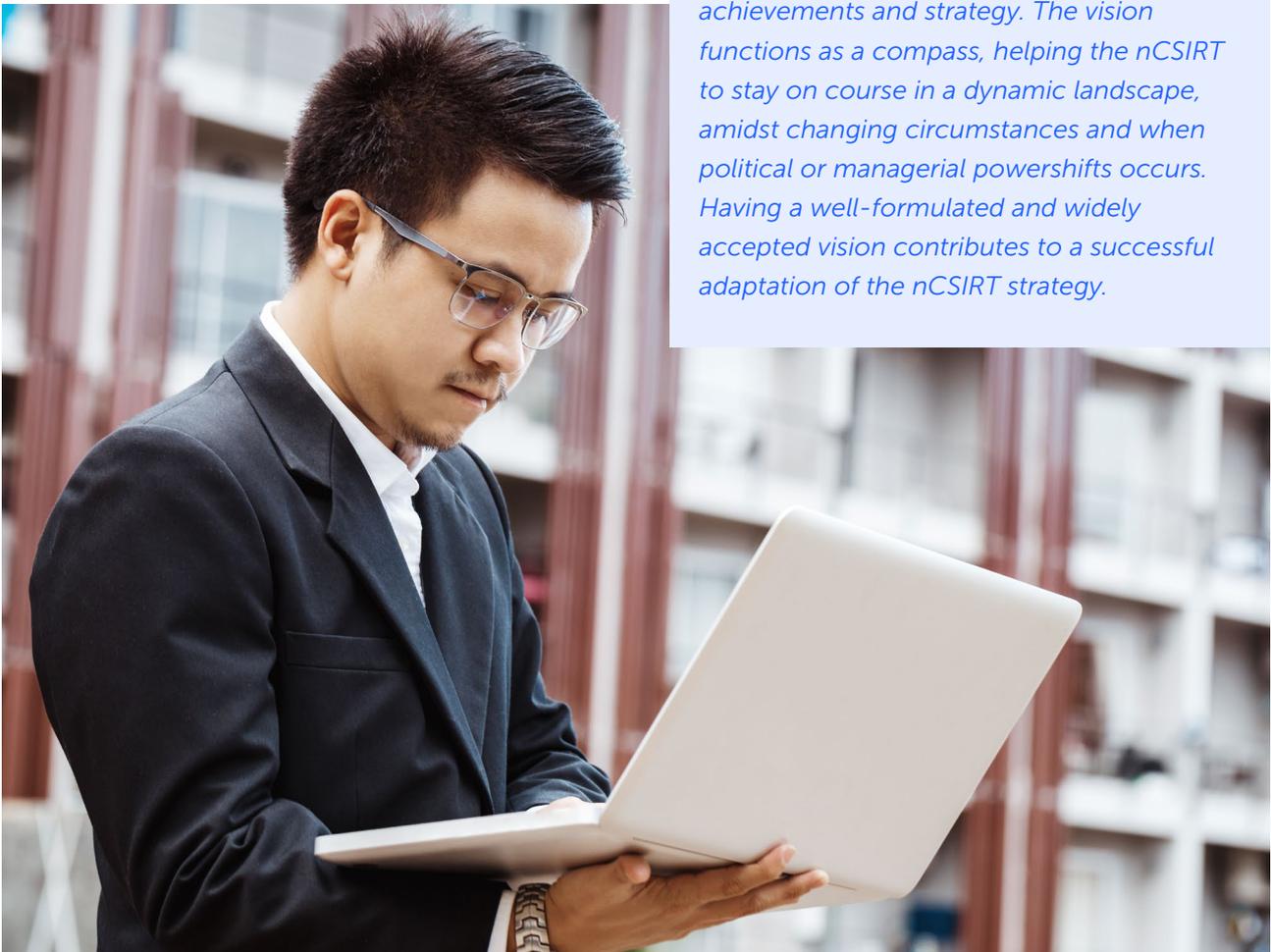
## Vision for your nCSIRT

Support for your nCSIRT strongly relies on the ability to demonstrate the added value of the nCSIRT initiative to the existing cyber capacities. Having a well-considered vision is essential to be able to communicate the nCSIRT's goals and ambitions clearly. It will help envision a path towards a realistic ideal in the future – for example, a national cyber landscape where all citizens and organisations are safe to work together and express themselves, with threats being countered swiftly and attacks mitigated in effective national and international cooperation.

A vision captures the ambition for the nCSIRT, and it outlines the direction of the team. It is the leading guide for strategic decisions. It will be the foundation for the nCSIRT's mandate. The vision also helps you build a strong business case with tangible ideas that describe the key elements of the nCSIRT, such as the added value it will bring to specific parts of the constituency; the authority and responsibility of the team; and the services it will provide.

### The benefits of having a vision

*Together with the business case, the vision will help decision-makers to weigh the costs and benefits and reach a decision about the initiative. Once the nCSIRT has been established, the vision will be the guide for evaluation and reflection on the nCSIRT's achievements and strategy. The vision functions as a compass, helping the nCSIRT to stay on course in a dynamic landscape, amidst changing circumstances and when political or managerial powershifts occurs. Having a well-formulated and widely accepted vision contributes to a successful adaptation of the nCSIRT strategy.*



So, where to start when you want to develop a strong vision? Like all other aspects in planning for an nCSIRT, this is something that should be done in a multi-stakeholder context. It is essential that the vision aligns with specific cultural and institutional aspects of your country. Make sure you understand where the most significant challenges and gaps are in your national cybersecurity and discuss with stakeholders (not only in the government but in the broader cyber ecosystem of your country) how an nCSIRT capacity can contribute to dealing with these challenges and gaps. If your country has an overall cybersecurity strategy, make sure the vision aligns with that strategy. Be realistic, but remember that the vision should focus on the long-term ambition. So, while the vision must be within the realm of reality, there is no need to be overly conservative. In other words: dare to be bold.

### **Acceptance of the national responsibility of your nCSIRT**

You will need to engage with all organisations that already contribute to or have a longstanding reputation in the cybersecurity of your country (or even cyber incident management specifically). Their acceptance of the position and national responsibility of your nCSIRT can make or break the initiative (hence, the importance of a multi-stakeholder approach).

Start a dialogue with them about the complementarity of their role and the envisioned role of your nCSIRT. If you neglect to do this, conflict or distrust will most likely occur. It makes no sense trying to fulfil a national responsibility when your constituency or other important entities do not accept your mandate. Having support from one Minister of State will not be sufficient if other parties in the government also have an interest in cybersecurity capacity building. Identifying and understanding how different interests and viewpoints intersect will help you to distinguish the nCSIRT's contribution in relation to other stakeholders. The understanding of and alignment with other entities and interests should also be reflected in the nCSIRT's mandate. Like the vision, this mandate should be widely supported.

Building trust with your constituency is critical for the success of the nCSIRT. This is all about getting to know the constituency and about having a shared understanding of the role of the nCSIRT.

In Thailand, organising on-site visits has proven to be an effective means of building trust.

As discussed in the section about community building, being internationally active offers a lot of potential benefits for an nCSIRT. Sharing knowledge, both technical and organisational, with (international) peers is essential to the success of any nCSIRT. To cooperate internationally, it is crucial to have national acceptance and endorsement of your nCSIRT in order to credibly present yourself as "the" nCSIRT for your country. Or at least being able to present yourself as the government-appointed leading team, as your country may have more teams with a national scope, for instance, a national educational research network CSIRT.

#### **Reality check**

*One of the biggest lessons learned in the past 30 years is that building trust takes time. Even when you have done a great job defining your vision, organising your mandate, and building your business case in an exemplary multi-stakeholder manner. Your nCSIRT will still need several years to build trust and gain acceptance, both nationally and internationally. Provided that you walk the talk and stay in close contact with your constituency and stakeholders.*



Although there are rare exceptions, it is generally recommended that the nCSIRT is embedded in a civilian agency. Being embedded in a civilian agency makes it easier to build relationships and exchange information with IT owners and operators. It should not be part of an intelligence, military, or law enforcement agency. The primary purpose of the nCSIRT is to protect IT assets and information – not collecting intelligence, investigating crimes, or conducting military operations. Keep in mind that the nCSIRT serves the whole country, and thus the entire government. So make sure to reconcile and account for all interests right from the start. If the nCSIRT is not embedded in a civilian agency, it will be much harder to achieve all of this.

Another good reason to embed the nCSIRT in a civilian agency is that the international cooperation between CSIRTs, including nCSIRTs, requires a great level of trust. Sometimes information is shared that cannot be directly acted upon, pending further research. An nCSIRT must be able to handle sensitive information conscientiously. If such provisions are ignored, the team will most likely be shut out of international cooperations. These are not just empty words, as this has happened to some nCSIRTs in the past – and they had a hard time gaining back trust. When an nCSIRT is embedded in a civilian agency, it is generally much easier to work this way, as law enforcement agencies are often legally obliged to act on the information they receive.

### **Institutional embedding of your nCSIRT**

It is necessary to consider the institutional arrangements of your nCSIRT thoroughly. Regardless of where the initiative may have emerged originally, identifying the most logical organisational structure and institutional embedding, given the nCSIRTs mandate, can significantly influence the success of the team; especially when it comes to gaining visibility, trust, and an effective fulfilling of the nCSIRT's role.

Having a national CSIRT helps to provide a focal point for cybersecurity issues. New nCSIRTs often have a steep hill to climb to gain visibility, respect, authority and expertise to truly move a nation toward better cybersecurity. The organisational embedding of the nCSIRT can play an important role in its ability to make a difference, as it affects the level of access to key stakeholders. In the case of CISA in the [USA](#), a change in institutional embedding has contributed to its visibility and impact.

In [New Zealand](#), like in many other countries, CERT NZ is not part of the intelligence or law enforcement community. This is important because there is a big difference in approaches between respectively the law enforcement and the cyber incident management community. For national CSIRTs, like CERT NZ, the imperative is to always share information, unless there is a good reason to keep the information to themselves. The prevailing approach in the intelligence or law enforcement community is usually the opposite; to keep information locked up, unless there is a good reason to share. National CSIRTs should always gravitate towards outward engagement.

The best institution to embed an nCSIRT in will differ from country to country. Generally speaking, the most obvious candidates are: the Ministry of Justice, the Ministry of the Interior, the Prime Minister's office, or the Ministry where the Internet is being handled (e.g. the Ministry of Economic affairs/Transport/Technology).

If the nCSIRT is embedded in a Ministry, you should consider the continuity of the team regardless of political shifts and changes in government. An nCSIRT is best situated when it can function inside some kind of agency, under the umbrella of a ministry. A distinct advantage of agencies is that they are usually leaner, which allows for faster decision-making processes. This is important for nCSIRTs as decisions often need to be made quickly and cannot wait for the outcome of a long-winded bureaucratic process.

Just make sure that you carefully consider which agency to embed the nCSIRT in, as there may be conflicts of interest that can hamper the effective operation of the nCSIRT. For instance, if the nCSIRT is part of a regulatory body or an agency that is responsible for potentially fining organisations affected by a cybersecurity incident, organisations will be less likely to report a security incident to such an nCSIRT.

**Not all nCSIRTs are government organisations. Some countries, like [Brazil](#), have made a conscious decision to establish a neutral organisation (with a government-issued mandate) that has no overriding interests in the government, national industry or elsewhere. It serves to advance Internet security and to coordinate incident response.**

Aside from the institutional embedding, the visibility and recognisability of your nCSIRT also rely on choosing the right name for the team. Whether it contains [CERT](#), [CSIRT](#), or [NCSC](#), it should be a name that is unique and easily recognisable as a Computer Security Incident Response Team with national responsibility. Confusing acronyms or other 'creative' names will only work against the team's recognition.

As the [NCSC-NL \(the Netherlands\)](#) and [CERT.br \(Brazil\)](#) stories illustrate, having a name that is confusing or not recognisable can hamper the visibility and effectivity of the nCSIRT. It is therefore wise to find a good, recognisable name as early as possible and to keep that name from that time forward. Names containing CSIRT or CERT are very recognisable. NCSC, in combination with a country's abbreviation, has also become an established naming format.

### **Gaining support for your initiative**

As mentioned, having a strong vision and a business case that clearly explains the added value and required investments makes it easier to argue the case for having an nCSIRT to decision-makers. However, you need more than that to gain support for an nCSIRT. It usually also relies on having momentum for the initiative. Momentum can emerge unexpectedly, for instance when a major incident occurs, when the need for an nCSIRT is (politically) recognised because neighbouring countries decide to start one as well, or when requested by international bodies. How and where political support and momentum can be proactively acquired, strongly depends on the cultural and institutional norms and values of your country. However, drawing from the successes of other countries across the globe, there are some valuable insights we would like to share with you.

Identify and reach out to those who can advocate for your ambition to establish an nCSIRT in your country. It can be useful to have sponsors in the government, but support can also come from other key stakeholders in your country, such as critical infrastructure operators, trade associations, technical experts at public or private organisations, or universities. With regard to universities, most countries have an educational research network, and often they are quite advanced in matters relating to cybersecurity. These educational research networks are usually government-funded and therefore a natural partner. If such parties explicitly support your cause, it can make all the difference when you engage with political decision-makers.

**Having support from local heroes or 'champions'**

who have the vision, drive and position to influence decision-making and build momentum for a national CSIRT, can speed up the process tremendously. Although times were different back in 2002, the history of the establishment of the first governmental CSIRT in [the Netherlands](#) (which later became NCSC-NL) demonstrates that with only a handful of motivated people a lot can happen in a short period of time. You just need to have the right people on board.

Momentum can also arise from a sense of urgency. Awareness campaigns and simulation exercises directed at the right (top-level) stakeholders can be very effective to create a sense of urgency among those with decision-making power.

In [Tunisia](#), politicians and decision-makers were involved in simulation exercises early on. Getting some first-hand experience with what it means to be the victim of a cyberattack, they gained a better understanding of the risks involved and the importance of building national cyber capacities.

This, in turn, created awareness and political support for the establishment of a national CSIRT.

In short, political support is an essential factor for your nCSIRT initiative. A strong vision, recognition of the national responsibility by the government and key stakeholders, generating and capitalising on momentum, and ensuring the right governmental embedding can be decisive factors in making the nCSIRT initiative a success. Political support can lead to a source of consistent funding for the nCSIRT (even though it is not the only way to get funding for the initiative, see [formulating a business case](#)). Last but not least, political support is crucial to get the right mandate and sufficient authority as an nCSIRT.



# Myths



**An nCSIRT is the national entity in charge of cybercriminal activity investigation.**



**When an incident occurs, nCSIRT employees will immediately take over IT security support for their constituents.**



**An nCSIRT is responsible for the entirety of the incident response in its constituency.**



**An nCSIRT cannot share information because everything it does is a secret.**

# FACTS



**Investigation and prosecution of cybercrimes is the responsibility of law enforcement organisations. If desired nCSIRTs can provide (technical) assistance.**



**An nCSIRT supports its constituency in times of an incident by coordinating the response, sharing information and providing services to those affected (and to the broader target audience). Though it depends on the mandate, in general, nCSIRTs will not perform the actual technical response in the IT systems of their constituency.**



**nCSIRT or no NCSIRT, every organisation (unit) is responsible for its own incident response. An nCSIRT facilitates improved incident response capabilities among its constituency through coordination and communication between partners and relevant stakeholders. Only when the escalation of an incident seems imminent does an nCSIRT have the mandate to intervene.**



**Due to the independent and coordinating role of an nCSIRT, openness and sharing are key to the way it operates. Information obtained about specific incidents can be treated confidentially, but the majority of what an nCSIRT does and learns is not a secret.**



# Formulating a Business Case

Whether you are trying to obtain support for the creation of an nCSIRT in your country or the decision has already been made and you are starting the planning stage for its establishment, it is very helpful to formulate a well-thought-out business case for the nCSIRT. A well-known format that can be used to formulate a business case is the “Business Model Canvas”<sup>6</sup>. It is a format that has been around for more than a decade and is widely used in many different industries and sectors. In this section, we introduce a version of the Business Model Canvas that is customised for setting up a national CSIRT.

## Formulating a business case

The process of formulating a business case helps to translate the vision for your nCSIRT into a concrete plan. The added value an nCSIRT can bring to your country's cybersecurity should be central to your business case. From there on, it is easier to identify other key aspects for the nCSIRT, such as the prospected constituency, required resources, and important stakeholders. A business case can help decision-makers to come to a balanced decision about the project, and it can facilitate the obtainment of endorsements from other relevant stakeholders. As part of the multi-stakeholder approach, involving different stakeholders in the process of formulating the business case is a very effective way to obtain support and build strong relationships that will continue once the nCSIRT is established.

## The Business Model Canvas for National CSIRTs

The Business Model Canvas for national CSIRTs consists of nine interrelated elements that envision how the nCSIRT will be defined: added value, constituency, communication channels, mandate, constituency, communication channels, mandate, added value, and key services.

key resources, key services, key stakeholders, institutional arrangements, and cost structure. The concise one-page format of the canvas facilitates an integrative focus, making sure that all elements are mutually coherent.

### Print the canvas

*The key strengths of The Business Model Canvas are its simple structure and intuitive format. By printing the canvas on a large surface, it is possible for groups of people to co-create the business model by sketching, adding sticky notes, or writing comments with board markers. Interacting around the canvas fosters creativity, discussion and a collaborative analysis of the relevance of each element in the business model.*

## The Business Model Canvas for National CSIRTs

<p><b>KEY STAKEHOLDERS</b> Who are our national and international stakeholders and why?</p> 	<p><b>KEY SERVICES</b> What services does the nCSIRT need to provide?</p> 	<p><b>ADDED VALUE</b> What is the added value of the nCSIRT?</p> 	<p><b>MANDATE</b> What are the mandate, authority and responsibilities of the nCSIRT?</p> 	<p><b>CONSTITUENCY</b> What is the constituency of the nCSIRT?</p> 
	<p><b>KEY RESOURCES</b> What resources are required?</p> 		<p><b>COMMUNICATION CHANNELS</b> Which communication channels are needed?</p> 	
<p><b>COST STRUCTURE</b> What is the funding scheme of the nCSIRT?</p> 		<p><b>INSTITUTIONAL ARRANGEMENTS</b> What is the institutional embedding of the nCSIRT?</p> 		

[Print version](#)

## Added value

Central to the Business Model Canvas for an nCSIRT is the description of its added value. This is where the reasons for establishing an nCSIRT should become clear. Depending on specific challenges and the cybersecurity capacities that are already available in the country, the nCSIRT fills particular gaps or needs that would otherwise be left unfilled or uncoordinated. It is important to understand the existing community and build upon the capacities that already exist. Engaging with relevant stakeholders will help you to identify the added value of the nCSIRT.

For relative latecomers to the field, it is important to realise that there are presumably already a lot of other parties that are performing incident response, information sharing or other relevant activities. As a new nCSIRT, it is critical to build upon those existing capacities, not trying to replace or work beside them. If you do, you risk undermining the value that has already been created. In [New Zealand](#), CERT NZ started from the idea that they could add value by becoming the glue that brings different people and stakeholders together.

National CSIRTs are important linking-pins in the national and international cybersecurity ecosystem. Due to their national responsibility and mandate, they play an essential role in the cybersecurity policy arena, as well as in society at large. In many cases, an nCSIRT is a facilitator that makes sure that the government and organisations in the country can respond better to incidents through support and coordination. In addition, they often play an important role in raising awareness in society about cybersecurity. Content-driven, technical incident response is generally limited to a smaller subset of the constituency. nCSIRTs do have a clear added value when severe incidents occur that affect national security or the economy. They are a vital part of the national crisis management structure.

The added value of national teams is often felt more clearly in the policy realm than in the technical realm. For national CSIRTs, it is therefore

important to focus on policy and planning for cybersecurity instead of adopting a purely technical focus on cybersecurity. Some national teams, such as CISA in the [USA](#), have learned this over time. New nCSIRTs have the opportunity to draw from these lessons right from the start.

Due to their coordinating and facilitating role, many nCSIRTs create added value by strategic collaborations for awareness building, information sharing and facilitating training to other CSIRTs in the country. Through those activities, nCSIRTs contribute to building a robust cybersecurity ecosystem, ensuring that all Internet users have a place to reach out to for incident response support.

Whether you operate in a big or small country, having a smaller nCSIRT team does not mean that the team cannot be effective. Some very successful nCSIRTs, such as CERT.br in [Brazil](#), prove that with a relatively small team, you can contribute significantly to a healthy and robust cybersecurity ecosystem in the country. Such small, highly skilled teams are essential in raising awareness and enabling other CSIRTs to improve their incident response, for instance, by training and offering triage or additional support in case of serious incidents.

## Constituency

To which target groups will the nCSIRT provide services to deliver the added value? Many nCSIRTs focus on a selected target audience ([The Netherlands](#) and [Thailand](#)) or they take a whole-of-nation approach ([Tunisia](#), [Cyprus](#) and the [USA](#)). Some countries have different nCSIRTs for different segments of Internet infrastructure users ([New Zealand](#)).

Including certain audiences in your constituency does not necessarily mean that the nCSIRT will provide all of its services to all constituents. For example, ThaiCERT in [Thailand](#) offers technical services to the government and advisory services to critical infrastructures and the general public. Services can also be offered to target audiences indirectly. [Brazil](#), for example, is simply too big of a country to be served by one team. Therefore, the approach taken by CERT.br is that it enables

and supports other CSIRTs (of large companies, of associations or sectoral CSIRTs) to provide services tailored to their specific constituency. In case of a serious incident, these teams can reach out to CERT.br for support and (international) coordination.

How do you define the constituency of your nCSIRT? You should look at the existing cyber threat and incident response landscape as well as the value that can be added for specific target audiences. Where are the most significant needs and what is feasible, taking the cost structure and resources into consideration? It is always better to start somewhere and expand later on, than try to do too much at once. An nCSIRT matures over time, which makes you more adaptable to the circumstances along the way.

### Communication channels

Which communication channels between your nCSIRT and the constituency are necessary to be able to deliver the added value? How can the constituents and other stakeholders reach your nCSIRT? Are there already existing communication channels that your nCSIRT can join or contribute to? These are the kind of questions you need to ask here.

First, you need to decide which channels (email, phone, online form, etc.) people can use to report incidents/threats or ask for your support. Consider who needs to reach you and which communication channels would work best. For instance, your constituency, and probably also other CSIRTs that you are in touch with (peer teams), should be able to reach you more easily than the rest of 'the world'. You need to make sure that you tell those who are eligible to contact you, how and when they can reach you.

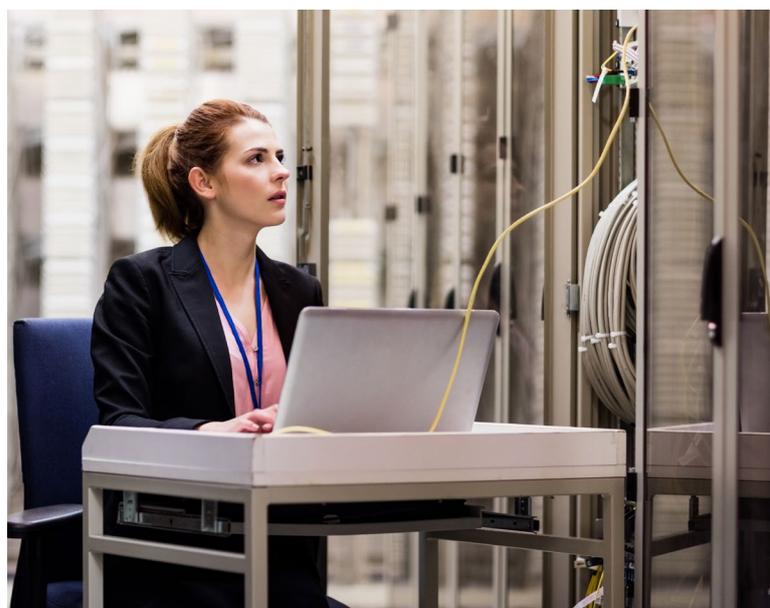
A good starting point for setting up your communication channels is the Internet standard rfc-2350<sup>7</sup>, which is a simple form that you can fill out and that will help you describe your team, who you work for (constituency), what the main services are that you offer, what your service windows are, and how you can be reached. The rfc-2350 was designed to fill out and publish on the CSIRT's

### Which communication channels should you use?

*"How you can be reached" in rfc-2350 is defined by an email address, phone number and fax. Most teams choose to be reachable by email and phone; however, this is up to you to decide. In any case, you should be reachable and tell your constituency and the world how they can reach you. You are free to add more contemporary communication channels to rfc-2350, like social media or perhaps a webform for reporting incidents. Remember that whatever channels you add here, your team should be able to respond and keep up with requests for support. Our advice is to keep it simple, especially for starting teams, as it is hard to predict how much those channels will actually be used.*

website. Preferably, it should be publicly available or at least accessible for your constituency. The best practice is to publish rfc-2350 online in your country's language(s), as well as in English, de facto the working language of the global CSIRT community.

Aside from being able to be reached, you also need to be able to reach out, especially to your constituency, but also to peer teams. And for this as well, you need to define, set up and maintain various communication channels. Make sure that you think about how to reach specific stakeholder groups. For instance, you may want to set up tailored communication channels for your constituency and your peers.



For communication with your constituency, you should consider common options, such as one or more email distribution lists, a website with advisories (and possibly also threat intel), and social media. Find out what works best for you and remember that too much communication is seldom effective, but that too little communication is even worse.

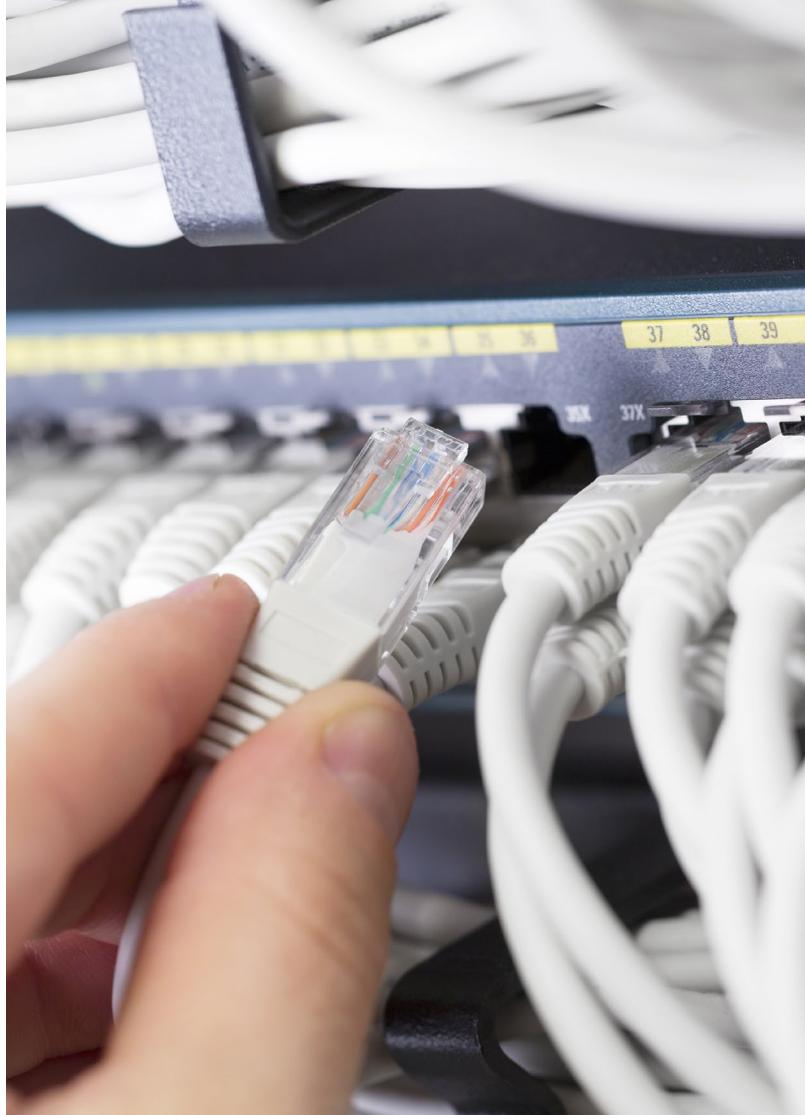
For communication with peer teams, you will generally use email, which is the worldwide standard. When you join international cooperations of CSIRTs, they will ask you to be able to send and receive PGP/GnuPG encrypted emails. In urgent cases, peer teams will reach out to you by phone, perhaps even outside of business hours. All international cooperations have provisions to avoid that emergency phone numbers become public. When handling an incident together, peer teams may also decide to exchange information using secure chat mechanisms. Most teams use a secure messenger tool based on open-source cryptography.

### **Mandate**

What is the mandate of an nCSIRT? The mandate describes the assignment the nCSIRT has received from a legitimate authority (i.e. a minister, regulator, or other government body) or derived from legislation.

[New nCSIRTs can greatly benefit from using SIM3, a generic Security Incident Management Maturity Model as a guiding framework. This framework can be used by all kinds of CSIRTs, including nCSIRTs. Although the national CSIRT in Cyprus was able to set up its nCSIRT capacity without a specific CSIRT framework or model, they stated that, in retrospect, it would have been beneficial to have known about SIM3 in an earlier stage. According to them, working with the SIM3 model feels like flying on autopilot.](#)

It is important to specify explicitly what authority the nCSIRT has towards its constituency. What is the nCSIRT allowed to do in order to accomplish its tasks? How much “power” does it have? In general, nCSIRTs play an advisory role and are the enablers and facilitators of effective cooperation



in the CSIRT landscape. This means the nCSIRT plays a crucial role, but generally does not have a lot of power. Its role is advisory, supportive and coordinating, not enforcing. It can even be risky to give an nCSIRT the authority to enforce, as this would, in many cases, discourage stakeholders from reporting to the team and work with it. In other words, too much authority can have a counterproductive effect. Therefore, even when an nCSIRT may be part of – for example the telecommunications regulator, it should not have the authority of the regulator, but instead, opt for a more cooperative role. On the other hand, the nCSIRT should not be completely powerless either. The nCSIRT must have efficient and fast options for escalation, especially within the government, towards some form of national crisis management.

[In The Netherlands, as in many other countries, the nCSIRT quickly learned that a cooperative approach to cybersecurity capacity building and cyber incident management is most effective. Of course, cultural differences have to be considered,](#)

but it is important to realise that the international Internet community is generally non-hierarchical, and cooperation is one of the core values that are upheld.

In a similar vein, you should specify explicitly what responsibility the nCSIRT has towards its constituency. Be clear what the nCSIRT is expected to do, based on its mandate and authority. In practice, a team's responsibility will be considerably bigger than its authority mandates. This comes with a warning: an nCSIRT should make sure that the scope of the responsibility and the mandated authority do not drift too far apart as trouble arises when expectations exceed the executional power of the team (and its capacity). So, make sure that when your nCSIRT's responsibility increases, its mandated authority does as well.

Defining the appropriate authority and responsibility of an nCSIRT can be rather complicated. It is about striking a balance between facilitating, coordinating and regulating specific aspects of the cybersecurity landscape. How can an nCSIRT incentivise other organisations in the country to react to or act on cyber threats and incidents? In [Thailand](#), ThaiCERT has found that stimulating government and critical infrastructures to collaborate is often much easier than stimulating collaboration in the private sector. The Thai government is currently preparing regulations to improve the incentives for private sector organisations to collaborate.

The added value of an explicit mandate is twofold: A) It helps the nCSIRT to focus its activities and resources, and B) it informs national and international stakeholders about what the nCSIRT is committed to and allowed to do. Of course, the mandate should be backed by funding and resources to make sure the nCSIRT can execute it.

### Key resources

A clear understanding of the required resources is necessary to build an nCSIRT business case. The resources should align with the services that the nCSIRT aims to provide. These include (but are not limited to) staff, facilities and tools.

### SIM3 maturity model

*The incident response community uses the SIM3 maturity model to increase their maturity overall. Mandate, authority and responsibility are important foundational aspects of this model. We advise nCSIRTs to use the [Global CSIRT Maturity Framework](#) to increase their maturity level, as it comes with recommended growth paths for each of these aspects.*

### nCSIRT Staff

The people working in the nCSIRT are paramount to its success, so recruiting the right people is essential. It can be difficult to assess how many staff members are required and what skills they need. In their paper "[What Skills Are Needed When Staffing Your CSIRT](#)", CERT/CC describes a minimum set of basic skills that each team member is expected to have. The two most critical skills are, without a doubt, technical and communication skills. Technical skills are essential to perform triage, incident analysis and coordination, and threat intelligence. Human communication skills are essential for almost all aspects of the CSIRT job, as it requires talking to people at different levels, writing readable advisories and reports, and so on.

It is essential to have team members with strong communication skills. As the [Thailand](#) story shows, it is not only about general communication skills. You should have the ability to gear the communication within your team towards different audiences such as political and technical audiences. Also, make sure to have staff members who are specialised in communicating with international stakeholders.

However, there are other aspects to consider as well. You need people to address and guide the nCSIRT's organisational development, its mission, its scope, and its influence. For awareness and training activities, additional expertise and competences are required. As such, an nCSIRT should have a mix of technical experts, stakeholder managers, and policy and planning experts. Good programme management and inspiring leadership



are needed to make it all fit logically together. The leadership should nurture an open, inviting atmosphere, with trust as a key building block. The nCSIRT's work is challenging, as the threats continuously change, and incidents can be time-critical and can touch on the gravest matters. Thus, you need to build a team of people who trust each other and are not afraid to admit making mistakes – and they will make mistakes; it is part of this challenging work. The shared belief of staff members needs to be: we learn by doing and together we stand strong.

For countries or teams with a small budget, hiring such a diverse set of people may pose a challenge. If you have a smaller team, make sure that key skills are available in different staff members to avoid single points of failure. Look for well-rounded people and also consider sharing some of the activities with external partners. This does not necessarily mean commercial hiring, as that can be expensive. Instead, explore other ways to expand capacity. For instance, by forming working groups with other stakeholders or collaborating with academic researchers who may already be working on specific issues. Hiring commercially is best suited for solving very specialised and ad hoc problems that require rapid action.

Employees working at a newly established national CSIRT often have to perform non-technical activities as well. For example, engaging with constituents, thinking about the organisational structure of the CSIRT, and travelling to meetings and events. In [Cyprus](#), CSIRT-CY consciously hired employees that do not only possess a technical degree but also have organisational and business skills. By doing so, they made sure that the team was able to perform a wide variety of tasks right from the start.

It is recommended to avoid an overly incremental approach to staffing. Aim for a relatively high number of staff members that is still realistic for the size of your country's economy. You may not always get enough budget but aim high and justify it. As a new nCSIRT, you need to prove your added value. You may face competition from within the government, and it takes time to gain a position of authority and trust – if you are understaffed, it will take much longer. A too incremental approach to building an nCSIRT is not optimal in today's cybersecurity and technology landscape.

COUNTRY	NAME nCSIRT	STAFF SIZE
Tunisia	TurnCERT	35
New Zealand	CERT NZ	35
USA	CISA	>500
Cyprus	CSIRT-CY	15
The Netherlands	NCSC-NL	>100
Brasil	CERT.br	10
Thailand	ThaiCERT	20

In general, the ideal staff size of your nCSIRT depends on the size of your country's economy, though other factors are also in play. For example, some countries want to have an nCSIRT because they have become convinced that it is a best practice. Other countries have a pressing cybercrime problem at hand or are dealing with different kinds of threats, including political ones. Always make sure to consider the economic dependency on cyber and on the Critical Information Infrastructure. Your business case should address real problems, as this will provide you with the best justification for the existence of your nCSIRT and therefore enables you to start with a reasonably sized team.

The human factor is vital for any CSIRT. This does not necessarily mean that the same approach works for all teams. A large team can have a dedicated staff for specific tasks. Smaller teams, such as CERT.br in [Brazil](#), focus on having people with a technical background and an interest in building additional skillsets to broaden the team's capabilities. Do realise that every team should start somewhere. Do not become paralysed by trying to create the perfect team all at once. Start somewhere, even if it is with a small number of people or with a limited set of services, there are many ways to grow and build the team over time.

### Facilities

The most important facilities for an nCSIRT to have are a good Internet connection, some computers and telephone equipment. Other facilities that are

generally required include an office space, desks, chairs and other office furniture. Although working remotely is becoming more common, most nCSIRTs will still need a central office-space. The specific requirements will depend on the size of the team, the types of services that will be provided, and the organisational embedding. In general, an nCSIRT will benefit from a transparent and approachable appearance because the team needs to engage intensively with stakeholders. However, keep in mind that some of the work of the team will involve confidential information. Therefore, it is crucial to prevent unauthorised access to specific resources and information.

### Tools

It can be very tempting to put a lot of effort and money into obtaining state-of-the-art incident response and threat intelligence tooling. There are a lot of advanced tools available that may seem indispensable for a professional incident response team. However, especially for starting teams, it is important to focus on the fundamentals and get them right. The fundamentals are the things that define your organisation; the mandate, constituency, responsibility and authority. It also includes the people working in your team and the main services you need to provide. Use these as a starting point and from there on envision the processes and select the right tools accordingly.

### Global CSIRT Maturity Framework

*The [Global CSIRT Maturity Framework](#) provides starting points for selecting the tools that you will need. Make sure you have at least a good incident tracking system, alerts & warnings tools, and a consolidated email system. Depending on the services that you will be providing, you can add additional tools that focus on incident prevention, detection and resolution. Also make sure that your phone, email and Internet access are resilient and that the uptime and time-to-fix service levels you agree upon with the providers of these systems align with the service level you want to provide to your constituency.*

Once your nCSIRT is up and running, you can add tools that will add value to your workflows and service levels at your discretion. Be aware that some of the most advanced and popular tools used in the CSIRT community are open-source tools developed by members of that same community. The support for these tools is very strong, and it is recommended to take this into account. If knowledge of these tools is not widely available in your team, it can be valuable to seek support from peer nCSIRTs that have experience deploying them. In general, the CSIRT community is very supporting and open to helping each other.

tunCERT in [Tunisia](#) has been a strong advocate of open-source tooling from the beginning, and they are still involved in several research and development programmes to stimulate the availability of such tools.

### Key services

Every nCSIRT needs to define the services it will offer to its constituents. The selection of services should align with the nCSIRT's mandate and responsibilities. Keep in mind that you should not try to offer too many services at once. Start with the most relevant services and expand from there. Ideally, the initial selection of services should be based on a thorough assessment (together with stakeholders) of what will yield the most added value. Be aware that the ecosystem in which an nCSIRT operates will evolve. So, it is recommended to periodically reassess the needs and gaps (together with stakeholders) and review and improve the service portfolio accordingly.



It is essential to thoroughly consider the services you want to offer to your constituency. Choose services based on an assessment of what is relevant and needed, instead of replicating what other teams are doing. If you are unable to offer added value with a specific service, it is not worth investing your time or resources in it, especially if there are other ways to create that value (outsourcing, incentivising other teams to provide that service, etc.). When in doubt, do not create a new service, but stick to what you have and grow from there. CERT.br in [Brazil](#) has made very conscious decisions about the services it provides to its constituents.

A good way to start defining the services you should offer is to engage with the constituency and gain an understanding of the most urgent needs and biggest security gaps. This will not only help you to identify the added value of the nCSIRT but also provide detailed information about how (i.e. through what specific services) this value can best be created. If the nCSIRT is expected to give support to a particular target audience, how this support is offered and organised can take many different forms. By engaging with your audience, you can determine the best fit for your nCSIRT.

Getting to know your constituency and their needs is essential to offer the right services and organise your workflows. In [New Zealand](#), the establishing team of CERT NZ put a lot of effort into engaging with its audiences to learn about their needs. This proved to be invaluable information to set up its services and manage the requests from their (very large) constituency.

A structured overview of incident response services is provided in the [FIRST CSIRT Services Framework](#). This framework has been developed with the input of a large group of experts and is based on extensive experience. The structure offers a good starting point for CSIRTs to select, expand or improve their service portfolio.

For CSIRT-CY in [Cyprus](#), the [FIRST CSIRT Services Framework](#) was a relevant resource to help decide on what services to offer. For people who are new to this field, the document can seem a bit overwhelming. What worked for CSIRT-CY was to visually map its incident handling procedures and link them to the relevant services from the framework.

## Key stakeholders

Follow a [multi-stakeholder approach](#) for building your business case. You will most likely already have a general idea of who the relevant stakeholders are both in your country and internationally. For the business case, it is essential to identify the most important stakeholders and make explicit what the relationship is that you have – or should have – with these stakeholders. Key stakeholders are those public and private partners and peers in your country and abroad that are required to fulfil your mandate and responsibilities. Who the specific stakeholders are varies between nCSIRTs, but we can give you some ideas of where to look. Within your country, look at (big) telecom operators, Internet Service Providers and Internet exchanges. Look at critical infrastructure providers, but also at universities, research institutions, and academic hospitals. Look inside the government, and make sure to include law and policymakers in the cyber area. Also look at law enforcement, the intelligence community, and the military. Outside your country, look at nCSIRTs of other nations, and team up with regional and global CSIRT cooperations, like FIRST.

Regardless of who is included at this moment in time, the list of key stakeholders should be dynamic and inviting, and not a closed club. This is important because the nCSIRT has to be representative of the country, and the set of stakeholders will change over time. Also, you want people to come to you; you do not want to shut them out.

## Institutional arrangements

Make sure to carefully consider the institutional embedding of your nCSIRT as this is closely related to the way different cybersecurity interests intersect in the political landscape. The nCSIRT should be recognisable and visible, and all stakeholders should acknowledge its legitimacy.

This is why institutional embedding is a critical aspect for the business case and is also important for [gaining political support](#) for the nCSIRT. The nCSIRT is often part of a government organisation or authority but can also be an independent (not-for-profit) organisation or part of a national network information centre or domain registrar.

## Cost structure

The main costs for your nCSIRT are your staff, facilities and tools. Acquiring funding for an nCSIRT is often difficult. Yet, the alternative is to have no nCSIRT and not be able to effectively respond to threats, incidents and attacks on a national scale. Without an nCSIRT, there will be little coordination, and the response will lack in quality, speed and consistency. Subsequently, the economy will suffer, even political stability may suffer. Thus, there really is no viable alternative.

A concerted approach towards safeguarding cyberspace is of vital importance. In this day and age, you cannot do without an nCSIRT just as you cannot do without the police, the army or an intelligence agency. And as the world is increasingly dependent on digital infrastructure and 'cyber' services, the necessity for an nCSIRT type of approach will only increase. Thus, not investing in an nCSIRT will cost you more than you might save. By building a strong business case, you can both gain (political) support for the nCSIRT and convince stakeholders that investing in an nCSIRT is of vital importance.



In many countries, most of the nCSIRT's costs are covered by government funding. It only seems natural that a service that benefits society at large is funded by taxes. There are also other ways to obtain funding, for instance, through sponsorships, grants or by reinvesting revenues from the public Internet infrastructure and services (such as domain registrations).

It may also seem alluring to charge for services offered to the constituents, but generally, this is not a recommended strategy. In times of economic downfall, constituents may cut costs and stop buying your nCSIRT's services and, by doing so, potentially harm the nation's cybersecurity. It is important to remember that the nCSIRT – constituent relationship is a two-way street, and neither party is free from obligations. It is not a commercial engagement but an important initiative to advance cybersecurity and resilience.

There are different business models to organise funding for an nCSIRT. Most nCSIRTs will predominantly be government-funded, which makes sense because it is a national capacity. But funding opportunities can also be tied to Internet services, like in [Brazil](#) where the revenues of domain registration etc. are reinvested in the Brazilian Internet infrastructure and services, including CERT.br.

### Coherence between elements

All of the elements in the Business Model Canvas for National CSIRTs are interrelated (Figure 2). Together they describe what is needed to create the desired added value for the prospective constituents. For your convenience, [a printable format of the Business Model Canvas for National CSIRTs is provided on the next page.](#)

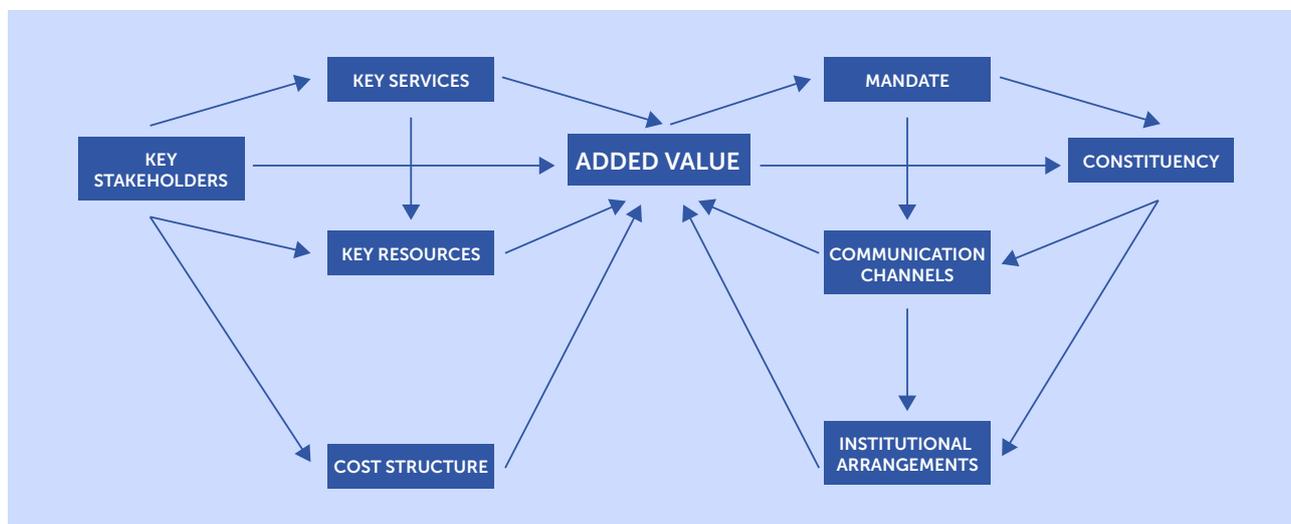


Figure 2 - Visualisation of the connection between the elements in the Business Model Canvas<sup>8</sup>.

<sup>6</sup> Osterwalder, Alexander; Pigneur, Yves; Clark, Tim (2010). *Business Model Generation: A Handbook For Visionaries, Game Changers, and Challengers*. Strategyzer series. Hoboken, NJ: John Wiley & Sons. ISBN 9780470876411

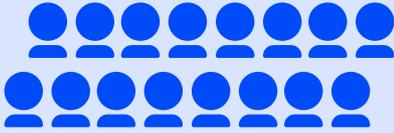
<sup>7</sup> <https://tools.ietf.org/html/rfc2350>

<sup>8</sup> Based on a similar visualization by the creator of the original Business Model Canvas retrieved from <https://web.archive.org/web/20080906034734/http://business-model-design.blogspot.com/2008/07/what-is-business-model.html>

# The Business Model Canvas for National CSIRTs

<p><b>KEY STAKEHOLDERS</b> Who are our national and international stakeholders and why?</p> 	<p><b>KEY SERVICES</b> What services does the nCSIRT need to provide?</p> 	<p><b>ADDED VALUE</b> What is the added value of the nCSIRT?</p> 	<p><b>MANDATE</b> What are the mandate, authority and responsibilities of the nCSIRT?</p> 	<p><b>CONSTITUENCY</b> What is the constituency of the nCSIRT?</p> 
<p><b>KEY RESOURCES</b> What resources are required?</p> 	<p><b>COST STRUCTURE</b> What is the funding scheme of the nCSIRT?</p> 		<p><b>COMMUNICATION CHANNELS</b> Which communication channels are needed?</p> 	<p><b>INSTITUTIONAL ARRANGEMENTS</b> What is the institutional embedding of the nCSIRT?</p> 

# Myths



**An nCSIRT requires a large number of staff members.**

# FACTS



**In most cases, to start an nCSIRT, just a handful of staff members will suffice. It is more important to start the process of bringing people and organisations together to further security than it is to strive for perfection. Start small and grow.**



**An nCSIRT requires advanced technical skills and equipment.**



**Depending on the services and tasks, an nCSIRT may function with basic equipment and skills. Advanced technical skills or equipment do not have the highest priority when starting an nCSIRT.**



**An nCSIRT requires an extensive team of highly skilled technical professionals.**



**The human factor is crucial for nCSIRTs. In general, it is better to have a small dedicated team with members who have in-depth knowledge and specific skills. But even more so, they need to be able to familiarise themselves quickly with new situations to understand what is necessary for mitigation and response.**



**An nCSIRT provides services to everyone in the country.**



**An nCSIRT provides services to a specific constituency (for instance to the government or critical infrastructures), especially at the start. However, the group of target audiences may expand over time. The exact set of target audiences depends on your country's situation and the mandate of the nCSIRT.**



# Wisdom from the field

When setting up your own nCSIRT, it is worth the effort to get inspired by and learn from other nCSIRTs who have preceded you. This can be particularly helpful in the decision-making and planning stages of setting up your nCSIRT. That is why we have collected a series of stories from nCSIRTs across the globe. Each story focusses on the lessons learned during the formation of the team and from present-day operational experience.

Each story is set in a particular context (which may be very different from your own). Nevertheless, we believe that the key insights of these stories will help you make informed decisions on how to set up your own nCSIRT.

[Tunisia](#)

[New Zealand](#)

[United States of America](#)

[Cyprus](#)

[The Netherlands](#)

[Brazil](#)

[Thailand](#)



## Tunisia

<b>Name of nCSIRT</b>	tunCERT (previously CERT-TCC)
<b>Year of establishment</b>	2004
<b>Constituency</b>	Whole-of-nation
<b>Organisational embedding</b>	Part of the National Agency for Computer Security under the Ministry of Communication Technologies
<b>Current size (2020)</b>	35 employees

tunCERT is the national CSIRT for Tunisia. The development of a national CSIRT in Tunisia dates back to the beginning of the 21st century. The worries about the possibly devastating effects of the Y2K bug created an initial level of awareness in the government about the importance of ICT (Information and communications technology ) security. As a result, a small task force was formed to work on a strategy and national plan for ICT security. The recommendations of the taskforce were confirmed by the council of ministers and eventually resulted in the promulgation of an original ICT security law in 2004. Part of the law was the establishment of the National Agency for Computer Security (NACS) under the Ministry of Communication Technologies. The agency was tasked with the implementation of the ICT security national plan and strategy. In 2004, the national CSIRT was officially launched (CERT-TCC, which in 2009 became tunCERT). In 2007, the team became a member of FIRST.

Tunisia was the first country in Africa to establish a national CSIRT, and it has since then played an important role in Africa, helping other countries in the region. Tunisia also played an important role in the launch of AfricaCERT, as a regional collaboration forum for African CSIRTs. The value of regional collaboration between national teams is that there is already a level of understanding of the local environment and culture. The lessons from a peer team in the same region are very valuable for starting teams and for assisting them as they grow.

In the years leading up to the establishment of the national CSIRT, a lot of work was done to convince decision-makers from the government and from NGOs about the importance of cybersecurity. A very effective strategy has been to provide awareness training to decision-makers, NGOs headers and

some politicians. This included involving them in attack simulation exercises. It does not have to be a very technical simulation, but it helps to make the reality of risks explicit and tangible for them, with a presentation of the financial and moral impacts of some past big attacks.

From the start, the Tunisian national CSIRT had a strong focus on building awareness about cybersecurity at all levels of society and even beyond. Their awareness campaigns included participation in regional exhibitions and events, development of a variety of materials, cartoons and games for children, radio broadcasts and other news media coverage. The team has a dedicated staff member for press relations.

This strong focus on awareness building also translated into collaboration with academic institutions. Since 2004, several Master programmes in ICT security have been launched throughout the country. What makes this collaboration unique is that the master’s degree includes the opportunity to obtain a NACS Certification, giving the holder of the degree the opportunity to become a certified independent security auditor. The ICT Security Law in Tunisia dictates an obligation for all public and (sensitive) private companies to perform annual security risk assessment audits. As a result, there is currently more ICT security expertise available in the country, there are more jobs in the field, and it contributes to the awareness among public and private organisations.

Especially in smaller or developing countries, there is often a lack of funding and a lack of skills or expertise. The collaboration with educational institutes in Tunisia has had a very positive effect on the availability of professional expertise. It has attracted students and private companies to the

field. tunCERT has also been a strong advocate of open-source tooling. If there is a lack of funding, offering open-source tools can get an organisation going until they have the budget to buy a commercial tool. At the start, it was not only about funding but also about a lack of available private solutions because the IT security industry was still developing. tunCERT has been involved in many research and development programmes to launch R&D activities in the field, based on open-source tools.

For the team itself, it has been very important to start small (3 or 4 employees), gain experience, and build expertise and skills as a team. From this nucleus, they have been able to perform a gradual and efficient growth into a team of now 35 skilled people covering almost all reactive and proactive services of a CSIRT.

The National Agency for Computer Security (which hosts tunCERT) is an agency under the Ministry of Communication Technology. Although there was some debate prior to establishment, it is seen as an important and effective choice to host the agency in a Ministry that is not primarily concerned with national security, defence or intelligence. It allows the agency to be open to everybody and focus on awareness building, providing technical advice and open collaboration based on trust and information sharing, while able to offer punctual and efficient technical assistance for operational people from national security, when needed, and without being involved in confidential constraining operational matters. The ICT security Law in Tunisia obligates public and private companies to inform the National Agency for Computer Security about big incidents. This is very important to be able to offer incident response guidance and be informed in time about incidents that can affect other information systems. It does require a level of trust, and this is also dealt

with in the Law. Members of the National Agency for Computer Security (including tunCERT) as well as certified auditors are obliged to protect the confidentiality of any information shared by the users. They are not allowed, by law, to share information with anybody, not even with their Minister or other authorities.



## New Zealand

<b>Name of nCSIRT</b>	CERT NZ
<b>Year of establishment</b>	2017
<b>Constituency</b>	Entire nation, with emphasis on the general public and small and medium businesses.
<b>Organisational embedding</b>	Ministry of Business Innovation & Employment
<b>Current size (2020)</b>	35 employees

In 2016, a policy group in New Zealand presented to the Minister for Communications (within the Ministry of Business Innovation and Employment) an idea to establish a new national CSIRT, complementary to the existing National Cyber Security Center (NCSC). Where the NCSC focuses primarily on government, critical infrastructure and large businesses, the new team would serve the needs of everybody else in New Zealand (the general public, small and medium businesses, etc.). The idea was accepted, and 9 months later, in April 2017, CERT NZ was launched. With the initiative, they could close a massive gap in the cybersecurity capability of New Zealand, where there was a very strong, world-class industry of IT security companies, particularly in Wellington, but there was no national CSIRT for the general public and most businesses.

At the start, CERT NZ had only 16 employees, with only five employees working as the incident response team. With 5 million inhabitants in New Zealand, this meant 5 million possible customers, so they had to get creative and approach things differently.

In the first place, they put a lot of effort into understanding what their constituency needed. The team had to take-off their technological hats and engage with their audiences to move beyond their assumptions and listen to what people actually need. They sat down with people, observing how they work on their computers and how they deal with problems. From these sessions, they learned that people are pretty good in helping themselves deal with cybersecurity issues once they know what the problem they are having is called. This important insight formed the basis for the reporting tool that is currently offered on CERT NZ's website. The tool guides the user through some simple questions to identify what the problem is. From there, it is much

easier to provide the right assistance or refer them to the right documents.

Even though the pre-triage, as part of the reporting tool helped to manage the many requests from individuals, 5 million customers was still a lot to deal with. CERT NZ soon realised they needed to work with other stakeholders to amplify the support they can provide. A good example of this strategy is their collaboration with banks. Banks have a lot of customers who experience cybersecurity issues with trojans or phishing attempts. In talking with the banks about how CERT NZ could help them, they found out that it can take 40 minutes for a bank to troubleshoot when a customer calls. So the support CERT NZ offered to the banks was to initially send the callers through to their reporting tool for the pre-triage and then CERT NZ could refer them back to the bank with a clearer idea on the problem, significantly shortening the time of the bank to provide support to their customers. This saved the banks a lot of money and gave CERT NZ a lot of credibility because they were solving a real problem. This also meant that a trusted relationship had been established between CERT NZ and the banks. They now also collaborate in awareness campaigns, where the banks distribute brochures about cybersecurity practices developed by CERT NZ among their customers and they show information from CERT NZ on ATM screens.

This way of working emerged initially from the constraints they had, but they soon realised this is a very effective strategy, which is now at the core of their approach.

When it comes to the supporting materials that CERT NZ creates, they make materials for different audiences, with different mindsets. Addressing, for instance, people who are not sure what they

---

need, or people who do not really care about cybersecurity because they do not have time and they just want a quick answer for their problem. For most materials, they make a technical and a non-technical version.

For small businesses, CERT NZ developed a series of guidelines that describe what is important and helps them get started. It makes their lives easier because it provides them with information about what they need from their service providers. The guidelines should always be easy to follow and should not take longer than 20 minutes to go through. Simply because their audiences do not have time to spend hours going through guidelines to find solutions. It has to be quick and easy.

In the relatively short time since their establishment, CERT NZ has built a very good trust base with their constituency. There are so many incidents that people cannot report officially, but they trust CERT NZ enough to pick up the phone and tell them about it off the record. This means that CERT NZ has considerably more valuable information even though they cannot share it officially.

CERT NZ is a branded business unit of the Ministry of Business Innovation and Employment. This means that they are not a part of the intelligence community and not related to Police or Law Enforcement. There have been discussions about whether or not they should move to Law Enforcement or Intelligence Services, but there was such an extraordinary backlash from the community that it did not happen. There was very strong and clear feedback from the community that they did not want CERT NZ to be part of the intelligence community. Their independent and unclassified position allows them to have better

engagement with their constituency.

The NCSC NZ is part of The Government Communications Security Bureau (GCSB). CERT NZ and NCSC NZ work together a lot at the operational level, they have regular meetings. CERT NZ has access to NCSC briefings, they have regular phone contact and reach out to each other if they encounter something that is relevant, they exchange cases.

During the establishing stage of CERT NZ, the team found that engaging with international peers was extremely valuable. Not only did they participate in regional networks such as APCERT and received valuable assistance from neighbouring country Australia, but they also had the opportunity to interact with nCSIRTs from other continents through participation in conferences. For instance, they interacted with a lot of other smaller European nCSIRTs, which proved to be a valuable addition to the interactions with larger nCSIRTs. It is always useful to share lessons about successes as well as failures.



## United States of America<sup>9</sup>

<b>Name of nCSIRT</b>	CISA (previously US-CERT)
<b>Year of establishment</b>	2003
<b>Constituency</b>	United States of America
<b>Organisational embedding</b>	Cybersecurity & Infrastructure Security Agency, Department of Homeland Security
<b>Current size (2020)</b>	500+

Beginning in 2003, the functions of a national CSIRT of the US were performed by US-CERT. Later, US-CERT became a branch of the National Cybersecurity and Communications Integration Center, which was also reorganised during the establishment of the Cybersecurity & Infrastructure Security Agency (CISA), under the Department of Homeland Security (DHS) in 2018. The US-CERT term is still used as a site for the distribution of cybersecurity alerts, information and other materials. Prior to establishing US-CERT in 2003, some nCERT functions, especially the provision of technical expertise in cybersecurity and incident response in government, were provided by CERT Coordination Center (CERT/CC) at the Software Engineering Institute which was established in 1988. CERT/CC supported US-CERT with these capabilities at its founding and continues to be a strong partner with DHS in cybersecurity.

The Homeland Security Act of 2002 gave DHS the homeland cybersecurity mission. This was facilitated by the advocacy for the mission at the National Security Council level. The mission of countering terrorism after 9/11 was a tsunami wave that carried missions like cybersecurity into existence in the government, when previously little attention had been paid in the government to this need. The success and competence of CERT/CC provided a model from which policymakers could envision the value of an nCSIRT. This has contributed significantly to the political support for the establishment of a governmental national CERT - US-CERT. Additionally, a growing awareness of the importance of technology to the operations of government and the health of the US economy spurred the need for government to establish a presence focused on cybersecurity. A growing increase in cybercrime also contributed to the government's incentive to increase its cybersecurity efforts.

The advice for new nCSIRT initiatives would be to leverage existing CSIRTs and their capabilities and best practices. Also, learn from other countries. Familiarise yourself with how they work, what roles and functions they perform, how they evolve and have conversations about this. Bringing those best practices back to your decision-makers can help to gain political support as it highlights the evidence-based added value of nCSIRTs. DHS formed the National Cyber Security Division (NCSA) to, among other things, establish US-CERT. Some of the other functions of the NCSA included public/private partnerships, critical infrastructure protection, and awareness-raising. US-CERT's initial focus was on protecting the Federal government.

From 2002 to 2006, NCSA/US-CERT existed under the Office of Infrastructure Protection, which was primarily focused on protecting physical assets and the counter-terrorism mission. In 2006, after increasing awareness of the importance of cybersecurity, a separate Office of Cybersecurity and Communications was created. This represented a significant increase in the visibility of cybersecurity in the DHS mission. And has helped US-CERT to establish deeper relationships with key stakeholders. As of today, the functions of US-CERT and ICS-CERT have been combined in CISA.

Initially, US-CERT was focused on technical issues, but gradually asserted more influence in the policy realm as a source of subject matter expertise in cybersecurity. This influence became possible as various nCSIRT functions became increasingly visible and important to higher-level departmental leadership, providing access to policy decision-makers and the US policymaking apparatus. In becoming more influential in policy as well as technical matters, US-CERT's successor agency CISA has increased its impact in building cyber capacity.

For new national CSIRTs, there should be a balance between technical, policy, planning and programme management efforts. As such, it is recommended to focus on policy and planning for cybersecurity right from the start and not get too focused on technical expertise. nCSIRT technical expertise should inform policy development, and policy should drive the development of technical expertise and capabilities. This also means that it is important to have leadership with the necessary experience and connections to engage with different audiences (public sector, government, private sector, technical community, etc.) and the right person is often not easy to find.

In the US, there are several research institutions that have contractual relationships with the government to provide technical expertise and analytical capability for the government in a long-term sustainable way. These institutions (such as CERT/CC) have a longstanding and trusted relationship with the federal government, including with CISA. In the past, this led to some confusion about who the US national CSIRT was, but nowadays, these strong ties between the national CSIRT and research institutions are regarded as a best practice and something to strive for in other countries.



## Cyprus

<b>Name of nCSIRT</b>	National Computer Security Incident Response Team of Cyprus (CSIRT-CY)
<b>Year of establishment</b>	2017
<b>Constituency</b>	Whole-of-nation (Government, Private and Public sectors)
<b>Organisational embedding</b>	Part of the National Agency for Computer Security under the Office of the Commissioner of Electronic Communications and Postal Regulation
<b>Current size (2020)</b>	15

---

CSIRT-CY falls under the auspices of the Deputy Ministry of research innovation and digital policy. It is hosted under the Commissioner of Electronic Communications. There is a formal working relationship with the security services and law enforcement agencies.

The vision of CSIRT-CY is: "National CSIRT-CY envisions the increase of the security posture of The Republic of Cyprus by enhancing cyber protection of its National Critical Information Infrastructures (CII), banks and ISPs. National CSIRT-CY shall coordinate and assist CII owners/administrators, banks and ISPs to ensure the existence of (at least) a minimum level of security, by implementing proactive and reactive security services to reduce the risks of network information and cybersecurity incidents, as well as respond to such incidents as and when they occur".

The Cyprus government sought to establish a capacity which allowed them to improve the protection and security of their CII. Incidents were occurring and needed to be mitigated. The nCSIRT was set up in 2017 with the idea to better fight these incidents that were going on.

The European NIS Directive spurred cybersecurity efforts on Cyprus. A competent regulatory authority was appointed inside the Ministry of Research Innovation and Digital Policy, and additionally a national cybersecurity point of contact (CSIRT-CY). A roadmap for CSIRT-CY was established and followed as a result of input by the ITU, a commercial contractor, and the team was originally run in the context of an EU Connecting European Facility (CEF) project. When the CEF project had finished, the regulatory authority continued the efforts and provided further funding.

The funding scheme changed over time. First, the team was set up with the support of a temporary grant from the earlier mentioned CEF grant and team members were first hired as subcontractors. Later, the government recognised the added value and is now in the process of securing national government funding through new legislation. In total, the transition from a project to law took about three years. It was stated that help from the government is needed and is helpful for a new nCSIRT.

In 2018-2019, the team members focused on drafting up policy and nCSIRT procedures. This was done in order to have a good foundation and structure at the beginning. The policy and procedures that were written up in the roadmap were inspired and updated along the lines of ISO/IEC 27000-series and Information Technology Infrastructure Library (ITIL) norms. Later on, they adapted their policies and procedures following the SIM3 model. SIM3 proved to be a highly valuable asset for further mature CSIRT-CY. They label the SIM3 model as a really helpful tool for beginning teams because it provides a structured overview of important elements a beginning CSIRT should think about, but also has all it takes inside to further mature to advanced levels.

FIRST membership and Trusted Introducer accreditation were quickly obtained thereafter. The accreditation and membership have been important for the team in order to gain trust with their peers and constituency. External support was provided by the ITU and a consultancy company in the field of cybersecurity capacity building. They informed them about relevant sources and important conferences and meetings. CSIRT-CY's management stimulated the team to go to national and international meetings and gatherings from the beginning. In this way, the team members

were able to quickly familiarise themselves with the forums and gain an understanding of the sorts of information that is available.

CSIRT-CY joined the EU CSIRTs Network, and by doing so, they have been able to gain relevant information from other European nCSIRTs, for example, information about software tools used. They were often inspired by the ideas, information or tooling other teams told them about. This helped them to speed up their maturity and posture in the beginning.

Other CSIRTs performed SIM3 peer reviews for CSIRT-CY. In preparation for these, CSIRT-CY mapped all SIM3 elements onto the existing internal documents and procedures. This visualised the relationship between what they on paper with SIM3. The SIM3 model was also used to declutter their policy documents. The SIM3 maturity scores showed that not all elements in their policy had to be written down as such.

The FIRST CSIRT Services Framework was a relevant resource during the early stages when the team was thinking about which services to establish, although the document can be a bit overwhelming for an unexperienced analyst. What helped CSIRT-CY is that they visually mapped out their incident handling procedure and then related the FIRST CSIRT Services on them.

Early on, the team already hosted some technical and cybersecurity awareness events on Cyprus, such as technical training, malware and forensic analysis and cyber drills. They also hosted one of the TF-CSIRT events on Cyprus, which attracted many peers from around Europe. These events helped to gain trust and recognition from their constituency. Furthermore, they also invite constituents for training in their office. This helps to get to know each other whilst improving security awareness. This helped to establish a good relationship with the constituency because they realised that CSIRT-CY could offer relevant and interesting knowledge. CERT-CY realised that organising such events is a lot of work for them as a new team. However, the benefits on the short and long-term were significant. Their constituency and other stakeholders were

made aware of the nCSIRT's role, existence and expertise.

CSIRT-CY stated that they were equipped with the right people from the start. Overall, the staff had technical degrees and backgrounds, but also theoretical, analytical and policy skills. The management hired people with both skill sets because it was found that one can learn techniques, but it is much harder to learn interpersonal and communication skills. Those skills were found to be very important for people working at a national CSIRT because a lot of events, outwards communication, community building had to take place in the beginning. The only way to make sure that people have such skills is to pay attention to it in the hiring procedure.

A recent development in Cyprus is the development of an academic CSIRT. CSIRT-CY helps and empowers them by, for example, stating they could use SIM3 parameters guide for guidance. The expertise from CERT-CY is leveraged to provide capacity building and support to further enhance the cybersecurity ecosystem on Cyprus.



## The Netherlands

<b>Name of nCSIRT</b>	NCSC-NL(formerlyGOVCERT-NL,originallyCERT-RO)
<b>Year of establishment</b>	2002
<b>Constituency</b>	Government and critical infrastructure
<b>Organisational embedding</b>	Ministry of Justice and Security
<b>Current size (2020)</b>	100+

The Internet in Europe was kickstarted in November 1989 and was at first almost exclusively taking place as research activity between universities. Around 1995, commercial companies started joining, as well as citizens. Soon after, governments got interested.

CSIRTs developed in a similar pace. Around 2000 the first governmental CSIRTs were formed – national teams came only later. In The Netherlands, in 2001, the Dutch Ministry of the Interior had available two independent reports that both advised starting a government team. But there was no political incentive yet to do so, nor big scale incidents that would create momentum. A successful CERT-of-last-resort already existed for the country, namely CERT-NL, the CSIRT for the academic & research community, the 2nd oldest CSIRT in Europe, founded in 1992<sup>10</sup>.

Then, towards the end of 2001, Roger van Boxtel (at that time the Minister of the Interior ad interim) attended an international conference where one of the topics was the security of the growing Internet and the role of governments therein. When Van Boxtel returned home, he immediately started the formation of a Dutch government CSIRT. He put considerable pressure on that process, which worked so well that only a mere six months later, on the 8th of May 2002, CERT-RO was formally established. It was still a fairly small project team of around five people, but they had a pretty successful take-off. Only about a month after establishment, CERT-RO became an Accredited member of the European regional cooperation TF-CSIRT, and a member of FIRST by the end of the year.

The fact that the establishment of CERT-RO took only six months and became a member of two essential cooperations (TF-CSIRT and FIRST) within the next six or seven months was a major accomplishment. What is more, this

accomplishment had been achieved with only a handful of people – which makes one wonder how this was possible and how it can serve as an example. It may be argued that this success, to a large extent, was achieved by the involvement of three “champions” – three individuals who were the driving forces behind the rapid development and success. These were three people who shared a vision and maintained that vision, and who were able to bring others on board based on their vision, persistency and drive.

The first driving force was a high-level political champion: the already mentioned Minister of the Interior. He had the vision to recognise that a governmental CSIRT was needed, and he had the courage and tact to make this happen inside his Ministry, whilst at the same time also engaging with his fellow Ministers and the Prime Minister. In 2003, when he had already resigned as Minister, he chaired the first international conference organised by CERT-RO, which took place in Amsterdam. He had the vision and stamina to act as a high-level champion for CERT-RO.

The second driving force was the project leader champion: the Ministry appointed a project leader to kickstart CERT-RO, who had an extraordinary drive to reach her targets. She was not an expert on the content nor tried to be, but she made sure that the team could do their work, that the communications took place at all levels, and was together with the 3rd champion the driving force that introduced CERT-RO to all sectors of the government and ensured that working relationships took off.

The third driving force was the CSIRT-expert champion: almost immediately after the project leader was appointed, she enlisted a renowned Dutch expert in the CSIRT area, with a global network. He

made sure that the CSIRT developed a solid CSIRT services portfolio, that the right people were hired, and that CERT-RO very quickly became a member of the international cooperations. He also took care of the crucial trust-building needed for that.

This was the Dutch approach, and it happened back in 2002, so it will be difficult to carbon-copy this approach. However, in general, the formation of an nCSIRT will be faster and more successful if you can enlist at least two champions – one on the policy level (inside the government) who makes sure that the right policies are set, and important governmental stakeholders are convinced – and the other as a champion for the building of the CSIRT, who steers the team in the right direction, who makes sure that the team defines their services based on a solid needs assessment, who oversees enlisting and training of the necessary human resources and who generally keeps an eye on the development of the team.

The Dutch story also offers some other lessons learned. The team was originally named CERT-RO, which was based on specific Dutch terminology. It turned out that this name was not so well chosen, as RO is internationally known as the 2-letter acronym for the country of Romania. To avoid confusion, the name was changed into GOVCERT-NL in 2007. And even though the team was already acknowledged as the Dutch national team, in 2011, they changed again, this time to NCSC-NL. This name change was related to a change in the constituency (from government bodies to a national reach) which caused the name to be no longer descriptive. At the same time, the team was relocated from the Ministry of the Interior to the newly formed Ministry of Justice and Security, where they became a function of the office of the National Coordinator for Security and Counterterrorism (NCTV). Changing the name of a team can be quite a hassle and may lead to confusion, so it is best to carefully consider what a good, recognisable name is and then keep that name.

Just like the name change, changing the institutional embedding of the nCSIRT at a later point in time made sense in the Dutch case, due to the establishment of a new Ministry of Justice

& Security. It is important that the nCSIRT has a logical institutional embedding that contributes to its effectiveness and access to the relevant stakeholders. However, for new teams, the lesson would be that it is worth thinking about the best institutional arrangements for the nCSIRT capacity as early on in the development process as possible. Every move and every change takes a lot of time, energy and money that would have been better spent against cyber threats.

An nCSIRT needs to cooperate inside the government, needs to work with the cybersecurity teams inside the critical infrastructures (energy, transport, banks, major hospitals, etc.), with the ISPs and other IT providers in the country, needs to reach out internationally, and so on. This is too complicated to achieve by means of coercion – and way more successful by means of cooperation. In part, this has to do with the complexity of the domain, but also – and perhaps more importantly – because the Internet community has a non-hierarchical structure and culture.

In the first few years of CERT-RO (now NCSC-NL), the team explored options to develop regulatory and other coercive policy instruments to strengthen its position as the coordinating body for other CSIRTs in the country. However, they quickly realised that a collaborative approach is much more effective. This almost seems ironical, since The Netherlands has a culture that strongly values cooperation and equality. This is also reflected in the well-known Dutch model for consensus-based decision-making (“poldermodel”). Thus, the best approach for the Dutch nCSIRT was to stay close to home and implement a cooperative, consensus-based model to facilitate national (and international) cybersecurity capacity building.

This lesson was not just learned in The Netherlands but in many countries. The nCSIRT is most effective when facilitating better cooperation – this requires good communications and trust-building with all major stakeholders. When the nCSIRT plays this role effectively, it means they can become the core of a web of trust inside the country that helps to more effectively defend the various networks and providers against threats and intrusions.



## Brazil

<b>Name of nCSIRT</b>	CERT.br (until 2005 name was NIC.br Security Office)
<b>Year of establishment</b>	1997
<b>Constituency</b>	Any network that uses Internet Resources allocated by NIC.br (IP addresses/autonomous systems/domains)
<b>Organisational embedding</b>	Part of NIC.br
<b>Current size (2020)</b>	10

In Brazil, unlike many countries, most of the Internet-related governance has not exclusively been a government initiative but has occurred with heavy involvement of different (private) sectors.

In the mid-1990s, when the Internet became more broadly used outside the academic world, the Brazilian government decided to separate the Telecom and Internet domains. And while Telecom was being regulated, the Internet became a free environment, open for commercial exploration. There still is no regulation of the Internet in Brazil.

In 1995 the decision was made to establish an Internet Steering Committee, which still exists today (CGI.br). The idea behind this steering committee was to assure effective participation of society in decisions about the implementation, management and use of the Internet in the country<sup>11</sup>. Today the committee is composed of a mix of representatives from the federal government, the corporate sector, the third sector, and from the scientific and technological community. Although the committee is created and coordinated by the government, the composition of the commission is always so that the government has a minority in seats.

In 1996 the Security Task Force that was formed by the Internet Steering Committee published a report that outlines the importance of creating an independent, neutral (not tied to government, industry or other interests) network security coordination organisation for the Internet in Brazil<sup>12</sup>. This led to the establishment of NBSO, the predecessor of CERT.br in June 1997. At this time it was operating on the basis of volunteers only, most of whom were experienced system administrators from different organisations in the country. These system administrators were already working together by reporting incidents and helping each other.

Initially, there was no funding for the committee. Most activities for domain registration and IP (Internet Protocol) assignment until then were done by a research organisation for free. When the use of the Internet started to grow, it was time to find a good business model and to professionalise the Internet-related activities. So, it was decided that the revenues from domain registrations etc. would be used not only for maintaining domains, but also to broaden security activities. When NBSO was first established, it was still operating with part-time staff members on a volunteer basis. From 1999, staff members (who had been volunteering until then) were hired fulltime, some of whom are still working with the team today. The team does not receive government funding. All funding still comes from NIC.br activities. NIC.br is a not-for-profit organisation, and they reinvest all revenues in the Brazilian Internet (infrastructure, exchange, services), including CERT.br.

In 2005 the name of the team changed to CERT.br, which is a much more recognisable name, not only in Brazil but more importantly also in the international community. The team has struggled for a long time with the naming part, mostly due to difficult acronyms that do not make sense.

The governance model in Brazil is rather unique. Because the Internet is not regulated, the Internet Steering Committee was created to coordinate and integrate Internet initiatives in Brazil. NIC.br was created to do domain registrations, IP assignments and related activities. But unlike most NIC organisations around the world, NIC.br does a lot more than registrations. CERT.br is part of NIC, and there are a number of other departments within NIC that implement projects and decisions from the Internet Steering Committee.

CERT.br is a small team, consisting of only ten people, in a very large country. In such a large country it is virtually impossible to have one team that caters to every user of the Internet. This is why CERT.br focuses on developing and offering training capabilities and enabling other teams. They strongly advocate the establishment of teams throughout the country, in particular in bigger companies and associations of organisations and enabling these teams to provide services to their constituencies. They are a last resort CSIRT, meaning that they help with triage for other established teams, shepherding and directing them to the right points. If necessary, they also are involved with serious incidents. They always have a team of three staff members on rotation for triage and support.

For CERT.br, as a small team, focusing on training and supporting other teams to improve their incident response is a much more effective approach than offering a hands-on response. It is important to stimulate a mindset that is open to learning, and this is what they focus on when working with other teams in the country. When it comes to deciding the range of services an nCSIRT provides for the constituency, it is important to really think about what is feasible and what is most effective in the specific situation. If an nCSIRT tries to do everything, they run the risk of ending up doing nothing really well. For this same reason, CERT.br does not create alerts for their constituency. There are so many things to focus on, and the country and network are so diverse that there are much better alternatives for all users to get alerts that are relevant for them. Instead, they incentivise specialised coordinating teams (like sectoral CSIRTs) to provide tailored advisories or alerts to their constituency. This has been a very conscious decision and a piece of important advice to new teams. All too often teams select services that sound relevant, perhaps because others are doing it too, but you have to really consider what the quality of service is that you can provide to your constituency and what the most added value will be that you can bring.

One of the strengths of CERT.br is that they emerged out of a bottom-up, multi-stakeholder

approach. Within the Internet community in Brazil, the realisation grew that it was important to invest in security. The initiative did not come from one person or agency. It came from people that were already talking together and working together. This has helped tremendously in building a strong community.

Another strength is that CERT.br have a very low rotation of staff. It is a small team with very skilled people that are motivated to stay. This has grown over the years and is not something that is easy to build. Rotation of staff can be a very big challenge to teams, so it is important to try and keep staff motivated and focusing on the continuity of the team. For continuity, it is essential to document the history of the team. Not just the formal decisions or formal documents, but also how these were reached and how the team evolves. Institutional memory is a key asset of any CSIRT and will be very valuable to get new staff members up to speed. Similarly, the network and collaborations with stakeholders are something that should be shared among all of the team members. If not, the rotation of staff can be devastating to the strength of the community and the reach of the nCSIRT.

When it comes to the composition of the team, CERT.br focuses on selecting people with a strong technical background who have some experience in the field. Because they are a small team, it is important that all team members know the technical side of things. From there, each team member further specialises in covering different areas of focus. Everybody has a different skill set. Some are better at communicating. Others have knowledge or experience in a specific area but all from a technical background. This means that they can adapt to different audiences. If they need additional skills, they tend to outsource certain tasks (such as making strong illustrations). To keep the staff motivated they are involved in training, there is attention for personal growth, and there are opportunities to attend conferences or being involved in specific projects — all to create an environment that focuses on building and maintaining a strong and motivated team.



## Thailand

<b>Name of nCSIRT</b>	ThaiCERT
<b>Year of establishment</b>	2000
<b>Constituency</b>	Government (technical services), critical infrastructure (advisory role), and the general public (advisory role)
<b>Organisational embedding</b>	Electronic Transaction Development Agency, part of the Ministry of Digital Economy & Society
<b>Current size (2020)</b>	20 employees in total, of which eight employees for incident handling

ThaiCERT has been the national CSIRT for Thailand since 2010. ThaiCERT was established in 2000 inside The National Electronics and Computer Technology Center (NECTEC) with the aim of being the last resort CSIRT for Thailand, with government backing right from the start, and was subsequently moved to inside the government in 2010 to act as a national team. They now reside under the Electronic Transactions Development Agency.

In 2000 a cryptographer, academic and army general recognised the need for building CSIRT capacity within Thailand, resulting in the establishment of the original ThaiCERT. Two of the three founders are still active within ThaiCERT today, one of which is currently the CEO. Apart from in 2000, the Thai army has not been involved anymore in the further development of the CSIRT.

Currently, ThaiCERT's main responsibility is coordination and communication to its constituency. For all incidents that come in at ThaiCERT, the owner must be identified. ThaiCERT is never fully in control and will never "push the button". What ThaiCERT will do is notify, provide information and advice. If necessary ThaiCERT can escalate higher up to enforce advice onto its constituency. Political escalation is very effective in Thailand, since most critical infrastructure, but also ISPs, and a large part of the hospitals and banks, are owned by the government.

For ThaiCERT, it is very important that employees also have strong communication skills. The CEO effectively communicates with politics, the technical lead is very knowledgeable but more importantly, communicatively strong, and an international staff member was appointed to do the international communication. This is very important, maybe even preconditional, for effective coordination and

communication, which is ThaiCERT's main task. Furthermore, PR and communication (a team within the Electronic Transactions Development Agency) support ThaiCERT with their communication.

As a national CSIRT, working in isolation is a no-go. Always involve your stakeholders. If no one supports you and there is no organisation that deems the nCSIRTs services valuable you might become obsolete. Hence, the advice is to not act as a group of technicians working in splendid isolation, but look outwards, communicate and cooperate with your stakeholders, including your constituency.

ThaiCERT's constituency consists of government, critical infrastructure and the general public. ThaiCERT provides advice and technical services to the government and related organisations. ThaiCERT has an advisory role towards critical infrastructure and the general public. Building a trust relationship with your constituency is considered to be crucial and will pay off during a national crisis. On-site visits by representatives from different organisational levels is an effective means for building trust.

In 2019 it was decided that the current team will move towards focusing on serving as the government CSIRT. The ThaiCERT name and function will move to a new team, serving as the national and C(II) team and cert-of-last-resort for Thailand. This move, however, has not completed yet, and the old team is de facto still the national CSIRT.

In the early stages of ThaiCERT's establishment, guidance was provided by JPCERT/CC (Japan). Currently, Japan is still helping various countries to build CSIRT capacity. An example of this is the train-the-trainer initiative funded by the ASEAN-Japan

Cyber Capacity Building Center. Where ASEAN is the Association of South-East Asian Nations, a partnership between ten South-East Asian countries at a ministerial level. ASEAN is a platform where the need for national CSIRTs and the importance of protecting a country's Critical Information and Infrastructures can be very effectively promoted cross-nationally.

Furthermore, in the Asia and Pacific region, there is cooperation between nCSIRTs in the form of a partnership (APCERT). This is a completely voluntary initiative. ThaiCERT was involved in the establishment of APCERT.

The most crucial advice to a country establishing a new national CSIRT is to ensure mandate and authority. With support from politics in the form of mandate and authority, the national CSIRT can perform its duties. Without, it cannot.

ThaiCERT processes enormous amounts of cyber threat intelligence information relevant for its constituency. To use this to the advantage of the nation works well inside the government and the critical infrastructures. It is more challenging in the private sector, especially in regard to ISPs. ISPs work in a highly competitive market and sometimes underestimate the importance of cybersecurity. Thailand is working on regulation in order to improve this situation, giving ISPs a better incentive to (re)act on cyber threats and incidents. Under all conditions, the role of the national team is one that informs and establishes good cooperation. For really urgent cases, the national team can also escalate to a national crisis management system.

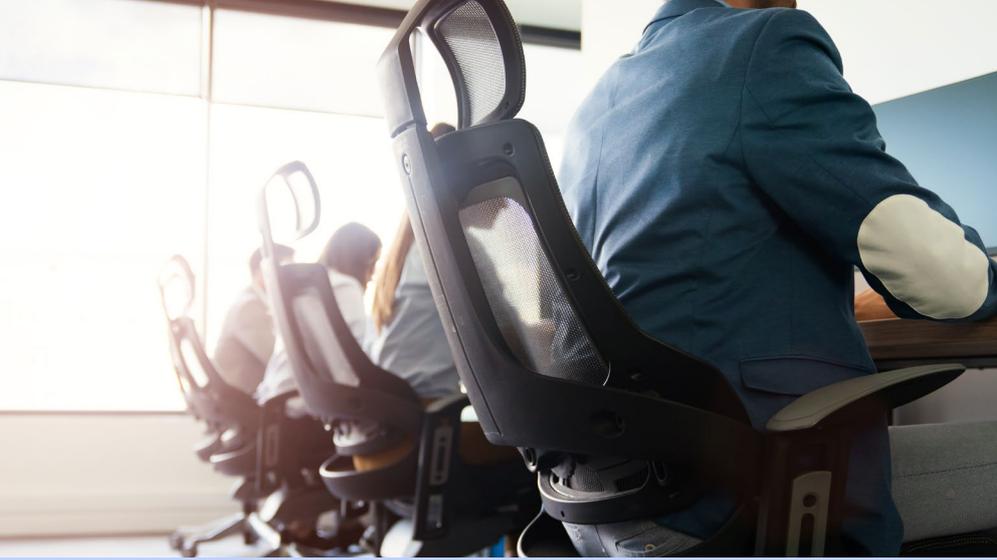
---

<sup>9</sup> This information was acquired from a former member of US-CERT with significant background in the development of cybersecurity capacity in the U.S. Government.

<sup>10</sup> In 2007 this team changed their name to SURFcert, on the request of the government.

<sup>11</sup> <https://www.cgi.br/pagina/our-history/149/>

<sup>12</sup> <https://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169>



# | Resource guide

Many organisations have written documents that contain information about establishing and improving a national CSIRT. However, in the early stages of establishing a national CSIRT, the sheer number of resources can be overwhelming. This can be a limiting factor when you are setting up your nCSIRT. For this reason, we have made the process of initial resource selection easier for you with this resource guide.

We have selected five documents that are all relevant in the very early stages of establishing an nCSIRT, according to experts in the field. There are many more documents available, and many of those are excellent too, but we have deliberately kept this list short in order to help you have a clear overview of the information, which is especially important at the start of the process.

The documents mentioned in this resource guide are meant to serve as a stepping stone. Each document contains references to other available resources. We encourage you to have a look at those too, but all in good time; we recommend that you start with the documents mentioned in this resource guide.

# Global CSIRT Maturity Framework (GCMF)

## Version 2

Publisher

**The Global Forum on Cyber Expertise (GFCE)**

Year of publication

**2021 (version 2)**

### What is it about?

The Global CSIRT Maturity Framework is a document that was written to support the development and maturity enhancement of national CSIRTs. It is based on (and also contains) the SIM3 maturity model that is well-known in the incident response community. The framework combines this model with a set of pre-defined nCSIRT maturity profiles.

SIM3 is made up of 44 measurable parameters that are divided into four quadrants (Organisational, Human, Tools and Processes). Together these parameters represent a wide range of aspects important to any CSIRT. The framework defines three maturity profiles (that focus on nCSIRTs): basic, intermediate and advanced. Each of these three profiles contains the minimum demands for all of the 44 SIM3 parameters.

Online tools are available to self-assess your nCSIRT's maturity based on SIM3 and compare it to the three maturity profiles. That way, you can see where your team is maturity-wise (and where the gaps are) and from there define a roadmap to reach higher levels of maturity in 1 or 2 years' time.

The GCMF is widely recognised as it is the result of a collaborative effort between the Global Forum on Cyber Expertise (GFCE), the European Union Agency for Cybersecurity

(ENISA) and the Open CSIRT Foundation (OCF).

### How can it be used in the early stages of developing an nCSIRT?

The GCMF can be used right from the start as you build your nCSIRT. Almost everything that has been discussed in this document is also covered by the SIM3 parameters. For example, you will find elements reflected in the parameters from in the [Business Model Canvas](#) for national CSIRTs, such as mandate, constituency, authority and responsibilities, but also topics such as reaching out to your constituency, (inter)national cooperations and the great importance of the human factor in CSIRTs.

With the SIM3 model, you can assess and measure these parameters in a fairly objective way (using the available online tools). By comparing your results with the GCMF's three maturity profiles, you can define your roadmap towards a higher maturity. You will instantly know what you need to focus on in order to achieve the desired progress.

You could do this assessment on your own, but for those new to the field it can be an overwhelming experience. It might be a good idea to have an experienced member of the CSIRT community help you. There are various programmes and projects available worldwide that provide such help at zero or low cost. Alternatively, you can hire an experienced consultant.

Whether you ask for help or decide to do it by yourself, we recommend that you use the GCMF approach right from the start. As your team advances, the GCMF will continue to be relevant as it covers all stages of maturity.

The GCMF can be downloaded from [Cybil](#), the Cybersecurity Capacity Building Portal.

# FIRST CSIRT Services Framework

Publisher

**Forum of Incident Response and Security Teams (FIRST)**

Year of publication

**2019**

## What is it about?

This resource provides a structured and comprehensive overview of the services a CSIRT may provide to its constituency. It is a generic framework, so it is not specifically written for nCSIRTs, but it certainly applies. The document has a hierarchy, starting with five main service areas:

1. Information Security Event Management
2. Information Security Incident Management
3. Vulnerability Management
4. Situational Awareness
5. Knowledge Transfer.

Each of these five is broken down into specific services, and each service is broken down into functions. The aim of this framework is not to encourage CSIRTs to offer a comprehensive set of services, but rather to have them make a careful selection of services (from a broad portfolio) to fulfil their mandate.

## How can it be used in the early stages of developing an nCSIRT?

The natural order for setting up your nCSIRT is to develop a vision first and to know what your constituency will be (it should be defined more precisely than just “the whole country”). Once defined, the vision and the constituency are used to develop a mandate, plus descriptions of the nCSIRT’s authority and responsibilities. The next logical next step is to use the mandate and the responsibilities as a starting point for a survey of the CSIRT Services Framework.

This framework should be treated as a menu: you pick and choose the services you need to fulfil your mandate and responsibilities. Be aware that there is one crucial condition: you need to have what it

takes. This means that you need to have the people and resources available to actually deliver on the services that you have chosen. An nCSIRT is like the fire brigade – it is essential that its core service is available and works well. Everything else is a bonus and can only be done with sufficient means. So, while we have pleaded elsewhere to be bold and ambitious, here we urge you to be conservative and only pick those services that you must perform and can perform. Just like with the GCMF, you can do this “menu selection” by yourself, or you can ask for help from an experienced member of the CSIRT community. The latter option could speed things up for you.

Be aware that, at the very least, an nCSIRT will need to provide some services/functions from the following service areas:

- Information Security Incident Management, namely the coordination of critical or nationwide incidents, which necessarily also includes some degree of incident analysis (though this does not have to be an in-depth analysis in the starting stages).
- Situational Awareness, as the nCSIRT will need to manage at least the basics of threat intelligence.
- Knowledge transfer, as it is crucial for an nCSIRT to not just gather information and analyse it, but also warn constituents and sometimes peer teams in the global CSIRT community as well.

You will probably pick some more services to offer to your constituency if your resources allow it. Do make sure to tell your constituency what services you offer, and, as we argued in the [Formulating a Business Case](#) section, use the rfc-2350 to publish those.

What was said about the GCMF applies here as well: the CSIRT Services Framework will continue to be useful throughout the lifetime of your nCSIRT or NCSC. Over time, more experience, more people, more tools, and more responsibility will lead to your team extending and improving on existing services, and also adopting additional ones.

This [link](#) leads you to a FIRST webpage that introduces the CSIRT Services Framework. It contains a direct download link to the most recent version of the framework.

# OAS Best Practices for Establishing a National CSIRT

Publisher

**Organization of American States**

Year of publication

**2016**

## What is it about?

This document is a best practice guide that discusses the process of managing a project for the creation and deployment of a CSIRT, with special attention for the establishment of national CSIRTs. It discusses both planning and implementation in the early stages of setting up a CSIRT.

## How can it be used in the early stages of developing an nCSIRT?

Though it was not written specifically for national CSIRTs, you will find that 90% or more applies to establishing an nCSIRT. The document is easy to read and contains clear illustrations; we recommend reading the entire document from front to back. It is a highly informative document that helps you become acquainted with the process of planning, establishment and implementation of your CSIRT.

The stakeholder management section is very detailed and covers examples of potential stakeholders, discussing how to interview and analyse them. This resource can be for [identifying relevant stakeholders](#) for your initiative.

The document is listed in the [document section](#) of the cybersecurity pages and available for download under the name '2016 - Best Practices CSIRT.pdf'. It is available in English and Spanish.

# How to set up CSIRT and SOC

Publisher

**European Union Agency for Cybersecurity (ENISA)**

Year of publication

**2020**

## What is it about?

"How to set up CSIRT and SOC" is a results-driven guide for those who set out to create a CSIRT or SOC. It can be used as an alternative or addition to the OAS document. Even though ENISA focuses on the European Community, this guide is globally applicable as lessons from all over the world were taken into consideration by the authors. It starts with assessment for readiness and then leads via design to implementation, and finally to operations and improvement.

## How can it be used in the early stages of developing an nCSIRT?

The document is highly usable for the formation of national teams, as ENISA's expertise in that area shines throughout, both in examples and approaches used. The strong focus on the early assessment stage and design and implementation, make it very useful for the early stages of team development. It is very well aligned with two other references mentioned in this resource guide: the FIRST CSIRT Services Framework and the GCMF (via the underlying SIM3 model). Important topics such as mandate, services, processes, organisation, and cooperation are all covered in practical ways. Other topics including CSIRT facilities, technologies and internal security are also addressed.

The document is listed as "[How to set up CSIRT and SOC](#)" on the ENISA webpages, and available as a PDF download. As of the publication on 10 December 2020, it was available only in English, but translations are to be expected.

# What Skills Are Needed When Staffing Your CSIRT?

Publisher

**CERT/CC**

Year of publication

**2017**

## What is it about?

This document describes the minimum set of skills that a CSIRT staff should have. It is based on the vast experience that CERT/CC has gathered, ever since the wake of the CSIRT community back in 1988.

Throughout this document, we have emphasised several times that the human factor is important to the success of your nCSIRT. In full agreement, CERT/CC's skill description starts with listing the personal skills that team members should have, these include:

- Communication (written and oral) skills
- Presentation and team skills
- Diplomacy skills
- The ability to follow policies
- Integrity
- Knowing one's limits
- Coping with stress
- Problem-solving and time management.

These skills are followed by a list of technical skills, related to what CSIRTs do on a day-to-day basis. All of these skills are worked out in detail in a very pragmatic manner, clearly demonstrating the great amount of real-life experiences the resources draw upon.

## How can it be used in the early stages of developing an nCSIRT?

CERT/CC's skillset document can be used right from the start as you set up your nCSIRT. It will help you define your staffing needs and can be used in the recruitment process for your nCSIRT.

You start by defining a number of roles for your nCSIRT. Examples of roles are (and these are rather basic examples): incident handler, senior incident handler, threat & incident analyst, and team manager.

After you have defined the roles, you select the necessary skills for each role from the CERT/CC document, making sure to not only focus on technical skills but just as much on personal skills.

These role/skillset combinations can be used when recruiting new people, as they help you to clearly define what you need to hire for. Do bear in mind that, all over the world, people with the right skills for CSIRTs are in short supply and hard to find. Therefore, you need to assume that you will need to further train your staff members once hired.

The role/skillset combinations are also essential ingredients for staff development plans and training (in house, as well as paid training given by external providers). Be aware that various organisations and programmes in the CSIRT community provide various kinds of training, often of excellent quality and in many cases at low or even zero costs (except your staffs travel expenses, of course).

The document is available in the [library](#) of the Software Engineering Institute.

# Glossary

## Authority

What the CSIRT is allowed to do within its constituency in order to accomplish its role<sup>13</sup>. The authority to enforce or escalate in order to satisfy the mandate of the CSIRT.

## Capability

A measurable activity that may be performed as part of an organisation's roles and responsibilities<sup>14</sup>.

## Capacity

The number of simultaneous process occurrences of a particular capability that an organisation can execute before it achieves some form of resource exhaustion<sup>15</sup>.

## Constituency

Who the CSIRT functions are aimed at, the "clients" of the CSIRT<sup>16</sup>.

## CERT

Computer Emergency Response Team. It is a registered mark licenced to Carnegie Mellon University. CSIRTs have to contact the Carnegie Mellon University CERT Division to use the CERT® mark.

## Critical infrastructure

System and assets, whether physical or virtual, so vital to [society] that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety,

or any combination of those matters<sup>17</sup>.

## Critical information infrastructure

The interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, economic or social well-being of people), of which the disruption or destruction would have serious consequences<sup>18</sup>.

## CSIRT

Computer Security Incident Response Team. This term can be used freely.

## Mandate

An nCSIRT needs to derive the justification for its existence and assignment from some of governance. This is called the nCSIRT mandate. Ideally, the mandate comes from the highest level of governance in your specific environment<sup>19</sup>.

## Maturity

How effectively an organisation executes a particular capability within its mission and authorities. It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services. The ability of an organisation will be determined by: the extent, quality of established policies and documentation, and the ability to execute a set process<sup>20</sup>.

## NCSC

National Cyber Security Centre. A term some countries use when multiple national cybersecurity capacities and functions are consolidated within one entity. It usually has a close relation to the national crisis management structure.

## PGP/GnuPG encrypted emails

A cryptography tool that is commonly used in the CSIRT community to send a confidential email.

## Responsibility

What the nCSIRT is expected to do towards their constituency in order to accomplish its role<sup>21</sup>.

## Service

A service is a set of recognisable, coherent functions towards a specific result. Such results may be expected or required by constituents or on behalf of the stakeholder of an entity<sup>22</sup>.

## Triage

In the context of cyber incident response, the moment after an incident at which the incident responder establishes an overview to determine: a) what needs to be done (to prevent further damage) and b) to define the next steps.

# Table of abbreviations

<b>APCERT</b>	Asia Pacific Computer Emergency Response Team	<b>ENISA</b>	European Union Agency for Cybersecurity	<b>NACS</b>	National Agency for Computer Security
<b>ASEAN</b>	Association of Southeast Asian Nations	<b>FIRST</b>	Forum of Incident Response and Security Teams	<b>NCSC</b>	National Cyber Security Centre
<b>CDC</b>	Cyber Defence Centre	<b>GCMF</b>	Global CSIRT Maturity Framework	<b>NCSO</b>	National Cybersecurity Division
<b>CEF</b>	Connecting European Facility	<b>GCSB</b>	Government Communications Security Bureau	<b>NCTV</b>	National Coordinator for Security and Counterterrorism
<b>CERT</b>	Computer Emergency Response Team	<b>GFCE</b>	Global Forum on Cyber Expertise	<b>NECTEC</b>	National Electronics and Computer Technology Center
<b>CII</b>	Critical Information Infrastructures	<b>ICT</b>	Information and communications technology	<b>OAS</b>	Organization of American States
<b>CIRT</b>	Cyber Incident Response Team	<b>IP</b>	Internet Protocol	<b>OCF</b>	Open CSIRT Foundation
<b>CISA</b>	Cybersecurity & Infrastructure Security Agency	<b>ISP</b>	Internet Service Providers	<b>SOC</b>	Security Operations Center
<b>CSIRT</b>	Computer Security Incident Response Team	<b>IT</b>	Information Technology		
<b>DDoS</b>	Distributed Denial-of-Service	<b>ITIL</b>	Information Technology Infrastructure Library		
<b>DHS</b>	Department of Homeland Security	<b>ITU</b>	International Telecommunication Union		

<sup>13</sup> Definition adopted from SIM3, <https://opencsirt.org/csirt-maturity/sim3-and-references/>

<sup>14</sup> Definition adopted from FIRST CSIRT Services Framework, CSIRT Services Framework Version 2.1 (first.org)

<sup>15</sup> Definition adopted from FIRST CSIRT Services Framework, CSIRT Services Framework Version 2.1 (first.org)

<sup>16</sup> Definition adopted from SIM3, <https://opencsirt.org/csirt-maturity/sim3-and-references/>

<sup>17</sup> Definition adopted (and generalized) from [https://csrc.nist.gov/glossary/term/critical\\_infrastructure](https://csrc.nist.gov/glossary/term/critical_infrastructure)

<sup>18</sup> Definition adopted from The GFCE-MERIDIAN (2016) Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. <https://cybilportal.org/tools/the-gfce-meridian-good-practice-guide-on-critical-information-infrastructure-protection-for-governmental-policy-makers>

<sup>19</sup> Definition adopted from SIM3, <https://opencsirt.org/csirt-maturity/sim3-and-references/>

<sup>20</sup> Definition adopted from FIRST CSIRT Services Framework, CSIRT Services Framework Version 2.1 (first.org)

<sup>21</sup> Definition adopted from SIM3, <https://opencsirt.org/csirt-maturity/sim3-and-references/>

<sup>22</sup> Definition adopted from FIRST CSIRT Services Framework, CSIRT Services Framework Version 2.1 (first.org)

# Authors

 <b>Hanneke Duijnhoven</b>	TNO	The Netherlands
 <b>Bram Poppink</b>	TNO	The Netherlands
 <b>Tom van Schie</b>	TNO	The Netherlands
 <b>Don Stikvoort</b>	m7	The Netherlands

# Contributing experts

 <b>Aart Jochem</b> Chief Information Security Officer   Ministry of the Interior & Kingdom Relations <b>The Netherlands</b>	 <b>Hielke Bontius</b> National Cyber Security Centre The Netherlands   NCSC-NL <b>The Netherlands</b>	 <b>Klaus-Peter Kossakowski</b> Professor, Hamburg University of Applied Science   HAW <b>Germany</b>
 <b>Andrea Dufkova</b> European Union Agency for Cybersecurity   ENISA <b>Greece</b>	 <b>Jean-Robert Hountomey</b> AfricaCERT <b>Africa</b>	 <b>Klee Aiken</b> National CERT of New Zealand   CERT NZ <b>New Zealand</b>
 <b>Andrea Rigoni</b> Deloitte Risk Advisory Italy Srl <b>Italy</b>	 <b>Kerry-Ann Barret</b> Organization of American States   OAS <b>United States</b>	 <b>Lorenzo Russo</b> Deloitte Risk Advisory Italy Srl <b>Italy</b>
 <b>Brittany Manley</b> CERT/CC <b>United States</b>	 <b>Kiru Pillay</b> Director of Cybersecurity, Department of Telecommunications and Postal Services <b>South Africa</b>	 <b>Maarten Van Horenbeeck</b> Chair of GFCE Working Group B, Task Force CIM & FIRST Board of Directors <b>United States</b>
 <b>Cristine Hoepers</b> Brazilian National Computer Emergency Response Team   CERT. br <b>Brazil</b>	 <b>Klaid Mägi</b> Cyber4Dev Key Expert <b>Estonia</b>	 <b>Marco Obiso</b> International Telecommunication Union   ITU <b>Switzerland</b>
 <b>Declan Ingram</b> Deputy Director CERT NZ <b>New Zealand</b>	 <b>Klaus Steding-Jessen</b> Brazilian National Computer Emergency Response Team   CERT.br <b>Brazil</b>	 <b>Martijn de Hamer</b> Amsterdam University of Applied Science   HvA <b>The Netherlands</b>
 <b>Diego Subero</b> Organization of American States   OAS <b>United States</b>		

 **Martijn van der Heide**

Computer Security Incident  
Response Team for Thailand |  
ThaiCERT  
Thailand

 **Masato Terada**

Hitachi Incident Response Team |  
HIRT & FIRST Board of Directors  
Japan

 **Mirosław Maj**

Open CSIRT Foundation | OCF  
Poland

 **Nabil Sahli**

Professor, National Computer  
Emergency Response Team of  
Tunisia | TunCERT  
Tunisia

 **Naoufel Frikha**

National Computer Emergency  
Response Team of Tunisia | TunCERT  
Tunisia

 **National CSIRT-CY**

2 members of the National  
Computer Security Incident  
Response Team of Cyprus  
Cyprus

 **Nynke Stegink**

National Cyber Security Centre The  
Netherlands | NCSC-NL  
The Netherlands

 **Olivier Caleff**

Open CSIRT Foundation | OCF  
France

 **Omo Oaiya**

Chief Strategy Officer, WACREN  
Nigeria

 **Perpetus Jacques  
Houngbo**

Expert Cybersecurity, OCWAR-C  
Benin

 **Richard B. Harris**

GFCE Advisory Board member and  
former member of US-CERT  
United States

 **Robin Ruefle**

CERT/CC  
United States

 **Roderick Mooi**

The South African National Research  
Network | SANReN  
South Africa

 **Rogério Gil Raposo**

GNR  
Portugal

 **Samuel Higgins**

Foreign Common Wealth Office  
United Kingdom  
United Kingdom

 **Seiichi Komura**

NTT Advanced Technology  
Corporation  
Japan

 **Serge Droz**

Chair Board of Directors FIRST  
Switzerland

 **Vilius Benetis**

NRD Cyber Security  
Lithuania

 **Yoshiki Sugiura**

NTT-CERT  
Japan