National Cyber Incident Classification

Handbook

CRITICAL
INFRASTUCTURE
PROTECTION

OSCE Organization for Security and Co-operation in Europe

Published by the Organization for Security and Co-operation in Europe

Vienna, October 2025

Layout and design by MaxNova, Belgrade.

ISBN 978-92-9271-534-2

Transnational Threats Department

OSCE Secretariat

Wallnerstrasse 6, A-1010 Vienna, Austria

https://www.osce.org/secretariat/cyber-ict-security

The publication of this report was made possible thanks to contributions from the Federal Republic of Germany and France. The content of this publication, including the views, opinions, findings, interpretations and conclusions expressed herein do not necessarily reflect those of these donors or participating States. It is not a consensus-based document.

National Cyber Incident Classification

Handbook

CRITICAL
INFRASTUCTURE
PROTECTION

OSCE Organization for Security and Co-operation in Europe

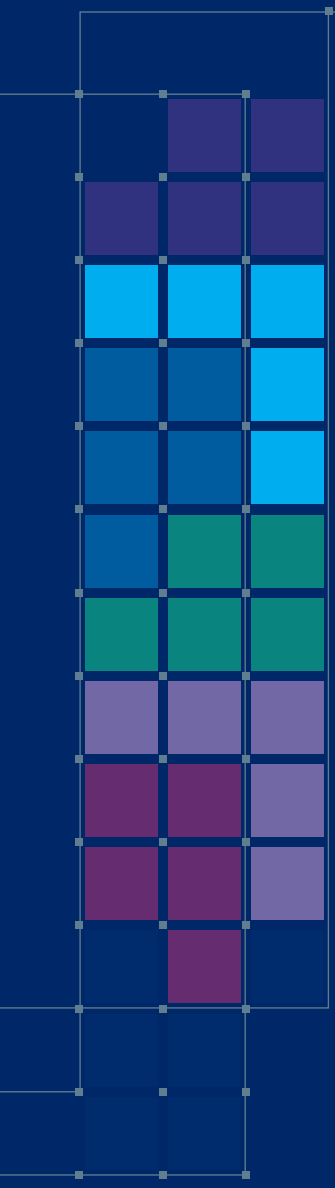
ACKNOWLEDGMENTS

This report was prepared by the OSCE Secretariat's Transnational Threats Department (TNTD) Co-ordination Cell under the direction of Ms. Szilvia Tóth, Cyber Security Officer. TNTD would like to thank Dr. James Shires for preparing the handbook, as well as to Dr. Serge Droz for his contribution. Valuable support was provided by Ms. Ružica Stojičić Bencun of TNTD Co-ordination Cell.

LIST OF ACRONYMS AND ABBREVIATIONS

CBM	— Confidence-Building Measure
CSIRT	— Computer Security Incident Response Team
CVE	— Common Vulnerabilities and Exposures
CVSS	— Common Vulnerability Scoring System
DDoS	— Distributed Denial of Service
ENISA	— European Union Agency for Cybersecurity
ICT	— Information and Communications Technology
IDS	— Intrusion Detection System
IOC	— Indicator of Compromise
IPS	— Intrusion Prevention System
ISAC	— Information-sharing and Analysis Centre
ISP	— Internet Service Provider
NCICS	— National Cyber Incident Classification System
NIS/NIS2	— Network and Information Security Directive
OSCE	— Organization for Security and Co-operation in Europe
SME	— Small and Medium-sized Enterprise
SOP	— Standard Operating Procedure
TLP	— Traffic Light Protocol
TTP	— Tactics, Techniques and Procedures
URL	— Uniform Resource Locator

Contents



Foreword

With digital networks connecting nations globally, the way we manage cyberspace shapes not only our security but also the very fabric of state-to-state relations.

Cyberspace has emerged as a new arena for international relations — a new place where states interact, compete and, more importantly, co-operate. As states increasingly use information and communications technology (ICT) to advance their national interests, the risks of misunderstanding, miscalculation and even conflict continue to grow. Cyber threats do not respect national borders and a single incident can have immediate spillover effects, destabilizing entire regions. This is why it is essential for states to come together and build trust.

Although the United Nations has been discussing issues related to state use of ICT since the late 1990s, the Organization for Security and Co-operation in Europe (OSCE) was the first multilateral organization to implement practical measures to build confidence and trust in this domain. This achievement underscores the OSCE's added value in cyber diplomacy: it translates broad international commitments into concrete actions. However, confidence-building measures (CBMs) only have value if states have the political will and capacity to implement them. CBM 15 on critical infrastructure protection is an area where political will is abundant.

In today's increasingly interconnected world, the threat posed by malicious cyber activity continues to grow in scale, sophistication and impact. As societies become more digitally reliant, the ability to effectively detect, assess and respond to cyber incidents particularly those targeting critical infrastructure — has become essential for both national and international security.

Recognizing this evolving landscape, the OSCE has taken a leading role in fostering co-operative approaches to cyber/ICT security. At the heart of this work lies the development and implementation of national cyber incident classification systems — a key tool for enhancing crisis response, ensuring co-ordinated action and promoting transparency between states.

Classification systems enable national authorities to assess and prioritize cyber incidents based on severity, helping to allocate resources efficiently and reduce the potential for cascading effects. Equally important, they provide a shared language that supports cross-border communication, contributing to the prevention of misunderstanding, misattribution and escalation — core objectives of the OSCE's cyber/ICT security CBMs.

This handbook highlights the OSCE's sustained efforts to support participating States in designing, refining and operationalizing national incident classification systems. As cyber threats continue to evolve, so too must our collective resilience. We hope this document serves as a practical resource for policymakers, technical experts and all stakeholders working to strengthen cybersecurity and protect critical infrastructure. Through collaboration and shared understanding, we move closer to a more secure, stable and co-operative cyber domain for all.

Alena Kupchyna
Co-ordinator of Activities to Address Transnational Threats
OSCE Secretariat

Executive Summary

This handbook is intended to guide participating States of the Organization for Security and Co-operation in Europe (OSCE) and other interested parties in developing and implementing a national cyber incident classification system. After an introduction and context-setting section explaining the benefits and challenges of cyber incident classification, the handbook divides the process of setting up a national system into six steps:

Step 1: Set the goals. This step explains the different goals states may pursue when developing a classification system, including: mitigating cyber incidents; national risk assessment; understanding the causes and consequences of cyber incidents; standardization between cyber and non-cyber incidents; and international co-ordination.

Step 2: Engage stakeholders. This step sets out how states can engage stakeholders at the start of the development process. As incident classification systems rely on the effective collection, analysis, assessment and communication of information (the "information cycle"), states should identify key stakeholders and means of engagement for all elements of the cycle.

Step 3: Establish reporting pathways. This step discusses how states can capture information on ongoing or potential cyber incidents as quickly and reliably as possible. Actions include developing smooth regulatory mechanisms for incident reporting from critical infrastructure organizations as well as facilitating reporting from other sources.

Step 4: Build on existing structures. This step emphasizes how most states already possess some ingredients for a cyber incident classification system, whether at sectoral levels or through analogous risk assessment functions for other areas. Consequently, states should build on these structures wherever possible to ensure a sound legal and policy basis for their system.

Step 5: Implement the system. This step emphasizes that successful implementation depends on thorough testing of all elements and a phased introduction that allows for adjustments based on early-phase feedback in. A crucial component of this testing is scenario-based exercises, which bring all relevant stakeholders together to work through challenges or issues.

Step 6: Refine the system. This step highlights how a cyber incident classification system is fundamentally an iterative process, with incremental improvements over time in pursuit of a state's strategic goals. Refining the system requires retaining people with the necessary skills and expertise, as well as cultivating increasingly productive relationships among stakeholders.

To illustrate the principles outlined in this handbook, we use the examples of two fictitious states representing different approaches to cyber incident classification. State A has a centralized governance model, driven by a top-down approach with clearly defined security priorities, while State B is more federalized, with decision-making powers in many areas delegated to regional provinces. While these examples are fictitious, the description of their approaches is informed by observations of existing cyber incident classification practices.

Introduction

Over the preceding decades, cyber incidents have grown in scale, frequency and complexity. They now frequently threaten critical infrastructure at national and regional levels, and cause significant financial and societal harm, from economic disruption, data deletion and extortion, as well as other forms of fraud and national security threats.

Given this rise in severity, cyber incidents have gone from being purely a matter for technical authorities and sectoral entities to requiring a multi-stakeholder response, incorporating public and private sector actors to mobilize sufficient technical and organizational capacities for incident response and recovery.

A national cyber incident classification system (NCICS) is necessary to support this multi-stakeholder response, bringing together all government actors and clarifying their capacity and mandate to intervene in private sector activities in case of a severe cyber incident. Classification schemes, however, do not only provide the basis for cross-government co-ordination, they also communicate an informed risk perspective to other stakeholders and the general public, nationally and internationally. In this way, national cyber incident classification schemes can contribute to appropriate understanding and response to cyber threats. In situations where such threats can potentially emanate from other states, a well-designed and implemented national classification scheme can contribute to de-escalation and peaceful interstate relations.

This handbook provides guidance to OSCE participating States for the development of national cyber incident classification systems. It builds on a previous OSCE report on *Cyber Incident Classification: A Report on Emerging Practices within the OSCE region*.[1] It draws on the contents of that report to outline the rationale and good practices for cyber incident classification among OSCE participating States, as well as the usefulness of such a system in building global cybersecurity capacity.

1 OSCE. 'Cyber Incident Classification: A Report on Emerging Practices within the OSCE Region'. Accessed 22 April 2025. **https://www.osce.org/secretariat/530293.**

The handbook is the final deliverable of the extra-budgetary project on "Facilitation of the development and implementation of national cyber incident severity scales (NCISS) and related measures to protect critical infrastructures". Through this project the OSCE Secretariat supported participating States in raising the implementation rate of the CBMs and therefore enhancing States' capacities to deal with significant cyber incidents in an effective way by providing support in developing national cyber incident classification systems.

How to use this handbook

Readers are advised to begin with the second section on benefits and challenges of cyber incident classification to obtain an overview of why and how states do incident classification, and the main obstacles involved.

Following this general section, the handbook is organized as a step-by-step guide, discussing in turn the six key steps that states can take to develop a cyber incident classification system listed in the executive summary above. These steps are presented in a logical order, providing an ideal sequence for a state to follow when creating a cyber incident classification system from scratch. For readers in states looking to establish a new system or generally wishing to learn about national cyber incident classification, the steps should simply be read in ascending order.

There might also be readers from states that have already taken some of the steps without following this step-by-step path. In such cases, we recommend that readers begin with the step that most closely relates to their current task or concerns; for example, engaging stakeholders or developing reporting pathways.

Those readers can then expand out forwards or backwards from that step as required, or skip steps that are not relevant. In general, we recommend that all readers visit the section on the "information cycle" in Step 1, because this cycle is at the core of all incident classification systems.

Illustrative example

To illustrate the principles outlined in this handbook, we use the examples of two fictitious states representing different approaches to cyber incident classification. While these examples are fictitious, the description of their approaches is informed by observations of existing cyber incident classification practices. Importantly, no value judgements are implied regarding the fictitious states or the relative merits of their respective approaches. Cyber incident classification systems vary according to national contexts.

These two fictitious states appear at the end of each step of the handbook, with a short vignette explaining how each state put that step into practice, what they did and why, as well as some of the impacts of their actions. These vignettes can be read as an illustrative part of each step to enhance understanding. They can also be read separately, after the main steps have been processed, as a benchmark for actual state contexts, or skipped altogether if the reader feels their state context diverges sufficiently to make these examples irrelevant.

State A

State A has a centralized governance model, driven by a top-down approach with clearly defined security priorities. The National Cybersecurity Centre, located within a Department for National Security, has significant regulatory authority over critical infrastructure operators. State A's National Cybersecurity Centre serves as the primary point of contact for all cybersecurity matters affecting national security.

In State A, existing non-cyber crisis management schemes are designed to provide a comprehensive risk overview for various security and emergency authorities, as well as national intelligence services. State A wishes to take the same approach to cyber incident classification, reflecting national risks and aligning with other environmental and political risk assessment structures. Overall, State A's approach is very inward focused, prioritizing internal risk assessment over external stakeholder relations.

State B

State B is more federalized, with decision-making powers in many areas delegated to regional provinces. Consequently, State B places a lot of responsibility for cybersecurity on critical infrastructure operators themselves. The National Cybersecurity Centre, situated in the Department of the Interior, sees itself as an enabler rather than enforcer, bridging gaps where individual responsibility is insufficient, and it tries to empower its constituents. It fosters collaboration and acts as a liaison with other government agencies, such as the security or intelligence services.

State B's National Cybersecurity Centre wants to use a national cyber incident classification system to produce comprehensive risk profiles to share with its constituents, enabling them to take appropriate measures. This bottom-up approach does not imply a 'laissez-faire' attitude. On the contrary, critical infrastructure operators are required to collaborate with the National Cybersecurity Centre, with financial penalties for noncompliance. Overall, in contrast to State A, State B's approach is primarily outward focused, prioritizing external stakeholders over a coherent cross-government perspective on cyber risk.

Benefits and challenges of cyber incident classification

In January 2022, the OSCE began analyzing emerging practices in cyber incident classification amongst OSCE participating States, as well as identifying their interests and needs in this area.

The resulting report drew from the results of two surveys and documentation provided by participating States.[2] In addition to serving as important input for further exchanges between participating States on the topic, the report highlights a range of approaches and practices that can serve as guidance for states and other relevant stakeholders on cyber incident classification.

The report argues that all OSCE participating States could benefit from developing a national cyber incident classification system to support national crisis management and incident response processes. Such a system provides a routine and consistent mechanism that can be used to objectively assess and prioritize cyber incidents in the national context, in a timely manner, and to identify gaps in existing defenses. It also informs national decision-making, including at strategic and political levels. Therefore, the system helps states to quickly communicate the nature of an incident and streamline procedures for moving from the identification of an incident to its handling and eventual resolution, while minimizing disruption to network operations. In this way, a cyber incident classification system is an important aspect of participating States' capacity to advance the OSCE confidence-building measures on Cyber/ICT security (Figure 1).

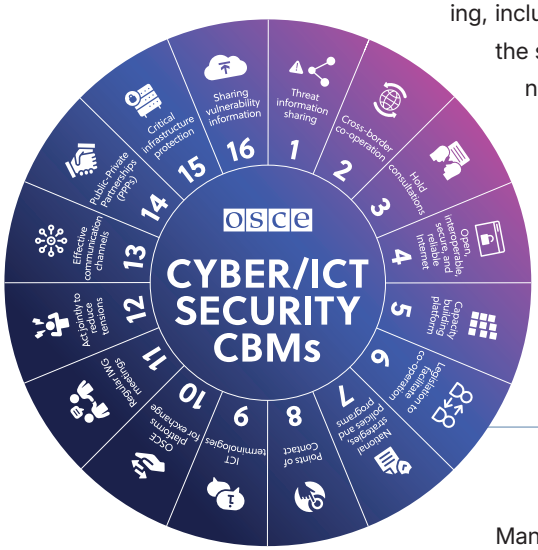


Figure 1: OSCE CBMs "round" figure

Many OSCE participating States have recognized the need for a cyber incident classification system (Table 1).

2 OSCE. 'Cyber Incident Classification: A Report on Emerging Practices within the OSCE Region'. Accessed 22 April 2025. **https://www.osce.org/secretariat/530293**.

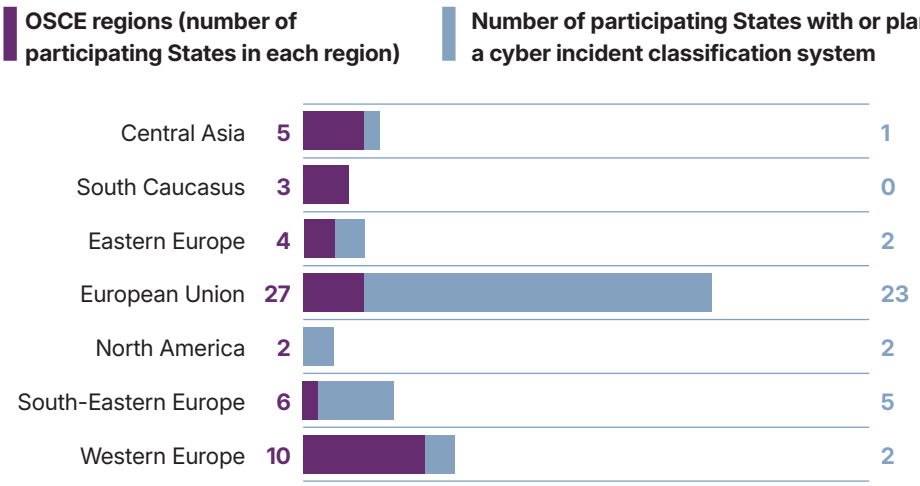


Table 1: National cyber incident classification system in OSCE participating States

While some OSCE participating States have had a cyber incident classification system in place for over two decades, most established them after 2015. Many of these classification systems and enabling legislative or regulatory instruments are publicly available online. Some participating States that do not currently have a system in place but plan to establish one in the near future.

Examples of existing classifications of cyber incidents, as used by France and the United States of America, are provided in Annex 2.

However, the report also notes that OSCE participating States have taken different approaches to cyber incident classification, identifying several challenges they faced in developing such a system related to design, implementation and maintenance, as follows.

Design

- *Objectivity:* A national cyber incident classification system cuts across the interests and mandates of multiple state entities, as well as private sector and non-governmental organizations. Consequently, states should aim to secure the support of all key stakeholders in the design of the system, which includes ensuring that all parties are confident enough that the assessment process will be fair and objective.
- *Applicability:* A national cyber incident classification system must meaningfully combine multiple sectoral contexts, comparing disparate practices and perspectives across critical infrastructure sectors to produce severity and risk assessments that apply equally well to all of these sectors.

Implementation:

- *Reporting requirements*: The primary objective should be to establish a solid legal, regulatory and policy foundation for reporting incidents and other notifications, along with the appropriate incentives. Without this foundation, an incident classification system may appear functional on paper but fail to encourage key actors to contribute effectively during real incidents.
- *Reporting thresholds:* Another common challenge is that key stakeholders are unaware of or do not understand national cyber incident classification system reporting and notification thresholds. Even when reporting requirements are in place, states must educate key stakeholders on threshold interpretation and associated actions.

Maintenance:

- *Retaining knowledge and expertise:* A national cyber incident classification system is an iterative process by nature because the categorization and prioritization of incidents will change over time and in different contexts. Sustaining this iterative refinement is challenging, especially when qualified and experienced personnel may leave or change roles.

Given these challenges — among others — the following sections of the handbook outline six key steps to support OSCE participating States in developing a cyber incident classification system. While the steps follow a similar path through design, implementation and maintenance, they do not address the challenges specifically. Rather, each step focuses on the most relevant challenges.

Step
01

Set the goals

Beyond the overall rationales outlined in the introduction and the previous section, states can develop their national cyber incident classification system for a variety of specific purposes. Without identifying these goals, however, the system is unlikely to be effective. Therefore, the first step states should take is to clearly set out the primary goals of their national cyber incident classification system.

This section introduces the five most common goals of national cyber incident classification. Most states will develop an incident classification system with at least one of these goals in mind. However, this list is neither mandatory nor exhaustive. It is not mandatory, as not all states will seek to achieve all the purposes discussed here, and may omit some, depending on their wider cybersecurity strategy, and national and regional political context. It is not exhaustive because states may seek to achieve other objectives through cyber incident classification, which may also influence the design and implementation of their systems.

The key message of this section is that states should have specific goals in mind when developing an incident classification system, which need to be outlined and prioritized at the start of the process. Only then can states engage relevant stakeholders (Step 2) to develop the system — which may, of course, involve revisiting the objectives of the system to ensure sufficient alignment with the overall vision.

KEY ACTIONS

- **Decide which national cyber incident classification system goals are relevant** to a specific state. Use the following list as a starting point, then think of additional goals that are specifically relevant to your state.
- **Differentiate between essential and desirable goals.** This enables states to determine which are the core goals for their national cyber incident classification system.
- **Arrange both essential and desirable goals**. In the event of a trade-off or conflict between different goals, this **order of priority** enables states to find an appropriate solution.
- **Ensure that the information-sharing cycle meets all goals of the national cyber incident classification system**; if not, amend the cycle to fit the goals.

Goal 1: mitigation of cyber incidents by enabling quick allocation of responsibility and action

The impact of many cyber incidents is mitigated by actors outside state structures, for example, corporate cybersecurity personnel, private sector security researchers or civil society organizations.[3]

3 See e.g. J. Kariuki, *The UK will work with international partners to dismantle the cyber criminal ecosystem: Statement by Ambassador James Kariuki, UK Deputy Permanent Representative to the UN, at the UN Security Council* (London: UK HMG, 2024), **https://www.gov.uk/government/speeches/the-uk-will-work-with-international-partners-to-dismantle-the-cyber-criminal-ecosystem-uk-statement-at-the-un-security-council**

Decisions by these actors are crucial, because successful mitigation often depends on front-line actors outside the state taking difficult decisions quickly, for example, segregating networks, disconnecting devices, suspending services and so on.

However, most cyber incidents of significant severity require intervention by national governments, at minimum to co-ordinate the actions of others and, in some cases, to step in at technical levels to assist in mitigation. A national cyber incident classification system enables states to mitigate national-level cyber incidents by allowing them to decide when to intervene, most obviously by deciding what counts as a national-level cyber incident. It also helps them to allocate responsibility to specific state entities and to pre-approve certain actions for particular classification levels. This enables state entities to know both who is responsible for acting and how they can act immediately, increasing the likelihood of swift and effective mitigation.

Goal 2: contribution to ongoing risk assessment including escalation, spread and recurrence

All serious incidents, including cyber ones, do not have clear-cut boundaries. Their effects unfold in complex sequences and spread over internal boundaries and international borders. Therefore, in addition to immediate mitigation, states must simultaneously make risk assessment decisions about the potential for further impacts, including:

- vertical escalation (to higher priority victims)
- horizontal spread (to other entities and states)
- recurrence (repeatedly compromising the same entities)

These risk assessments require an understanding of the threat actor, or "threat intelligence", and how their motivations and characteristics may lead to these different kinds of further impacts.[4]

4 ISO, *What is threat intelligence?* (Geneva: International Standards Organization, n.d.), **https://www.iso.org/information-security/threat-intelligence**

An example of such a national risk assessment is the "risk radar" system used in Switzerland (Figure 2 below).[5]

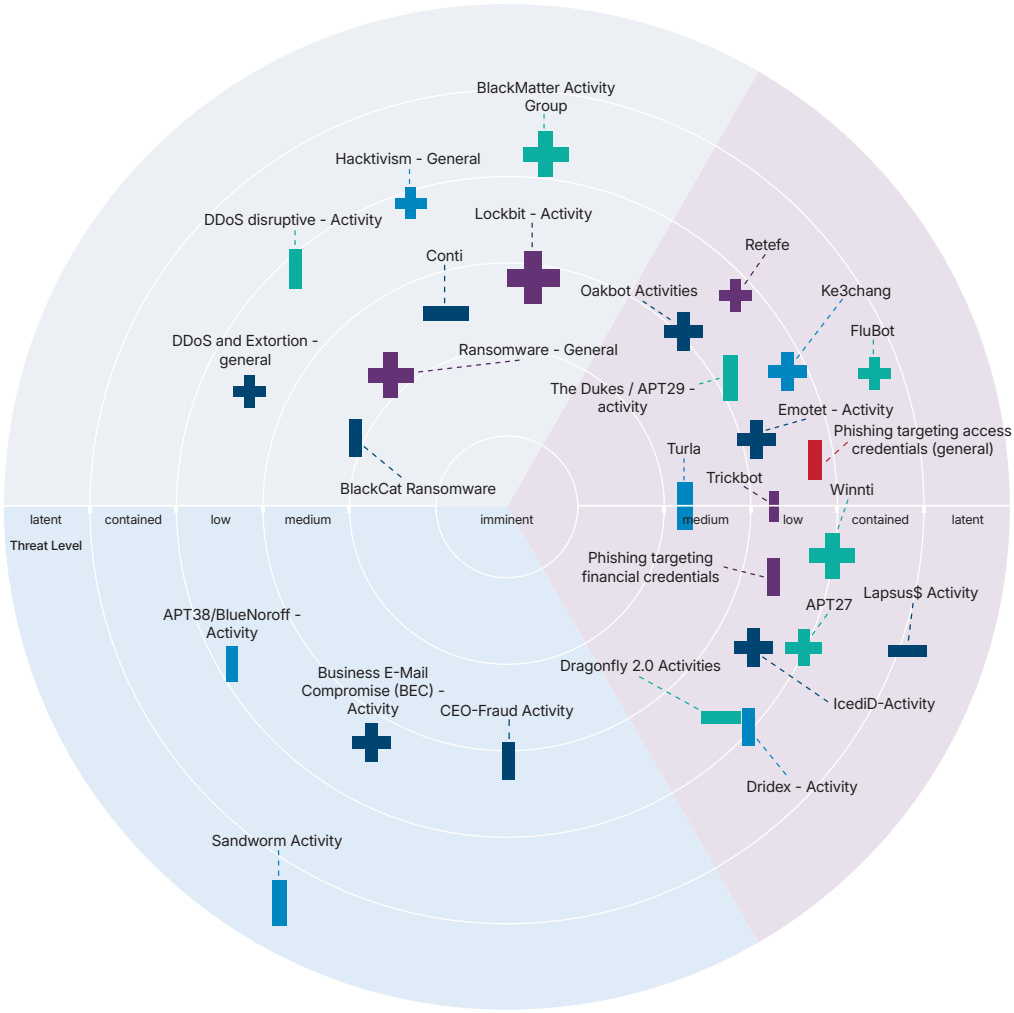


Figure 2: Sample risk radar used by the National Cyber Security Centre of Switzerland (ncsc.ch)

5 A risk radar is a methodology and tool used for identifying, managing, and analyzing risks within an organization. It provides a comprehensive view of an organization's risk profile, enabling better prioritization and action planning to mitigate potential threats. See e.g. L.F.C. Sperb and A. Marshall, The Risk Radar and the View of Risk (Southampton: Centre for Risk Research, Southampton Business School, University of Southampton, 2022). For a cyber-specific example, see Swisscom, Cybersecurity Threat Radar 2025: Cyber Resilience Despite Geopolitical Challenges (Bern: Swisscom, 2025), **https://www.swisscom.ch/en/about/news/2025/04/29-cybersecurity-threat-radar.html**

Therefore, a second goal of a national cyber incident classification system is to contribute to state and organizational risk assessments regarding future incidents or the activities of specific threat actors, helping them to prepare for and become more resilient against such threats, as well as acting to mitigate a specific incident (Goal 1).

Goal 3: greater national understanding of the causes of cyber incidents

While threat intelligence is important for risk assessment, many cyber incidents do not result from high-profile or sophisticated threat actors, rather, they result from accidental errors or technological failures. For example, data breaches with significant implications for national security can result from human error rather than adversarial compromise. Even incidents caused by malicious action are often enabled by standard security weaknesses with known solutions and clear recovery paths.

Therefore, it is useful for states to develop a national understanding of the causes and impacts of different kinds of cyber incidents. This understanding is distinct from both mitigation and risk assessment, as it helps states to develop actor-agnostic policies and practices to enhance cybersecurity across critical infrastructure and other sectors.

A national cyber incident classification system can contribute to this goal by cataloguing the most frequent types of incidents over a long period of time, as well as which attack vectors or vulnerabilities are involved in the most severe or impactful incidents. This understanding can either draw on direct incident reporting to the state (e.g., from critical infrastructure operators), or on aggregate reporting fed to state assessment bodies indirectly (e.g., by sectoral cybersecurity associations or regulators). Unlike the goals of mitigation or risk assessment above, this casual analysis can take place in slower time, with an emphasis on the rigour and reliability of the findings rather than swift action.

Goal 4: Standardization between and integration of cyber and non-cyber incidents

Nearly all states already have non-cyber crisis management and risk assessment structures in place for natural disasters, such as avalanches, earthquakes, floods and wildfires, as well as human-contributed crises, such as disease outbreaks and pandemics. Since crisis management officials may be less familiar with cyber incidents than with other kinds of events, one goal of a national cyber incident classification system could be to standardize responses to cyber and non-cyber events. This would contribute to the effective governance of and response to multiple independent crises since impact levels could be measured according to similar standards.

However, many incidents posing national-level risks are likely to be a mixture of cyber and non-cyber elements. For example, a cyber attack against a major supermarket chain occurring during a drought and an economic shock affecting the grocery sector. These three factors would combine to limit the availability of fresh produce in stores nationwide.

In such cases, standardizing cyber and non-cyber systems similar thresholds and categories is not sufficient. Instead, cyber incidents should be integrated into broader crisis management systems to enable effective responses to incidents with both cyber and non-cyber elements. This integration could have a range of potential modalities, from a joint task force to working groups aiming to align incident classification systems across sectors and identify how they can connect. These modalities are discussed in more detail in Step 2 on stakeholder engagement.

Goal 5: International co-operation including sharing national approaches to cyber incident classification

Due to the cross-border nature of cyber incidents, another goal of a national cyber incident classification system could be to facilitate bilateral or multilateral co-ordination of incident response. While such co-ordination will depend on wider multilateral relationships, developing and exchanging incident classification systems can help foster a shared language and terminology.

The information-sharing cycle

Information-sharing is at the heart of national cyber incident classification, because the purpose of such a system is to enable states to categorize cyber incidents according to a set of thresholds or similar criteria using all available information. This section only discusses information-sharing at a national level, as there are additional complexities when considering information-sharing at the international level. At the national level, it includes both information-sharing between government entities, and between government entities and non-government actors (discussed further in Step 2 below).

Information-sharing includes technical information about specific incidents, as well as strategic or contextual information about threat actors, vulnerabilities, or other trends (discussed further in Step 3). Information-sharing processes are typically represented as a cycle, as shown in Figure 3 below.[6]

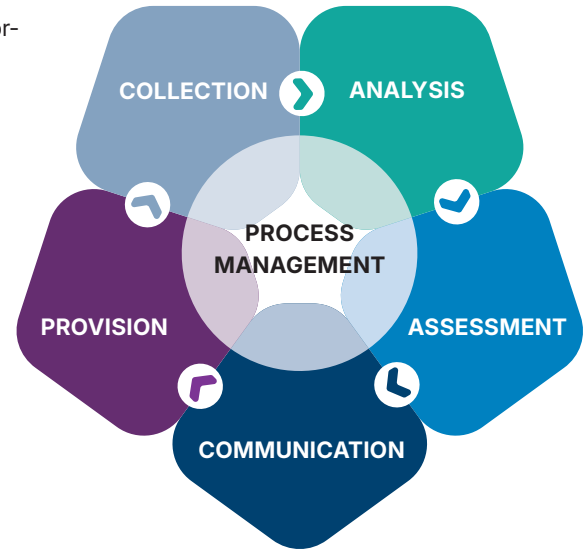


Figure 3: The information-sharing cycle

6 For an introduction, see World Economic Forum, *Cyber Information Sharing: Building Collective Security* (Geneva: WEF, 2020), **https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf**

Although most cybersecurity practitioners recognize the value of information-sharing, it can be limited due to a lack of trust between entities and/or restrictions on disseminating and handling information. For example, restrictions may be imposed by cybersecurity industry standards such as the Traffic Light Protocol (TLP).[7] While such restrictions must be respected — as demonstrated respect and the correct application of such restrictions contributes to the trust relationships that enable information-sharing — a national information-sharing community, like one around a national incident classification system, must overcome these obstacles. Step 3 below therefore discusses introducing suitable incentives for information-sharing.

Setting aside the obstacles to information-sharing, categorization through a national classification system enables further collection, analysis and assessment, as well as various actions based on the rapid communication of this categorization (discussed in the five common goals above). The cyclical nature of the above model implies that communication leads to further provision, thus starting the cycle again.

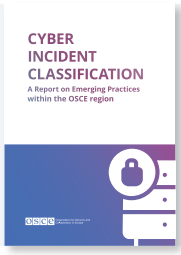
As we stress throughout this handbook, a national cyber incident classification system is an iterative process both within the classification of a specific incident, and in implementation and refinement of the system overall. This cycle model reflects that iterative approach.

Additionally, it is important to align the above information-sharing cycle with the goals of the national cyber incident classification system as identified in Step 1. If the information-sharing cycle does not accurately represent key goals for the national cyber incident classification system, states should modify it according to those goals and complete the stakeholder identification process discussed here for each element of their modified cycle. For example, a national cyber incident classification system focused on standardizing cyber and non-cyber processes (Goal 4) may include an additional step between analysis and assessment, rather than integrating into these steps.

7 First.org (2022), Traffic Light Protocol Version 2.0, **https://www.first.org/tlp/**

Recommendations from the good practice report

Three recommendations from the previous report are relevant to this section and will support states with selecting and prioritizing the various goals discussed here.



1. "The purpose of a NCICS is to generate a clear picture of the cyber threat landscape…" (Goal 3) "…and ensure a prompt response to cyber/ICT incidents and minimize the damage they cause." (Goal 1) "A NCICS supports national crisis management by providing a routine and consistent mechanism to objectively assess the risk of a cyber incident in the national context…" (Goal 2) "…in a timely manner, and detect possible gaps in existing defences."

8. "A standard approach to categorizing and prioritizing cyber incidents in accordance with their severity and scale is important for diagnosing an incident and relating the importance of the incident to its impact on a specific institution, entity or sector and its urgency, relative to the timing of the incident." (Goal 4) "Categorization speeds up the process of incident classification and creates greater efficiency within the process flow…" (Goal 1) "…while priority assignment can help ensure a common lexicon when an incident is being discussed, help determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement." (Goal 2) "Incident priority designation can help ensure a common lexicon when an incident is being discussed. It also helps determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement."

13. "Sharing national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident with other States can contribute to building confidence between States and help avoid potential misunderstandings that may emerge around cyber incidents and related response measures, thus contributing to regional and international security and stability." (Goal 5).

Illustrative example

Two states have created a National Cybersecurity Strategy that includes the development of a national incident classification system as a core element. In each state, the goals of the classification system flow from the broader national strategy goals.

State A

Given State A's focus is on internal government communication with senior decision-makers, the incident classification system has two main goals, in order of priority:

1. **Is there an emergency requiring an immediate response?**
2. **What is the overall risk level compared to other risks?**

The classification system should enable the National Cybersecurity Centre to quickly decide whether and where to intervene. To this end, the primary goal of the classification system is to provide sufficient information for these decisions. Consequently, State A decides to narrow the scope of the classification system, including only incidents affecting critical infrastructure in its main decision-making structures.

To conduct an overall risk assessment, State A also needs to be aware of the 'background noise', i.e. the sum of smaller, non-critical incidents that may affect critical infrastructure. However, this background noise, is a secondary priority to the immediate response, therefore State A decides to implement a less stringent data collection process for non-critical infrastructure incidents.

State B

Given that State B emphasizes enabling and empowering other actors as well as taking action itself, it has identified very similar aims but placed them in the reverse order of priority:

1. **What cyber incidents are occurring within critical infrastructure and the wider economy?**

2. **Are there any incidents requiring intervention by the National Computer Security Incident Response Team (CSIRT)?**

To answer the first question, the incident classification system in State B must incorporate all nationwide incidents to a certain degree and with greater precision and timeliness than State A's system. However, this wider scope comes with a trade-off, as reporting structures accommodating all kinds of organizations cannot aim for the same level of detail and reliability as would be expected of critical infrastructure operators. Therefore, State B has developed a two-tier system in which incident reporting is mandatory for critical infrastructure operators and voluntary for all others, including the general public.

Step
02

Engage stakeholders

Once a state has defined the goals of their cyber incident classification system, the next step is to engage all relevant stakeholders. Involving a wide range of stakeholders is generally valuable as they bring expertise and authority from across different sectors together, offering contrasting perspectives that contribute to utility and legitimacy.

For cybersecurity information-sharing in particular, many key sources of information lie in the private sector or civil society, and involving these stakeholders helps states be aware of all relevant incidents and make accurate assessments of those incidents. Since information-sharing is central to cyber incident classification, this section focuses on how to identify and connect stakeholders for optimal information-sharing, as well as modalities for stakeholder engagement.

KEY ACTIONS

- **Nominate a lead authority** from within government **for each element of the information-sharing cycle**, including for the overall management of the cycle
- **Identify all other stakeholders** for each element across public and private sectors
- **Define the relationships between stakeholders** for each element

The first task of stakeholder engagement is to nominate a lead authority for each stage of the information-sharing cycle, including its overall management, which should be a government entity. It is likely to be the national cybersecurity authority or centre, which naturally hosts/houses the national cyber incident classification system and is therefore well positioned to manage the information-sharing cycle overall and its individual elements. Such an entity is also likely to contain the national CSIRT, which fulfills key functions within the information-sharing cycle.

However, depending on their national governance structure, states may choose to nominate other government entities to lead specific elements of the cycle. For example, sectoral regulators can work closely with critical infrastructure entities to collect information according to sectoral regulation and policy, and therefore may be better suited to co-ordinate the provision and/or collection elements of the cycle. This option adds an extra step, as the national authority would then become an indirect recipient of (potentially redacted or aggregated) information from sectoral regulators. While this arrangement could create efficiencies by eliminating the need for the national authority to possess the sector-specific expertise required to assess detailed information from all sectors, it could also lead to longer lead times for assessment. This is because the national authority may need to communicate individually with multiple sectoral entities to ensure it has all relevant information.

Another example is choosing a security or intelligence agency to lead the analysis and/or assessment elements of the information-sharing cycle.

Since these elements may draw on sensitive sources of information to complement those provided by critical infrastructure operators or open sources, a security or intelligence agency may be a good candidate to lead on these elements. In such a scenario, however, that agency might need to adjust its internal culture to facilitate effective communication about these sources within and outside the government. Alternatively, the agency could second individuals to the national cybersecurity centre to provide intelligence to the classification process.

Regardless of which government entity is selected to lead each element, states should specify responsibilities within that entity, even at the team and individual analyst levels. For example, if the national cybersecurity agency is designated as lead authority for analysis, which team will analyze the information from a particular critical infrastructure sector? Do they have the necessary knowledge to provide an informed assessment? How is this team structured to work with and learn from sector-specific bodies, such as regulators? How do they recruit and retain relevant expertise? Asking such questions will not only help locate key individuals and teams, but also help clarify the underlying logic behind state allocation of lead authorities for each element.

After the government entity that will act as lead authority for each element of the cycle is nominated, the next task is to identify all the other relevant stakeholders for each element (as presented in Figure 4).

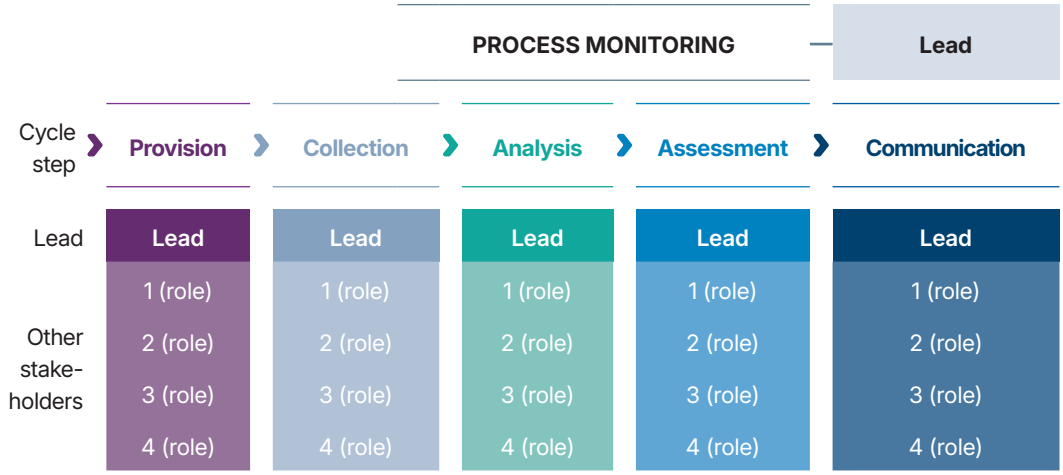


Figure 4: Stakeholder identification for each element of the information cycle

The appropriate method for identifying stakeholders will vary according to the domestic political context. States should select the method that best suits the desired stakeholder input and existing stakeholder engagement practices.

On one end of the spectrum, states may conduct consultations based on proposed principles or standard operating procedures (SOP) with minimal ongoing relationship-building and maximized openness and transparency. Such consultations should have clear and feasible deadlines for responses, open response submission and publication of replies to those responses. To ensure a wide range of submissions, states should also advertise the consultation in relevant forums and via suitable channels (e.g. social media).

On the other end of the spectrum, states may select individuals to serve on an advisory board, participate in workshops or join focus groups to provide advice on the overall system or particular aspects of it. Depending on the selection process for participation and the extent of public access to reports about group deliberations or activities, this approach may be less open and transparent. However, it provides states with the opportunity to develop trusted relationships with representatives of the private sector and civil society, allowing them to intervene at a more detailed level via ongoing dialogue, with potentially more useful input as a result.

Some of the relevant stakeholders will be obvious across all modalities of stakeholder engagement, for example, critical infrastructure operators. However, states should also aim to identify additional stakeholders beyond the obvious ones. For example, do specific cybersecurity companies provide threat intelligence feeds to multiple critical infrastructure operators? Do operators in a specific sector all use the same intrusion detection system/intrusion prevention system (IDS/IPS)? If so, then those commercial actors could be key stakeholders for information provision — if, as discussed in the following section, states can develop an appropriate legal and contractual basis for sharing client information.

The following table (Table 2) provides a list of sample non-government stakeholders in a national cyber incident classification system, across all elements of the information-sharing cycle. This list is not exhaustive but designed to give readers a sense of the breadth of potential stakeholder engagement needed for a comprehensive incident classification system.

Stakeholder	Sector (public/private/other)	Likely role in cycle elements
Critical infrastructure operators	Public/private	Provision, Collection
Threat intelligence vendors	Private	Provision, Analysis
Cybersecurity product/service vendors	Private	Provision
Incident responders	Public/private	Collection, Analysis, Assessment
IT/OT product/service vendors	Private	Provision
Business service providers (e.g. HR)	Private	Provision
Legal services	Private	Provision, Assessment, Communication
Security researchers	Private/Other	Provision, Collection, Analysis, Assessment
Media organizations	Private/Other	Communication
Academia (e.g. university research departments)	Other	Provision, Analysis, Assessment, Communication
Civil society organizations (e.g. think tanks)	Other	Assessment, Communication
Individual citizens	Other	Provision

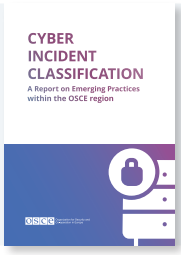
Table 2: Sample non-government stakeholder list

When identifying stakeholders, states should be aware of potential overlaps and duplication of roles and responsibilities among stakeholders for each element, as indicated in the above table. Such overlaps are not necessarily negative, as they can indicate helpful redundancy in the system. However, the lead authority for each element should be prepared to co-ordinate between stakeholders whose roles overlap to ensure the cycle flows smoothly.

Finally, it is important to note that stakeholders, especially those from the private sector or civil society, could provide expert or alternative perspectives on the overall objectives of the system, as well as contribute to effective information-sharing. If so, Step 2 can be approached iteratively with Step 1 above: set goals, test those goals with selected stakeholders, adjust them, test again, etc.

Recommendations from the good practice report

This step of the handbook is connected to the following report recommendations:



4. "Establishing clear criteria to determine the stakeholders or constituencies that a national cyber incident classification will serve, including how critical they are to society and economy requires serious consideration. The approach should be flexible enough to accommodate new stakeholders and constituents as the threat landscape changes."

7. "Cyber incident classification is generally a centralized process co-ordinated by a central entity or authority and involving a range of government bodies. Depending on the context, it may also include essential or important services/critical infrastructure asset owners or operators, digital service providers and other private sector entities."

11. "Engagement of relevant stakeholders and constituencies in the development of the classification system can contribute to building trust between public and private actors and within and across sectors and services."

Illustrative example

The two states now identify key stakeholders for their national cyber incident classification system that are aligned with its overall goals and those of their national cybersecurity strategy.

State A

Given State A's centralized approach to government, decision-making is hierarchical. The National Cybersecurity Centre maintains direct relationships with each critical infrastructure operator and communicates clear expectations to them. The most important stakeholders in these relationships are the relevant security teams and compliance officers.

This hierarchical structure generally means that the flow of information to these stakeholders is bidirectional, going from the National Cybersecurity Centre to critical infrastructure operators. This information flow is valuable because it shares operational and actionable information about specific cybersecurity threats, as well as broader updates on the landscape and new technological or policy developments (e.g., through annual online meetings).

State A maintains fairly stringent standards for critical infrastructure operators. These standards are developed with relevant specialists from the private sector and academia, focusing on efficient implementation — i.e., cybersecurity requirements should not create an undue burden. During a crisis warranting government intervention, the national CSIRT collaborates directly with the affected organization.

State B

Unlike State A, State B takes a community-focused approach. Organizations across the national economy collaborate within sector-based Information-sharing and Analysis Centres (ISACs), which then communicate with the National Cybersecurity Centre. Additionally, State B runs an information exchange platform that is open to all critical infrastructure operators and other relevant organizations. These operators also have regular access to State B's updated national risk radar, including through weekly video conferences.

In this way, the flow of information in State B is bidirectional, with as much information going towards the National Cybersecurity Centre from ISACs and the platform as goes towards organizations. However, while operational, day-to-day information is shared through the ISACs, in an emergency, the national CSIRT attempts to provide direct assistance.

Additionally, Small and Medium-sized Enterprises (SMEs) and citizens can report incidents via an online platform. They are then directed to the relevant organizations for assistance, which is often provided by law enforcement, provincial authorities, or relevant non-profit organizations. To improve broader societal cybersecurity, the National Cybersecurity Centre operates a web portal that publishes information on current risks and self-help resources. Finally, State B organizes an annual event open to all members in the national cyber security community, including non-profits and SMEs. The National Cybersecurity Centre regularly seeks feedback from its constituents.

Step
03

Establish reporting pathways

Establishing appropriate reporting pathways is absolutely essential for a successful national cyber incident classification system. These reporting pathways facilitate the provision and collection elements of the above information cycle. Consequently, these pathways should include incentives to reward information-sharing as well as regulatory or legal mechanisms to compel relevant stakeholders to share information when necessary.

This step should occur in tandem with the below Step 4 on "Building on Existing Structures" and iterate between the two to find the right balance between transposing or expanding existing information-sharing initiatives and ensuring that information-sharing for a national cyber incident classification system accommodates the unique characteristics of cyber incidents.

KEY ACTIONS

- Identify **achievable and appropriate incentives** for information-sharing
- Develop **standard templates and formats** for information-sharing
- Develop **reasonable timelines** for stakeholders to share information
- Specify **how information shared will be used** and by whom

Many states have introduced or are introducing mandatory cybersecurity reporting requirements for some sectors, such as government organizations or critical infrastructure operators — although the introduction of mandatory reporting is ultimately a national decision. In such cases, states have additional leverage to persuade these stakeholders to provide information relevant to a national cyber incident classification system. However, states should not rely solely on this leverage in mandatory reporting contexts, because without appropriate incentives entities with mandatory reporting requirements may look for ways to avoid or minimize these requirements, or conduct "tick-box" exercises simply to fulfil requirements without meaningfully contributing to national cyber incident classification.

Instead, states should develop a national cyber incident classification system that identifies achievable and appropriate incentives for information-sharing, altering the decision calculus of key stakeholders, leading them to conclude that transparent sharing of meaningful, relevant information is in their interests as well as those of the national cyber incident classification system.

The following table suggest some sample incentives:

Sample state-provided incentives for information-sharing		
Recipient	*What this incentive involves*	*Why this incentive works*
Critical infrastructure operators	The national cybersecurity centre or similar entity could provide **incident response assistance** to participating organizations if affected by a cyber incident.	Participating organizations are more likely to share information if they can lower the cost or improve the speed of mitigating incidents by drawing on national resources.
Critical infrastructure operators	Sector regulators could develop **streamlined regulatory processes** (e.g., on cybersecurity audits) for participating organizations.	Participating organizations are more likely to share information if they can benefit from less intensive regulatory compliance procedures.
Government entities	The national cybersecurity centre, or a similar entity, could provide participating government entities **with enhanced cybersecurity protection**.	Participating government entities are more likely to share information if they can benefit from more rigorous cybersecurity defences.

Table 3: Sample incentives for information-sharing

Beyond government and critical infrastructure operators, states may wish to include other organizations as well as individual citizens in the reporting pathways of their national classification system. The advantage of widening reporting pathways in this way is to capture the constant background of low level malicious cyber activity, where each individual incident causes little damage and does not meet national severity thresholds, but cumulatively can meet those thresholds. For example, individuals could report phishing URLs or scam numbers to a government fraud information website and receive advice on how to respond in return. Additionally, States may also seek larger aggregate data on fraud trends from law enforcement agencies.

Once the appropriate incentives are in place, the next task is to simplify and streamline the information-sharing process. States should develop standard templates or forms for relevant entities to submit information, with a minimum of compulsory fields and optional additional information. The following table provides suggested fields, with the first four (white background) essential for any national cyber incident classification system and the following five (grey background) desirable in a more comprehensive national cyber incident classification system. As this table shows, there is a trade-off between the amount of information shared and the ease of sharing, particularly for entities with limited capacity. Any entity should be able to fill out the first four fields,

but fewer will be able to fill out the last five, especially given limited time. An example of this of format, as used by Switzerland, is provided in Annex 2.

Field name	Type of field	Compulsory or optional
Date and time incident started	Date/time	Optional
Date and time incident was detected	Date/time	Compulsory
Is the incident ongoing?	Yes/no	Compulsory
Type of incident	Select options	Compulsory
Onward distribution conditions (e.g. TLP)	Select options	Compulsory
Relevant vulnerabilities and severity (e.g. using CVE number and CVSS score)	Set fields	Optional
Tactics, techniques, procedures or TTPs (e.g. using frameworks like MITRE ATT&CK[8])	Set fields	Optional
Indicators of compromise (IOCs)	Text/file upload	Optional
Detection rules	Text/file upload	Optional
Structured threat intelligence (e.g. MISP object)	Link or file upload	Optional

Table 4: Suggested reporting template

8 MITRE ATT&CK Matrix for Enterprise: **https://attack.mitre.org/**

After developing formats and templates, the next task is to establish timelines for information-sharing. For the provision and collection elements of the information-sharing cycle, most states will look to collect information about an incident within a short timeframe after detection (e.g., 24 hours), to enable a rapid assessment and response. This timeframe could be built into critical infrastructure regulation, however, as discussed above, even if this is mandated, incentives must be in place to ensure compliance.

The European Union's (EU) Network and Information Security (NIS) and NIS2 directives are a useful example of how reporting requirements can evolve over time.[9] Under the NIS, adopted by EU Member states in 2016, operators of essential services in seven sectors were required to report incidents with a "substantial impact" on service provision, as defined by each Member State individually, with no mandatory deadline for reporting. In contrast, the NIS2 directive, adopted in 2023, requires essential and important entities in 16 sectors to report a "significant" incident (defined within the directive as primarily based on people impacted, duration and geographic spread) within 24 hours, with further information within 72 hours and a final report within a month.

The information-sharing timeline should also cover the other elements of the information-sharing cycle, including analysis and assessment (i.e., how long information providers should expect responsible authorities to take in categorizing an incident based on their information) and ultimately communication: by when will the initial categorization decision be made and who will be informed? As the form above demonstrates, timelines should allow providers to update information or share additional information as the incident progresses and as their knowledge and understanding of the incident improves.

Finally, a sound legal and policy basis should cover all elements of the information-sharing cycle. This includes specifying how information-sharing will ultimately be used to mitigate and categorize an incident. The following checklist provides states with a list of suggested ways to establish this legal and policy basis, including overall mandates and specific reporting policies and regulations. Perhaps the most important item in this checklist is the last one, which requires legal limits on national cyber incident classification system owners to not use shared information for purposes beyond those of the system. This item enables sharers to trust the system, because they know the information will not be used for other purposes, such as being shared with competitors or to monitor other non-cybersecurity regulations.

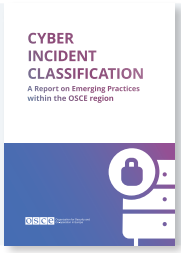
9 European Union, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems* (Brussels: EU, 2016); European Union, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity* (Brussels: EU, 2022).

Checklist for sound legal and policy basis
Statutory mandate for setting up a national cyber incident classification system in the appropriate cybersecurity or critical infrastructure legislation and strategic documents.
Legal requirement for critical infrastructure operators to collect relevant information (e.g., in critical infrastructure cybersecurity law or similar)
Policy guidance for appropriate information-sharing (timelines and format) and consequences of not sharing within these parameters (can be included in contracts for privatized critical infrastructure operators)
Legal and policy specification of incentives for information-sharing
Appropriate provision in data protection law for sharing, especially regarding sensitive or personal information
Contractual agreement with suppliers/services to critical infrastructure operators, permitting sharing of their information with national government for incident classification
Legal limits on responsible national cyber incident classification system owners not to use shared information for purposes beyond national cyber incident classification system, including data protection and handling requirements

Table 5: Checklist for sound legal and policy basis

Recommendations from the good practice report

This step of the handbook is connected to the following report recommendations:



3. "A sound policy and/or legal base for cyber incident classification is critical to ensuring its effectiveness as well as its sustainability. Introducing clear provisions on overall responsibility for the system, interagency co-operation, reporting and notification requirements and procedures, data-handling procedures, resource allocation and review procedures are equally important."

5. "Uniform and consistent reporting on incidents is critical to the effectiveness of cyber incident classification systems and helps determine the nature of the response. In some jurisdictions and depending on the severity of an incident and the entity affected, incident reporting is legally required."

Illustrative example

The two states have now implemented different reporting structures for their incident classification system. While both include mandatory reporting for critical infrastructure operators, other aspects of the reporting structure differ significantly.

State A

State A's mandatory reporting for critical infrastructure operators includes clear guidelines on what constitutes an incident that needs to be reported. Thresholds in these guidelines typically relate to qualitative and quantitative criteria such as the number of affected users, loss of personally identifiable information, or length of outages. The National Cybersecurity Centre operates a 24/7 hotline and maintains a POC directory which is tested biannually. Failure to report an incident may result in severe fines and critical infrastructure operators are expected to implement an alternative reporting system in case of failure or compromise of the default system.

Incidents must be reported via a web application within 12 hours and reports are filed using the ENISA Reference Incident Classification Taxonomy.[10] Within the same timeframe, the national CSIRT decides whether to provide support. Once an incident has been filed, the National Cybersecurity Centre expects to receive daily updates. Incident reports and updates are not confidential and may be shared across government where necessary. To classify incidents, State A uses a traditional 1–5 severity scale and attempts to align damage and cost assessments to existing schemas from other areas.

10 ENISA, *Reference Incident Classification Taxonomy: Task Force Status and Way Forward* (Heraklion: European Union Agency for Network and Information Security, 2018), **https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy**

State B

In State B, the national CISRT has collaborated with its constituents to develop an effective reporting scheme. The timeframes are longer than those in State A: 24 hours for the initial report and 72 hours for an updated assessment. Once a report has been filed, critical infrastructure operators can choose to receive support from the national CSIRT. As in State A, the incident classification system defines reporting thresholds. Unlike State A, the National Cybersecurity Centre treats reported incidents as confidential unless otherwise required by law. In addition, State B emphasizes that incidents will only be reported in an anonymized and aggregated form to regulators, in order to maximize trust.

In State B, non-critical organizations can also report incidents, but are not eligible for support. If resources permit, the national CISRT can assist, which has contributed to building its reputation as a trusted partner in the wider security community. The National Cybersecurity Centre also collaborates with security researchers who report incidents and vulnerabilities. State B also opted for a 1-5 severity scale to classify incidents. However, rather than prioritizing alignment with non-cyber schemas, it attempted to assign these levels to categories of incidents (e.g. DDoS or malware) from a defined catalogue and map them per sector, creating a detailed picture.

Build on existing structures

National cyber incident classification systems are likely to overlap with existing structures. This step explores how states can build on existing structures develop a national cyber incident classification system as efficient as possible and avoid conflict with those structures.

As with the previous step, this step should be pursued iteratively with Step 3 as many of the key ingredients of a national cyber incident classification system — especially the sound legal and policy basis — will stem from other places, but will need to be amended where necessary. This section also revisits the central question of scope, especially regarding the relationship between critical infrastructure organizations and other entities, and between cyber and non-cyber assessment structures.

KEY ACTIONS

- Review **national cybersecurity laws and policies**, especially those related to critical infrastructure sectors
- Compare and align the national cyber incident classification system with **relevant non-cyber crisis management systems**
- Identify opportunities to expand **sector-specific initiatives** to the national level

The starting point for building on existing structures is a clear understanding of the scope of a national cyber incident classification system. So far, this handbook has assumed that such a system would focus on government entities and critical infrastructure operators, recognizing that terminology around critical infrastructure varies significantly (critical information infrastructure, ICT-enabled critical infrastructure, essential services/functions, critical activities, etc.).[11] The exact sectors included in national definitions of critical infrastructure or associated terms also vary, as does the extent to which suppliers to those sectors — especially SMEs, open-source communities, or international suppliers — are included within those sectoral boundaries. Consequently, the question of which existing structures are relevant for the national cyber incident classification system depends on its scope, which in turn depends on its goals, as illustrated in Figure 5.

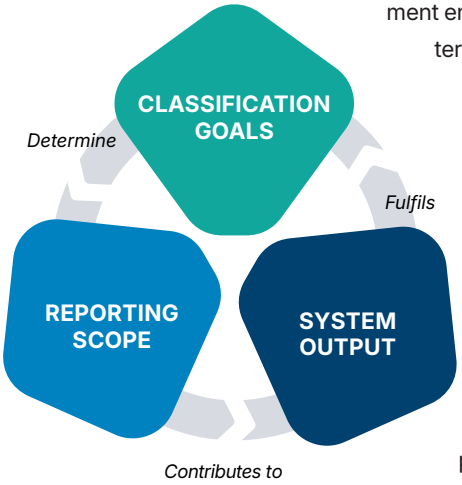


Figure 5: Relationship between classification goals, output and scope

One simple way to address this interdependence is to examine how critical infrastructure is treated in existing non-cyber structures. If non-cyber crisis management structures operate within sectoral boundaries (e.g., managing a national water incident or national electricity outage with separate crisis management procedures), then the national cyber incident classification system could build on a combination of existing sectoral schemes for

11 For further details on terminology see the initiatives undertaken under OSCE CBM 9 (**https://cbm9.gov.rs/**). In CBM 15, the OSCE participating States refer to "ICT-enabled critical infrastructure".

non-cyber events. On the other hand, if there is a single national (non-cyber) crisis management structure treats impacts on different sectors cumulatively (i.e., the number of sectors affected is a factor in the categorization of an event), then this existing structure could be a useful model for the national cyber incident classification system. As noted in Step 1 (Goal 4), in both cases, a national cyber incident classification system could borrow and integrate with existing non-cyber structures to accommodate combined cyber/non-cyber events.

After identifying which existing structures are relevant, the next step is to examine each critical infrastructure sector in more detail, especially for cybersecurity-specific structures that enable information-sharing within that sector. Figure 6 identifies three such structures: mandatory reporting, security standards and incident taxonomies. Each of these structures can be adapted and developed into a national cyber incident classification system; for example, by using incident taxonomies as the basis for the national cyber incident classification system reporting form, or using security standards to estimate realistic timelines and level of detail for reporting.

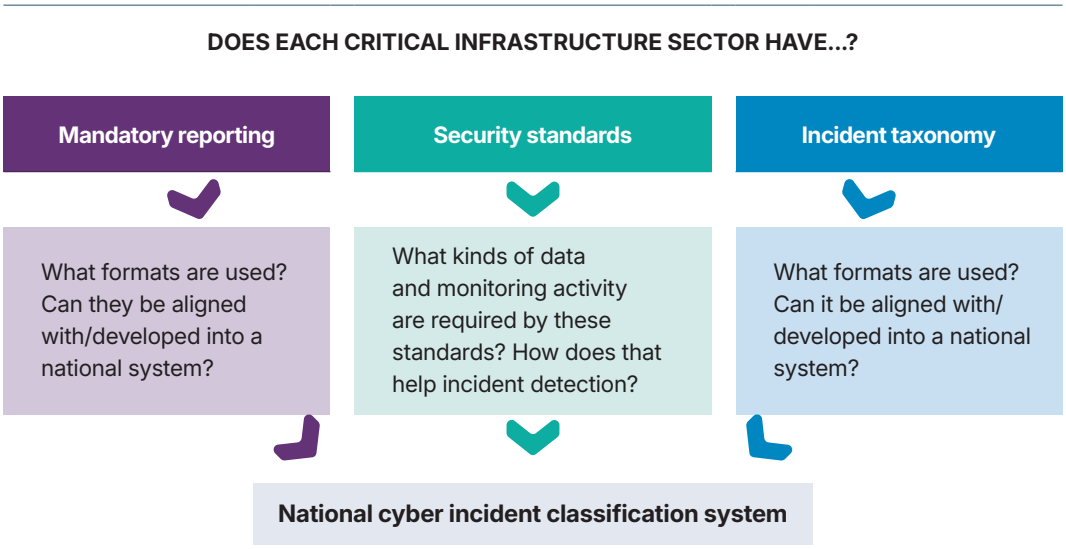
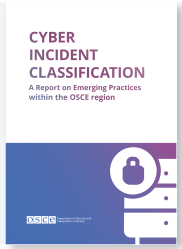


Figure 6: Building on existing structures

However, there are two main challenges in drawing on sector-specific processes, which states should be aware of and proactively address. The first challenge is ensuring that processes developed for one sector function equally well in other sectors. The second challenge is stakeholder management, ensuring that a national cyber incident classification system built on sector-specific indicators obtains sufficient buy-in from other sectors that may perceive a lack of objectivity in design.

Recommendation from the good practice report

This step of the handbook is connected to the following report recommendation:



2. "Cyber incident classification systems are generally anchored in national policy and other relevant frameworks and often flow from or are anchored in national legislation."

Illustrative example

The two states already had existing structures stemming from sector-specific regulators that required the reporting of certain incidents. However, this was not the case for all sectors, particularly those with little or no regulation, such as logistics. Both states therefore devoted time to optimizing existing resources and establishing a legal basis for their reporting requirements.

State A

When developing its cyber incident classification system, State A consulted with all regulatory authorities that were already reporting to a central government authority. It also consulted extensively with other government agencies that already had reporting requirements. After identifying gaps and discrepancies, State A standardized reporting requirements to make shared information comparable.

Initially, State A planned to create a central government reporting portal for all types of incidents, whether cyber-related or not. However, this was not feasible as different types of reporting often required different stakeholders. Nevertheless, the government ensured that there would be no double reporting requirements.

State B

Rather than beginning by consulting other government agencies and regulators, State B initially collaborated with critical infrastructure sector representatives to identify existing reporting schemes and explore ways to expand or repurpose them. It acknowledged its constituents' reluctance toward mandatory reporting, recognizing that unpopular requirements would lead to poor data quality.

Similarly, the National Cybersecurity Centre collaborated with sectors that had no existing reporting requirements to understand how the national classification system could apply to and be useful for them as well. A new legal basis was required for State B to process voluntary reports from non-critical organizations.

Most of the work involved in extending the incident classification system in this way was identifying meaningful thresholds that would warrant a report, as different organizations had varying interpretations of what constitutes 'important'. For example, the National Cybersecurity Centre would not consider important 1,000 customers being offline due to a broken fibre, but a small internet service provider (ISP) would. Conversely, 500 malware-infected endpoints may seem like a relatively insignificant issue to an ISP, but could be crucial information for the National Cybersecurity Centre. Extended dialogue between stakeholders led to increased understanding of each other's' perspectives and definitions that worked sufficiently for all parties.

Step
05

Implement the system

This step moves from design to implementation. All the key ingredients should now be in place, with responsible authorities and key stakeholders across all elements of the information-sharing cycle and appropriate connections with other national incident classification systems, as well as narrower, sector-level cybersecurity reporting processes.

However, as with all complex projects, a national cyber incident classification system requires extensive and thorough testing before launch. The transition from design to implementation should therefore focus on three things: testing, communications and stakeholder management, which are addressed in this section.

KEY ACTIONS:

- **Thoroughly test all stages of the information cycle**, especially through exercises
- Develop **clear communication around the launch** schedule and responsibilities
- **Introduce a grace period** for operations if necessary

Most states have experience in conducting national cybersecurity drills and exercises and many have also participated in bilateral or international exercises, including with intergovernmental organizations. These exercises are designed to ensure that the particular state structures involved function as intended in situations approximating real-life crises. Such exercises can vary in scope from simple table-top, paper-based scenarios to multi-stage and multi-track scenarios involving live injections and realistic multimedia components.

For states who hold such exercises regularly, the easiest way to test a national cyber incident classification system as a whole is to integrate it into these exercises.

For example, states could design a scenario where incident classification is key to the scenario response, and include key national cyber incident classification system stakeholders in the exercises itself. In contrast, states without a regular exercise rhythm may wish to use their development of a national cyber incident classification system as the impetus to start national cybersecurity exercises. In such cases, stakeholders of the national cyber incident classification system are a natural starting point for exercise attendees and scenarios can centre on key decisions made in the national cyber incident classification system process, their considerations and impacts. In both above-mentioned cases, exercises should incorporate anomalies and edge cases to thoroughly understand the limits of the national cyber incident classification system.

However, before incorporating a national cyber incident classification system into national exercises, each component should be tested, individually and in all relevant combinations. Here, exercises can focus on different elements of the information-sharing cycle, first combining provision and collection, analysis and assessment, with communications as a separate element (Figure 7). Only then should the entire system be tested as a whole, focusing on the combination of all elements and overall process management.

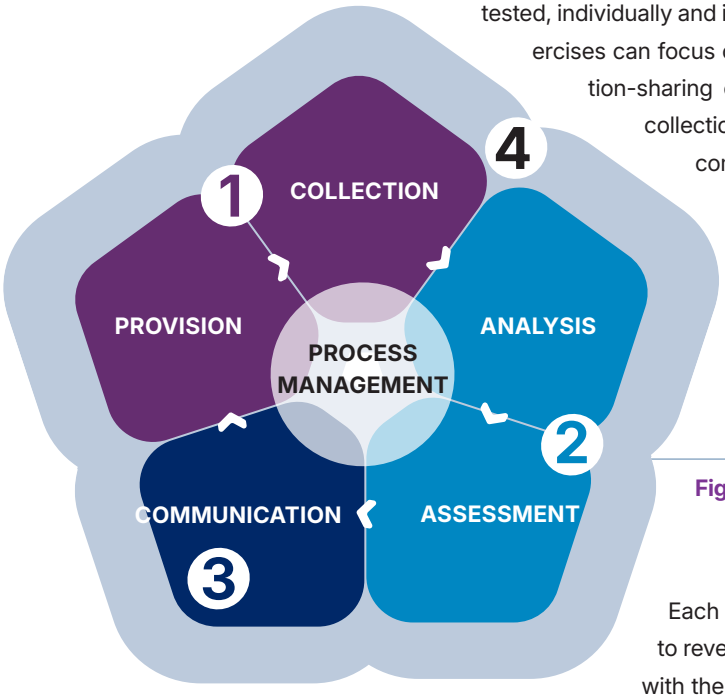


Figure 7: Exercise sequencing for implementation

Each of these exercises and tests are likely to reveal unanticipated challenges or issues with the national cyber incident classification system. During implementation, states should therefore ensure that they allocate sufficient time for a series of exercises of increasing complexity and realism, and for troubleshooting and resolving issue between each exercise. Throughout the process, the implementing parties should on including all stakeholders in the exercises and troubleshooting; for example, to develop a reporting infrastructure in the first two cycle elements that is as customer-friendly as possible. During the testing phase, states should produce detailed and accessible guidance for all stakeholders on using and interacting with the national cyber incident classification system. This guidance can then be repurposed for live use at launch.

At launch, states have two major considerations (setting aside the functioning of the system itself, which we assume has been thoroughly tested). The first consideration is communications, especially with external entities — both national and international — who are likely to have limited awareness of the national cyber incident classification system or its development.

When the output of the national cyber incident classification system is public, then external entities may use the output of the classification system to inform their own assessments and actions. However, if these external entities are not sufficiently aware of the assessment processes underlying any public output, including the definition of key terms, then their misunderstanding or misinterpretation of the public output could lead to undesirable consequences. For example, external entities over- or under-estimating the impact of an ongoing cyber incident classified by the national system. To avoid this outcome, states should ensure that any public output from their classification system is accompanied by suitable context and explanatory materials, including definition of key terms.

The second consideration is internal: ensuring that all stakeholders are comfortable with the launch schedule and, if necessary, making use of gradual phase-ins across sectors or grace periods for reporting. Figure 8 incorporates these considerations into the overall development process for a national cyber incident classification system, culminating in its implementation and launch.

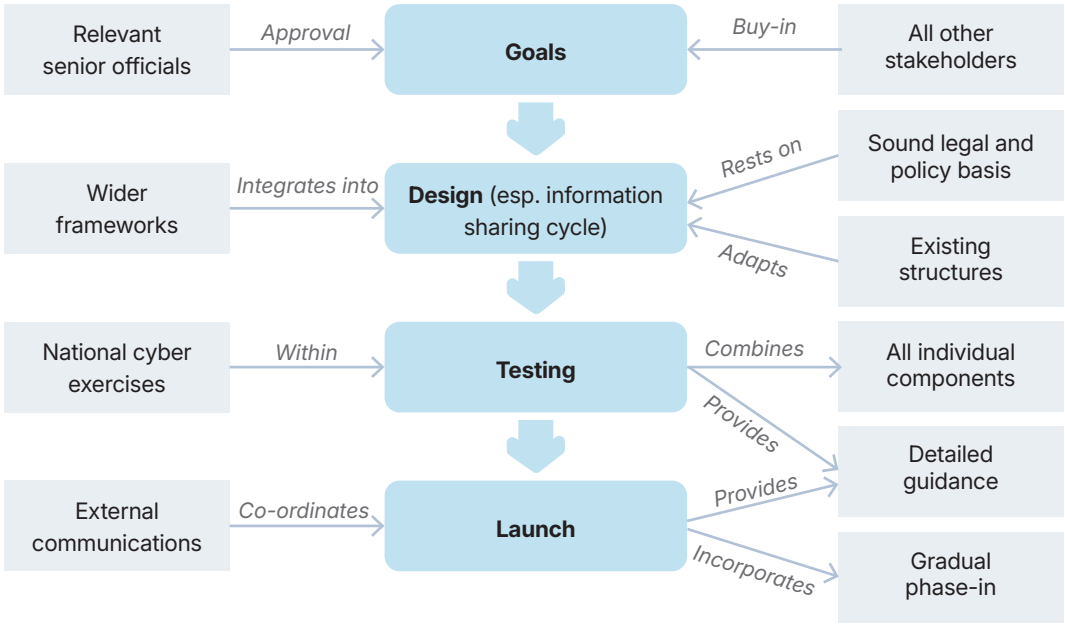
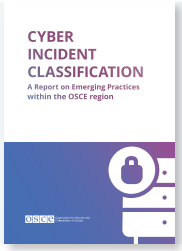


Figure 8: Flowchart for launch of the classification system

Recommendations from the good practice report

This step of the handbook is connected to the following report recommendations:



6. "Clearly articulated guidance contributes to the effective implementation and socialization of a cyber incident classification system. Such guidance can specify: the purpose of the cyber incident classification system and its policy and/or legal basis; who co-ordinates its development and implementation; its scope/coverage in terms of its key stakeholders/constituencies; definitions and explanations of categories and priorities; the response mechanisms for incidents, including an explanation of what would activate a specific classification, which organization responds and what actions they would take; and how regularly the incident classification system is reviewed and what the review process entails."

10. "Continuous political commitment, skilled personnel, including a dedicated incident response entity or team with sound expertise in both general and cyber crisis management, and adequate and stable budgets are critical to the development and management of cyber incident classification systems."

12. "It is important to establish protocols that determine how to proceed when challenges relevant to categorization of incidents are encountered."

Illustrative example

The two states have now tested all aspects of their incident classification system thoroughly before launching. While these tests were focused on achieving the divergent goals of each system, both states engaged key stakeholders in the testing phase and continued this engagement after launch.

State A

State A drew on its extensive experience in testing and implementing incident classification systems in other sectors. Before launching the system, it tested the overall scheme and the separate data processing steps involved, including the application of thresholds and the core 1-5 categories. In a second stage, the National Cybersecurity Centre invited select critical infrastructure operators to review past events against the classification system, using the data to further check all the elements of the analysis pipeline.

This compartmentalized testing proved to be crucial, as mapping to existing severity scales was not straightforward. To align with these scales, a core aspect of State A's approach, State A also tested the cyber incident classification system as part of a wider national incident risk assessment mechanism, including through a joint cyber/physical scenario exercise.

State B

Similarly, State B began testing with its constituents well before reporting became mandatory. Participating organizations reported incidents and received risk radars tailored to their sectors and organizational characteristics in return (see Figure 9 below).

Over time, the analysis was refined. The National Cybersecurity Centre started with the more mature sectors, such as finance and telecoms. Although time-consuming, the process proved valuable when reporting became mandatory after an agreed-upon grace period. A phased and carefully communicated implementation ultimately meant that, by the time the system went live, processes were already in place, leading to acceptance of the new obligations.

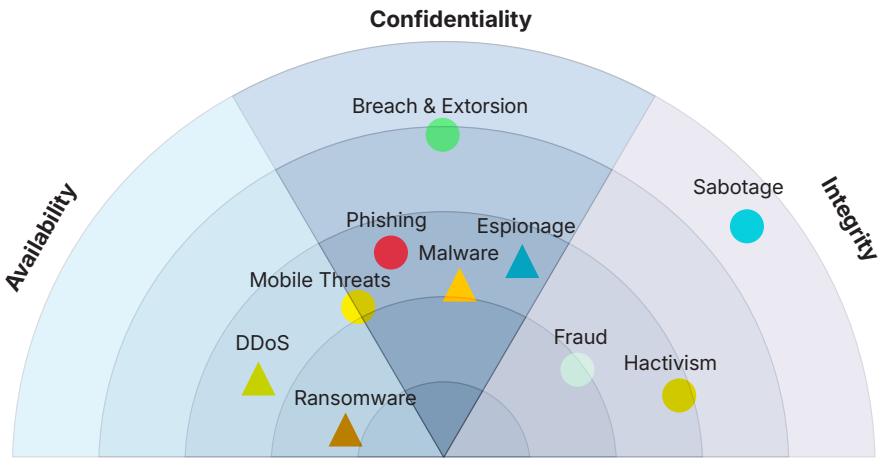


Figure 9: Fictitious risk radar used by State B

Refine the system

Now that the national cyber incident classification system is up and running, this step addresses one of the main challenges noted in the OSCE good practice report: it is an iterative process, requiring continual refinement and adjustment based on feedback and changing circumstances. This section first discusses the basis for refinement, centred on key indicators of success and then moves on to lessons learned.

KEY ACTIONS

- Translate **high-level goals into key indicators** agreed upon by the relevant stakeholders
- Measure **success against these indicators,** ideally in an objective and repeatable manner
- **Incorporate lessons learned** from prior incidents

The best way to refine a national cyber incident classification system is to use it. The more it is used, the more data is generated internally and through feedback from external stakeholders and partners that can be used in the refining process. Refinement should align with the strategic goals set at the beginning of the development process. Most of the time, this means refining the system to better achieve those strategic goals. However, periodically, it may be useful to use the refinement process to re-evaluate the strategic goals. These intervals should be regular but relatively lengthy, at least a few years.

To leverage data gathered from prior usage of the system to evaluate the achievement or continued relevance of strategic goals, the goals must first be translated into key indicators. Key indicators should be measurable, ideally in a repeatable and objective manner, and can include quantitative and/or qualitative components. Qualitative indicators focus on understanding stakeholder experiences through non-numerical data, such as interviews and observations, while quantitative indicators measure variables and scores using numerical data.

The following table (Table 6) includes at the top five indicators that are relevant to any national cyber incident classification system. The first three quantitative indicators can be calculated internally by the responsible authority for the information-sharing cycle, while the second two are likely to be obtained through surveys, interviews or similar stakeholder engagement. As with the information-sharing cycle overall, it is important to incentivize stakeholders to provide feedback; without this, refinement will be less effective.

It is also important to calibrate the appropriate level of use. Although thresholds are set during the design phase to align with overall goals, implementers should be wary of too many and too few incidents passing through the system. If the thresholds are set too high, and very few incidents pass through the information-sharing cycle for categorization, then the system itself may malfunction. In such a situation, a national cyber incident classification system may face weakening commitment from stakeholders both feeding into it (such as critical infrastructure operators) and looking to benefit from it (such as senior government decision-makers). In contrast, if the thresholds are set too low, and too many incidents are reported by information-sharing partners, then the system will be overwhelmed and unable to provide accurate and reliable categorizations. Consequently, the first three indicators below should be judged relative to a target number, rather than measuring success simply through higher numbers.

Goal	Indicator	Type
All	Number of incidents reported	Quantitative
All	Number of incidents analysed	Quantitative
All	Number of incidents categorized	Quantitative
All	Feedback on reporting infrastructure including ease of use	Qualitative (text) and quantitative (rating)
All	Feedback on timeliness of analysis, assessment and communications	Qualitative (text) and quantitative (rating)
1	Number of actions taken based on incident categorization	Quantitative
1	Significance of actions taken based on incident categorization	Qualitative
2	Number of times contributed to national cyber risk assessments	Quantitative
2	Significance of contributions to national cyber risk assessments	Qualitative
3	Number of references in research or policy on causes of cyber incidents	Quantitative
3	Significance of references in research or policy on causes of cyber incidents	Qualitative
4	Number of times contributed to holistic assessment of combined cyber and non-cyber incidents	Quantitative
4	Number of references by non-cyber classification systems	Quantitative

Goal	Indicator	Type
4	Significance of references by non-cyber classification systems	Qualitative
5	Number of references by international partners	Quantitative
5	Number of reporting instances received from international partners	Quantitative
5	Extent to which analysis methodologies or criteria are also used by international partners	Qualitative

Table 6: Suggested impact indicators

The remaining indicators in the table above (with a white background) are examples of potential indicators that could be used to translate the five goals listed in Step 1 into measurable elements, as reflected in their associated goals in column 1 of the table.

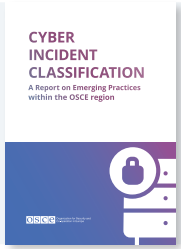
These indicators show how refinement is connected to key goals; if only some of the goals in Step 1 are relevant to a particular state, or different goals are chosen, then that state should adjust its key indicators accordingly.

Effective stakeholder management is crucial in developing the list of indicators. If all stakeholders are aware of and agree on the list of indicators, they are more likely to accept requests for data collection. When the national cyber incident classification system needs improvement, it is important to use the list of indicators to demonstrate recognition of the need for improvement and a commitment to make such improvements in a transparent and objective way.

Refinement should also draw from major incidents that occur during the initial live phase. Such incidents are likely to reveal issues that may not have been detected without the time and political pressures generated by that incident, which can provide an excellent platform for improvement. The key to using such incidents for lessons learned exercises is to distinguish between aspects that were unique to that incident and aspects that are likely to occur again with other incidents, and that should be used as the basis for refinement. Such major incidents will likely feature heavily in the qualitative indicators listed in Table 6 above.

Recommendation from the good practice report

This step of the handbook is connected to the following report recommendation:



9. "Once established, a cyber incident classification system should be regularly reviewed to assess its effectiveness and ensure it is appropriately informing a country's incident response and its risk or emergency management posture. Any changes to the incident classification schema deriving from the review process should be introduced in a manner that allows for long-term comparative analysis."

Illustrative example

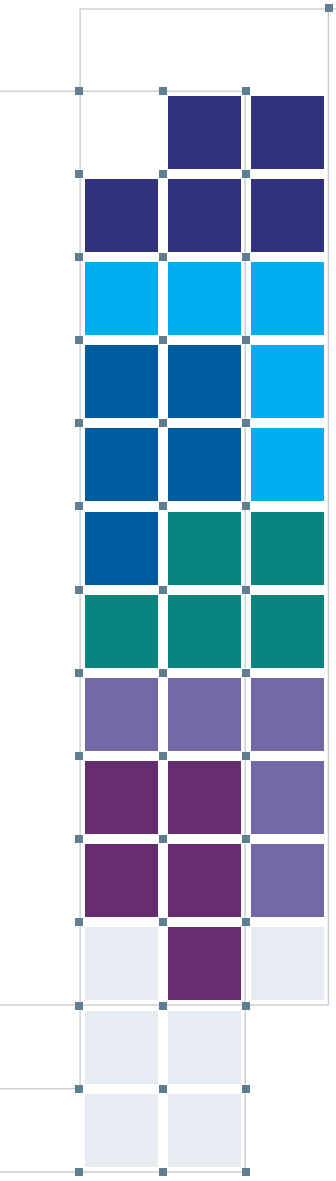
State A

State A reviews its processes regularly, every couple of years. Changes are reluctantly introduced in order to maintain comparability with historic data. However, unlike other types of risk, stakeholder involvement is crucial to achieving cyber resilience. It is likely that State A will seek a more collaborative approach in future, working with its constituents in line with OSCE CBM 15. This will likely be a slow process, as public-private partnerships require a high level of trust and a history of collaboration.

State B

State B also reviews its modus operandi periodically. It has appointed an external oversight committee to monitor the implementation of the national cyber strategy. This independent body helps to collect crucial feedback. However, State B is also a victim of its own success, with critical infrastructure operators enthusiastically reporting incidents in the hope of receiving support from the national CSIRT. As a result, this system may fail to scale, especially as other stakeholders also feel a growing need for support.

Conclusion



This handbook provides six key steps for states to develop a national cyber incident classification system. Each step is accompanied by illustrative examples of hypothetical states with significantly diverging decisions on their goals, stakeholders, reporting pathways, and ultimately different implementation and refinement.

The handbook underscores that developing a national cyber incident classification system is an important step forward. By setting clear goals, engaging stakeholders, building on existing structures, and implementing and refining systems through iterative testing and collaboration, states can strengthen their resilience to cyber threats while fostering trust and transparency among domestic and international partners. A well-designed classification framework not only enhances national risk management and crisis response but also contributes to broader regional and global stability by enabling more effective co-operation, de-escalation and confidence-building in cyberspace.

Annexes

Annex 1

OSCE PERMANENT COUNCIL DECISION NO. 1202

OSCE

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/1202
10 March 2016

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202
OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, *inter alia*, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of

PCOEW6464

political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms *inter alia*, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals from the Consolidated List

circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, *inter alia*, to:

– Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;

– Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and

– Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, *inter alia*, include:

– Sharing information on ICT threats;

– Exchanging best practices;

– Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;

– Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;

– Sharing national views of categories of ICT-enabled infrastructure States consider critical;

– Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and

– Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

Practical Considerations[1]

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group

1 First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013.

established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

Considerations[2]

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group's work in support of voluntary non-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

2 First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.

Annex 2

EXAMPLES OF NATIONAL CYBER INCIDENT SEVERITY SCALES AND A CYBER INCIDENT REPORTING FORM

The United States of America — approach to cyber incident categorization through a scoring system based on eight different categories of incidents.

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

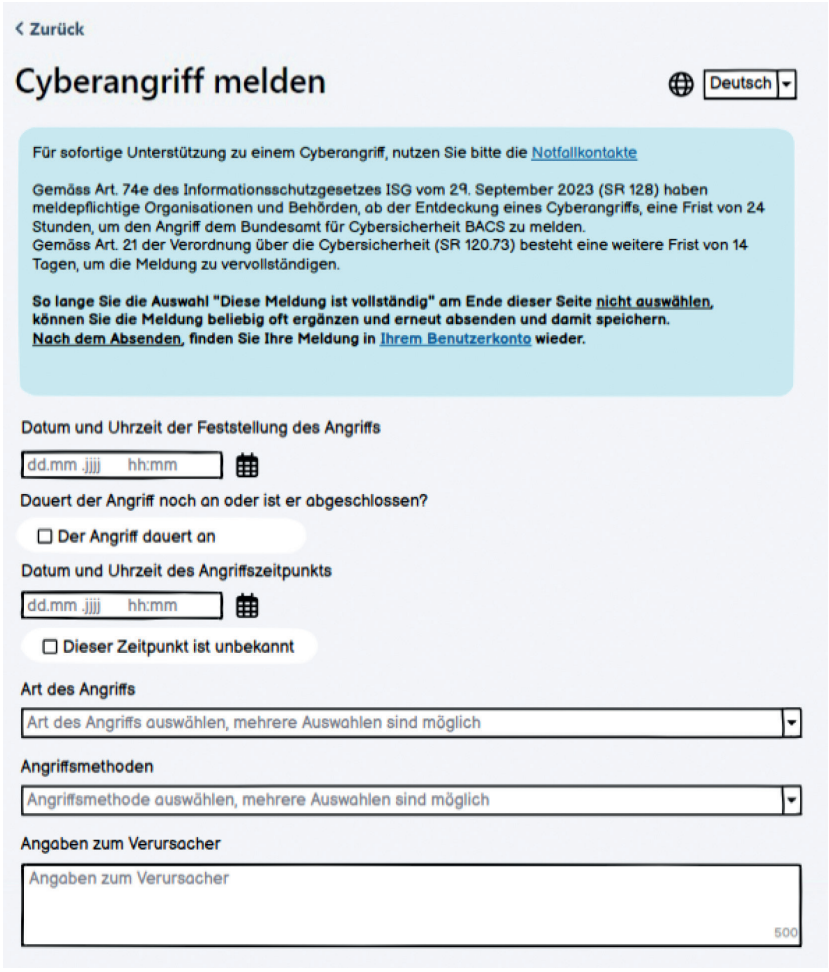
Source: OSCE Good Practice Report on "Cyber Incident Classification: A Report on Emerging Practices within the OSCE region" **https://www.osce.org/files/f/documents/6/5/530293_1.pdf** (pg. 26)

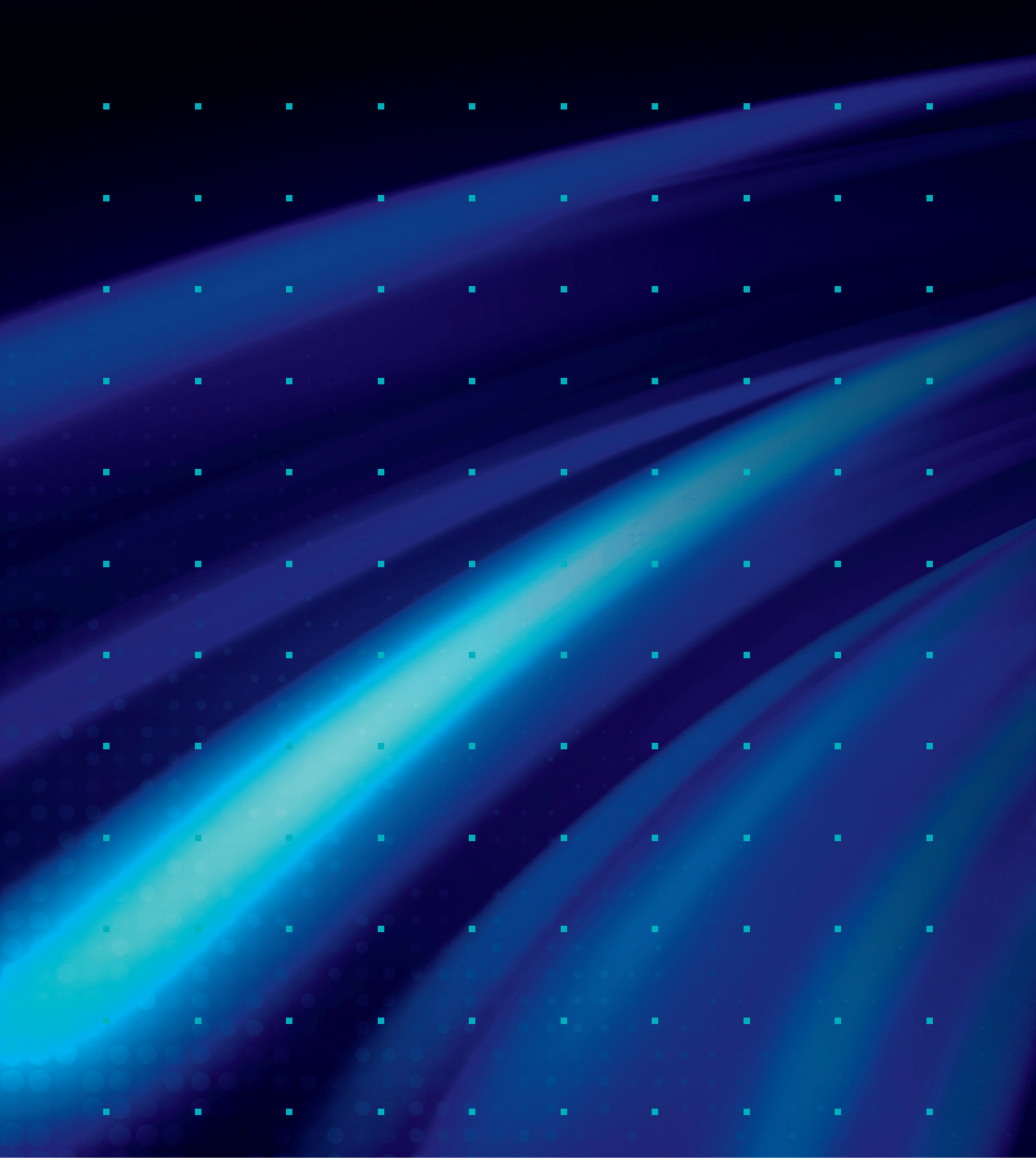
France – the severity of cyber incidents is assessed using a structured classification system which categorizes incidents into six levels. Each level corresponds to a specific color code and is determined based on factors such as impact, scope and urgency.

GRAVITY SCALE	EQUIVALENCE WITH THE US CISS	IMPACTS	CHARACTERIZATION AS ARMED AGGRESSION WITHIN THE MEANING OF ARTICLE 51 OF THE UNITED NATIONS
LEVEL 5 - EXTREME EMERGENCY	Level 5 Emergency (Black)	Extreme Impact	Probably possible: to be considered on a case by case basis.
LEVEL 4 - MAJOR CRISIS	Level 4 Severe (Red)	Major Impact	
LEVEL 3 - CRISIS	Level 3 High (Orange)	Strong and Extensive Impact	Probably not possible: actions corresponding to these levels could nonetheless constitute other internationally wrongful acts (intervention, violation of sovereignty, use of force, etc.).
LEVEL 2 - SERIOUS INCIDENT	Level 2 Medium (Yellow)	Strong and circumscribed impact	
LEVEL 1B - INCIDENT	Level 1 Low (Green)	Medium and circumscribed impact	
LEVEL 1A - SIGNIFICANT EVENT		Low impact	
LEVEL 0 - EVENT	Level 0 Baseline (White)	Negligible Impact	

Source: OSCE Good Practice Report on "Cyber Incident Classification: A Report on Emerging Practices within the OSCE region" **https://www.osce.org/files/f/documents/6/5/530293_1.pdf** (pg. 27)

Switzerland – reporting form for cyber incident





Follow OSCE

OSCE Secretariat
Transnational Threats Department
Wallnerstrasse 6
1010 Vienna, Austria

Organization for Security and Co-operation in Europe

cybersec@osce.org
www.osce.org/secretariat/cyber-ict-security