27 October 2025 | National Cyber Security Centre NCSC

Federal processes for coordinated cyberincident response

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

Contents

1 Background

In its decision of 1 May 2024 (EXE 2024.0416), the Federal Council tasked the Federal Department of Defence, Civil Protection and Sport (DDPS) with clarifying how cyberincident response is coordinated between the Confederation, the cantons and suppliers. The mandate – carried out by the National Cyber Security Centre (NCSC) and the State Secretariat for Security Policy (SEPOS), both in the DDPS – also asks them to set out the criteria for assessing the scale of cyberattacks.

This mandate forms part of the measures defined in response to the cyberattack on Xplain AG, which resulted in sensitive data being leaked from both federal and cantonal authorities. To manage this incident, the Federal Council had established a policy and strategic crisis management unit, which was dissolved on 1 May 2024. The incident highlighted the need for greater clarity regarding the circumstances in which a policy and strategic crisis management unit should be established in the future, and the involvement of the cantons and other potential stakeholders.

Following the entry into force of the Information Security Act (ISA; SR 128) in 2024, the Cybersecurity Ordinance (CySO; SR 128.51) in 2025, and the Ordinance on Crisis Organisation of the Federal Administration (OCOFA; SR 172.010.8) in 2025, the legal foundations for coordinated cyberincident response are now in place. This document explains how cyberincidents are classified by severity, and the coordination mechanisms applied by each organisation at each level. It also provides recommendations on the severity levels at which a policy and strategic crisis management unit should be established.

2 Core processes in coordinated cyberincident response

Under Article 5 of the Information Security Act (ISA), a cyberincident is defined as an incident occurring during the use of information technology that compromises the confidentiality, availability or integrity of information, or the traceability of its processing. A cyberincident that has been triggered intentionally is considered a cyberattack. This includes unauthorised access to computer systems via malware or the exploitation of vulnerabilities, as well as attacks that disrupt service availability through denial-of-service attacks.

When a cyberincident occurs, countermeasures must be taken. These measures are generally referred to as 'incident response'. The National Institute of Standards and Technology (NIST) has summarised the key incident response processes in its Incident Response Life Cycle Model (see Figure 1).

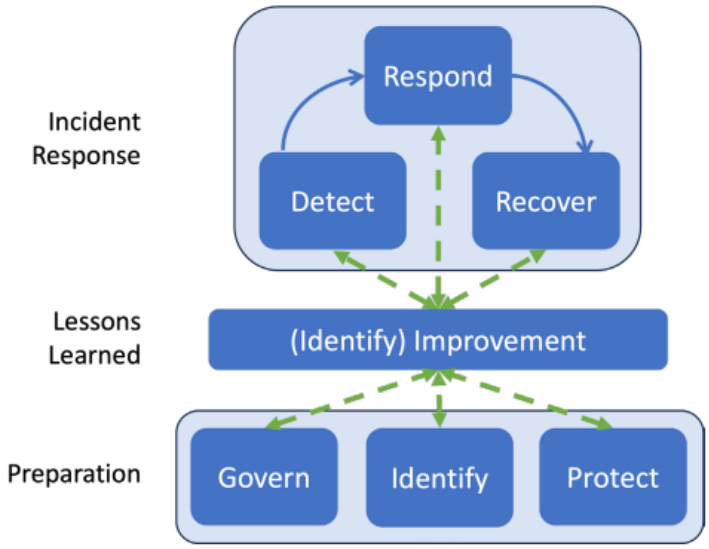

Figure 1: *Core processes in incident response (A. Nelson et al., NIST Special Publication 800,)*

The core processes for responding to cyberincidents are: Detect, Respond and Recover. In the Detect phase, potential cyberincidents are identified and analysed as early as possible to determine their origin and the motives behind them, and to identify their technical characteristics (e.g. the type of malware used). The Respond phase focuses on implementing measures to stop the cyberincident or at least limit its impact. The final phase, Recover, involves repairing the damage caused and restoring affected data and systems to a functioning state.

These processes are integral to every incident response, although the extent to which they are implemented varies depending on the type of incident and its effects. In most cases, these steps can be carried out directly and within a short time by the responsible security team, which also initiates further processes to improve the organisation's protection against future incidents ('Lessons Learned' and 'Preparation').

However, as digital interconnectivity increases, it is becoming more common for cyberincidents to extend beyond the boundaries of a single organisation. They may, for example, affect systems operated by third parties or systems with interfaces or dependencies involving third parties. Moreover, disruptions caused by cyberincidents often have rapid knock-on effects on other entities. In many cases, organisations also outsource their security operations to managed security service providers (MSSPs). This means that responsibility is shared between at least two parties, who must coordinate with each other – or be coordinated by someone else. Depending on the incident and its impact, coordination may be handled by the organisation directly affected, by another organisation impacted by the incident, by a cybersecurity company acting on behalf of one of these organisations, or by the NCSC in the case of large-scale incidents.

When several parties are directly involved in responding to an incident, careful coordination – that is, coordinated cyberincident response – is essential. For this to work, it is crucial to establish quickly who is responsible for which processes and how they are to be implemented. Therefore, a transparent, traceable classification of cyberincidents is crucial to ensure efficient incident response.

This is particularly important when the federal administration is involved in incident response, as public interests are affected. Under Article 73a ISA, the NCSC conducts technical analyses to assess and counter cyberincidents and cyberthreats, and supports critical infrastructures in responding to them. In such cases, the NCSC plays a key role in coordinated cyberincident response. However, this role is subject to limitations: the NCSC provides subsidiary support and does not take on tasks that can reasonably be carried out by private providers within an appropriate timeframe (Art. 74 para. 3 ISA). In order to ensure effective cooperation between private-sector actors, the cantons and the Confederation in the event of a coordinated cyberincident, it is essential to clearly define the Confederation's role in each type of incident.

3 Classification of cyberincidents

A clear and transparent classification of cyberincidents is essential for allocating roles effectively during an incident. However, it is important to note that such classifications can never be fixed universally and often change during the course of an incident response. Each organisation will assess an incident from its own perspective, and initial assessments often require adjustment as the situation evolves. This subjectivity and the changing nature of incidents present a challenge for coordinated cyberincident response, which must be addressed through careful and continuous communication between all parties involved. The classification itself, by contrast, is simple. It is based on two interrelated factors:

- Scope: Which systems and organisations are (directly or indirectly) affected by the cyberincident, and how significant are they?
- Impact: What impact has the cyberincident already had, and what further impact can be expected?

These two dimensions can usually be assessed quickly for a single organisation. Many security teams apply such criteria intuitively and quickly decide which internal structures to use for handling the incident.

In a coordinated incident response involving several affected organisations, it is crucial that all parties understand how their partners are evaluating the situation. Even if a cyberincident severely affects many systems within one organisation, this does not necessarily mean that other actors will reach the same assessment. For example, the encryption of systems in a ransomware attack may constitute a critical incident for the affected organisation, but for others – including the Confederation, from the perspective of protecting the public interest – it will rarely be considered an incident requiring immediate action.

At federal level, incidents must be assessed in terms of their impact on society as a whole. The NCSC classifies incidents according to how many organisations in Switzerland are affected, and whether the incident affects the functioning of the economy or well-being of the population. In its coordinating role for cyberincident response, the NCSC uses a four-tier model to distinguish between cyberincidents of low, moderate, serious and critical severity. This model ensures that the relevant legal requirements are met at all times, and that coordinated incident response is carried out according to consistent procedures.

Severity	Affected entities	Impact
Low	Individuals or organisations that are not part of critical infrastructure	The cyberincident causes no functional disruption, or only minor effects on the functioning of the economy or the well-being of the population.
Moderate	Individual critical infrastructure systems or organisations	The cyberincident is a reportable cyberattack under Art. 74*d* ISA or an incident that has endangered functionality, led to manipulation or resulted in a data leak.
Serious	Several critical infrastructure systems or organisations	
Critical	A large number of companies or critical infrastructure subsectors	Serious effects on the functioning of the economy or the wellbeing of the population.

Table 1: *Classification of cyberincidents*

4 Federal processes for coordinated cyberincident response

The appropriate process for coordinated incident response is selected based on how a cyberincident is classified. This section explains the processes applied by the NCSC in its coordinating role for each incident category. It is important to note that an incident's classification can change dynamically and that the response processes are adjusted accordingly.

4.1 Processes for cyberincidents in the 'low' category

Cyberincidents in the 'low' category can be voluntarily reported to the NCSC (Art. 73b paras. 1 and 2 ISA). The NCSC will accept the report and, if requested, provide a recommendation on how to proceed, unless further analysis or clarification is required (Art. 73b para. 12 ISA). In such cases, responsibility for managing the incident lies with the affected organisation or person. The Confederation does not take on a coordinating role.

4.2 Processes for cyberincidents in the 'moderate' category

Cyberattacks against operators of critical infrastructure have been subject to mandatory reporting since 1 April 2025 under Art. 74a ISA. In return, the Confederation (specifically the NCSC) is obliged to support affected parties with incident response if commercial assistance cannot be obtained in time (Art. 74a, para. 3, ISA). To this end, the NCSC operates the Government Computer Emergency Response Team (GovCERT), which coordinates first-response assistance directly with affected companies. In the event of cyberincidents affecting the Federal Administration, the NCSC may take on a more active role in supporting and advising affected federal units (Art. 12 para. 3 Information Security Ordinance ISO; SR 128.1).

If several organisations across Switzerland are affected by the same cyberincident at the same time, or if the incident cannot be resolved within a reasonable timeframe using established methods, the NCSC's focus is on ensuring the flow of information between all the organisations involved. To this end, it uses the Cyber Security Hub (CSH) information platform, where it publishes warnings, assessments and recommendations. The CSH also provides affected parties with a platform for mutual exchange, thereby contributing to a coordinated cyberincident response.

4.3 Processes for cyberincidents in the 'serious' category

At this level, the NCSC plays a more central role in coordinating the response to cyberincidents. If the cyberincident affects the Federal Administration, the State Secretariat for Security Policy (SEPOS) leads the response. SEPOS may transfer lead responsibility for managing the incident to the NCSC (Art. 12 para. 7 ISO). Technical support and coordination by the NCSC is key in cases where the incident affects several operators of critical infrastructure, has serious consequences (e.g. service disruptions) or continues despite standard countermeasures. Figure 2 shows the practical implementation of these coordination and support tasks and the involvement of partner organisations. The diagram illustrates that the NCSC's support is limited to the core processes of detection and response. Full recovery of system functionality remains the sole responsibility of the affected organisations.

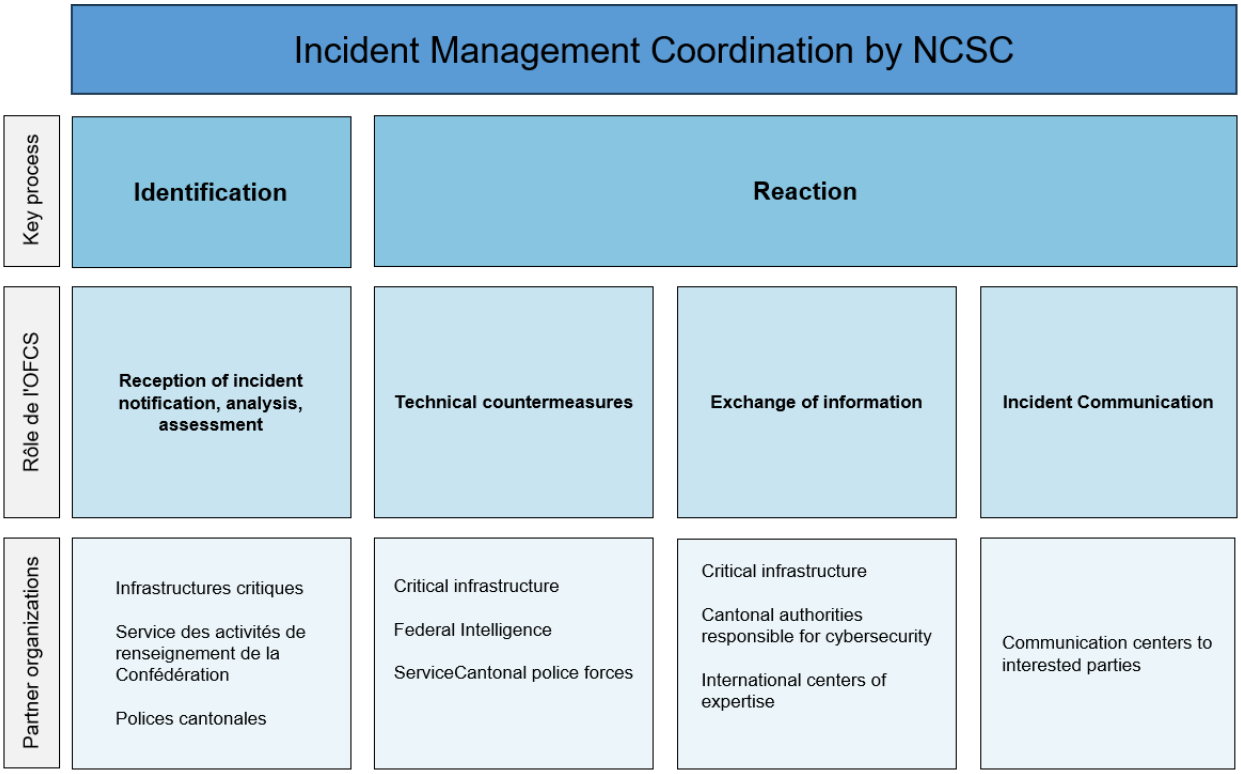

Figure 2: *Coordination of cyberincident response by the NCSC*

4.4 Processes for cyberincidents in the 'critical' category

Incidents at 'critical' level are cyberincidents that have already caused, or could potentially cause, a crisis. As these incidents pose an immediate and serious threat to the state, society, and the economy, the Federal Council appoints a crisis management team to coordinate the response and mitigate the impact. The establishment and coordination of a crisis management team are governed by the 20 December 2024 Ordinance on the Crisis Organisation of the Federal Administration (OCOFA). The specific setup of the crisis management team – particularly which department takes the lead – depends on which critical sectors are affected. If critical sectors experience major outages, the primary focus becomes dealing with these failures. The same processes used for 'serious' cyberincidents can also be applied to manage 'critical' incidents. Where necessary, the policy and strategic crisis management unit may also direct operational crisis and incident response through political-strategic directives (Art. 5, para. 3, let. b, OCOFA).

5 Implementation

The NCSC's approach to coordinating incident response, as set out in this document, is grounded in existing legal foundations. In recent months, these have been supplemented by the adoption of the OCOFA and the amendment to the ISA on 29 September 2023, which introduced a reporting obligation for cyberattacks on critical infrastructure, effective from 1 April 2025.

As the processes for coordinated incident response are already standard practice, there is no immediate need for further action to strengthen implementation, such as creating new legal provisions. However, it is important that the classification of cyberincidents and the corresponding incident response processes are communicated more clearly. Coordinated incident response only works if all partners know from the outset who is responsible for what and what support they can expect.

The NCSC will therefore continue to work closely with the cantons and operators of critical infrastructure to align the processes for coordinated incident response and the classification of cyberincidents, while also communicating its tasks and responsibilities transparently.