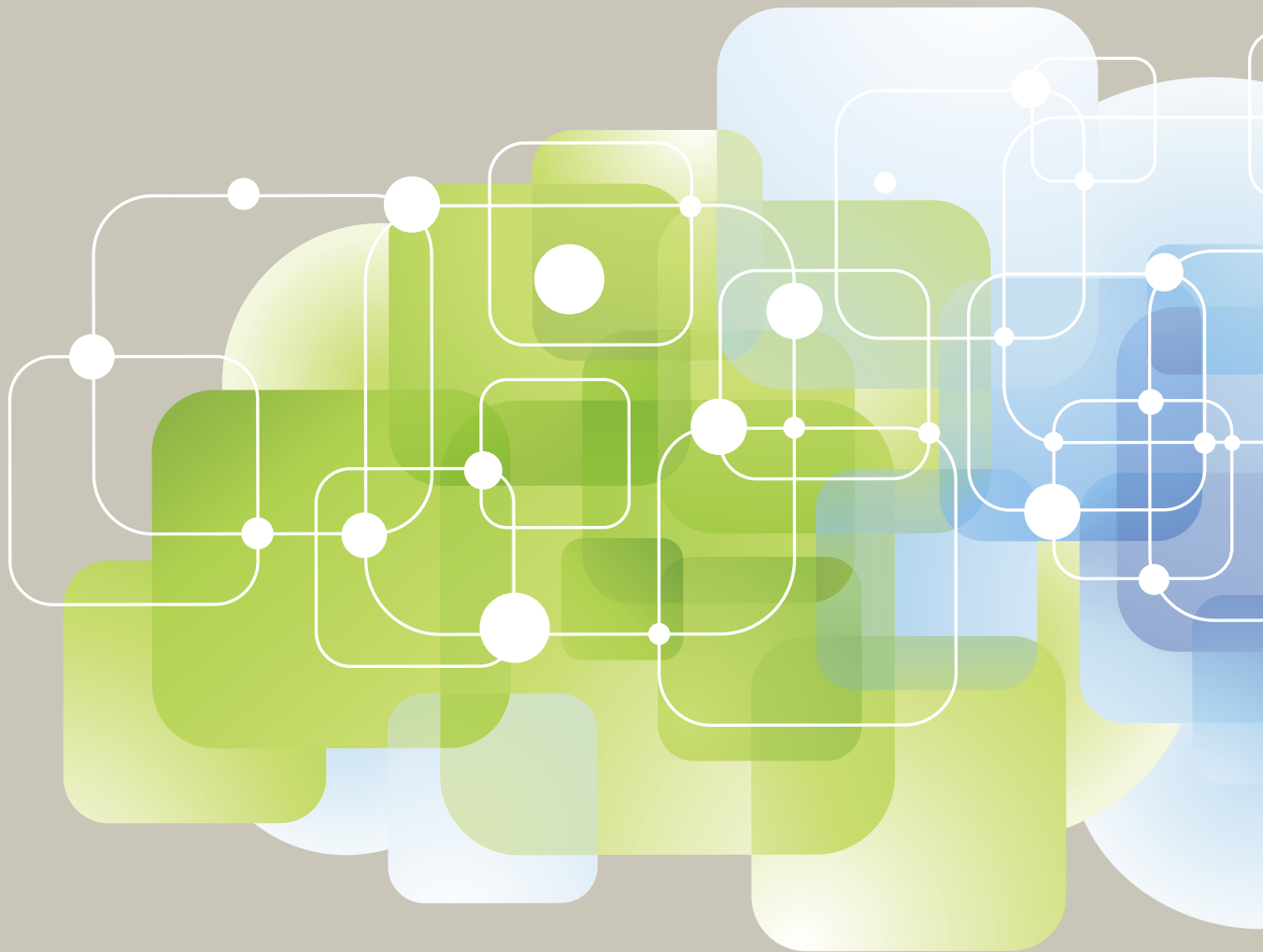
Swedish Civil Contingencies Agency

NISÖ 2018

After Action Report



NISÖ 2018 – After Action Report

This publication is also available in Swedish
NISÖ 2018 – Erfarenhetsrapport
Order. No: MSB1326 - december 2018 ISBN: 978-91-7383-900-6

Swedish Civil Contingencies Agency (MSB)

Layout: Advant

Order No: MSB1330 - December 2018
ISBN: 978-91-7383-904-4

Foreword

The role of the Swedish Civil Contingencies Agency (MSB) is to develop and support the capability of Swedish society to deal with emergencies and crises. The MSB's exercises play a central role in this respect. The MSB has a duty to promote exercises, primarily cross-sector exercises. The goal is for participants to use the exercises to help improve their ability to limit the consequences of emergencies and crises, to lead and make decisions within their own area of responsibility, and to collaborate with others.

As more and more social functions are digitised and connected, information security and cybersecurity failings are emerging in all sectors. Secure digitisation depends on raising the minimum standards of information security and cybersecurity throughout society, and this is particularly relevant in total defence. The MSB has a specific mandate to coordinate and support information- and cybersecurity activities throughout society. This includes ensuring that Sweden has a national body tasked with supporting societal efforts to prevent and manage IT-incidents. The MSB's work in the field of information security is aimed at other agencies, municipalities and businesses, all the way down to individual citizens.

On 14-15 February 2018, the MSB carried out the NISÖ 2018 national information security exercise. The aim of the exercise was to improve Sweden's ability to manage national IT-related crises, primarily through developing the capability for collaboration and cooperation between private and public sector entities in designated sectors.

This report is a summary of NISÖ 2018 and presents the main lessons learned and necessary improvements in order to improve Sweden's crisis preparedness, specifically relating to information security and cybersecurity.

Stockholm, 30/11/2018

Åke Holmgren
Head of Office of Cybersecurity and Critical Infrastructure Protection

Innehåll

Summary

In order to improve the exercises that are carried out in future and to ensure that the crisis management system continues to evolve, it is necessary to learn from the experience gained from previous exercises. This report describes the exercise called the *National Cyber Security Exercise 2018* (NISÖ 2018), which was conducted on 14–15 February 2018. The report also sets out the experience gained from the planning and execution of the exercise, as well as necessary cross-entity improvements.

NISÖ 2018 was planned, executed and evaluated by the *NISÖ 2018* project. The exercise consisted of a simulation exercise with role-play at the Swedish Armed Forces Command and Control Regiment in Enköping.

NISÖ is designed to strengthen the capability to manage major IT-related crises

Exercises are an important part of efforts to strengthen the capability to manage various events and crises. Exercises are planned over the long term, allowing each exercise to contribute to planned capability improvements and also to maintain the existing capability. The exercises in the NISÖ series aim to strengthen Sweden's crisis management capability and the capability to manage major IT-related crises.

Focus on coordination between private and public sector entities

The aim of NISÖ 2018 was to improve Sweden's ability to manage national IT-related crises, primarily through developing the capability for collaboration and coordination between private and public sector entities in the following sectors:

- Energy
- Healthcare
- Information and communication
- Local and regional authorities
- Transport

Two overarching areas for improvement were identified

The Swedish Defence University was tasked with conducting a formal evaluation of how the cross-entity objectives were achieved in the exercise. The areas for improvement presented by the MSB in this report are based on the results of the evaluation by the Centre for Societal Security (CTSS) and on the debriefing seminar which was held after the exercise.

MSB has classified the identified areas and aligned them with the wider development work taking place within the Agency. Two main overarching areas were identified as needing improvement during NISÖ 2018: *collaboration and system knowledge and information sharing and situational awareness.*

Collaboration and system knowledge

The evaluation of NISÖ 2018 indicates that further improvement is needed in the way the private and public sectors collaborate during IT-related crises. In addition, there needs to be greater awareness of the crisis management system. On the basis of the encountered shortcomings in collaboration and system knowledge, three specific areas for improvement were identified in the continuing development work:

- Private-public collaboration
- Awareness of collaboration forums
- Awareness of the needs and capabilities of local and regional entities

Information sharing and situational awareness

The evaluation also indicates that activities around information sharing and situational awareness require improvement in several respects. The following specific areas for improvement were identified to boost information sharing and situational awareness capability:

- Resilient and secure communications
- Traditional communication channels
- Situational information and situational awareness

Lessons learned and conclusions after evaluation and seminars

The report concludes with a summary of conclusions and lessons learned from the planning, execution and evaluation of NISÖ 2018. The conclusions are based on the outcome of the process evaluation carried out in conjunction with NISÖ 2018 and on discussions during the debriefing seminar in May 2018.

1. Introduction

1.1 Societal information security and IT-related crises

Swedish society depends on a functioning IT infrastructure. This is equally true for citizens, businesses and public authorities. A functioning IT infrastructure is also vital in enabling the public and private operators of essential services to fulfil their mission.

Businesses and public authorities use IT and communication technology in their day-to-day activities. Vulnerabilities in the IT system can therefore have serious consequences for individuals and for society at large. For example, IT-related crises can affect healthcare, the media, energy supplies, government authorities, municipal entities and transport. This in turn could potentially destabilise essential services – by disabling information systems, severing traditional communication links and impairing important means of transport. In order to prevent and manage IT-related crises, Swedish society must improve its capability to manage such events. This capability must be improved in both private and public sector operators of essential services.

IT-related crises generally unfold very quickly, so the entities involved must be able to detect anomalies and manage the situation at the earliest stages. Organisations affected by an IT-related crisis must also coordinate their responses and quickly establish a shared situational awareness with other entities in the crisis management system.

1.1.1 Developments in the field of information security and cybersecurity

The field of information security and cybersecurity changes very quickly and there is a pressing need for improved IT and information security throughout society. Decision-makers are constantly striving to enact laws and regulations to meet the new challenges facing an increasingly IT-dependent society. Policy development in the field of Information- and cybersecurity has progressed at a rapid pace since the first National Cyber Security Exercise (NISÖ) took place in 2010.

There have been developments at both national and international level. The EU's cybersecurity strategy was adopted in 2013[1]. It was the impetus behind the *NIS Directive*[2], which was adopted in 2016 and implemented in Swedish legislation on 1 August 2018. The aim of the Directive is to harmonise the information security requirements which the EU imposes on the Member States, operators of essential service and digital service providers.

Alongside developments at European level, a number of analysis and policy documents have been created for the Swedish context. Relevant examples include the NISU analysis[3] published in 2015 and the government's strategy published in 2016[4].

1. European Commission (2013;2009) *Cybersecurity Strategy of the EU*, (JOIN (2013) 1 final); *On Critical Information Infrastructure Protection*, KOM(2009)149
2. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ('NIS Directive')*
3. Ministry of Justice (2015) *Cybersecurity in Sweden – strategy and measures for secure information in central government [Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten]*, SOU 2015:23
4. Ministry of Justice and the Government (2016) *National strategy for societal information security and cybersecurity [Nationell strategi för samhällets informations- och cybersäkerhet]*, Skr. 2016/17:213

It is certainly necessary to formulate new policies, but the rapid developments in the field of IT and information security present the operators of essential services with some difficult challenges. The fast pace of national and international policy development therefore places an additional strain on these organisations over and above the technological and organisational challenges which characterise the field of IT and information security. The entities involved require training and exercises in order to maintain their ability to prevent and manage future IT-related crisis events and to keep pace with developments.

1.2 IT-related crises and the need for exercises

Experience from past IT incidents and IT-related crises shows how important it is for organisations to be prepared for the particular challenges they face in IT crisis situations. Regular national exercises are essential in developing and evaluating the organisations' ability to manage IT-related crisis events.

The national cross-sector exercises, which aim to develop coordination and collaboration across society, are especially important. IT-related crises also demand high standards of technical expertise and presuppose collaboration between technical experts and other staff members such as management or communicators. Exercises and training in the management of technical aspects of IT-related crises are therefore important in building up capability.

In Sweden, the exercises in the NISÖ series play an important part in the wider exercise activity. The first NISÖ exercise was conducted in 2010, and a second in 2012. This is in line with national and international directives aimed at strengthening Swedish and EU capability in IT and information security.

1.2.1 European and international exercises

At the international level, the European Commission urges the EU Member States to conduct exercises to test responses during and after large-scale IT incidents. The European Commission also highlights the need for exercises at European level.[5]

A number of international exercises have been conducted in recent years. The first pan-European exercise – *Cyber Europe 2010* – took place in November 2010. This was followed by Cyber Europe 2012, 2014, 2016 and 2018. The US security services, too, have conducted related activities, which have been open to participation by European entities. One example is the *Cyber Storm* exercise. NISÖ 2018 was executed and planned on the basis of experience gained from these earlier activities.

1.3 The National Cyber Security Exercise series (NISÖ)

The Swedish Civil Contingencies Agency (MSB) is responsible for the NISÖ series of exercises. NISÖ aims to strengthen Sweden's crisis management capability and its capability to manage major IT-related crises. Exercises are also intended to broadly strengthen collaboration in the crisis management system. NISÖ 2018 is the third exercise in the series, and the next is planned for 2021.

5. *Cybersecurity Strategy of the EU; On Critical Information Infrastructure Protection*

1.4 Content of this report

This report describes the NISÖ 2018 exercise. It sets out the experience gained from planning and execution, and describes the necessary cross-entity improvements which were identified. The individual responses and specific objectives of the participants are not included in the report – these aspects will be addressed separately by the organisation in question.

The report aims to describe the experience gained and lessons learned during NISÖ 2018, and to detail the necessary improvements to the crisis management system identified in the exercise. From a broader perspective, the report therefore aims to strengthen the country's capability to manage IT-related crises.

The Swedish Defence University's *Centre for Societal Security* (CTSS) was tasked with conducting a formal evaluation of NISÖ 2018. The areas for improvement presented by MSB in this report are based on the results of the CTSS evaluation of NISÖ 2018.

2. Planning of NISÖ 2018

NISÖ 2018 was planned, executed and evaluated by a project, also called *NISÖ 2018*. The project was a long-term collaboration between the Office of Cybersecurity and Critical Infrastructure Protection and the Exercises Section in MSB. The project was staffed with personnel from MSB and external consultants. It was financed using 2:4 funding allocated to the project. Planning, execution and evaluation of NISÖ 2018 took place over two years, from 2016 to execution in 2018.

2.1 Planning structure

The project group planned NISÖ 2018 on the basis of MSB's planning model for simulation exercises involving role-play, emphasising the involvement of participating entities. The planning process aimed to give all participating entities the opportunity to prepare for execution according to their chosen level of ambition and available personnel. The project also had to arrange a sufficiently comprehensive role-play with individuals able to play the outside world and provide the participating entities with injects as the exercise proceeded.

Formal planning began when the project directive was approved in 2016. The project ran workshops and briefings for the participating entities in the form of a kick-off meeting and three planning conferences. Scripting sessions were also held for the injects. The scripting sessions involved exercise leaders and designated inject scripters, who jointly scripted injects developed from the overall exercise scenario.

2.1.1 Participating entities

The entities participating in NISÖ 2018 were drawn from the following sectors:

- Energy
- Healthcare
- Information and communication
- Local and regional authorities
- Transport

The selection of sectors represented in NISÖ 2018 largely corresponds to the prioritised sectors in the NIS Directive.

The following entities participated in NISÖ 2018
Svenska kraftnät
CGI
Eon
Swedish Energy Agency
Evry
Swedish Armed Forces
Port of Gävle
Gävle Municipality
Swedish National Civil Aviation Authority
Gävleborg County Administrative Board
Stockholm County Administrative Board

Västra Götaland County Administrative Board
Swedish Civil Contingencies Agency
Swedish Post and Telecom Authority
SJ
Stockholm County Council
Swedish Security Service
Tele 2
Telia
Teracom
Tieto
Swedish Transport Administration
Swedish Transport Agency
Uniper
Vattenfall

2.1.2 Project organisation

The project was led by the project manager appointed by MSB and was organised according to established principles for the planning of collaboration exercises. The process was based on international exercise planning standards[6] and on MSB's structured support tools. The procedures and documents used by the project were based on the project management model selected by MSB.

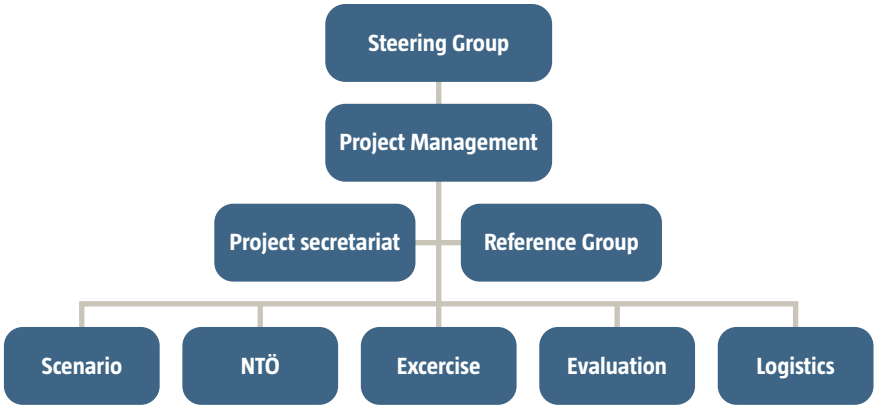


Figure 1. *Planning organisation for NISÖ 2018*

The intention behind structuring the project organisation in this way was to create the conditions in which the various parts of the exercise could be planned and prepared. The project was staffed mainly by MSB personnel and consultants recruited from elsewhere. When the exercise had been executed, the project organisation was scaled down and only the parts involved in evaluation remained in the project.

The participating organisations' local exercise leaders (LEL) acted as a reference group in the planning phase, attending the planning meetings and contributing their knowledge and opinions before execution. They also reviewed the materials issued ahead of the planning meetings. The local exercise leaders were an important resource in inject scripting, too, adding knowledge about their own organisation.

6. Swedish Standards Institute (2013), *Societal security - Guidelines for exercises*, SS-ISO 22398:2013, IDT

2.1.3 Schedule

The schedule used in the project followed standard practice for the planning of large-scale exercises.

Date	Event
11 May 2016	Approval of the project directive
8 March 2017	Kick-off meeting
18-19 May 2017	Planning meeting 1
30–31 August 2017	Planning meeting 2
4-5 October 2017	Scripting session 1
8-9 November 2017	Scripting session 2
22-23 November 2017	Planning meeting 3
23 January 2018	Scripting session 3
25 January 2018	Execution of technical test
14–15 February 2018	Execution of NISÖ 2018
20 March 2018	Evaluation seminar
24 May 2018	Debriefing seminar
30 November 2018	Conclusion of the project

Schedule for NISÖ 2018, joint activities in the project

2.1.4 Exercise documentation

A number of documents were created before the exercise in order to describe:

- How the planning process should be organised and carried out
- How the different parts of the activities that make up the exercise should be conducted
- How the evaluation should be carried out and where the emphasis should lie

This information is contained in the following documents:

- Exercise planning guidelines
- Exercise execution guidelines
- Logistics plan
- Exercise control guidelines
- Evaluation plan[7]

7. These documents were determined by the project steering group with the exception of the logistics plan and the exercise control guidelines. The exercise control guidelines and the logistics plan are not policy documents so they were determined by the project manager.

3. Execution of NISÖ 2018

3.1 Aims and objectives of the exercise

The aim of NISÖ 2018 was to improve Sweden's ability to manage national IT-related crises, primarily through developing the capability for collaboration and cooperation between private and public sector entities in designated sectors.

The objective of NISÖ 2018 was to improve Sweden's ability to manage major IT-related crises, primarily through developing the capability for collaboration and coordination between private and public sector entities. The exercise objectives were based on four key processes:

- Situational awareness
- Reporting of impact assessments for IT incidents
- Response assessments for IT incidents
- Coordination of messages to the media and the public

The following cross-entity objectives were specified for the exercise:

1. **To create a situational awareness focused on the event and its impact** using information collected internally and information provided by others, and
   - support coordination of situational awareness by making the results available to others
   - if necessary, incorporate the situational awareness of other entities into a common situational awareness.
2. **To take decisions about the response, and plan measures** on the basis of an internal, an external and a common situational awareness, and
   - share information about the response and planned measures with relevant (in other words affected or potentially affected) entities.
3. **To perform and if necessary coordinate information and communication activities for the public and the media**, about
   - the event and the impact
   - the response.
4. **To test existing**
   - routines for incident reporting
   - action plans
   - working practices.

3.2 Exercise configuration

NISÖ 2018 was executed over two days on 14–15 February 2018, at the Swedish Armed Forces Command and Control Regiment in Enköping (LedR). All participants – role-players as well as exercise players – were present at LedR.

During the exercise, each exercise player was represented by a cadre organisation. The reason why relatively small cadre organisations (which are small groups made up of individual representatives from the functions that would have acted in similar situations in real life) were used is that the main purpose of the exercise is to learn lessons and make improvements from a system perspective – rather than preparing for an actual crisis management organisation.

Each organisation chose which functions to include in the exercise according to its own individual objectives.

The exercise was subject to the following constraints:

- NISÖ 2018 only considered aspects relating to information security and cybersecurity (logical or electronic security).
- NISÖ 2018 did not address the handling of the physical consequences of IT incidents.

3.3 Method and execution

NISÖ 2018 was executed as a simulation exercise with role-play.

3.3.1 Simulation exercise in a realistic environment

A simulation exercise is an exercise that tests the participating entities' individual and joint crisis management capability in accordance with applicable directions and principles.[8] In general, the exercise format known as simulation exercise with role-play takes place in an environment and with activities that are as realistic a representation of a crisis as possible. A simulation exercise with role-play has two main parts: the exercise players and the active role-players. A participating entity can split up so that some parts of the organisation are involved on the exercise playing side and others are involved on the role-playing side.[9] The exercise players are only allowed to communicate with each other or with the role-players.

3.3.2 Execution – prerequisites and play organisation

NISÖ 2018 was run in a simulated environment on LedR premises, and the role-players were representatives from the relevant entities. During the exercise, the exercise directing staff and the role-players were kept separate from the exercise players who were in a different building. The role-players were divided into modules, with central play directing staff in the middle. The exercise players were arranged so that 2–3 of them shared a room, but they could physically collaborate with other exercise players in adjacent rooms. The players brought their own computers with them to connect to the Exercise Web [Övningswebben] (see below), their own crisis management system (if any), and the play support system for role-players. The information sharing tool *Web-based Information System* (WIS) was simulated by means of a directory on the server.

On the basis of an overall scenario, the exercise players responded to events that were injected in order to create conditions similar to a real crisis event. To make the exercise as realistic as possible, a number of technical tools were also used.

One such tool was the Exercise Web, a portal page which constituted the exercise players' Internet. Here, for example, an information sharing directory and the scenario storyline were published. The exercise players also used the Exercise Web to access to the exercise media such as newspapers and social media. Also through the Exercise Web, participants could publish their own social media posts and communicate internally and externally during the exercise. Throughout the exercise, staff were available in two teams, one with the exercise players and one attached to the role-playing side. They were able to provide technical and logistical support.

8. MSB (2013) *Exercise guidance: Methods – Simulation exercise with role-play [Övningsvägledning: Metodhäfte – Simuleringsövning med motspel]*, MSB604
9. MSB (2016) *Exercise guidance: Fundamentals – Introduction to and fundamentals of exercise planning [Övningsvägledning: Grundbok – Introduktion till och grunder i övningsplanering]*, MSB602, p. 45

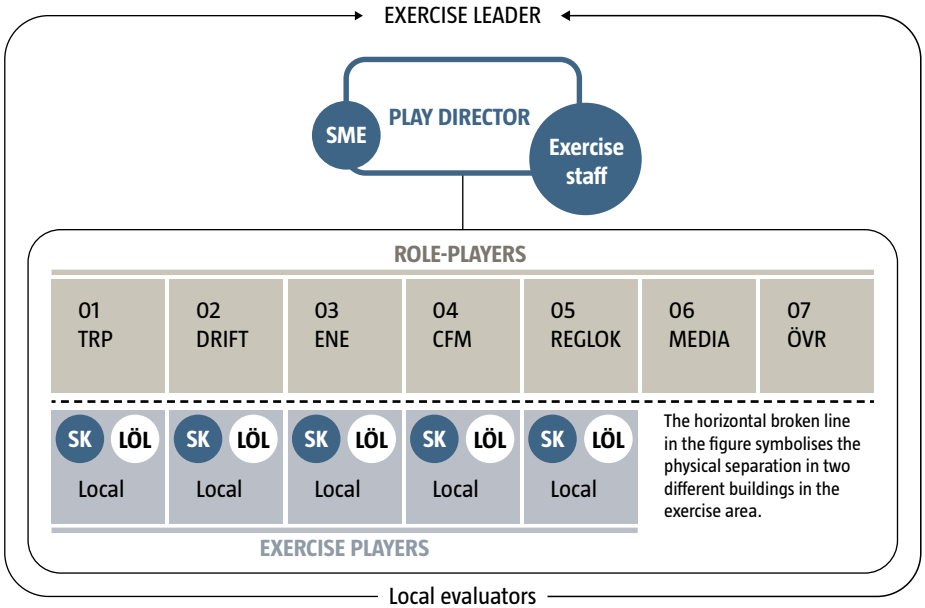


Figure 2: *Execution organisation for NISÖ 2018 Subject-matter experts (SME), the transport sector (TRP), service providers in the IT sector (DRIFT), the energy sector (ENE), central administrative authorities (CFM), (REGLOK) regional and local entities, media (MEDIA), Rest of the World (ÖVR), play coordinator (SK), local exercise leader (LÖL)*

All the functions contained in the figure apart from the exercise players belonged to the play organisation (in other words the play directing staff and the role-players).

The exercise director's role during the exercise was primarily to coordinate the start and end of the exercise and to terminate the exercise if necessary. The actual simulation, however, was led by the play director, who was responsible for the role-playing side. The play director was assisted by exercise staff, who manned the staff teams and looked after the technical systems. The play director was also assisted with information security and communication issues by a number of subject-matter experts (SME).

The role-players manned six different modules, divided according to the affected sectors. The MEDIA module was manned by hired journalists who produced articles in the fictional Krispressen, intended to resemble an evening newspaper. They also inserted injects and posted comments in the simulated social media in the Exercise Web. The journalists also conducted interviews with the exercise players.

In the rooms containing the exercise players, there were five play coordinators (SK), one for each role-playing module apart from MEDIA. The play coordinators were the play director's eyes and ears among the exercise players, along with a local exercise leader for each organisation. The local exercise leaders' role during execution was mainly as follows:

- To help the exercise players settle in and get up and running in the rooms before the exercise started.
- To inform the role-players how the exercise players reacted to injects during the exercise, and whether the pace needed to be faster or slower.

The local exercise leaders were also tasked with collaborating with the play coordinators and the local evaluators.

4. Evaluation

Swedish Defence University's *Centre for Societal Security* (CTSS) was tasked with supporting MSB in evaluating whether the exercise objectives were achieved. The task of CTSS was to coordinate the Evaluation subproject and to act as the evaluation director while the exercise was running. The task was completed on 2018 when CTSS submitted an evaluation report to MSB. The result of CTSS's evaluation then formed the basis of the areas for improvement presented by MSB in this report.

4.1 Purpose of the evaluation

The purpose of the evaluation was to benefit from the experience gained and lessons learned from the exercise, and to identify any improvements which may be necessary. An assessment of the degree to which the objectives have been achieved is planned for a later stage.

The experience collected during the evaluation forms the basis of a long-term project formulating and eventually implementing action plans in the participating sectors. The purpose of the evaluation was therefore not to formulate development plans as such, but to provide a general picture of the areas for improvement identified by the exercise. The evaluation also aimed to give tentative recommendations concerning focus areas for future measures to improve capabilities.

The exercise was not an examination, so the purpose of the evaluation was not to assess the quality of the analyses, judgements and decisions made and reported during the exercise. Instead, the emphasis was on assessing the ability to collaborate by studying the aspects of collaboration identified in the NIS Directive. Collaboration was also evaluated between the authorities[10] which are responsible for supervision according to the NIS Directive.

4.2 Evaluation process

The material used in the cross-entity evaluation of NISÖ 2018 was collected through participatory observation and from questionnaires completed by the exercise players.

In addition, a number of observers were present at LedR in Enköping during the exercise. The observers were responsible for monitoring various issues and sectors. The observations were then submitted to the evaluation director in report form. The exercise players were also asked to answer follow-up questions after the exercise about the needs they felt they had and whether they felt that the information provided during the exercise was usable. These questions were sent to the exercising organisations as a questionnaire immediately after the end of the exercise.

The result of the evaluation was then summarised in an evaluation report. The evaluation report contained analyses of each objective and conclusions, and identified lessons learned and necessary improvements.

MSB and the entities participating in NISÖ 2018 worked jointly to benefit from the findings of the evaluation. An evaluation seminar was held in March 2018. The purpose of the seminar was to quality-assure and consolidate the conclusions of the evaluation. In April 2018, the evaluation report was sent to MSB for comment and quality assurance. The result was then adjusted in light of the conclusions from an evaluation seminar, and an adjusted evaluation report was submitted to MSB in April 2018. A debriefing seminar was then held in May 2018 involving representatives from the exercise players. The purpose of the seminar was to share the findings with the participating entities.

10. Swedish Energy Agency, Swedish Transport Agency, FI (Finansinspektionen), Swedish Health and Social Care Inspectorate, National Food Administration and Swedish Post and Telecom Authority.

5. Prioritised areas for improvement

CTSS identified nine cross-entity areas for improvement in its evaluation of NISÖ 2018:

- Greater awareness of different collaboration forums
- Secure and resilient communications
- Use of traditional communication channels
- Use of traditional information sharing methods
- Feedback and response to submitted data
- Requirement definition and expertise in eliciting information (from other entities)
- Awareness of the needs and capabilities of local and regional entities
- Awareness of different entities' needs regarding information and knowledge
- Bridging the gap between private and public

The first three areas were highlighted in the NISÖ 2012 evaluation, too. At that time, a need to improve situational awareness was also identified. The NISÖ 2018 evaluation also includes aspects of situational awareness and information sharing in a number of the areas for improvement above.

MSB reorganised the identified areas in order to create coherent improvement measures and to align them with the wider ongoing improvement activities, including those resulting from the SAMÖ 2018 collaboration exercise.

MSB organised the areas for improvement as follows:

- Collaboration and system knowledge
  - *Area for improvement 1:* Private-public collaboration in crisis situations
  - *Area for improvement 2:* Awareness of collaboration forums
  - *Area for improvement 3:* Awareness of the needs and capabilities of local and regional entities
- Information sharing and situational awareness
  - *Area for improvement 4:* Access to resilient and secure communications
  - *Area for improvement 5:* Use of traditional communication channels
  - *Area for improvement 6:* Situational information and situational awareness

Apart from the above areas for improvement, MSB will also continue to develop a coordinated national capability to detect, issue alerts for, provide support during, and manage IT-related incidents and crises. Additional measures will also be presented in a national action plan for information security and cybersecurity[11] (due on 1 March 2019). Furthermore, the development of societal capability to manage major IT-related crises is closely related to the general development of crisis preparedness and total defence. A number of other areas for improvement will therefore be presented in the *National Risk and Capability Assessment [Nationell risk- och förmågebedömning]*.

11. Government to MSB (2018) *Commission to prepare a comprehensive information security and cybersecurity plan for the years 2019–2022 [Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022]*, Ju2018/03737/SSK

5.1 Collaboration and system knowledge

5.1.1 Private-public collaboration in crisis situations

Improving the capability for collaboration between private and public entities was also one of the aims in past exercises in the NISÖ exercise series. This is because the capability for collaboration is an essential component of effective crisis preparedness in Sweden. The evaluation of NISÖ 2018 indicates that further improvement is needed in the way the private and public sectors collaborate during IT-related crises.

The evaluation indicates challenges that are by no means new, but that are becoming increasingly evident as more and more entities from diverse sections of society participate in exercises of this kind. NISÖ 2018 showed how the crisis preparedness system is mainly organised among the public authorities. The private entities which increasingly own the systems and installations which are affected by, or which need to be used during, an IT-related crisis are left out of the established structures. This contributes to the gaps in knowledge that were flagged up in the previous sections of this report. Because the structure is built around public authorities, there are also shortcomings in how the information with relevance to collaboration in a crisis can be disseminated, for example for situational awareness. The shortcomings were observed in both private and public entities during the exercise. Another observation which needs to be addressed in future development activities is that private businesses are often transnational with important functions in countries other than Sweden, and this affects the basis on which collaboration takes place during an IT-related crisis.

AREA FOR IMPROVEMENT 1

Private-public collaboration must continue to be strengthened by developing clear points of entry to the crisis preparedness structures and the envisaged reporting paths.

The public crisis preparedness structures and the cross-sector services provided by private entities must be harmonised to a greater extent. The prospects for collaboration can be further boosted by formalising and strengthening the information sharing processes of the affected entities.

MSB intends to continue its ongoing work to develop private-public collaboration in this connection, as set out in its response to the governmental commission concerning private-public collaboration in the field of information security and cybersecurity[12]. Additional measures relating to private-public collaboration may also be included in the national action plan due to be delivered on 1 March 2019. Work on private-public collaboration is also a central part of development activities in the field of total defence.

5.1.2 Awareness of collaboration forums

Collaboration is a central concept in Swedish crisis management because there is no single entity with responsibility for crisis leadership. All affected entities must be able to collaborate in decision-making and when taking action in the event of an IT-related crisis.

12. MSB (2018) *Private-public collaboration in the field of information security and cybersecurity [Privat-offentlig samverkan på informations- och cybersäkerhetsområdet]*, 2017-7117

Collaboration in Swedish crisis management is based on the *principle of responsibility*. The principle of responsibility means that the entity which performs the affected social activity under normal circumstances is correspondingly responsible for maintaining the activity in crisis situations. The principle of responsibility therefore involves initiating and managing the collaboration. To facilitate collaboration during crises, there are a number of collaboration forums and networks throughout Swedish society.

The NISÖ 2018 evaluation showed that there is a continuing need to raise awareness among the affected entities of the available collaboration forums and how they work. Awareness of various collaboration forums is judged to be too dependent on individuals. Over and above the observations made during the 2012 exercise, NISÖ 2018 shows that private entities must be familiar with the forums catering for public authorities in their particular field even if they do not necessarily participate themselves.

AREA FOR IMPROVEMENT 2

Awareness of different collaboration forums must be spread to a larger group of employees in the affected entities.

There must be clear instructions setting out how and in what forms affected entities collaborate in different forums. At the same time, everyone working in the crisis preparedness system must be very familiar with the available collaboration forums and their particular function.

MSB intends to continue spreading awareness of the available collaboration forums in this connection, as part of the Agency's activities concerning collaboration in information security and cybersecurity (see also private-public collaboration above). It may be possible to support this work through ongoing developments in total defence.

5.1.3 Needs and capabilities of local and regional entities

The interaction between national, regional and local levels is crucial in any crisis, including IT-related crises. In 2018, regional and local entities participated in the NISÖ exercise series for the first time. It was precisely at the local and regional level that the scenario events produced the kind of societal disruption that generates the need to collaborate on which the exercise was focused. The need to plan the more practical aspects of crisis management arose at the local and regional level too, and useful knowledge and capability exists locally and regionally to provide the necessary response. Central authorities need to learn more about the activities of local and regional entities in the event of an IT-related crisis.

AREA FOR IMPROVEMENT 3

Central authorities must increase their awareness of, and create the right expectations for, local and regional entities. This is fundamental to establishing an effective capability to provide information and feedback to regional entities and to collaborate with them.

MSB intends to continue its efforts to increase awareness of the needs and capabilities of local and regional entities. It will do so in the context of the Agency's broader activities concerning information security and cybersecurity, and also in the context of planning and executing the total defence exercise (TFÖ) 2020.

5.2 Information sharing and situational awareness

5.2.1 Access to secure and resilient communications

Effective crisis management during a serious IT-related crisis is only possible if all the entities concerned have access to secure and resilient communications.

Work is ongoing to develop and provide access to secure and resilient communications, for example signal protection systems. The evaluation indicates that this work must be intensified and given greater priority in order to develop functioning shared channels and methods for secure communication between all affected entities in an IT-related crisis. The need for secure communications and systems was already identified in NISÖ 2012, but NISÖ 2018 specifically highlighted the need to develop the ability to share information (for example situational awareness) in an accessible way in secure and resilient systems and channels. Secure and resilient communications capable of also sharing secret data are required in order to communicate information to other affected entities, not just to the public.

AREA FOR IMPROVEMENT 4

The capability to communicate securely during IT-related crises must be strengthened.

Systems such as Rakel and WIS are deliberately restricted to the entities specified in laws and regulations. They must be made available to more entities, private as well as public. The systems must also be capable of sharing sensitive and classified information. To increase familiarity, the affected entities must also be drilled in the use of systems such as Rakel and WIS. At present, the systems are used to varying degrees at municipal level. One way to simplify the use of Rakel in crisis situations is to encourage the municipalities to use the system in their day-to-day activities too. Information campaigns, training activities and exercises in Rakel should therefore take place at municipal level.

MSB intends to continue its efforts to improve access to and awareness of secure and resilient communications. This includes ongoing development work around Rakel, *Swedish Government Secure Intranet* (SGSI) and WIS. MSB will also issue guidance on secure and resilient collaboration in late 2018 as part of its efforts to increase awareness of secure and resilient communications.

5.2.2 Use of traditional communication channels

For private as well as public entities, the ability to disseminate information about what is happening, and to give advice and recommendations to wider society, is a crucial part of crisis management.

To enable them to manage a major IT-related crisis, affected entities must have extensive knowledge of different types of communication activities. Crisis communication is important, and should be characterised by speed, openness and accuracy.[13] In addition, the crisis communication itself can influence the event as it happens.[14] Affected entities must be able to communicate using digital communication channels and via traditional media, and to establish alternative communication channels if necessary.

13. MSB (2014), *Common foundations for collaboration and leadership in societal disruptions [Gemensamma grunder för samverkan och ledning vid samhällsstörningar]*, MSB777, pp.71–73
14. *Common foundations for collaboration and leadership in societal disruptions [Gemensamma grunder för samverkan och ledning vid samhällsstörningar],* pp.71–73

The evaluation of NISÖ 2018 suggests there is good reason to continue efforts to reinforce the entities' ability to communicate using traditional and also alternative communication channels. It is understandable that in an information security and cybersecurity exercise, the participating entities are very familiar with and comfortable using digital communication channels. During NISÖ 2018, this manifested itself in a misdirected focus on crisis communication using digital communication channels rather than using media contacts and local communication activities. In a major IT-related crisis, it is highly likely that precisely these digital channels will not be fully operational, making wide-ranging communications expertise essential in successful crisis management. This is a compelling argument to strengthen the communications expertise among the affected entities.

AREA FOR IMPROVEMENT 5

Affected entities must develop their knowledge and skills in using traditional and alternative communication channels.

Affected entities must also increase their awareness of the role played by public service broadcasters in crisis preparedness and in requesting an 'important public announcement' (VMA) or an announcement from the authorities. This is crucial in boosting the ability of effected entities to communicate with the public and other entities during a serious IT-related crisis.

MSB intends to continue national development activities around the dissemination of information during serious societal disruptions. These development activities are directly linked to the development of crisis preparedness and total defence, for example in the total defence exercise (TFÖ) 2020.

In addition, MSB will continue its efforts to support emergency planning and collaboration by media companies, for example in the Media Preparedness Council. These efforts include close collaboration with the public service broadcasters Sveriges Radio and Sveriges Television. MSB is also the body responsible for running and developing the VMA public announcement system. Work is ongoing to identify new methods and techniques to complement the existing VMA system.

5.2.3 Situational information and situational awareness

Information sharing and situational awareness are central elements in Swedish crisis management. Access to a common (shared) situational awareness is essential in order to manage crises of all kinds, including IT-related crises. In a crisis, it is very important to be able to analyse and present the sequence of events quickly. IT-related incidents and crises may also require situational awareness that focuses on aspects relating to information security and cybersecurity, in addition to a wider-ranging, national situational awareness.

Although in NISÖ 2018, the central authorities managed to make the collected information available and formulate situational awareness in accordance with the relevant legislation[15], the other entities found the information sharing process to be one-sided. Furthermore, the information provided by the central authorities was not always picked up by the entities affected by the information.

15. The *Ordinance on crisis preparedness and the surveillance authorities' actions at times of high alert [Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap] (2015:1052)* contains requirements concerning the reporting of certain aspects of incident management to central authorities, but not how the information is to be shared further down the system hierarchy. This approach is found even if the focus is on reporting to surveillance authorities and further to MSB and the Swedish Government Offices.

The existing system to disseminate situational awareness to affected entities presupposes that the entities are aware of, have access to, and are able to monitor and participate in the forums in which the information is published. They must also be able to use the relevant sharing interfaces. Greater awareness is therefore necessary, and possibly also new approaches in the field of situational awareness. The purpose of the formulated situational awareness must also be communicated more clearly: what it is expected to contain and which target groups are involved.

Expertise in eliciting information and an ability to define requirements concerning situational awareness are essential in enabling entities to formulate correct situational awareness and take considered decisions during a crisis, even when under time pressure. NISÖ 2018 revealed an inability among the entities to define requirements for or explicitly elicit specific information from other entities.

CTSS's evaluation suggested that prevailing management principles, a consensus culture and the division of responsibilities made it difficult for the exercising players to express dissatisfaction with the information shared and with the working practices used in the exercise. Instead of requesting the correct material and quicker answers, the entities took their own independent steps to resolve the problems they experienced with time-critical information. This approach among the entities suggests a solution-oriented attitude, which is a good thing, but also indicates shortcomings in terms of requirement definition and expertise in eliciting information.

AREA FOR IMPROVEMENT 6

More work must be done in the field of situational awareness so that affected entities feel that central authorities are sufficiently attuned to their needs when communicating with them.

Improvements are necessary to the working process and the resulting situational awareness, and to the situational awareness presentation tools. This area for improvement applies to the public and private sectors. Private entities may also need greater clarity about what they can expect from the central authorities and about what information the national authorities expect from them. The entities' work processes to specify time-critical information must also be developed. Increased awareness and further development around roles and functions are necessary so that the internal and external need for information during an IT-related crisis can be identified even under time pressure. It is important to develop mutual understanding among affected entities to make it easier to decide what information and knowledge is relevant in each organisation's decision-making and management processes.

MSB intends to continue development activities around situational awareness relating to information security and cybersecurity. This is part of the continuing development of the capability to manage major IT-related crises. Regarding the general development activity around information sharing and common situational awareness, MSB continues to offer training on the implementation of *Common foundations for collaboration and leadership in societal disruptions [Gemensamma grunder för samverkan och ledning vid samhällsstörningar]*.[16] The incident reporting that takes place from government authorities and forms part of the NIS Directive also helps to improve the ongoing exchange of situational information in society.

16. For example a course entitled 'Information sharing and common situational awareness – shared foundations for collaboration and leadership' will be offered in 2019.

6. Conclusions from planning, execution and evaluation of NISÖ 2018

This section presents the overarching conclusions and lessons learned from the planning, execution and evaluation of NISÖ 2018. The conclusions build on the output from the process evaluation and the discussions which took place during the debriefing seminar in May 2018. Below, the NISÖ 2018 project arranges the experience gained into three categories for consideration when future exercises are planned in the field of information security.

6.1 Need for clear communication with participating entities

The planning method used in NISÖ 2018 is based on cooperation between all affected parties over a relatively long period. The exercise project must communicate clearly with the participating entities to establish a shared vision of how planning should proceed and what work needs to be done by the participating entities alone. For example the project must communicate how the participating entities should plan their personnel provision so they can make an active and constructive contribution to exercise planning. Constant communication activities are also necessary in order to keep the participating entities updated and – importantly – engaged. Examples of such communication activities include the distribution of progress reports and deadlines.

It is also important at an early stage to create reasonable expectations of the amount of time that needs to be devoted in order to get the best out of participating in NISÖ. Also required are awareness-raising communication measures which can act as models and examples of good solutions on the practical side of the exercise, for example what a 'good' inject looks like. In addition, the information communicated by the project should be clear and instructive so it is easy for the participating entities to assimilate.

6.2 Levels of ambition, engagement and knowledge among participating entities

The participating entities must take responsibility for the continuity of their own process by being present throughout the planning work, and by completing their part of the work between planning conferences and scripting sessions. Because NISÖ is intended to identify capability shortcomings at system level, it is essential for the participating entities to have a high level of ambition and be willing to participate in the exercise for their own sake and also to achieve the common objectives. It is also important for the entities to have a basic knowledge of the crisis preparedness system, of each other, of the form of the exercise and of the exercise method.

6.3 Exercise design

6.3.1 Method

NISÖ 2018 was a pure simulation exercise carried out at a joint exercise location, as opposed to NISÖ 2012, which was executed as a combined table-top and simulation exercise. It is evident that whichever exercise configuration is selected, some of the benefits of the other configuration are lost. Before future exercises take place, there must be a wide-ranging discussion between all stakeholders involved in the exercise about the pros and cons of the various types of exercise configuration. The needs of the entities in terms of the exercise format must also be discussed. This applies to the choice of exercise methods and to the practical requirements of the exercise, for example if the exercise takes place at a single location.

6.3.2 Design

Before future exercises, thought must be given to what is the best design for exercises in IT and information security. In terms of the process to design a large-scale simulation exercise with many participating entities, it is also important to consider how the entities develop their injects. In future exercises, those responsible for the overall scenario should ensure at an early stage that the entities collaborate during inject development in order to avoid misunderstandings and unnecessary revisions.

It is also useful if exercises which bring together a large number of affected and important entities leave space for networking alongside the scenario-based exercise. More than two days are probably needed if the exercise is to be long enough to create the conditions needed for collaboration while also leaving enough spare time for fruitful meetings between the exercise players.

6.3.3 Personnel provision during the exercise

From the experience gained in relation to personnel provision during the exercise and during exercise configuration, particular attention should be paid to two main findings.

The first finding is that scenario development should be decided with the authority of the personnel who will participate in the exercise in question. The exercise personnel must have the everyday authority within their organisation to take the decisions needed to keep the fictional exercise scenario moving. To enable the relevant functions and capabilities to be tested, it is important for the participating entities to deploy personal in a way that makes it possible to achieve the cross-entity objectives.

To make the exercise as realistic as possible, clear requirements must be defined concerning which entities must take part and which scenario play functions the entities must participate in. The crisis management system is complex and consists of a series of built-in interdependencies between the operators of essential services. Of course, not all entities can always be represented in the actual exercise. That is why it is important when designing future exercises to analyse the interdependencies that might arise in real emergencies. The analysis of such interdependencies should then form the basis for planning of personnel provision and scenario play design. This does not mean that exercises cannot take place without the involvement of these entities – just that this aspect must be addressed at an early stage in the project.

Appendix 1: Detailed specification of objectives in NISÖ 2018

OBJECTIVE 1

The exercise players must create situational awareness focused on the event and its impact ...

... using information collected internally and information provided by others ...

... support coordination of situational awareness by making the results available to others ...

... and if necessary, incorporate the situational awareness of other entities into a common situational awareness.

This objective corresponds to NIS Directive Chapter II, Article 10 and Chapter IV, Article 14. Observations relating to this objective focus on the processes for detecting, verifying and monitoring larger patterns in the event of IT incidents:

- Whether and how participating entities detect an IT incident
- Whether, how and when participating entities exchange information with each other when an IT incident is detected
- Whether and how participating entities verify IT incidents and whether they work together to formulate a common situational awareness
- Whether and how participating entities work together to update and maintain a common situational awareness.

OBJECTIVE 2

Participating entities take decisions about the response, and plan measures ...

... on the basis of an internal, an external and a common situational awareness ...

... and share information about the response and planned measures with relevant (affected or potentially affected) entities.

This objective corresponds to NIS Directive Chapter IV, Article 14 and Chapter V, Article 16. Observations relating to this objective focus on alerting and reporting processes and methods for IT incidents, and on the impact and response assessments to be performed when an incident is identified:

- Whether, when and how the participating entities analyse and describe the impact, planned measures and resource requirements, and whether the information is shared with other organisations
- Whether, how, when information is exchanged with which participating entities about identified problems and needs.

OBJECTIVE 3

Participating entities perform and if necessary coordinate information and communication activities for the public and the media ...

... about the event and its impact ...

... about the response.

This objective corresponds to NIS Directive Chapter II, Article 10 and Chapter IV, Article 14. Observations relating to this objective focus on processes and methods allowing the participating entities to collaborate and coordinate their information for the public, the media and other organisations represented in the exercise, either as an exercise player or a role-player:

- Whether, when and how communication activities relating to the IT incident are introduced
- What is the focus of communication activities in the different phases (detection, verification, response) – aimed internally within the organisation, aimed at the public, the media, or other organisations?
- Whether, how and when information is exchanged between which information managers of the participating entities
- Whether, how and when collaboration takes place between which information managers of the participating entities to coordinate their information for the public and the media

OBJECTIVE 4

The exercise players did their work according to prevailing ...

... routines ...

... working practices ...

... and action plans.

This objectives primarily concerns the exercise players' own needs and wishes for the exercise, and is therefore covered by the entity-specific objectives and the local evaluations of the organisations. The entity-specific objectives may have a different emphasis and do not form part of this evaluation.

All objectives also correspond to NIS Directive Chapter III, Article 11 concerning collaboration in IT-related crisis management. Because it is a means rather than an end, collaboration is more of a basis on which the observation points are formulated and not something to be evaluated per se.

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en
Order No. MSB1330 - December 2018 ISBN 978-91-7383-904-4