



# Instructions for organising cyber exercises

## A manual for cyber exercise organisers



# Contents

1	Introduction	3
2	What is a cyber exercise?	4
2.1	Why should I organise a cyber exercise?	5
3	Different types of exercises	6
3.1	Table top exercise	7
3.2	Root cause exercise (pre-mortem)	8
3.3	Functional exercise	8
3.4	Technical exercise	9
3.5	Capture the Flag	9
3.6	Major joint exercises	10
4	Preparations for an exercise	11
4.1	Setting an objective	12
4.2	Selecting the exercise type	13
5	Planning an exercise	14
5.1	Convening a planning team	15
5.2	Selecting participants	16
5.3	Preparing for an exercise	16
5.4	Supporting tasks and observers	17
5.5	Facilities	18
6	Contents of an exercise	19
6.1	Exercise scenario	20
6.2	Injects	20
6.3	State of the world	22
6.4	Communications related to an exercise	22
6.5	Marking exercise documents	23
6.6	Aborting an exercise	24
6.7	Modelling the operating environment of an exercise	24
6.8	Teams in a technical exercise	24
7	Lessons learned from an exercise	26
7.1	Planning a feedback survey	27
8	Exercise activities as part of cyber security management	29
8.1	Long-term planning	30
9	Conclusion	32
9.1	Contact details	32
9.2	Key concepts	33

# 1 Introduction

These instructions for organising cyber exercises were prepared by the Finnish Transport and Communications Agency's National Cyber Security Centre together with the National Emergency Supply Agency. No experience of cyber exercises is required to use these instructions. The instructions are intended for those responsible for information security and information management in organisations, including tasks to ensure the organisation's cyber security.

The need for Finnish cyber exercise instructions came up in the course of the National Emergency Supply Agency's KYBER-2020 programme. Plenty of information about different types of exercises is available online, but we wished to collect practical instructions for organising cyber exercises in a single document.

These instructions explain what cyber exercises are, how they should be organised, and how regular exercises can optimally support preparedness in your organisation.

Our instructions contain background information about the importance of cyber exercises, practical advice for organising an exercise, and a short glossary related to cyber exercises. The document also contains instructions for integrating exercise activities in the organisation's annual planning.

We hope that, rather than limiting your activities, the outline created by our instructions will support and motivate you in arranging cyber exercises when it is time to put plans into practice.

The National Cyber Security Centre's support services provide individual support and assistance for the cyber exercise activities of organisations critical for security of supply. The support services' contact details are included at the end of this document.

## **The cyber exercise instructions will help the organisation:**

1. to learn about good practices in organising exercises
2. to launch its cyber exercise activities
3. to plan its first exercise
4. to enhance its existing exercise programme
5. to improve its ability to prepare for and recover from information security incidents and disruptions.



## 2 What is a cyber exercise?

A cyber exercise is an event in which the organisation models and tests its preparedness for various cyber incidents. An exercise means modelling in the most appropriate way a fictive scenario that the organisation might encounter.

Cyber incidents are abnormal situations in an organisation's ICT operating environment that affect the organisation's operations. In cyber exercises, cyber incidents are simulated (modelled). This means creating imaginary conditions in which the impacts of the incident and recovery from them can be tested.

An exercise can be regarded as a safe opportunity to rehearse acting in a crisis facing the organisation, with the organisation being able to choose the timing and impacts of the crisis. Lessons learned from crisis situations are extremely valuable, and through an exercise, this method of learning can be used without an actual crisis that would hamper the organisation's operation. An exercise is often a cost-effective way of detecting shortcomings in crisis preparedness.

Many organisations have arranged various exercises for a number of years. To maintain fire safety, for example, fire and evacuation drills are organised on many premises. Organisations have also provided first aid training for staff to learn and practise critical skills.

Unlike exercises in the physical world, a cyber exercise focuses on the organisation's cyber environment. This means that the impacts of an incident in an extensively networked operating environment are evaluated beyond information systems; in other words, the exercise is not exclusively about computer malfunctions. A cyber exercise is about more than just IT.

The impacts of cyber incidents typically extend beyond the actual office environment, including disruptions of production or logistics.

For example, a cyber exercise can simulate an incident in a logistics centre's information systems which affects the deliveries and reception of goods.

At best, a cyber exercise makes the extensive impacts of IT incidents plain to all parties, and the organisation's dependence on well-functioning information systems becomes clearer. The exercise may also highlight the organisation's hidden dependencies. Learning these lessons would be highly valuable for the organisation's risk management work and preparedness for a diverse range of risks.

The exercises emphasise not only the practices followed in emergency conditions but also communication and leadership. The organisation's different functions can often be coordinated in an exercise in the same way as in real life, building up an understanding of collaboration between different divisions. In the era of social media, communications play a particularly important role in the management of cyber incidents.

A cyber exercise may be arranged by the organisation itself or by a third party. Major collaborative exercises with representatives from different organisations are excellent opportunities for developing network-based cooperation and establishing contacts between organisations. Various cooperation or training organisations, including educational institutions or central government organisations, take charge of implementing large exercises. Participation in large joint exercises is extremely useful.

Continuous and regular cyber exercises are an essential part of a modern organisation's cyber security management. If your organisation is not yet arranging exercises, these instructions will help you get started.

## 2.1 Why should I organise a cyber exercise?

Exercising purely for its own sake is not worthwhile. If your organisation plans and implements an exercise to meet your specific needs and you translate the lessons learned into practices, your organisation is guaranteed to become more resilient and better functioning.

Do your incident management processes work? An exercise is an excellent way for an organisation to ensure that the practices agreed for emergency situations are appropriate, effective and fit for purpose. In an exercise, the agreed practices can be applied actively, rather than examined passively. An exercise can also serve as a test for revised processes to examine their effectiveness in real life.

A cyber exercise will highlight strengths and weaknesses. Discussing and recalling crisis instructions regularly will be particularly helpful when a crisis hits in real life. In some exercises, the participants completely forgot about the

existence of incident management instructions, even though the organisation had them in place!

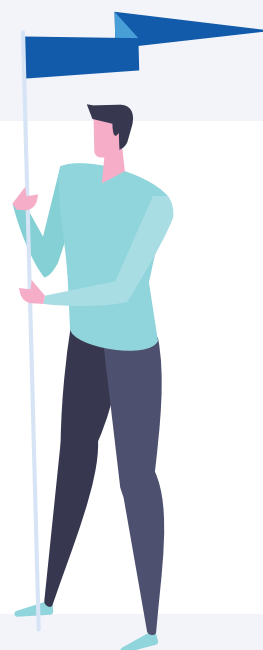
Many organisations keep postponing the launch of their exercise programmes. This is understandable, as exercising may appear demanding, difficult and something that only large organisations should do. However, you can start arranging exercises almost from scratch without expending too much time and trouble.

An effective and balanced programme may contain small-scale exercises that are easy to organise and more complex functional exercises. Table top exercises, which only require light organisation, are an easy way of bringing benefits for the organisation.

Your first step could be organising a simple table top exercise. Appetite usually comes with eating, and this can be the start of your journey towards more diverse, challenging and interesting exercises.

### **The benefits of exercises:**

- improved crisis resilience
- increased understanding of information system dependencies
- improved understanding of the extensive impacts incidents may have
- improved internal and external communications
- improved leadership in emergencies
- better internal processes through analysing exercise outcomes
- improved mutual understanding with service providers and customers
- clarified areas of responsibility
- increased confidence in coping with uncertainty.



### 3 Different exercise types

There are numerous different types of cyber exercises. When planning your exercise, you should remember that it can be implemented in a number of ways. In fact, any controlled examination of your processes can serve as an exercise. The different exercise types are defined by the level of detail at which the events are simulated, the exercise environment, technical requirements and time use. You can combine elements of several different types in your exercise as needed.

The choice of a suitable exercise depends on the available resources, the objectives of

the exercise and the target group. An exercise for technical staff differs from a managers' crisis management exercise, both in its method of implementation and its objectives. The objectives and participants of the exercise should be defined and selected before a method is picked.

Similar exercises cannot be used to improve the management's crisis preparedness and the technical staff's skills. Your choice of an exercise type should be guided by the skills and capabilities you wish to focus on. For example, table top or functional exercises are highly suitable when the focus is on leadership. Participants with a high level of technical skills, on the other hand, require an exercise that is technically more challenging. A leadership exercise and a technical exercise can also be integrated by combining exercise types. However, combining objectives requires more planning as the exercise becomes more complicated.



### 3.1 Table top exercise

**Suitable for cyber incident management, leadership, and reviewing and evaluating processes.**

Table top exercises, which are entirely based on using written material, are the most easily implemented and common exercises. These exercises do not require modelling the environment in which the incident takes place. The events of the exercise and the assignments associated with them are usually handed to the participants at the beginning of the exercise.

The goal is to find and document solutions and answers to the events and assignments devised for the exercise. This exercise type is easy to arrange, and it does not require lengthy advance preparations. It is enough to get the participants together at a pre-arranged location and time to work on the tasks that come up in the game.

Table top exercises do not usually involve scheduled injects or interactivity, and the participants take their time to consider and resolve the tasks. In an exercise consisting of several assignments, for example, the first hour can be dedicated to considering situation 1, and the second hour to situation 2. The outcome usually is written answers to the questions and a separate list of issues that need to be investigated later.

An assignment in a table top exercise may consist of a fictional state of the world description and a task associated with it, which often is formulated as a question, for example as follows:

**'A significant hardware and service supplier announces that they have sold their entire business to country X. Does this merger require changes in the service reliability assessment?'**

In exercises of this type, it is more important to prepare contingency plans or check that existing plans are fit for purpose and up to date than to analyse the root cause of the incident or tackle technical details.

A table top exercise is also known as a 'paper exercise' as no technical environment is needed to organise it. The game content can be planned in advance and printed on sheets of paper, which are handed out in the war room. The game begins as the state of the world description is handed out. A technical environment or a suitable tool may, of course, also be used when organising a table top exercise.

Table top exercises also work well as 'preliminaries' for more intensive exercises. This allows the participants to get in the mood for the exercise, or revise the knowledge and skills they will need in a future exercise.

### 3.2 Root cause exercise (pre-mortem)

**Suitable for anticipating problems and targeting risk management actions.**

A root cause exercise, which is also known as a pre-mortem, is organised similarly to a table top exercise. It is operationally light and easy to arrange. The objective of a root cause exercise is to identify the original causes of risks which, when realised, will result in a cyber incident.

An actual cyber incident is presented to the participants, and their task is to consider which

factors in their operating environment could lead to the described end result. The exercise is played as if starting from the middle and looking back to the starting point of the events.

Identified risks can be used as the basis of scenario work in future exercises. Examples of realised risks that can be used in a root cause exercise include a data breach in which customer data has ended up in the public sphere. The participants' task is to come up with different information security incidents that have caused the data breach in this case.

### 3.3 Functional exercise

**Suitable for exercises focusing on crisis leadership, crisis communications and cooperation.**

A functional exercise is a more realistic method than a table top exercise. The time constraints, among other things, are clearly more stringent as the participants process scheduled injects. The injects are fed to the participants following a pre-written playbook, which moves the story of the exercise along.

The injects are individual messages that describe what happens during the exercise. An inject may be any piece of information that moves the game forward, for example:

- an email message
- a telephone call
- a tweet
- a piece of news
- a Facebook post
- information given to a participant from the control room by telephone
- a request for an interview.

This exercise type stresses the participants' ability to immerse themselves in the situation, communicate with each other and build an up-to-date situational picture of how the events of the exercise will affect the organisation.

In a good exercise, the participants receive information about the events bit by bit, and a number of events from many different directions come into play. The challenges posed by the social media and communications, for instance, can easily be included in the game by means of news items and social media messages commenting on game events. Requests for interviews from the media and 'real' interviews that are recorded provide an opportunity to practise external communications in difficult situations. They also raise the bar of the exercise.

An efficient and dynamic control room plays a key part in a functional exercise. The control room is an area separate from the war room from which the game planners direct the game. The task of the control room is to lead the game and to send the injects to the participants during it. In addition to pre-planned main injects, the leaders can use conditional injects as a response to the participants' solutions and decisions. New injects may also be needed if the participants take the game into an unexpected direction.

To assist planning, an exercise simulator can be used to collect the injects into a single view in which the participants can access and examine them. For more information on exercise simulators, see section 6.7, Modelling the operating environment of the exercise.

### 3.4 Technical exercise

**Suitable for improving technical preparedness, familiarisation with systems and recovery tests.**

A technical exercise requires plenty of initial preparation. The idea is to take the exercise experience directly into the IT environment by creating an emergency in it. The exercise consists of identifying, investigating, eliminating and documenting this emergency.

Different incidents, malfunctions and threats can be simulated quite realistically in a technical exercise. The exercise may also be based on testing backup system deployment, recovery from backup copies, or some other method for securing the operation of production systems in emergencies.

The exercise could consist of an unknown device connected to the organisation's network which communicates with a computer controlled by an 'attacker' from outside the organisation. In this exercise type, a simulated malicious device, which generates exceptional traffic, is connected to the production network. The exercise begins as the participants are informed of an initial observation, on the basis of which they have to take the correct action in order to solve the problem.

The exercise environment plays a key role in this, as this exercise type can get very close to actual operating models and processes. Naturally, producing or procuring different devices or programmes that simulate malware take up plenty of resources. Conducting technical exercises is recommended for organisations in which the response to emergency situations has already been examined using other exercise types, ensuring that their processes are effective and up to date.

A technical exercise can also be implemented in a fully simulated environment. In a simulated environment a network, workstations and services are created for the participants, and the incidents occurring in them are investigated using publicly available or generally used tools. Such aspects as the participants' inability to use their own tools and differences between the exercise environment and the participants' actual production environment may affect their experience, even if the exercise is realistic. The participants are thus required to have an ability to adapt to the situation and follow the organisation's processes also in an unfamiliar IT environment.


### 3.5 Capture the flag

**Suitable for improving technical skills and familiarising the participants with systems.**

In Capture The Flag, or CTF, the participants or teams score points by finding 'flags' in IT systems. These flags may be certain strings of characters and letters that the participant enters in the scoring system once they have been found. While the flags may be hidden in many

different locations in a CTF exercise, participants must typically gain access to a protected system and carry out different investigations within it to discover the flags.

CTF is a technical exercise in which a competition between participants or teams is in the main role. CTF exercises can be organised in connection with different events or training days, or as open events over the internet.



Various virtual machines set up for organising technical exercises are freely available online for organisations to use when arranging their own CTF exercises. You can find these exercises on the internet with search terms such as ‘CTF challenge’ or ‘capture the flag cyber exercise’.

A CTF challenge is an easy way of organising technical exercises at the start. An organisation can put together a team and participate in a CTF

competition or event. While the responsibility for organising the exercise is carried by somebody else, the exercise also gives the technical staff good practice in discovering and investigating vulnerabilities in their own networks.

Public CTF virtual machines or exercise platforms are less suitable for examining an organisation’s own processes, but they work well in building up the skills of technical personnel.

### 3.6 Major joint exercises

**Suitable for creating networks, strengthening cooperation and forming situational awareness.**

Many large-scale joint exercises have been organised in Finland over the years, ranging from joint exercises of the authorities to creating interactive networks between organisations. These exercises mainly follow the rules of functional exercises, combined with features of table top exercises. Simulated online environments have also been used. This has contributed technical content to the exercise.

Rather than improving the organisation’s internal processes, the objectives of a joint exercise are associated with examining its networks and value chains. Joint exercises focus on creating shared situational awareness and coordinating the organisation’s and its partners’ activities. Goals also often include practising information exchanges and building a shared understanding of the attacker’s motives, operating methods and objectives.

Some joint exercises are played as technical games, in which the participating teams

compete against each other, defend their game environment and score points.

Earlier experience of exercises is not usually required in order for an organisation to participate in a joint exercise. At the beginning of the exercise, a briefing is held to discuss the objectives, participants and practical aspects of the exercise. While organising a joint exercise often is highly labour-intensive, the investments required from participating organisations are minor compared to the benefits.

As a rule, participation in joint exercises is by invitation. If your organisation is invited to participate in a joint exercise, you should grasp this opportunity, as joint exercises are also excellent venues for getting acquainted with different exercise methods.

Before the exercise, the organisation should determine its own objectives and prepare as far as possible. This way, it can reap the greatest benefit out of the joint exercise. The roles and responsibilities of the persons sent to the exercise, in particular, should be considered carefully, ensuring that they correspond to real-life needs.

## 4 Preparations for an exercise

The lifecycle of an exercise can be divided into three stages: preparation, implementation and evaluation. Analysing the exercise afterwards and putting the lessons learned from it to practice in the organisation's operations are particularly important in terms of the exercise's usefulness. Meticulous planning, on the other hand, ensures that the general course and details of the exercise have been considered carefully. While the preparation and evaluation account for a lion's share of the exercise as a whole, they also prepare the ground for the following exercise. Preparation, implementation and evaluation thus add up to a continuum - a cycle of exercises.

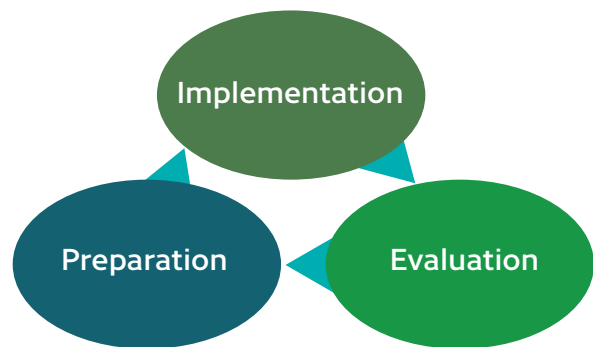
The amount of work involved in the preparations is influenced by the selected exercise type. Preparations required to organise a table top or root cause exercise are lighter than those involved in an functional exercise, but sufficient resources should be reserved for analysing the outcomes.

It may often be justified to organise several light-weight exercises close together, rather than investing a lot of time and effort in a single major exercise every year.

Preparations are the most labour-intensive stage of the exercise. Even if the exercise is outsourced as a service, all parties concerned should set aside a sufficient amount of time for the planning meetings. These meetings should take place well before the actual exercise, starting at least three months before the event.

The commitment of the persons assigned to plan the exercise to the preparations should be ensured early on. Working time should be allocated to the planning, and this should be taken into account in arrangements for these employees' other duties. If the planners are absent from planning meetings, this undermines the implementation of the entire exercise, as they must be familiar with the exercise as a whole.

While everything cannot be planned precisely in advance, the outline of the exercise should be determined accurately enough to minimise any surprises. Using an external organiser is often a good solution, as planning the exercise takes up a large chunk of the employees' working time in the organisation.



Planning a cyber exercise is like carrying out a small project. If it is planned within the organisation, the following sample outline can be followed:

**Kickoff meeting**

- establishment of initial facts
  - objective of the exercise
  - scale of the exercise
  - focus of the exercise
  - possible implementation dates
- initial scheduling of the planning work
- division of responsibilities.

**Planning meeting 1:**

- launch of the project
- assignment of a project team
- allocation of resources to the project
- decision on the objective of the exercise
- selection of the exercise type.

**Planning meeting 2:**

- outlining the content of the exercise
- preparing documentation on the exercise
- selection of participants and invitations
- booking of facilities.

**Planning meeting 3:**

- working on exercise content or injects
- checking and finalising the documentation
- confirming the participants.

**Implementation**

- preparation
- exercise
- debriefing immediately after the exercise (Hot Wash-up).

**Actions following the exercise**

- finalising the observers' reports
- discussions on the lessons learned between the groups involved in the exercise
- monitoring the practical implementation of the lessons learned.

**Conclusion and overall evaluation of the project****Planning a new exercise following an annual cycle**

The organisation can arrange an exercise itself; the benefits of this include lower costs and the possibility of organising exercises flexibly at its own pace. A large part of the planning and preparation work required for an exercise can also be outsourced. This saves the organisation's time, especially if it is supported by an experienced professional. Using outsourced services requires a strong input from the customer, however, as the exercise must be planned to match the organisation's objectives and operating environment. An individualised exercise cannot be purchased as an 'out-of-the box' service.


Plenty of written documentation is created in the planning stage. All documents should be prepared and saved to ensure that they are easily available for use in the future. Many documents, such as feedback questionnaires, different form templates or general instructions for the participants, may be reused with little or no change.

## 4.1 Setting an objective

The progress of the exercise from planning to the evaluation stage is directed by its main objective, which should be defined at the very start of the process. It may concern improved efficiency, safety and security, improving skills or testing a process. The main objective is derived from the organisation's strategy and risk management work.

The objectives should reflect genuine and existing needs. If exercise activities are continued year round, the main goals of each year can be divided into sub-objectives, with a separate exercise organised to address each one of them.

The main objective could be 'cyber crisis management following the Major Incident Management process', and sub-objectives could be 'applying the crisis communication instructions', 'testing the transition to backup system use' and 'verifying up-to-date contact details'. Based on these objectives, the organisation can, for example, start planning a functional exercise



simulating a crisis associated with communication needs and liaison with service providers.

If the objectives are sufficiently concrete, the organisation is able to determine afterwards whether they were achieved. If the objective is of the type 'Improving process x', success or failure is difficult to identify or observe.

The objective of the exercise may be associated with the following aspects:

- developing crisis leadership or communications
- improving technical capabilities
- recovering from an incident
- identifying threats
- reporting
- testing communication methods and backup methods
- testing incident management processes
- testing technical systems to assess cooperation with service and hardware suppliers or to clarify the division of responsibilities.

The objectives should be reiterated at each planning meeting to make sure they are not forgotten. They should also be clearly explained to the participants, ensuring that all those involved have a common goal.

## 4.2 Selecting the exercise type

Any event in which the organisation's activities are tested and developed can be implemented as an exercise. This principle should be remembered when selecting the exercise type, once the objectives, scale and participants have been determined.

Rather than being binding, the features and characteristics of different exercise types can be freely combined. For example, features of a table top exercise and technical exercise can be added to a functional exercise.

Resorting to outside help pays off when planning a multi-stage exercise. An experienced commercial actor will focus on the essential aspects and can help an organisation launch its own exercise activities.

An exercise does not always require physical presence. The participants do not necessarily need to convene at the same location to consider the questions. Using remote connections reduces the need to travel, especially in organisations operating across a large geographical area. Some participants may have consultative roles and be 'on call' during the exercise, participating in the game at times over the telephone or some other type of remote connection. For example, support may sometimes be needed in legal issues.

Participation via a remote connection and while performing other duties may impede concentration, however. This is why remote participants, too, should set aside enough uninterrupted time for the exercise.

If the organisation decides to involve a large number of participants at a time, specific areas may be reserved for remote participation in all decentralised facilities. For example, videoconferencing, instant messenger systems, mobile phones or email can be used for remote participation. The use of remote connections is a good way of testing the organisation's communication tools and, if necessary, backup connections if the situation simulated in the exercise prevents the use of the primary communication tools.

## 5 Planning an exercise

The key part in an exercise is played by the organisation's leadership and the planners, participants and persons in supporting roles. The larger the scale of the exercise, the more people will be needed in different roles.

The management must clearly express its commitment to and engagement with the exercise and the lessons learned from it. Managers' failure to give their unequivocal support to the exercise has a negative effect on the planning

work, as the planners may feel that their working time is wasted on unnecessary work.

If the continuity of the organisation's operation in emergency conditions can be tested in the exercise and the outcome is that the capability to operate is maintained, this knowledge also benefits the management.

The following section describes the key tasks and arrangements in planning and implementing an exercise.



## 5.1 Convening a planning team

At least three or four meetings should be reserved for planning an exercise. Preparing a story and injects for the exercise also requires separate working time. The planning team members should not be participants, as their advance knowledge of the game events would unavoidably influence the course of the game. The planning team could also be known as the project group.

The planning team must have a leader who convenes the team and assumes responsibility for leading the exercise. He or she also serves as the project manager of the exercise. The team should also include experts who are sufficiently familiar with the organisation's operation to take responsibility for the content of the exercise. External experts, service providers or other representatives of the organisation's partners may also be invited to participate in the team and contribute new perspectives and skills to its work.

All planning team members must know their roles and tasks. When an external partner is involved, they usually take charge of leading the planning work, organising the planning team meetings and assigning roles to the planners according to their strengths.

An example of planning team members and their roles:

- exercise leader: head of information security or an external partner
- leader of scenario work: information security expert or an external partner
- internal and external communications in the exercise: communications expert or head of communications
- information management, information systems and third-party suppliers
- business unit representative: key account manager or similar
- service provider: a partner company's representative
- service provider: a representative of information security services.

This composition would already be adequate for determining what type of exercise would be the most beneficial for the organisation and how it should be prepared. The list of team members above is only an example that organisations can use to support their planning.

## 5.2 Selecting participants

If the objective of the exercise is to improve leadership in a crisis, the participants must include at least the organisation's managers and communications unit. If, on the other hand, the objective is to improve the operation of the production system in emergency conditions, employees working with the production system should be selected as participants. The appropriate participants in a technical exercise are the organisation's IT personnel, including their supervisors.

The exercise may contain assignments that require the participation of representatives from several different personnel groups. The communications unit should be present in all exercises, as this function plays an important role in cyber incident management – especially in cases where the impacts of the incident are visible outside the organisation. In exercises focusing on internal incidents, communications can help by preparing suitable messages for the organisation's personnel and stakeholders.

Participants with minor roles can perform supporting tasks for the game from their usual desks while performing their normal duties. A participant should not be asked to attend the entire exercise if their role is limited to answering a few questions, for example. Whether the participant's role is small or large, a deputy should be selected for each one to perform the original participant's tasks in their absence. This way, unexpected absences will not stall the exercise.

Employees essential for the content of the exercise are often involved in planning it and usually do not participate in the actual exercise. Deputies can be trained to take their place, or they may only be contacted by telephone during the exercise. In this role, the planner should focus on solving problems coming up in the exercise only in the light of the facts reported by the participants. A planning team member may partici-

pate as a player, but as they know the twists and turns of the exercise, their role in the game should be modified accordingly.

Quality rather than quantity should be stressed in the number of roles. If an excessive number of participants are invited to attend, the situation may become chaotic. There is no need for higher management to attend an exercise organised for technical personnel, for example. In situations that require decision-making, on the other hand, having access to middle management or team supervisors is important.

As a rule, the participants' roles in the game should be relevant to their real-life job descriptions.


Those selected to participate must make time for the exercise. A typical exercise can easily take the whole day, including preparations and the debriefing.

## 5.3 Preparing for an exercise

The exercise is an exceptional situation for many of the participants, and consequently, it should not be taken for granted that they know how to prepare for it.

The participants should be informed in advance of what accessories or tools they will need. If they will need personal computers in the exercise, this should be made clear, and the sufficiency of network connections in the war room should be ensured. Sometimes it is better to avoid the distractions created by computers, as the messages pinging into the work mailbox and mobile phones can easily divert the participants' attention. However, the invitation should state clearly what the participants should bring and what devices may not be used during the exercise.

The most important thing is to have an open mind and a positive attitude towards the exercise as well as to act as indicated by the game events. Sometimes participants may 'play against the game', or try and find loopholes for bypassing challenging game situations.



At other times, participants may get carried away and make moves that would never be considered in real life because of the enormous costs alone. For example: The system used for border surveillance is malfunctioning, and there is a suspicion that it has been hacked. The problem is solved by closing the country's external borders, eliminating the need to use the system.

In real life, this solution would naturally never be used. The exercise should always aim for realism, both in the events and their solutions.

It is the task of the control room to keep both underperformance and excesses in check. The control room can inform the participants that the selected solution will not work and that they have to come up with another one. The participants should be informed of the risks of both underperforming and overdoing it before the game, making them aware of the limitations of their actions and the opportunities offered by the exercise.

## 5.4 Supporting tasks and observers

Employees from other organisations or units can also be assigned on-call roles in the exercise. While they are not present in the war room, they are prepared to answer the participants' questions during the exercise. A typical example of persons in these roles include lawyers, whom the players can contact for support in legal issues if necessary. An on-call role is also suitable for hardware or service suppliers, who may need to answer questions about their capabilities and response times during the exercise.

The participants' supervisors and higher management can also take on supportive roles, unless they are involved in the exercise as actual participants. Independent decision-making and alternative models for making decisions can also be practised by removing some of the persons in supporting tasks during the exercise.

Observers should also be used, as they are important in the evaluation stage. An observer

makes observations but does not intervene in the players' actions. They also report on their observations to the participants and organisers after the exercise. The observer may come from within the organisation or be an outsider.

It is essential that observers do not interfere with the players' moves or decisions. In practice, the observer should not even talk to the participants. The observer may inform the control room about the progress of the exercise and any problems occurring during it if necessary. This should be agreed on in advance.

The observer writes down their observations in a memorandum. If possible, several observers can be used to monitor different areas of the game. One can focus on decision-making, while the other evaluates the exercise arrangements.

In the evaluation stage of the game, the observers give immediate feedback to the participants and organisers. They later submit a finalised memorandum on their observations. These notes help improve future exercises. Instead of writing a memorandum, the observers can also respond to a feedback questionnaire sent to them after the exercise, in which the respondents' roles are itemised.

A form can be prepared for the observers' memorandum, covering the areas to be monitored in the form of questions or fields to be completed. This can help direct the observations. The questions in this form may include:

- How were the leadership responsibilities divided?
- Was enough attention paid to communications at the right time?

It is impossible, and indeed unnecessary, to prepare an all-inclusive and generally applicable form. Each form should be tailored to an individual situation, taking into account the objectives, emphases and participants of the exercise. By using the same form again in similar exercises, the organisation can monitor its development in organising exercises.



## 5.5 Facilities

Well-managed facilities arrangements are important for a smoothly running exercise. The type of the exercise, the venue and the number of participants to a great extent determine the facilities needs. A group focusing on a specific area always needs a room of its own: one room must be reserved for the participants and another for use as a potential control room. In a table top exercise, for example, no control room is needed, and the entire exercise can conveniently be implemented in a single room.

If there are several participant groups with different tasks, they should be placed in separate rooms, or their areas should be separated with screens. Good air conditioning and sufficient space are needed to ensure that a long exercise session does not become unnecessarily tiring. Paper and pens for taking notes, a flap chart or a whiteboard, and refreshments if necessary should be available in the facilities.

Bringing the participants together in the same room helps them focus on the exercise. The situation often feels artificial compared to an actual crisis. A real-life crisis would take several days, whereas in an exercise, it can typically be shortened to a few hours.

The facilities should be labelled clearly, for example “EXERCISE IN PROGRESS”, including the date. Corridors adjacent to the war room and other areas used by the participants should be marked clearly to avoid misunderstandings. If a participant talks about issues related to the exercise on the phone in the corridor, a passer-by

may overhear some of the call and become worried. An example of the importance of exercise hygiene: An employee who was unaware of the exercise overheard a telephone call in which a participant talked about a chemical container overturned in the warehouse, and a real-life fire alarm was raised.

The facilities in which telephone calls related to the exercise can be made, or in which issues relevant to it can be talked about, should be made clear to the participants. Marking the facilities is particularly important if control rooms or other operative facilities are used in the exercise.

In a functional exercise, a one-way video link between the control room and the war room can be set up. This link can be used to observe the participants and guide the game based on their reactions. The video and audio link can, for instance, be set up by means of a video call on a laptop, in which the video camera at the control room's end has been covered and the microphone turned off.

The participants often have a lunch break during the exercise. A ‘time leap’ in the exercise may be built in the lunch break, for example to the following day, making it possible for game time to exceed the time reserved for the exercise.

If the exercise has a large number of participants, separate facilities for having lunch should be provided. A discussion about the exercise in the staff restaurant may leak from one table to the next and get rumours going.

## 6 Contents of an exercise

The events of an exercise usually take place in the present time and current operating environment, and the participants act as indicated by the organisation's existing structures and daily activity. If necessary, imaginary conditions may be created, such as exercises set in the future or emergency circumstances. An exercise taking place in the future may, for example, be based on international operations which are only being planned in reality but have already been launched in the exercise.

Exercises can also be set in a completely fictive environment. This method may be used in large joint exercises, where it is impossible for each participant to act as indicated by their real-life job descriptions. In this case, the objectives of the exercise can also be set at a higher level, such as developing network-based co-operation.



## 6.1 Exercise scenario

The exercise scenario is a story that sets out the fictive conditions and events of the exercise. It is typically based on an information security problem and its background.

The organisation's risk management work is a good starting point for creating a scenario. Starting from identified risks, scenarios can be based on events that would follow from the realisation of risks. Alternatively, a short informal meeting can be held at which the participants come up with different threats that might affect the organisation. Technology sector news and the National Cyber Security Centre's Cyber Weather can also be used to create scenarios.

Scenario creation begins with a concise description of a problem, which defines the core of the scenario. For example, 'our inventory management system will be out of action for 72 hours'. This underlying problem is used as the basis of the exercise scenario: not only the conditions that created the problems but also the consequences of the problems. The participants' task is to solve these problems. The causal chain could be as follows:

'A former employee has fallen out with their supervisor. The employee had access to the central server of our inventory management system and installed on it malware that wipes the server hard disk clean at midnight on 1 March. The game events take place in the morning of 2 March.'

The first employees arrive at the logistics centre but are unable to print dispatch notes or check orders. The centre's operation grinds to a halt. The entrance gate becomes jammed as trucks cannot get the products they need from our warehouse. This also causes congestion in the local area.'

In a functional exercise, the participants are not immediately informed of the scenario. The first inject is, for example, based on the

message that employees in the morning shift send to information management. The injects are scripted to fit in with the scenario, and their purpose is to inform the participants of the scenario events as the exercise progresses.

In a table top exercise, the scenario may be described to the participants at the beginning, e.g. in the form of an example. In this exercise type, the participants identify and solve problems and problem situations arising from the scenario.

## 6.2 Injects

The injects contain information on the basis of which the participants make their moves. An inject is sent from the control room to the players using a communication device. The uses and contents of injects vary in different game types.

In practice, an inject is an information package that gives the participants information about game events. An inject may be:

- an email message
- a photograph
- a letter
- a telephone call
- a news article
- a social media post
- a physical object
- a file
- a notification from the authorities or something else that describes the events of the scenario in some way.

Such tools as a spreadsheet program can be used to prepare the injects, making it easy to keep them in chronological order. This table can be used to follow up the progress of the game. It is a good idea to create the injects hierarchically, and to collect injects related to a certain event under the same heading. This clarifies the planning of the exercise and helps the planners to keep the events straight.

An example of a table with hierarchically organised injects:

### Case 1

#### Attack against the customer database

- Event 1.1 – Data breach
  - Inject 1.1.1 – Email
  - Inject 1.1.2 – Telephone call
  - Inject 1.1.3 – Request for an interview
- Event 1.2 – Blackmail
  - Inject 1.2.1 – Notification to the authorities
  - Inject 1.2.2 – Urgent request

### Case 2

#### Critical equipment malfunction

- Event 2.1 – Production system outage
  - Inject 2.1.1 – Telephone call
  - Inject 2.1.2 – Email
- Event 2.2 – Public notification
  - Inject 2.2.1 – Email

The information related to the injects collected in the table may contain some of the following:

- ordinal
- publication time
- event to which the inject is relevant
- inject description
- recipient
- sender
- inject type (email, telephone call, letter, image...)
- inject content (email message, script for a telephone call...)
- inject status (played, waiting, to be rejected)
- dependencies on other injects.

The injects should be prepared in advance as far as possible, ensuring that they can be sent to the players without delay. The control room monitors the inject table throughout the exercise and sends the inject messages at the scheduled time or as a reaction to some decision or action taken by the participants.

Time	No.	Event	Description of input	Sender	Recipient	Input type	Content of input	Status
9.00	1	Instructions for game	STARTEX	Game Centre	All exercise participants	Email	<p>***EXERCISE***EXERCISE***EXERCISE***</p> <p>The exercise has begun. Inputs will be sent from this email address.</p> <p>***EXERCISE***EXERCISE***EXERCISE***</p>	Completed
9.30	2	Disruption in the Registry	Malware	Game Centre	ICT Services	Email	<p>***EXERCISE***EXERCISE***EXERCISE***</p> <p>From: <a href="mailto:jukks@gmail">jukks@gmail</a></p> <p>To: <a href="mailto:ITsupport@organisation.fi">ITsupport@organisation.fi</a></p> <p>Subject: Registry computer frozen — help!</p> <p>Hi!</p> <p>We appear to be having a problem with one of our computers here at the Registry. It won't let us log in, and there's a strange image on the screen. Could someone pop by here at the <a href="#">Loimaa</a> office to take a look at it?</p> <p>You can reach me at 044 xxx xxxx. My work email isn't working at the moment, so I'm sending this from my personal address.</p> <p>Best,</p> <p><a href="#">Jukka Järvinen</a></p> <p>Registry</p> <p>***EXERCISE***EXERCISE***EXERCISE***</p>	Awaiting completion

When preparing the injects, the planners should note that it can take the participants an unexpectedly long time to process an individual inject, and an exact estimate of how long it takes to process an inject is thus impossible to give. However, the estimated time it takes to do so should be taken into account when planning the game. The actions the participants are presumed to take can be listed underneath the inject, helping the planners to estimate how long the interval between the injects should be. The number of injects should be kept reasonable.

The participant group often consists of experts or directors in different fields. In this case, one inject can be sent to information management, while another one is simultaneously sent to communications. Participants representing different functions can play parallel events that require their particular expertise. In a game planned to a high standard, the injects played in parallel are interlinked and guide the participants to co-operate but also to manage their own tasks.

The creation of injects is only limited by the planner's imagination. In crisis leadership exercises, one of the injects can be contacts made by journalists. A journalist and a cameraman can even be sent to the participants to record a real-time interview concerning the game events. Different injects provide opportunities for practising many types of skills required to cope with a cyber incident leading to a crisis.

### **6.3 State of the world**

If the exercise is set in circumstances differing from real life, background description material ('state of the world') can be created to support the exercise scenario. A typical exercise is played in the organisation's current and real-world operating environment, in which case no state of the world descriptions are needed.

For example, the state of the world may draw on news about a strained political, economic,

environmental or social situation. While their influence on the game is not straightforward, they can be used to guide and restrict the participants' options for making decisions and to liven up the game. The participants may be provided with background information in advance to increase their motivation and help them immerse themselves in the game.

As an introduction to the exercise can be used a news broadcast prepared in advance, for instance, which is shown to the participants just before the exercise starts. The broadcast may either be directly about issues concerning the organisation or contain background information related to the circumstances.

### **6.4 Communications related to an exercise**

Key elements of the exercise are communicated to the participants and the rest of the organisation in messages prepared in advance.

A general information bulletin about the exercise should be prepared and distributed inside the organisation. It should include the time and place of the exercise and a list of participants invited to it. The invitation to the exercise should be sent out early enough. This way, confirmation of participation and binding registrations can be obtained.

A week or two before the exercise, instructions are sent to the participants, which contain information about the practical arrangements, the objective of the exercise, a list of participants and the schedule followed on the day of the exercise.

After the exercise, a thank-you message as well as a summary of the exercise and the feedback collected on it are sent to the participants. It is also a good idea to prepare a short message describing the outcome of the exercise and the feedback collected on it for the entire organisation. A public press release should also always

be prepared on the exercise, as these exercises strengthen the organisation's public image as an actor that takes cyber incidents seriously.

The importance of communications is stressed especially in functional exercises, in which communication between the participants and the control room is in key role. The control room should at the very least have an email inbox reserved for the exercise and a telephone number that works as the command centre's 'exchange'. By contacting the exchange, the players can ask for any person they need to talk to. It is then up to the control room to play the required role on the phone or to say that the requested person is not available.

In addition to the exchange, dedicated telephone numbers can be reserved for those playing different roles in the control room, enabling the control room representatives to talk to different participants simultaneously.

A specific joint number can be organised for any authorities participating in the exercise, at which the participants can contact the police, the National Cyber Security Centre or any other authority whose support is needed in the exercise. These telephone numbers and email addresses are collected in a phone book, which is printed out for the game participants. No other contact details may be used during the exercise, and this is why the contact details of those performing supporting tasks or participating in the exercise by a remote connection should also be included in the book.

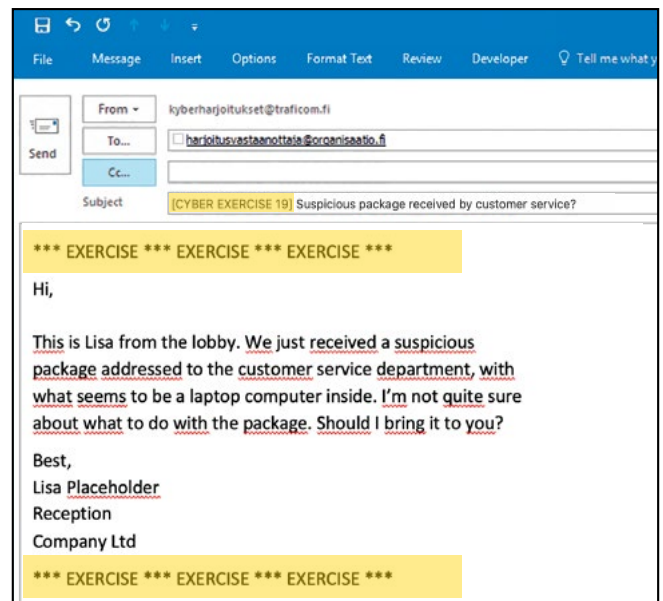
The control room's inbox should be monitored continuously during the exercise. Any messages received should be read and responded to without delay and systematically. If the injects are sent to the participants as email messages, the control room officer in charge of the inbox can also send the injects.

## 6.5 Marking exercise documents

Any messages and documents related to the exercise should be marked so that they can be clearly identified. For example, it is a good idea to add the word EXERCISE in document headers and footers in a red font.

Documents containing imaginary personal data should also be processed in compliance with data protection legislation in the exercise. Unwanted documents should be destroyed after the exercise as indicated by their confidentiality classification; documents associated with the exercise may also contain genuinely sensitive data.

Following an established practice, email messages can be marked as shown in the example. Markings related to the exercise are highlighted:



The heading of an incoming message contains the exercise identifier. This way, messages related to the exercise can be located and filtered easily.

The content field of a message should begin with an identifier that clearly labels it as a message related to an exercise, for example one containing the word 'exercise'. The content field should also end with an identifier referring to the exercise.

Labelling messages clearly is important in the interest of exercise hygiene. Out of context, a message related to an exercise may be misinterpreted. The content field should clearly indicate the sender, as messages are typically sent from the control room's address.

## **6.6 Aborting an exercise**

In some cases, an exercise may need to be aborted. This may happen if the organisation encounters a genuine crisis in the middle of the exercise. In this case, the code word 'real-world threat' can be used to indicate that the current problem is not part of the exercise.

Issues related to aborting the exercise are set out in the exercise documentation. An aborted exercise is usually not continued later, as concentration on its content would have been disrupted. Real-world and exercise events may get mixed up in the participants' minds, with negative impacts on the exercise outcome.

## **6.7 Modelling the operating environment of an exercise**

Simulating or modelling the exercise environment means representing real-world functions and resources as credibly as possible in the game context. Media sources or social media, for instance, can be modelled using appropriate software or facsimiles.

Modelling public communications is relatively straightforward, as they usually are one-directional. Technical solutions are not needed to prepare press releases in a table top exercise, for instance. In a functional exercise, the control room may receive press releases prepared by the participants and produce injects based on them.

Modelling the media and especially social media, however, requires a technical environment. Various exercise simulators, which can be used to communicate in the social media and also to

model other communications, are ideal for this purpose. Different types of instant messaging or publishing software are also an option if they can be applied and used creatively.

In a technical exercise, the technical operating environment in which the exercise events mainly take place is modelled. There are several exercise platforms in the market for modelling servers and workstations. The platforms often have a selection of out-of-the-box sample exercises, which the organisation should familiarise itself with.

While simulations using different systems are needed to create the environment for a technical exercise, a simulator can also be used in a functional exercise to move the game story along. By using simulators, you can ensure that the participants have simultaneous access to the information needed in the exercise.

Out-of-the-box solutions for simulating an exercise are available in the market. A simple exercise simulator can be based on a free WWW publishing platform, for instance, on which scheduled injects are created in the form of articles. However, this solution does not have the purpose-built features offered by the exercise simulators in the market.

## **6.8 Teams in a technical exercise**

In major joint exercises played in a technical environment, colour codes are commonly used to identify different teams' roles and tasks. The most common team colours are red, blue, white and green. Purple, yellow, grey or other colours may also be used as required by the game and its needs. The teams' colour-coded tasks are usually specified in the exercise documentation, as excluding red or blue, the colours do not have standardised international interpretations.

The common practice is that the actual participants are known as the blue team.

In major joint exercises, there may be several blue teams. In these situations, the blue teams may compete against each other for points scored by successfully defending the systems.

The opponent of the blue team is the red team. The task of the red team is to attempt to achieve its pre-defined goals, for example taking over and controlling a technical system protected by the blue team.

The red team is tasked to set a challenge to the blue team, adapting it to the defenders'

actions and counterattacks. The red team usually consists of the exercise's organisers or technical experts specifically invited to join in the game.

The organisers, the participating teams' contact persons, or the persons representing the control room or other game administrators are the white team. The green team is responsible for maintaining the network and game infrastructure as well as providing technical support during the game.



## 7 Lessons learned from an exercise


Through careful analysis, the best benefits can be obtained from an exercise. The observers play a key role in this work. By combining the observations of the participants, organisers and observers, a versatile picture of the exercise can be put together, which can be used as the basis of future development efforts. Evaluation and analysis should be understood as the most important stage of the exercise.

In addition to identifying development areas, concrete actions for intervening in them should be set out in the evaluation stage. These actions should be scheduled and followed up to ensure they are not forgotten about.

The exercise fosters a feeling of being able to manage crises and emergencies, but regrettably often the organisation relies on individual employees for the lessons learned. A precondition for ensuring that the lessons learned from the exercise benefit the entire organisation is making actual changes in the operations. We should remember that observations based on which the organisation's operation can be improved may already come up in the planning stage of the exercise.

When setting the objectives of the exercise, the activity that the exercise will improve is identified. This assumption may be correct, or the exercise may bring up completely new and unexpected development pathways and areas. Both outcomes are useful. The purpose of the objectives is to point the direction for the planning of the exercise, not to limit the benefits derived from it.





An immediate debriefing is organised after the exercise at which the participants and organisers can express their initial impressions and observations of whether or not the exercise was successful. At the same time, opinions on the organisation of the exercise can be collected, and the tension building up during the exercise can be released. The participants often also have questions that they were unable to ask during the exercise. A control room representative should be prepared to explain about the exercise' implementation, story and state of the world to the participants and justify the choices made in the exercise.

It is also a good idea to ask the participants and organisers to give written feedback. Freely worded answers or a form that enables gauging the exercise's success also in numerical terms are good choices for this.

The observers finalise their feedback and submit it to the organisers. If a questionnaire has been prepared for the feedback, it can be used multiple times, in which case information on development achieved in the interval between the exercises can be collected in a 'response database'.

A summary of the lessons learned and proposed actions is distributed to the participants for information. Proving that the exercise has helped identify areas of development and that it will be used to change practices will also motivate employees to participate in future exercises.

When the lessons learned have been put into practice in the organisation's daily work, they will be accounted for in the following exercise. For example, once a process has been developed, it is a good idea to re-test it in different circumstances and when facing with a different challenge to see if the development is headed in the right direction. An effective existing process can also be used in an exercise scenario; this may help modify it and improve it further.

The purpose of an exercise is to pinpoint weaknesses in processes and practices, not in employees. It is important to avoid strong experiences of personal failure in the exercise. The participants should be reassured that they can safely take action and try out bold solutions in the exercise – also in chaotic situations.


Positive experiences are important for the continuity of exercises. The successes of participants who did particularly well should be highlighted at the debriefing.

## **7.1 Planning a feedback survey**

A survey tool should be used when collecting feedback. Among other things, browser-based tools are highly suitable for this. The tool makes it easy to repeat the same survey after the following exercise and, at the same time, evaluate improvements achieved in the exercise activities. The survey also gives the participants more time to provide feedback and compile their observations. While it does not replace oral feedback, giving written feedback suits some people better.

An exercise organised by a third party usually includes a feedback questionnaire, which contains questions about the arrangements of the exercise and the organisation's incident management. The purpose of the questionnaire is primarily to collect information about the investigation of the actual cyber incident, and only in second place to gather feedback on the arrangement of the exercise.

Whereas giving critical feedback orally in front of the participants may appear impossible to many, giving written feedback is easier. Any criticism levelled at the exercise should be received with an open mind, attempting to understand what the feedback is based on. It is often possible to take the issue or phenomenon in the backdrop of the criticism into account in the next exercise.



Critical feedback is a positive thing, as it creates an opportunity to improve exercise activities.

Giving clear-cut scores to different areas of the exercise facilitates evaluating the exercise as

a whole and provides an opportunity to report on the exercise experiences in clear-cut figures. A feedback questionnaire on an exercise should cover at least the following:

**Respondent's role in the exercise**

- organiser, observer, participant, other supporting tasks
- leadership, information management, service provision, other unit

**Practical arrangements**

- facilities
- scheduling
- information
- refreshments

**Method of arrangement**

- Were the participants selected appropriately?
- Was the method used in the exercise appropriate?
- Were the instructions sufficient?

**Game content**

- Was the scenario credible?
- Was sufficient information about the events provided during the exercise?
- Were the state of the world descriptions credible and compatible with the exercise?

**Development of professional competence (subjective evaluation)**

- Can be presented as a set of claims: 'I found the exercise useful' etc.
- Was situational leadership successful?
- Were the existing incident management processes developed successfully?

**Willingness to participate in following exercises**

- 'I will be happy to participate in future exercises.'
- 'I will recommend exercises to my colleagues.'
- 'I experienced the exercise as meaningful.'

**Open feedback on the exercise**

- What I liked/did not like, ideas for developing the exercise, freely worded feedback.

Once feedback has been collected, it is compiled into a clear presentation, removing any identifying information, and distributed to the participants.

## 8 Exercise activities as part of cyber security management

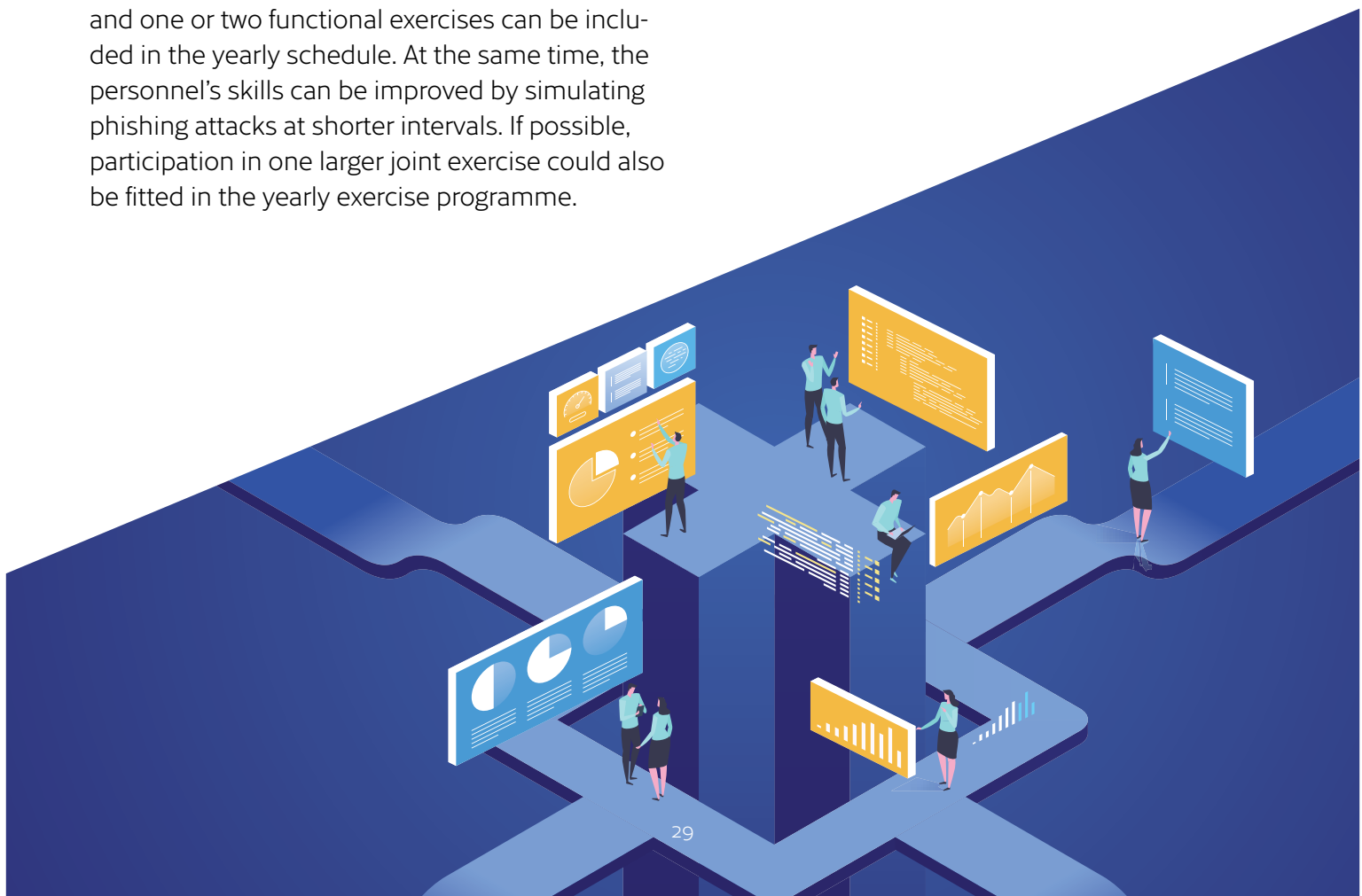
The ownership of the exercise activities within an organisation affects the way in which they will be developed. Cyber exercises do not differ significantly from other crisis exercises, and if your organisation already has experience and competence related to exercises, for example in the industrial security unit, you should utilise it when planning cyber exercises.

Rather than remaining isolated events, exercise activities should assume a key role in cyber security management. This way, the organisation's continuously improving cyber security activities and culture can be scheduled and tested. Exercises can also help strengthen cooperation between the organisation's different divisions.

Rather than repeating similar exercises every few months, different exercise types can be scheduled around the year as a series that forms a clear entity. For example, a few table top exercises and one or two functional exercises can be included in the yearly schedule. At the same time, the personnel's skills can be improved by simulating phishing attacks at shorter intervals. If possible, participation in one larger joint exercise could also be fitted in the yearly exercise programme.

The scale of its exercise activities naturally depends on the organisation's size and resources. Small organisations have more limited possibilities of arranging exercises than larger ones.

Relying on cooperation networks when organising exercises is also a good idea. Different communities, information exchange networks or expert groups can implement an exercise played in connection with a joint meeting or seminar, for instance. Alternatively, a meeting can prepare an exercise that each member plays in its own organisation. Finally, the outcomes can be examined together and compared. A jointly planned cyber exercise played simultaneously across organisational boundaries opens up excellent opportunities for practising cooperation in major incidents.



Strategic goals lay the foundation for selecting the main objectives of the exercise programme in a specific year, and the goals of individual exercises can be derived from these main objectives. This way, rather than being isolated from other information security work, the exercises become a key part of it.

The exercises can be divided into different annual themes in terms of their content. They do not necessarily have to be cyber themed, as the same exercise methods can be used to practise for different physical world and business crises. The impacts of problems associated with cyber incidents extend far beyond the actual information systems.

At best, the entire organisation can participate in regular exercises. While information management and senior management naturally use different methods and practise different aspects, the exercises of both groups are significant, important and part of well-planned cyber security management.

## 8.1 Long-term planning

Planning the following year's exercises should be started in good time by putting together the main themes for developing the organisation's cyber security work in that year.

In a large organisation, the list of themes and the schedule on which a yearly calendar of exercises can be based could be such as the following:

### **March 2020, table top exercise**

- theme: long-term disruption of production system operation, testing of backup methods
- participants: production managers, line supervisors, communications.

### **May 2020, technical exercise**

- theme: recognising attackers' actions and logging them in the production system
- participants: SOC, information management.

### **June 2020, table top exercise:**

- theme: a key hardware supplier will cease to operate or is sold overseas
- participants: management, communications.

### **September 2020, technical exercise**

- theme: recovery from backup copies
- participants: information management.

### **November 2020, functional exercise for the management**

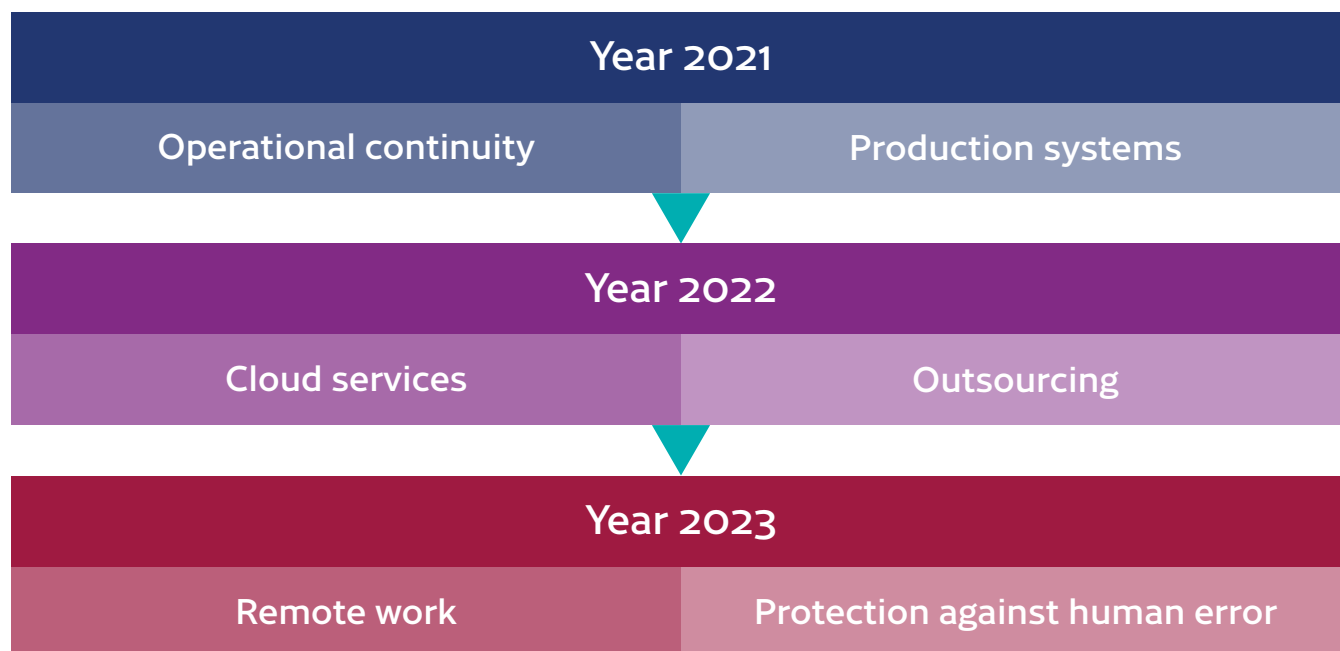
- theme: data breach in the production system, malfunction, insiders as an information security threat
- participants: management, major incident, management team, communications.

In example X, the exercises in 2021 focus on guaranteeing and testing the reliability of the production system. While the themes are linked, they target different parts of the organisation. The annual schedule includes table top, technical and functional exercises. As they are based on a common theme, the exercises support each other and form a clear-cut whole. Some of the exercises are light-weight and easy to arrange, while others require slightly more time. If you alternate between light and more heavy-weight exercises, this gives you an opportunity to organise versatile exercises throughout the year. A regular cycle helps employees keep the themes covered in the exercises in mind around the year.

As the overarching theme of the year can be selected an abstract entity, such as 'data protection' or 'technical information security'.

The organisation's risk management work as well as the operating environment and changes occurring in it point the direction for selecting themes. The themes can be planned to form a continuum that provides a natural bridge between the yearly programmes. Annual themes also help target information security work, as the security issues relevant to the theme receive more attention.

Each organisation determines its annual objectives and plans its exercise cycle around its basic operations. In the above example, two annual themes have been selected, but each organisation must choose their themes as indicated by their own needs. Annual themes can be further broken down into objectives in keeping with the policies defined in the organisation's information security strategy.



## 9 Conclusion

We hope that these instructions have been helpful in planning and launching your organisation's cyber exercises. Starting exercise activities is easy and straightforward, as the simplest exercise methods can be translated from an idea into practice within minutes.

After starting with simple issues, the organisation can gradually transition to more complex ones, and making up the devilish scenarios and extravagant plots for a larger exercise may soon become the highlight of the information security year.

More information about organising exercises is available in the following publicly available works, among other things:

- Handbook for planning, running and evaluating information technology and cyber security exercises (Center For Asymmetric Threat Studies, Swedish National Defence College, 2011)
- Exercise Guidance Basic Manual – An Introduction to the Fundamentals of Exercise Planning (Swedish Civil Contingencies Agency MSB, 2009)
- Manual and script for organizing cyber crisis exercises based on Cyber Crisis Exercise OZON (SURF Utrecht, 2017)
- Planning an Effective Incident Response Tabletop Exercise (Secureworks, 2018).

### 9.1 Contact details

The National Cyber Security Centre's support services for exercise activities are available for organisations critical for security of supply. If you are interested in organising your first cyber exercise or finding a suitable partner to support your exercise activities, or you would like some help with organising an exercise, please contact our support service for exercise activities by email at [kyberharjoitukset@traficom.fi](mailto:kyberharjoitukset@traficom.fi)



## 9.2 Key concepts

### Exercise hygiene

A practice for ensuring that the contents of the exercise do not leak outside the group of participants or the facilities. See sections 5.5. Facilities and 6.4 Communications related to an exercise.

### Exercise programme

An annual programme prepared by an organisation that describes its exercise activities at a general level. The exercise programme contains all exercises planned and played during the year. See section 8.1 Long-term planning.

### Exercise simulator

An information system devised for describing the events of an exercise and used to inform the participants of the events. See section 6.7 Modelling the operating environment of the exercise.

### Exercise scenario

An entity consisting of the events and state of the world descriptions of the exercise, which sets out the content of the exercise. Also 'scenario'. See section 6.1 Exercise scenario.

### Exercise teams (e.g. blue and red team)

Colour codes for participants and organisers with different roles in the exercise. Used especially in technical exercises. See section 6.8 Teams in a technical exercise.

### Exercise type

The method of playing and the type of game selected for the exercise. For example a table top, functional or technical exercise. See Chapter 3, Different types of exercises.

### Exercise environment

A technical environment in which the exercise is implemented. The exercise environment may be an information system or a company's field of operation. For the concept of a technical exercise, see section 3.4 Technical exercise.

### Hot wash-up

A debriefing session immediately after the exercise. See Chapter 7 Lessons learned from an exercise.

### Evaluation

Collecting and analysing the lessons learned after an exercise, evaluating them and translating them into practical actions. See section 7 Lessons learned from an exercise.

### Cyber exercise

A security exercise focusing on incidents affecting information systems or information security and their extensive impacts on an organisation. See Chapter 2 What is a cyber exercise?

### Player

A participant in an exercise. See section 5.2 Selecting participants.

### Control room

A room from which an on-going game is directed and moved forward. See section 5.5 Facilities.

### Pre-mortem

A root cause exercise which starts from the consequences and looks for their potential root causes. See section 3.2 Root cause exercise (pre-mortem).

### Simulation

Describing imaginary events as part of an exercise. See section 6.7 Modelling the operating environment of the exercise.

### STARTEX, ENDEX

Commands that start and end an exercise, shortened from "start exercise" and "end exercise". The exercise begins and ends with the STARTEX and ENDEX messages.

### State of the world

A background story describing the initial situation of the exercise that can be used to create emergency conditions for the purposes of the exercise. See section 6.3 State of the world.

### Inject

An individual event or message, or other information communicated to the participants, that moves the story along in an exercise. See section 6.2 Injects.

### Inject table

A table of game injects which forms the game content in an exercise. See section 6.2 Injects.

### Observer

A person whose task is to observe an exercise and make notes of their observations. See section 5.4 Supporting tasks and observers.

### Real-world threat

An expression used to abort an exercise and to communicate about a real-life problem or hazard. See section 6.4 communications related to an exercise.

**For more information about cyber  
security, please contact us via:**  
[ncsc-fi@ncsc.fi](mailto:ncsc-fi@ncsc.fi)

**Finnish Transport and Communications  
Agency Traficom  
National Cyber Security Centre Finland**

PO Box 320, FI-00059 TRAFICOM  
tel. +358 (0)29 534 5000  
[traficom.fi](http://traficom.fi)

**TRAFICOM**  
Finnish Transport and Communications Agency  
National Cyber Security Centre