December

enisa
European Network and Information Security Agency

This report is part of ENISA's Multi-annual Thematic Program One (MTP 1), Resilience of Public e-Communication Networks.

With this Program the Agency, among others, takes stock of and analyses Member States (MS) regulatory and policy environments related to resilience of public e-Communication Networks.

This report is based on the responses given by experts from public and private stakeholders from several Member States and overseas. ENISA would like to thank them all for their excellent contributions and insights.

ENISA would also like to thank IDC CEMA for their professionalism and dedication to manage the stock taking and contribute to this report.

More information on this report or ENISA's activities on the resilience of public eCommunications Networks can be obtained by

Dr. Vangelis Ouzounis

Senior Expert, Network Security Policies, ENISA

Email: resilience@enisa.europa.eu, Web: http://www.enisa.europa.eu/act/res

The European Commission and Member States are focusing attention on the role that exercises can play in increasing the resilience of public eCommunications networks.

Exercises enable national competent authorities responsible for public communications networks to target specific weaknesses, increase cooperation across the sector, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience.

Several Member States have been conducting exercises for years, including a wide range of discussion-based exercises and operations-based exercises. Those conducting exercises experienced all benefits mentioned above. As a result, momentum and interest on exercises among relevant stakeholders is spreading.

ENISA prepared a good practice guide to assist authorities in Member States to better understand the complexities of exercises and help them prepare local and national ones. This guide was prepared by interviewing experts on exercises throughout the EU and beyond with the aim to identify good practices that were already applied and proved to be effective.

This guide examines these practices by first giving an introduction to the subject of exercises, then reviewing the life-cycle of an exercise (identifying, planning, conducting, and evaluating) systematically. Also, the roles of the involved stakeholders are presented. Throughout the guide, good practices are highlighted for easy identification.

Some of the key findings and practices discussed in this guide include:

- Identifying the Exercise:
    - Identify the measures to be tested first. That includes identifying the processes that need testing, and the people involved in those processes. Then build the exercise (type, scenario, participants, etc.) around these critical factors.
    - Keep in mind potentially limiting factors, such as budget, resources, experience with exercises, and level of commitment of the desired participants. Where any of these factors are in short supply, it is best to start modestly with simple, small exercises, and then build up from there.
- Planning the Exercise:

- Planning is a large endeavour that often exceeds expectations in terms of resources, budget and time required. Ensure that you have more than enough of all of these at the start of planning.
- Include key exercise participants in the planning phase, in order to ensure that the exercise addresses the issues that they consider most important, that the scenario is as realistic as possible, and that participants are fully committed to the exercise.
- Use a gradual planning process to build consensus, commitment and trust among participants.
- Ensure that scenarios are realistic, that they prepare moderators for the varied responses and actions of participants, and that they include the necessary injects that drive the scenario along.
- Ensure during planning that monitors are selected, trained, and outfitted with any necessary tools or materials, so that they can carry out their duties during the exercise without a hitch.
- Consider the media's role in the exercise, possibly providing scenario injects, as well as what policy you will want toward the media during and after the exercise.
- Prepare all required tools and materials to enable all participants, monitors and other players to perform their duties effectively.

- Conducting the Exercise:
  - Provide training or briefing for participants at the start of the exercise. The scenario must remain secret, but the participants will need to understand the general conditions, the rules of the exercise, their roles, and the roles of the monitors. And they may require some training, if special tools will be used to simulate their duties.
  - Ensure that there is a central exercise management team or moderator managing the scenario, while monitors sit closely with the teams of participants. The monitors will observe participants for the later evaluation, as well as report actions and decisions of the participants back to the moderator, and then take new information from the moderator in order to provide the scenario injects to participants.
  - You may need to notify the media in advance of the exercise, and possibly have a media policy in place for handling media inquiries during the exercise.

- Evaluating the Exercise:
    - Give the evaluation process a high level of commitment, in order to ensure that the lessons from the exercise are effectively learned and acted upon.
    - Avoid blaming participants or preparing a pass/fail-type of evaluation. It is crucial to generalize the conclusions and recommendations, in order to ensure that participants remain cooperative and willing to participate in future exercises.
    - Evaluation should be a process that includes participating stakeholders and builds consensus around the conclusions and recommendations. The process can also be extended to later follow-up on recommendations, develop an action plan, or otherwise develop forums for cooperatively addressing the issues raised in the exercise.
    - Consider how you will measure success of the exercise, and include steps that will enable you to measure. For example, surveys of participants before and after the exercise to measure changed perception of certain issues, or a survey at the end to evaluate the effectiveness of the planning and execution.

Many more details are discussed in this guide. Still, this guide is but an introduction to many of these issues. To help take readers further, this guide also includes references to some additional materials that can help authorities to organize exercises to help take you further.

Beyond the materials, the interviews with experts revealed that there is an enormous wealth of knowledge and experience with exercises from which others can learn. Just as one major benefit of exercises is to build cooperation across the sector, the interviewed experts expressed much interest in cooperation themselves. And for those new to exercises, one of the most effective steps you can take will be to participate with these experts in cooperative efforts across the EU, developing contacts, and asking further questions.

In recent years, the use of public eCommunications networks has expanded rapidly to encompass a far wider range of services and applications. This transformation, expansion, and broadening of uses continues unabated. These networks have become critical infrastructure for Europe's Member States, public institutions, societies and economies.

The European Union's institutions have recognized the importance of public eCommunications networks and the need to expand the efforts to ensure their resilience.

The Commission in the context of its i2010 Program (COM(2005) 229) issued a strategy for secure information society (COM(2006)251) giving emphasis on dialogue, partnership and empowerment. This strategy initiated a dialogue on the security and resilience of public communication infrastructures.

The policy debate in the Council and the Parliament and the public consultation pave the way for the CIIP Communication in 2009 "*Protecting Europe From Large Scale Cyber-Attacks And Disruptions: Enhancing Preparedness, Security And Resilience* (COM (2009) 149).

This communication focused mostly on "prevention, preparedness, and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs."

Among the actions proposed in this communication are steps to:

- Improve coordination and cooperation across the EU;
- Define a minimum level of capabilities of national and governmental CERTs;
- Foster a European Public Private Partnership for Resilience (EP3R);
- Develop principles and guidelines for Internet resilience;
- And conduct pan-European exercises on large-scale network security incidents by the end of 2010, and prepare a proposed framework and roadmap for European participation in global exercises.

The CIIP communication recognised that simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIIs.

Via the CIIP Action Plan, the European Commission invited Member States to develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination.

The involvement of ENISA was called upon to support the exchange of good practices between Member States in that area. The CIIP Action Plan further proposes the development of pan-European exercises on Internet security incidents, which may also constitute the operational platform for pan-European participation in international network security incidents exercises, like the US Cyber Storm.

The Commission's Communication was discussed at the EU Ministerial Conference on Critical Information Infrastructure Protection in Tallinn, Estonia in April 2009. After two days of discussion, the Member States and the Commissioner for Information Society, Viviane Reding, agreed on the "Tallinn process" to proceed with the objectives set out in the Commission's communication, including conducting a pan-European exercise in 2010.

Given this strong commitment to CIIP by both the EU institutions and the Member States, as well as the role designated to ENISA, and the objectives to proceed with pan-European exercises, ENISA has undertaken initially to help Member States and the EU institutions to proceed toward pan-European exercises by facilitating an exchange of ideas and experience with exercises and identification of good practices. This guide is a key element of this effort.

This guide aims to support stakeholders to design, plan, execute and monitor a national exercise on the resilience of public communications networks. In particular, this guide aims to support public authorities that do not have significant experience in planning exercises.

These exercises aim at testing the preparedness of a sector (or multiple sectors) to cope with and recover from incidents that disrupt or threaten the availability or the security of critical information infrastructures.

It aims to help stakeholders to identify and develop the skills needed to identify measures and processes to be tested, plan, execute and evaluate sectoral and cross-sectoral exercises themselves and use this experience gained by the stakeholders to improve their measures and processes.

This guide was prepared by surveying and interviewing public authorities, network operators, IT industry players, and network security experts about their experiences, expertise, and recommendations for effective practices in planning and executing exercises. The project began

initially with questionnaires distributed to these experts. The experts were located primarily in the EU, though some were also located in other parts of the world, particularly in the United States. After distributing the questionnaires, the completed questionnaires were collected and arrange interviews with as many of the experts as possible.

The questionnaires were initially sent out in July 2009, with interviews then taking place in August and September 2009. In total, 26 questionnaires were received, 29 interviews conducted, and a total of 32 organizations contributed either by the questionnaire, the interview, or both.

In parallel to the survey and interviews, secondary research was also conducted to identify exercises and practices in the critical information infrastructure sector on other regions of the world. Furthermore, discussions with some key experts were followed up on some of the exercises and practices identified through this procedure.

Following completion of this research, good practices were identified and assembled in this Good Practices document.

The results of the research and the Good Practices guide were reviewed by ENISA, and also distributed to experts for commenting. As a result, this document represents a broad consensus of a wide selection of public and private-sector experts on good practices in preparing exercises to enhance resilience of critical information infrastructures and public eCommunications networks.

This guide examines the good practices for organizing exercises by first giving an introduction to the subject of exercises, then reviewing the life-cycle of an exercise (identifying, planning, conducting, and evaluating) systematically. Each of these four life-cycle steps is reviewed in a separate chapter. Each chapter breaks down the discussion into sections that discuss the key issues that organizers will need to address while they are working through that step in the life-cycle. Examples and quotes from the interviews are included where relevant to reinforce provide the reader specific examples and expert views.

Throughout the guide, good practices are presented in separate boxes for easy identification.

Preparedness exercises have long been widely used in various sectors, and they have been adopted by many players in the ICT sector, especially telecoms network operators and computer emergency response teams (CERTs). Exercises are particularly useful for training staff on procedures to follow in the event of an emergency at some point in the future. They form an integral part of many organizations' business continuity planning, as they provide crucial benefits:

- Exercises ensure that staff are fully prepared and capable of responding to incidents by efficiently following business continuity and disaster recovery procedures.
- Exercises can reveal weaknesses in those procedures, such as unexpected implications of a given type of incident, enabling managers to revise and improve the procedures.

Most exercises are conducted internally by an organization, to test preparedness for potential disruptions, attacks, or other emergencies. However, many incidents affect more than one organization.

Some incidents affect many different organizations at once, such as a natural disaster that damages many types of infrastructure at once. Additionally, many such incidents reveal interdependencies between organizations. Below are two examples.

: An incident disrupts telephone calls in a given area, impacting other organizations

- Such an incident may affect the calls of other telecoms operators that depend on part of that network.
- Or it may disrupt the telephone services of emergency services in the area.
- Or the disruption may prevent technicians in the area from being called in to fix an electrical outage.

: A flood causes widespread failures in a telecoms network, knocks out electrical power, makes key transportation routes unusable, and puts lives in danger. Such an incident involves numerous interdependencies:

- The power outage may disrupt additional parts of the telecoms network.
- The telecoms network outage may prevent technicians from being called to fix the electrical outage.
- Technicians may not be able to reach the backup telecoms facilities, due to closed transportation routes.
- People at risk may not be able to call emergency services for assistance.
- Emergency services may not be able to coordinate their response to these diverse challenges. Etc.

In such ways, incidents can cascade from one organization to another, often in complex ways.

Similarly, many incidents require more than one organization to work together in order to solve the problem.

: A computer security attack occurs in which a botnet with widely scattered computers launches a distributed denial of service (DDoS) attack against a company's servers. Such an incident may require a response from multiple organizations:

- The company will need to take actions internally to cope with the attack.
- Their network operator may assist by blocking some traffic or IP addresses.
- Other organizations whose PCs have been infected and controlled by the botnet may need to disinfect the PCs and then coordinate with network operators and blacklist managers to unblock its IP traffic.
- Software vendors may have security patches to fix the vulnerability that enabled infection by the botnet.
- Other organizations (such as CERTs) may have been tracking this botnet's activities, and may have some advice on how to thwart it or to disinfect the botnet's computers.
- And public authorities may need to get involved to conduct a criminal investigation, or to consider possible national security implications.

In such a scenario, some means for quickly sharing information across these organizations and coordinating the response is desired.

And exercises across these organizations are an important way to ensure that such communications and coordination procedures function correctly, and to ensure that all organizations are prepared to act as required.

Such exercises can be held across a sector, or even across multiple sectors. By training together, the participating organizations can achieve many benefits:

- They can identify interdependencies that they may not have been aware of.
- They can practice working together with their counterparts at other organizations.
- They can share best practices in their procedures.
- They can test whether their own procedures work well in practice.
- They can test emergency contact information and channels of communications across organizations.
- They can develop trust across organizations to jointly work toward more resilient networks.
- They can demonstrate preparedness to their customers, partners, and regulators.

crisis preparedness to be able to play with other stakeholders; crisis preparedness is vital for our

Such exercises also yield other benefits for the public authorities responsible for resilience of public communications networks. These authorities usually do not have high visibility into how the individual players and their infrastructure will cope with an emergency.

The authorities' duties include:

- Determining how resilient the networks will be,
- Identifying weaknesses in network resilience,

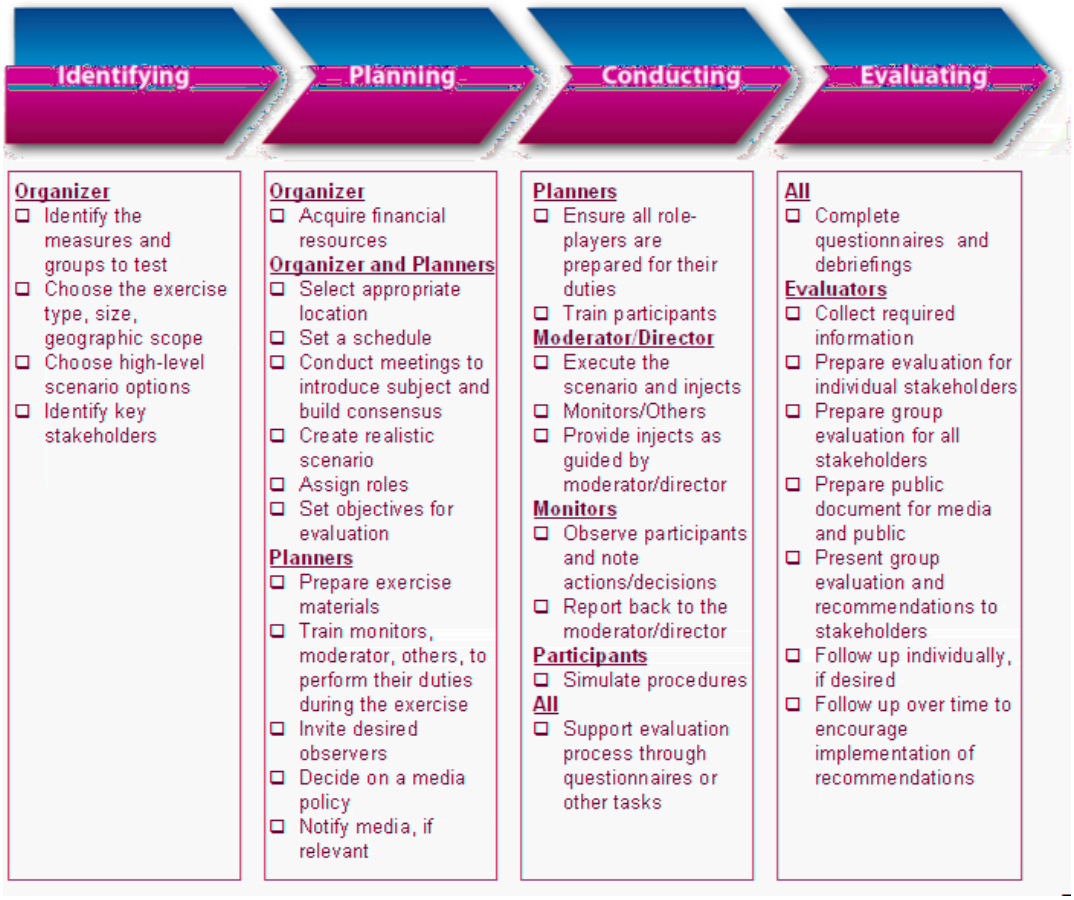
- Identifying weaknesses in incident response procedures,
- Targeting action plans for improvements,
- And measuring improvements.

Exercises can be a powerful tool to help authorities with these duties:

- The authorities can observe incident handling in practice.
- They can increase awareness of interdependencies among the various organizations responsible for public communications networks.
- They can stimulate cooperation and public-private partnership in the efforts to increase resilience of public communications networks.
- They can target scenarios that they deem important, or specific procedures or functions where they have identified a need for improvement.
- And by repeating exercises, they can track changes over time.

Planning and executing an exercise effectively are challenging goals. To achieve success, it is necessary to carefully and diligently proceed through many individual steps, working out a huge amount of detail in the process, while balancing the sensitivities of various organizations and individuals whom you would like to commit their time, resources, and attention. These numerous steps together form the life-cycle of an exercise.

An exercise's life-cycle can be divided into four segments, as follows:



These lifecycle segments broadly involve the following elements:

1. : In this segment, the organizer must identify a need for an exercise. This need will include identification of procedures or measures that require practice or improvement and should be exercised. Based on this need, organizers can then select what type of exercise to conduct, and what organizations should participate.

2. : In this segment, the organizer will drive the planning process. This process will involve recruiting the participants; acquiring financial resources for the exercise; selecting (and booking) the location, developing the scenario, rules, tools, and training materials for the exercise; selecting monitors and other role-players, and specifying what and how they will perform their duties; and planning the evaluation process.

3. : In this segment, the exercise itself takes place. As specified in the planning process, participants go through (by discussing or actually acting out) the scenario and their response procedures and decisions. Monitors observe and note these actions, and inject information into the scenario.

4. : Finally, after the exercise itself, the evaluation process takes place. This process tends to include a final evaluation report, or multiple reports tailored for different audiences. These reports review the exercise, identifying weaknesses, and recommending improvements. Furthermore, this process may include an ongoing process or forum by which to continue to address the weaknesses and recommendations identified.

The following chapters examine each of these segments of the exercise life-cycle in detail, identifying practices that have been shown to be effective by those authorities conducting exercises to improve

- Setting up and dismantling the exercise environment;
- Starting and ending the exercise;
- Acting as the central point of contact for questions and problems which arise in the course of the exercise;
- Making ad hoc changes to the plans or calling a premature halt to the exercise in the event of serious complications which cannot be resolved;
- Facilitating tabletop exercises;
- Managing the scenario;
- Coordinating supplies for the exercise participants (e.g. catering);
- And other related duties.

In smaller exercises, such as desktop exercises, these responsibilities may lie entirely or mostly in one key person, possibly called the Moderator. In larger exercises, these roles may be more finely subdivided, possibly with an exercise director, scenario manager, and other support players, possibly acting jointly as the exercise leadership team. In this guide, we generally use the terms director or moderator to encompass this range of responsibilities.

- The roles of monitors and facilitators are related and overlap. In this guide, the term monitor is used to apply to both. Those in this role brief the participants on the initial situation before the exercise, and inject new information during the exercise. They then observe and record the actions and decisions of the participants during the exercise, checking performance of the tested measures, noting effectiveness and weaknesses, communicating with the moderator, and providing much of the material that will be required for evaluating the exercise.
- Observers are individuals or organizations that are invited to observe the exercise, without participating nor monitoring performance. They may include stakeholders who are not otherwise participating, such as additional organizations outside the scope of the exercise (e.g. neighbouring regions or countries), public authorities that do not have an active part to play in the exercise, or others.
- Evaluators are those individuals involved in the process of evaluating the exercise. These may include some or all of the same people and organizations who participated in planning and/or the exercise itself.

At the beginning of the exercise life-cycle, the organizers will need to specify what are their needs and resources for exercising, and identify the most suitable kind of exercise to prepare. Departing from some general considerations, which we should introduce at the beginning of this section, the organizers will make important decisions on the outlook of the future exercise. The present section will review these decisions, focusing on several key points, as summarized in the following figure:

Conducting an exercise brings many benefits in the efforts to increase resilience, but it is a challenging task. There are many different types of exercises, they can vary significantly in complexity and size, and they can test any number of different procedures and scenarios. To get started, organizers must consider several issues, such as:

- The measures and processes to be tested. Accordingly, the exercise might focus on testing command communications lines, drilling a specific function, or on developing a business continuity plan.
- The target group for the exercise. For example, the exercise might focus on the performance of operational staff, operational managers, or senior managers.
- The resources available for planning and conducting the exercise. That involves human resources, especially experts among the organizers' staff who can devote their time to preparing the exercise, and also the budget allocated to the exercise.
- The degree of commitment that can be expected from participants.
- The previous experience with exercise on the side of both the organizers and participants.

First of all, the decisions about the targeted measures and groups are critical. Based on the answers to these questions, organizers can begin to specify an exercise type and general outline of the scale and scope.

The other items should also be considered from the start, as they set parameters about what is possible and feasible. A successful exercise requires resources for planning and execution, as well as commitment from participants. It also requires significant skill during each phase of the exercise life-cycle. But exercises vary greatly in complexity, with some very simple ones requiring little planning, resources, or experience, while at the other end of the spectrum, full-scale exercises can include hundreds of organizations and thousands of people, requiring very large amounts of planning, resources and experience.

Organizers should have some understanding of these factors, in order to plan an exercise that has a high chance of success.

If these factors are judged insufficient for a given exercise, there are ways to address the shortcoming. For example:

- Organizers can take time and effort to build commitment from participants,
- They can increase their resources and exercise skills by hiring or partnering with external organizations to assist,
- And they can increase their (and the participant's) exercise skills through experience by starting with smaller exercises and building toward larger goals.

All of these issues are discussed in detail in the rest of this chapter.

- *Consider what needs to be tested and the target group for the exercise first.*

- *Keep in mind that the resources available for an exercise, the commitment of participants, and the skill required to plan them vary greatly, depending on the measures to be tested and the type of exercise. These factors will define the limits of what is feasible in your situation.*
- *If necessary, work to expand these limiting factors by building consensus among desired participants about the need to exercise, by gaining experience with small exercises first, and by hiring or partnering with external organizations for assistance.*

An important initial step in organizing an exercise is to identify a need. The exercise should test some specific measures that will be taken or processes that should be followed in the event of an incident. Organizers should seek to identify specific measures that require practice, training, review, or improvement.

> *[NL] As one expert explained, the first thing is to identify the goal or purpose of exercising with the stakeholders/organizer(s); the rest follows quite logically then, including the scale, type, scenario, and location.*
>
> *enarios. Stay*
> *focused on these objectives. And measure the outcome and success of the exercise based on*

In sectoral exercises or cross-sectoral exercises, these measures should include cooperation and coordination activities across organizations, in order to test and improve cooperation, and to reveal interdependencies.

The measures selected may address different target groups, from lower levels of operations, up to senior management levels, depending on the specific needs identified.

And the exercise may focus narrowly on one specific function or procedure, or may encompass comprehensive incident response procedures across organizations and sectors, as in a full-scale exercise.

One of the most common examples of measures tested by several of the interviewed experts was communications lines between organizations. In the event of an incident, one of the first steps to take is to notify various agencies dealing with response (e.g. CERTs), authorities, suppliers and customers about the incident, so that they can take action as needed. Several experts mentioned testing these communications channels, confirming that contact details are up to date and that people can be reached right away.

Many other functions and procedures can be tested in a similar way.

Some examples of measures tested include:

- The common situational awareness of the participants,
- Elements of business continuity plans,
- Adherence to those plans,
- Speed of response,
- Decision processes,
- Information sharing (internally and externally),
- Collaboration (internally and externally) to address the problem,
- Coordination of resources, logistics and support capabilities,
- Resilience of the environment (what survived and what didn't),
- And many other topics.

To put this into context, we can see some real-world examples from past exercises:

[FR] Organizers noted testing response and recovery times, testing new procedures, identifying vulnerabilities, and discussing counter-measures.

[DE] Exercises tested contact details (such as availability and reaction time), procedures (such as Standard Operation Procedures (SOPs), escalation levels), and situational awareness.

[HU] Exercises tested counter-measures, preparedness, incident handling procedures, standard operating procedures, and preparedness.

[FI] Exercises tested capacity for cooperation, modes of cooperation between various organizations, operability and usability of various communications and information systems in an emergency situation, ability to form situation picture, operational readiness, sufficiency of the powers of the authorities, and best practices.

As organizers consider the measures to be tested, they may also want to consider some options, including alternative measures to test. They may want to prioritize these measures to decide which to test.

- *Identify a need in the form of one or more measures that require testing.*

- *Consider some alternative measures of similarly high priority for testing.*
- *Identify the stakeholders that are responsible for those measures and that would play key roles in exercising these measures.*
- *It is useful to choose measures that address coordination and cooperation across organizations, in order to test and improve cooperation and to reveal interdependencies.*

Once decisions are made about the measures to test, organizers can start to consider plausible high-level scenarios that might be developed to enable testing of these measures. A realistic scenario is critical to the success of the exercise.

The scenario will be developed in detail during the planning process that incorporates key stakeholders. This process is discussed in detail below.

However, before involving other stakeholder organizations in the planning, organizers should consider high-level scenarios that address the organizer's goals and suit its preferences. Choosing a suitable high-level scenario at this time is useful for two important reasons:

- It can help in recruiting participants to the planning process, giving stakeholders a concrete idea of the purpose of the exercise.
- It sets a clear path forward for the planners, before those planners are recruited. By contrast, if the choice of high-level scenario is left until the planning discussions are underway and stakeholders have gotten involved, organizers may have a more difficult time steering planning in the direction that they want it to go.

Although organizers should choose a high-level scenario at this early stage as an option, they should also consider that the planning process may reveal problems with this choice, or reveal that another scenario might be more suitable. Many organizers will therefore want to consider and select some alternative high-level scenarios at this stage for consideration early in the planning phase.

- *Start to focus on a high-level scenario that enables the exercising of the measures you have identified for testing.*
- *Consider some alternative high-level scenarios, as well.*

There are many different kinds of exercises that you may choose to conduct, each with different formats, benefits, challenges, and costs. There is no international standard taxonomy of types of exercises, though there are many commonly used terms and categories.

Most practitioners of exercises distinguish between discussion-based exercises, and operations-based exercises.

Discussion-based exercises enable planners and participants to examine scenarios, develop response procedures, test those procedures, and test decision-making. Participants only discuss these topics, rather than acting them out. Such exercises may include *seminars*, *workshops*, *tabletop exercises*, or *games*.

- A provides instruction and discussion of plans and procedures, for example to instruct staff on new or changed procedures.
- In a , experts and managers will gather to hold a constructive discussion in which they work through a theoretical scenario, considering implications, procedures, interdependencies, and decisions. Such exercises are particularly useful for jointly developing new procedures to cope with possible incidents.
- In a , participants will gather to work through a scenario and existing procedures for responding to it. Typically a facilitator will guide them through, with participants stating the steps they would take and the decisions they would make, as the scenario unfolds. Such exercises are particularly useful for ensuring preparedness and familiarity with the procedures.
- A is similar to a tabletop exercise, except that participants are divided into two or more teams that work through the scenario separately in a competitive atmosphere.

Example:

- *The telecoms authorities in Ireland organize regular exercises, with one recent example being a tabletop exercise in which several telecoms network operators simulated a physical incident in this case a chemical spill at a switch. The exercise focused on performance and mutual communication of teams.*

Operations-based exercises enable the testing of procedures and ensure preparedness of staff to follow them. These exercises involve acting out the procedures in practice. They may be narrowly focused on a specific operation or function, such as a drill to test a communications link. Or they may be larger in scale, exercising the coordination of different departments or organizations. Or they can be much larger in scale, involving many organizations, many departments, and large numbers of people acting out their roles through a scenario. Of course, the larger exercises require far more planning and commitment.

Examples:

- *ministries (Interior, Economic Affairs, Water Management & Transport, and other), crisis response centres, water boards, emergency structure, police and rescue forces, military support, and others. The scenario also integrated local scenarios into the core national scenario. Over 10,000 people participated during one week. The scenario included large scale flooding of several parts of the country. Planning lasted two years, and preparation involved the work of hundreds of people.*

- *Norway has several authorities conducting exercises, including annual national exercises, such as one in December 2008, called ICT 08, that focused on IT and telecoms networks. This exercise was a countrywide exercise that covered several sectors, including network operators, service providers, power providers, finance, and various kinds of customers vital to communities. The Norwegian Post and Telecommunication Authority (NPT) conducts its exercises every second year.*

- *Cyber Storm is a series of full-scale exercises organized by the United States Department of Homeland Security. Cyber Storm I and II took place in 2006 and 2008. The first was a national exercise, while the second was international in scope. Participants included public (international, country and state level) and private (companies or sector associations) organizations across multiple sectors. The exercises tested response to and recovery from cyber-attack on national critical infrastructure. A sequel, Cyber Storm III, is planned for 2010.*

Each of these exercise types yields different benefits, enables the testing of different measures, and involves differing degrees of costs and challenges. A robust exercise strategy

will likely include multiple types, in order to test all of the measures that the organizers have identified a need to test.

- *Choose the exercise type to fit the need you have identified and the measures that should be tested.*
- *Consider a strategy that incorporates different kinds of exercises to test various measures.*

Choosing the participants clearly follows from the decisions about the measures to test and the type of exercise.

Once the objectives have been decided and sectors considered, the individual participating organizations can be considered.

There are different roles that people and organizations may play in an exercise. These roles are discussed in the section above, *Overview of Exercises: Exercise Roles*. These roles broadly consist of the organizer, planners, participants, exercise director/moderator, monitors, and evaluators.

A stakeholder can have several roles in the exercise lifecycle, and typically, the major stakeholders contribute individuals to several or most of these roles. For example, a major stakeholder may contribute to the planning process, have other individuals participate in the exercise itself, have others (possibly, but not exclusively, the individuals involved in planning) serve as monitors, and then have some individuals additionally participate in the evaluation. Conversely, stakeholders could serve only a single role.

At this point in the exercise's life-cycle, the most important roles to consider are the key exercise participants. The desired participants should be key stakeholders in the measures to be tested. The choice of these key participants will enable organizers to begin recruiting them to participate in planning and the exercise itself.

In a sectoral exercise, planners may want to involve all key players in that sector. In other cases, such as cross-sectoral exercises, or geographically localized exercises, it may be sufficient to ensure participation by a representative of each sector, or representatives in the exercise's region of focus.

Not all organizations will want to take part. Organizers may need to take this willingness (or lack thereof) into account in choosing key participants. On the other hand, there are ways to increase willingness to participate, which are discussed in the next chapter, under "Recruiting Participants".

The decisions about key participants should be made early in the planning process, to involve their input into creating a realistic scenario and to ensure their enthusiastic participation.

Examples:

-
-

- *Choose the participating organizations based on the measures to be tested, and which organizations are relevant to those measures either directly or indirectly.*
- *Consider also their willingness to participate and the geographic focus of the exercise.*
- *Select the most important participants early in the planning process, so that you can include them in the planning itself to ensure their commitment and a realistic scenario.*

The issue of the size of exercises was a frequent topic of discussion during research for this guide. Experts emphasized that organizing a large exercise, such as a full-scale operational exercise, requires very large amounts of resources, as well as substantial skill, experience, and commitment of participants. For example:

> *[NL] The Waterproef exercise mentioned above required two years of planning and involved hundreds of people.*

Size of the exercise is largely affected by the type of exercise chosen, the measures to be tested, the target groups, participating organizations, and details of the scenario. Based on the research, we have summarized some key advantages and disadvantages of small and large exercises in the table below.

	Large Exercises	Small Exercises
Advantages	• Generate awareness of the issue and need for preparedness at all levels • Generate publicity for participants which can help in recruiting them	• Quick to plan and execute. • Short planning cycle allows for frequent repetition—where useful—or a quick move onto the next topic. • Easy, manageable effort for organizers

	• Give training to large numbers of participants at all levels • Reveal interdependencies across the system • Simulate the stress and tension of real-life incidents, revealing how these affect participants' reactions.	and participants. • Limited number of participants is easy to recruit • Simple to plan and execute (even for beginners) • Focused on specific measures to test and train
Disadvantages	• More costly, in terms of time and budgets • More difficult to plan and execute • Lessons may get lost or diluted in the complexity of the scenario • Large exercises can take a very long time and be difficult to plan effectively	• Attract less publicity and generate less widespread awareness of the issues. • Do not generate the experience of putting all the pieces of emergency management together • May not generate the tension and stress of real-life incidents (particularly in the case of many discussion-based exercises)

Clearly both large and small exercises have merits and a place in the exercise repertoire. Nonetheless, organizers should consider the size of exercises very early in the planning process.

- *Be aware of the advantages and disadvantages of the size of exercises, and ensure your choice corresponds both to your objectives and to any limitations you are under (resources, budget, skills, commitment of participants, time, etc.).*

The geographic scope of an exercise is also an important factor. It can affect the size of an exercise, with a wider geographic scale for an operations-based exercise involving larger numbers of organizations and individuals. However, even if the geographic scope of an exercise is wide, an exercise can be kept simple and include few participants. In any case, size and distance can make planning exercises with wide geographic scope more challenging and costly. But despite the potentially greater challenges, exercises with a wide geographic coverage can spread the benefits of participation to a larger number of organizations and individuals.

Aside from the logistics of planning and the benefits of participation, it is perhaps even more important to consider the nature of the incidents that can occur and for which exercises can help prepare. In fact, while many incidents will be local (a local disaster, terrorist attack, or network fault), many other incidents (or at least their implications) are themselves spread across a wide geographic scale, for multiple reasons. For example:

- A local incident can cascade to other regions, as when a local fire knocks out a critical network node and disrupts wider national and international communications.
- Some potential incidents may take place in multiple locations at once, such as a coordinated terrorist attack.
- Many incidents are themselves geographically dispersed by nature, such as the distributed denial of service (DDoS) attacks launched by international botnets on Estonia in 2007.
- And some incidents may require a widely coordinated response in order to solve the crisis, such as when international knowledge-sharing and cooperation are required to cope with a large-scale natural disaster. This wide geographic coordination can involve incident responders who come from different national and institutional cultures (as well as speaking different languages), adding further challenges.

Since incidents and their responses are sometimes local, regional, national, and international in scope, there is a clear justification for exercising together and preparing for such incidents at all of these scales.

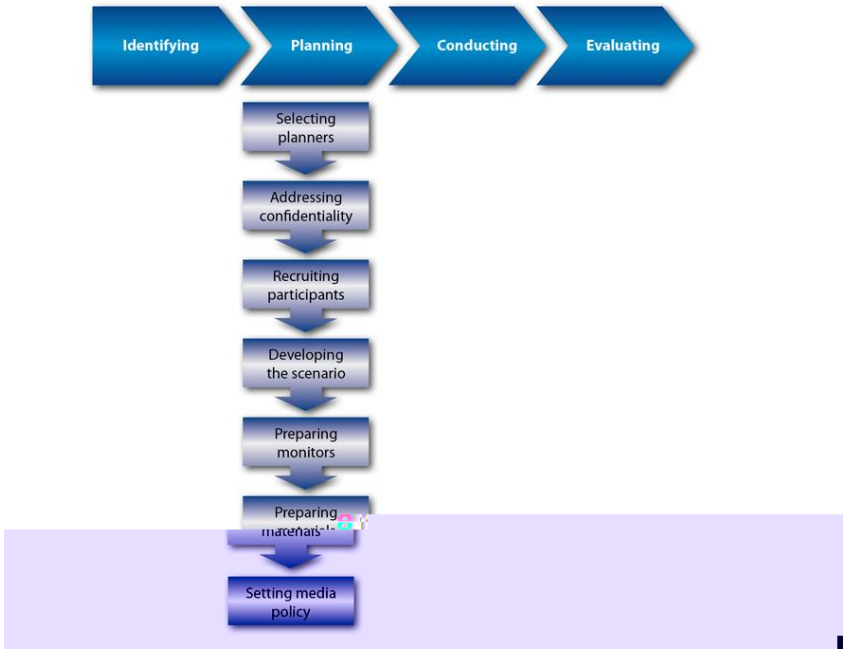
- *Consider exercises with a mix of geographic scales, in order to exercise the procedures to respond to incidents at each of those scales.*
- *Where the everyday cooperation is less established, as often in international scenarios, start small.*

Now that you have made decisions about the needs that the exercise will address, the type of exercise, the desired participants, and the measures to test, you can begin planning the exercise.

Exercises typically require extensive work in the planning phase. Some exercises are simpler than others, as discussed above, but most of them will require an extended planning process to be executed carefully.

The planning phase is important for many reasons. The success of an exercise depends upon the realism of the scenario, the commitment of the participants, and the precision with which desired objectives are aligned with the measures tested, the scenario, and the execution. All of these are essentially decided during the planning phase. Furthermore, the planning phase is a long process that involves extensive examination – and sharing of views – on threats, risks, scenarios, interdependencies, procedures, resources, and other elements of incident preparedness and response. As such, the planning phase is actually where much of the benefit of exercising is gained by stakeholders.

This section examines the planning phase in detail, focusing especially on these key issues:



Before starting the planning process in earnest, you must first decide who will lead the process.

In most cases, the organization that decides on the need for an exercise also leads the planning process. Frequently, the organizer is the public authority responsible for resilience of public communications networks.

If an authority that decides on the need designates others to lead the planning, they will need to ensure that the leader fully embraces the needs and objectives that they have specified, and probably also manage them closely through the planning process.

Organizers in several Member States (and beyond) reported hiring third-party facilitators (consultants) to take on much of the workload in organizing exercises. These experts highlighted the use of consultants for a couple of reasons:

1. They bring expertise (and tools) for development of exercises, which some authorities do not yet have.
2. And they provide many of the resources (including staff) for planning the exercise.

Using such consultants clearly creates a new budget item for the planning authority, but by dedicating these resources to the process, one avoids the problem of adding exercise planning tasks to already-busy internal staff who may not have sufficient time to devote to the tasks.

Hiring such consultants is not unusual, though one expert in Germany emphasized that even with third-party contractors, they need to allocate their own full-time employees to the exercises to work with the consultants and ensure results fit their needs and objectives.

- *If you have identified the need, you will either need to lead the planning process, or ensure that the leader you select fully embraces the same needs and objectives. Even then, you should expect to have to manage them closely.*
- *Ensure that you have enough resources allocated to planning the exercise.*
- *You may want to bring in external consultants to aid in planning the exercise, as they can bring useful experience, tools, and resources.*
- *Even if you use external resources, make sure that you have enough resources internally to work with them, educate them about your objectives, and to ensure their planning stays on track.*

Many of the experts interviewed for this guide emphasized that the planning process tends to be very lengthy and challenging.

- *dou*
-

Experts varied in their estimates of the amount of time needed to plan an exercise. Schedules will vary, based on:

- Size and complexity of the exercise;
- Preference;
- Degree of commitment by participants that exists;
- Amount of resources dedicated to it.

The estimate of planning cycles for major exercises usually varied from 8 months to 18 months, though a few estimated slightly less than that, and a few others estimated even more. Some countries and authorities plan major exercises every second year.

Examples:

g process will take approximately 1 year and is driven by monthly meetings of

These extended cycles allow for setting the date of the exercise very far in advance, ensuring commitment, building consensus on the concept and objectives, and gradually hammering out the details.

- *For full-scale operational exercises, allow extended planning cycles of at least a year, until experience is gained that suggests a shorter duration. Smaller exercises, such as tabletops should also start with planning cycles of several months, though this schedule can be adjusted based on the details of the chosen exercise.*

- *For the first exercise, allow extra time. That enables you to ensure commitment from key participants, build consensus on the concept and objectives, and carefully work out all the necessary details.*

Beyond the leadership of the planning process, the question of who else participates in planning is a crucial one. Decisions about participants in planning should be based on the need to make the scenario realistic, and also to gradually build interest in and generate commitment to participating in the exercise. Those organisations or individuals participating in the planning of the exercise are performing the role of the "planner" during the exercise lifecycle.

One key category of participants in planning is that of the key stakeholders in the exercise itself. Experts consistently recommend including representatives of these key organizations in planning.

Once decisions are made about the general concept and objectives, these organizations can be recruited to participate in workshops on the resilience of public communication networks and challenges, and then gradually recruited into planning and commitment to the exercise itself.

It is also important that these participating organizations also contribute to the preparation of the scenario. The specific individuals will not participate in the exercise itself, as the scenario should be kept secret from exercise participants until the event itself. However, in order to ensure that the scenario is realistic, these individuals who have insight into the technical details of how incidents will affect that company, and how the company will react, should contribute to the detailed scenario planning.

In addition to including the key participating organizations in planning, organizers also should consider whether there are other subject-matter experts who might play a valuable role in planning. Such subject-matter experts can bring additional experience and different perspectives to the exercise planning. These experts may stem from various different positions:

- Academia and other research institutions;
- Consultancies;
- The media;

- Think tanks;
- Technology vendors and solution providers;
- Non-profit organizations;
- User's organisations;
- Freelance consultants;
- And other positions.

These organizations and individuals can add insight into how an incident may originate and evolve, what responses from stakeholders may include, how responses of stakeholders (counter-measures) may affect the incident, what interdependencies there are and how they will be affected by a type of incident, and how similar incidents have unfolded and been addressed elsewhere.

Organizers should consider whether there are subject-matter experts who could play a valuable role in the exercise they are planning, such as aiding in the planning of a realistic scenario, moderating, monitoring or evaluating the exercise.

Depending on the role these experts might play, the time required, and their willingness to commit, organizers may wish to consider simply inviting them to contribute, or contracting them to fulfil the desired roles.

- *Include in the planning process representatives of the key organizations that should participate in the exercise. That ensures that the scenario will be as realistic as possible.*
- *Empower these stakeholder organizations to take action by giving them a role in planning.*
- *Consider whether other subject-matter experts or consultants are required, or could help significantly with the exercise planning or other roles, and invite them or contract them to fulfil these roles.*

In selection participants, one topic that may come up is how to cope with confidentiality issues. Companies will frequently be concerned with sensitive corporate information. At the same time, government organizations are likely to have similar concerns about divulging certain aspects of their operations and procedures. In the latter case, some government organizations may want to participate, but will have trouble doing so if for example participation, monitoring, and even planning

these elements of the scenario require security clearances. Organizers will have to cope with these concerns.

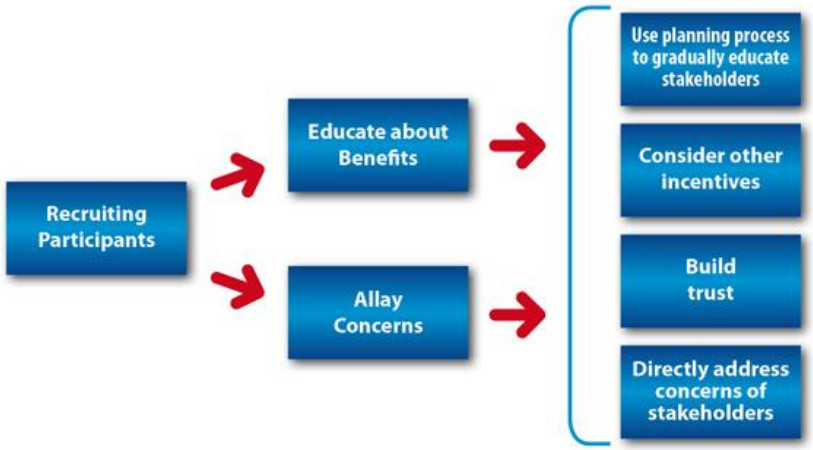
One part of the solution is to reassure participants about confidential issues generally, by emphasizing what information will be collected, by whom, and how it will be used. That includes being clear about how the evaluation process will be conducted. These issues will be discussed in more detail below.

Another part of the solution can be to encourage organizations to develop their own internal scenarios that link to the external scenario and extend from it. Such a choice may not include responses from these groups back to the scenario manager or moderator, and they may not be planned openly with the planning team, but they can still be a useful endeavour for participants.

Finally, in some cases, multiple organizations may like to participate in the scenario, requiring the sharing of confidential data in planning and the exercise itself. In such cases, organizers may like to enable multiple planning teams operating separately, allowing one group with appropriate clearances to handle confidential data, without exposing that data to those without clearance.

- *Plan to enable participants to keep control of their confidential data, and reassure them of this fact throughout.*
- *Consider establishing separate planning groups, so that one can handle confidential data and scenario elements, without divulging that information to those without appropriate clearances.*

Now that you have decided who will lead, who should participate, and how much time to allow, you can begin the planning process in earnest. A key element to planning is recruiting participants and ensuring their commitment. This is a complicated task that can be briefly summarized in the following diagram:



As noted in the previous section, desired participants may not always be interested in participating.

> *Recruitment took over half a year, and only a few agreed in the end. The main problem identified was that they did not want to share security information with an organization with which they did not previously have a relationship.*

There are a few common reasons:

- Organizations may be reluctant to allocate the resources required.
- They may not recognize benefits of participation.
- They may be concerned about confidentiality of their internal procedures or weaknesses that might be revealed during the exercise.
- And some experts pointed out the large number of exercises that can take place, and that participants may need to prioritize.

This reluctance may result in their refusal to participate, or in poor results, if they participate only half-heartedly.

As a result of this reluctance, organizers may need to work to recruit participants.

The first step in recruiting participants, especially reluctant ones, is to raise awareness about the benefits of exercises. The overwhelming feedback from private-sector companies contacted for this Guide was that exercises are very useful for participants. Once a company has participated in effective exercises, they tend to be interested to participate in others, due to the significant benefits they have experienced.

Some of the key benefits to be gained by participants of exercises were discussed above. Highlighting again just a few:

- They can ensure that staff are fully prepared to respond to incidents by efficiently following business continuity plans;
- They can identify weaknesses in those procedures that need attention;
- They can identify interdependencies with other organizations that may need to be addressed in continuity plans;
- They can exercise cooperative procedures across organizations to cope with interdependencies;
- And they can strengthen their working relationship and trust with authorities, customers, and partners

In the *Overview of Exercises* section an extensive list of the benefits of participating in exercises is provided. The key for organizers is to reluctant participants aware about these and other benefits, and the planning process is a key part of that.

The planning process is itself a useful tool in recruiting participants.

Planning processes can start with general seminars and workshops on the themes of resilience, vulnerabilities, and interdependencies. Asking the leading stakeholders in different sectors to present their own views and concerns in these areas is an effective way of engaging them in the process. And by involving the stakeholders in a series of discussions, you can bring them into the community of like-minded stakeholders interested to work together toward resilience.

Once there is broad consensus about the general issues, later steps can move toward identifying the specific need for an exercise, helping to plan it, and committing to participate in it.

This gradual process can convince stakeholders of the need for an exercise, that resource requirements and costs are reasonable, and that they can trust the organizers and other stakeholders.

The most obvious solution for recruiting participants is probably to provide positive or negative incentives. Positive incentives could include financial incentives, such as covering some of the costs of participation. For example, the organizers could ensure that some travel expenses, catering, or other incidental expenses can be covered by the exercise budget. However, the organizers of exercises consistently explained that they are not able to provide financial incentives to cover such costs as the labour time involved.

Similarly, making participation mandatory is not within the authority of most organizers.

As a result, recruitment tends to rely on allaying fears (confidentiality issues), and emphasizing the benefits. These benefits are many, and they are detailed above, while the means for allaying fears follows.

> *[US] Private sector engagement is not given financial incentives, but the private sector often wants to participate to improve security and resilience of the ecosystem at large.*

"Trust" is an extremely important term mentioned over and over again by organizers of exercises. The planning process is a way to jump-start trust, by bringing stakeholders together to share views on resilience and interdependencies, and then working together on a scenario and procedures. Through participation, they can control what is shared voluntarily, recognize the value of the cooperation, and become more comfortable with cooperation with the other stakeholders.

Aside from the exercise planning, many experts emphasized that their key to success has been a gradual development of trust over years. For example:

> *[HU] One organizer mentioned that first exercises should be simple communication checks that enhance trust and cooperation. Then there is progress towards more complex scenarios, and possibly more demanding formats.*

Prior trust has enabled organizers to recruit participants and launch exercises. There are several elements to trust-building that have been mentioned by authorities in Member States. Most authorities have used a combination of some or all of these tools for building trust over time:

- Stating clearly what information will be shared and how it will be used;

- Conducting exercises, of course;
- Ensuring that there is no public criticism of the company from prior exercises or cooperative efforts;
- Maintaining an effective incident reporting process that again is careful not to divulge sensitive data, but that adds value to the resilience effort;
- Preparing analysis of incidents and threats;
- Organizing seminars and trainings on resilience issues;
- And by organizing or participating constructively in forums, working groups or other bodies that help address resilience issues.

Overall, these efforts to build trust and develop a collaborative environment between authorities and other stakeholders were mentioned many times by the experts (both public and private) as being crucial to the successful cooperation and improved resilience over the years.

Exercises rely on this trust, but they also offer a significant way to build it.

[FI] During the planning phase and the introduction period of the exercise the trust is built with

- ith experience have the trust in place from previous exercises.

planning process, including sharing aims and objectives at the start of the planning process, while r

[DE] One organizer explained that you should not expect private partners to do a full-scale exercise with you immediately. Instead, start from smaller scale. Additionally, avoid any negative publicity for the participants in the press in the exercises, or their willingness to participate in the future will disappear.

- *Adopt a gradual planning process that starts with seminars or workshops about resilience, vulnerabilities, and interdependencies. Use this process to build trust among stakeholders, and to educate them about the wider sectoral issues, benefits of cooperation, and benefits of exercises. Then include these stakeholders further through the planning process.*
- *Focus on the trust issue. Trust is built gradually through years of cooperation.*

- *Where trust is already well established, organizers can use that trust to move more quickly in recruiting participants and planning the exercise.*
- *But where cooperation has been less common, and trust is not as fully developed, organizers should take their time to slowly work through recruitment of participants and the planning process.*
- *Leverage a range of tools for building trust, including various other forms of interaction and cooperation with the stakeholders.*

Most of the above steps in planning an exercise are quite broad in nature. But when development of the scenario begins, the focus of organizers will turn to a great deal of detail.

Experienced organizers recommend several guidelines for those developing scenarios.

First of all, the scenario should be as realistic as possible. The incidents should be chosen to seem plausible. That starts from the initial decision about the broad outline of the scenario, and extends through the detailed planning.

[NL] One organizer explained that it is necessary to avoid the situation when participants begin

To ensure scenarios are as realistic as possible, it is necessary to have a good understanding of how the participating organizations function, and how they will respond to incidents. For that reason, it is preferable to include representatives of the participating organizations in developing the scenario.

However, depending on the scenario, the goals, and the type of exercise some non-realistic elements in the scenario may be required. These must clearly be communicated to the participants to avoid discussion about the realism of the scenario ("don't fight the scenario").

Scenarios need to enable exercise moderators to respond flexibly during the exercise. The actions taken by participants will influence the evolution of the scenario for other participants. And since participants will sometimes act differently than expected, the scenario needs to allow for multiple responses and actions of the participants. Since planning for all possible directions that the scenario might take increases costs and can get away from testing of the desired measures, experts recommend preparing to include guiding injects that get the scenario back on the desired course.

The scenario's flexibility should also enable moderators to control the amount of pressure on participants. They should be placed under pressure, but the pressure should not be so great that the

participants completely fail. Moderators will need to balance the pressure throughout the exercise. There should be prepared injects that they can use to do so.

To prepare the scenario, a planning committee will start with a broad concept that suits expectations of key stakeholders. They will then elaborate upon the details, while incorporating input from key participants about the implications of the scenario on their operations, and the procedures they would expect to follow. This process can be expected to require an extended period of time, regular meetings, and substantial work.

> *[SE] One organizer explained that as the organizer of the exercise, they first develop a broad scenario idea at a very high level that everyone could be involved in, then start thinking about the details. Participating organizations are represented in the planning team to help work out those details.*
>
> *[NO] Similarly, in Norway, an organizer reported interviewing the main stakeholders about their objectives, and using that to decide the central scenario. In this case, the decision-making was by consensus.*

- *Scenarios should be as realistic as possible*
- *Scenarios must prepare moderators for varied actions by participants that might steer the scenario in different directions. That might include many different possibilities within the scenario, and it may also include flexibility for the moderator to improvise.*
- *Scenarios need to include detailed injects of new information, both those that planners intend to introduce from the beginning, and others that may be called upon optionally by the moderator, depending on how the exercise proceeds.*
- *Planners need to align the broad scenario concept with the objectives of key stakeholders.*
- *Planners need to then coordinate the details with them through an extended process.*

Monitors have a very critical role in ensuring the effectiveness of an exercise. They perform several crucial tasks:

- Observe and evaluate the participants' actions, decisions, and effectiveness
- Report this information to moderators

- Relay injects and other necessary information to participants
- Answer participant questions
- And provide essential input for the post-exercise evaluation.

During the planning process, monitors for the exercise will need to be selected. Additionally, the monitoring process and measurements will need to be designed, so that the monitors have clear guidance on what to measure during the exercise itself, and tools for doing so, if needed.

The choice of monitors varies, though they should usually have been involved in the planning process, so that they fully understand the scenario and the responsibilities and procedures of the participants they will be observing.

Ideally, the monitors should have experience monitoring exercises. Where the organizer has already planned several exercises, they may have such people on staff. Alternatively, they may like to bring in other organizations or consultancies with experience monitoring exercises. Or combine the two options. Experienced monitors will be more effective in evaluating the actions of those they are monitoring and providing the additional scenario injects.

There is a question about whether monitors should be employees of the organizations they monitor, or independent of them. In most exercises, planners choose to use independent monitors. Such monitors can come from the organizing authority, from other institutions, or consultancies specialized in exercises. Such monitors bring objectivity and independence. However, independent monitors may make participants more tense about conducting their duties under this external observer.

Less commonly, the monitors in some exercises are representatives of the participating organizations, in a form of self-monitoring. Self-monitoring ensures that someone who is very familiar with the internal procedures of a company observes these procedures in action. However, self-monitoring is also likely to result in far fewer critical details being reported to the evaluation team.

- *One exercise organizer explained that individual stakeholder organizations monitor themselves, prepare their own analysis of the internal results, identify internal lessons learned, and decide how and whether to act on the lessons learned. In this way, each exercise is an opportunity for each stakeholder to practice and learn from others, but it is up to them each to decide what was learned and what to do with that knowledge.*

- *External monitors are recommended for exercises in which organizers expect to obtain a full report about effectiveness of the exercise and to be able to make and follow up on recommendations for improvements.*
- *Self-monitoring may be best for cases where organizers are less concerned with learning the lessons themselves, than with providing an opportunity for each organization to learn its own lessons and decide what to do with them.*
- *Experienced monitors are of course preferred; where inexperienced monitors are used, they will need training in advance on their roles.*

Monitors will also need training on their roles in advance of the exercise. Their roles can be quite challenging, as they must understand what to observe, how to record their observations, what and how to communicate to the moderator, what and how to communicate to participants, and what their responsibilities are for assisting the evaluation process.

In order to ensure the monitors carry out these duties as effectively as possible, they should receive training, including training materials (discussed below), and also briefings, seminars and/or rehearsals.

[SE] One organizer noted that the monitors receive two to three training sessions.

- *Ensure that monitors have sufficient training so that they are ready and comfortable in carrying out their duties.*
- *The monitors will need some specific materials for conducting their jobs, as well as training in using them, possibly including some form of rehearsal or acting out of their roles.*

Monitors' roles during an exercise are discussed further in the chapter on *Conducting an Exercise.*

Planners will need to consider whether observers should be invited to the exercise. Observers can include organizations relevant to the scope of the exercise, or to the wider effort to ensure network resilience, but that are not actively participating in the exercise in other roles; also, they are excluded from decision-making procedures.

For example, they might be public authorities involved in planning the national emergency management strategy who should understand the challenges faced by the ICT sector. Or high-level officials interested in the overall emergency management capabilities. Or critical information infrastructure managers in other regions not part of the exercise.

There can be various other reasons planners may wish to invite other observers. Planners simply need to consider whom they want or need to invite during planning, so that they can ensure the observers have a chance to attend.

- *Consider during planning whether there are additional organizations or individuals who should be invited to observe the exercise.*

During planning, the organizers will need to decide on a media policy. That policy may be simply to notify the media in advance of the exercise, or even not to engage with the media. In discussion-based exercises, little or no media involvement may be feasible and preferred, depending on the exercise. However, media policy can be quite important for a few reasons:

- Participants will be wary of allowing the media to see any vulnerabilities or weaknesses that might emerge during the exercise, or in any evaluation reports.
- On the other hand, participants may want the publicity of participating in major preparedness exercises, potentially being a factor in their decision whether to participate.
- It may be necessary to inform the media about the exercise at least at a high level, so that they will not misinterpret activities of participants as a real emergency.
- The media may be an important participant in the exercise, since the media often plays an important role during emergencies, such as keeping the public informed about emergency procedures, evacuations, etc.
- And communications with the media are an important part of crisis management that itself includes procedures that should be practiced and may be tested in exercises.

Generally, most experts view little role for media in these exercises, due to confidentiality concerns of participants. In order to convince stakeholders to participate and potentially reveal weaknesses to external parties, they typically need reassurance that information about any such weaknesses would be held confidential. As a result, key stakeholders will almost universally want to avoid allowing media full access to exercise planning, the exercise itself, or the after-action reports.

On the other hand, many stakeholders will value the perception gained by being a participant in an important critical information infrastructure exercise. By participating, they can demonstrate their importance to government and economy, their openness to supporting public services, their act of preparing for any and all possible incidents. As a result, there can be some benefit to having a public

relations policy for exercises that ensures sanitized information about the exercise and participants is released to the media.

Media policies may also be important to ensure that the exercise is not misinterpreted by the media as a real incident. Organizers in at least one Member State cited this as a real risk, having observed it in one of their earlier exercises.

The media may also be a relevant participant in an exercise, in their role of communicating information to the public and breaking news to participants.

It is also worth noting that many exercises simulate media activities to provide the injects during the exercise. News media may be the channel by which news is distributed to stakeholders in the event of a real incident, so planners sometimes simulate news reports to participants. These will be prepared as part of scenario development, but planners should be aware of this complex relationship that most exercises have with media coverage.

Finally, since media communications are an important part of crisis management, exercises may incorporate this role into an exercise, testing the procedures and key actors in their responsibilities.

- *Consider the media policy before the exercise takes place. Make a decision about the policy and then prepare any materials needed.*
- *Most likely, for smaller exercises, such as most discussion-based exercises, organizers and stakeholders will not need or want to inform the media.*
- *For larger exercises, you may need to notify the media, to avoid mistaken alarm.*
- *You may also want to promote the exercise and participants in a positive way to media through press releases, websites, press conferences, etc.*
- *And upon completion of the evaluation, you may want to send a sanitized final report to the media, promoting the benefits of the exercise, without pointing fingers at any specific participants nor revealing any key vulnerabilities.*

Finally, the planning process will also require the development of some other materials that will be used to conduct the exercise. These materials will likely include:

- In order to carry out their jobs effectively, the monitors will need training on how to do so. Many or all of the monitors may have participated in the planning process, so the exercise will not be new to them. However, they will need guidance

on what exactly to observe, how to measure it, what to record, how to record it, how to communicate with participants and the moderator, how to inject information, and how to respond to participant questions. Monitors will need training materials, as well as practice in advance.

- These should include an explanation of the exercise, an explanation of the reason for the exercise and the efforts to increase resilience; clear instructions to enable participants to carry out their duties during the exercise; rules of the exercise; and anything else they may need to complete the exercise. This training or briefing may be simply a written document, an oral briefing, or a combination. And it may take place just before the exercise, or possibly a week or two in advance, if there is significant new material for them to understand in advance. This subject is discussed in more detail in the next section.

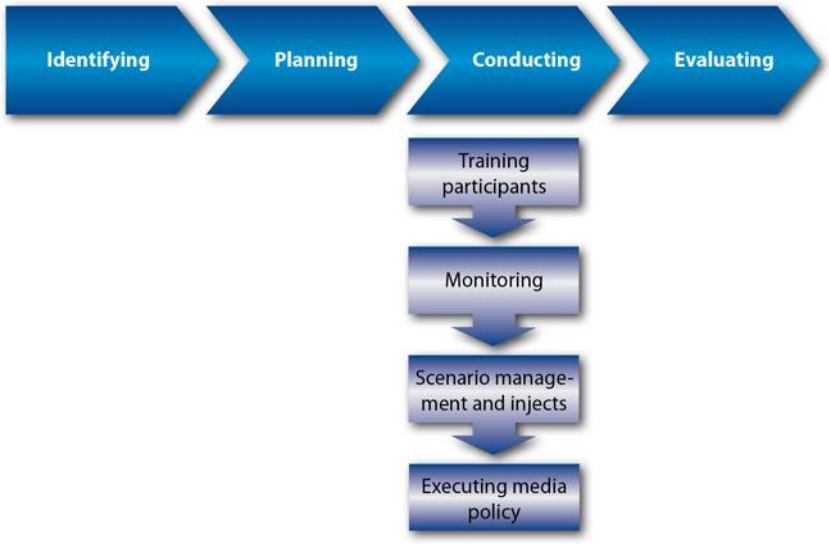
- The exercise may require various tools. Some exercises use a software tool to manage the scenario during the exercise. Monitors will need questionnaires or other tools to record their observations. Monitors will need a means to communicate with the moderator during the exercise. Participants may need tools to simulate their activities and decisions. And other tools may also be required.

The specific requirements for these materials will be determined by the planning team as they develop the scenario.

- *Make sure to carefully identify well in advance what materials are needed. You may need the time to develop some of the tools, especially where potentially complex software tools may be needed.*

- *Provide monitors with all their materials well in advance, and then provide training and rehearsals to ensure everyone is ready.*

Once advance planning is completed, the exercise itself will be conducted. To kick it off, some form of training of the participants will be required. Additionally, monitors will be in place to observe the actions of the participants and to inject new information as the scenario unfolds. Finally, the media may or may not be engaged during the exercise itself. Each of these issues is reviewed below.



The planning process will map out the scenario to be played in detail, but it must be kept secret from exercise participants until the event itself. Still, the participants will need some understanding of what will happen, what their roles are, how they should act, etc. As a result, the planning team will need to prepare some training materials for participants.

These briefings may be oral, written, or both.

In some cases, this information is extremely limited with participants simply receiving a date and brief explanation of the objectives, and then simply receiving the scenario injects at the start.

In most cases, however, there tends to be a bit more information shared. This information may include the following:

- In tabletop exercises or games, participants need a briefing about the rules and regulations for participation, as well as a briefing about the background of the scenario.
- Some exercises include a seminar or online training in advance about the tools used during the exercise.
- They may also include briefing materials or training about resilience of public communications networks and objectives and other context for the exercise.
- Generally, it is advisable to make the participants feel comfortable with the broad reasons for conducting the exercise and anything they need to know about how it will be conducted.

But as already mentioned, the scenario itself is kept secret until the start of the exercise.

Training is provided via conference call and distributed documents to participants. Scenario

Be sure to train participants in any background information, tools, rules and other details required for them to conduct the exercise and realistically simulate their procedures and actions.

The monitoring procedure and the selection of monitors will have been specified in the planning phase. They are discussed here as their role comes into effect during the exercise itself.

There will need to be some central management of the exercise (e.g. a moderator, an Exercise Director, or an exercise management team) controlling all activities and coordinating the individual monitors. We will refer to this individual or team as the moderator. The moderator must:

- Manage the overall scenario;

- Take the incoming information on decisions and actions taken by the various participants;
- Determine the effects of those steps on the scenario and individual participants/teams;
- Determine how new injections of scenario information ("injects") affect the unfolding scenario;
- And relay this new information about the changing scenario to the monitors.

Individual monitors will sit with the participating individuals or teams. They will:

- Observe participants' actions, decisions, and procedures, including their effectiveness.
- Note these observations during the exercise for later evaluation.
- Report the participants' actions back to the exercise management.
- Relay additional information from exercise management to participants as the scenario unfolds, either due to the actions (and their effects) taken by the various participants, or due to pre-planned scenario injects.
- And keep participants on track, for example by preventing participants from fighting the scenario or starting discussions about unrelated issues things.

Examples:

- *[NO] One expert reported that they usually have one observer in each of the groups that exercise. The observer stays in contact with exercise management whenever necessary, also to perform relevant assistance or changes locally. He/she takes notes throughout the exercise on problem solving, group dynamics and other relevant issues. He/she also conducts a brief (usually 30-* *-*
  exercise to immediately collect thoughts and observations from participants while the thoughts are fresh.
-
-

- *Ensure that there is a central exercise management team prepared to control the scenario, receive updates on actions taken by participants, integrate this information with the scenario, and distribute this information back to participants, via the monitors.*
- *Ensure that there is a clear structure and process for the monitoring team to follow, including the details they should watch for in evaluating the participants; procedures for communicating with the exercise managers; and procedures for relaying new information to the participants*

During the course of the exercise, the scenario needs to be managed and adapted in response to the actions of participants and pre-planned injects of new information. This process is crucial to the success of the exercise.

The moderator centrally controls the exercise, either with a software tool developed for the exercise, or with a scenario book.

The moderator requires incoming information for all of the participants, relayed by the monitors located on site with each team of participants. A communications system may be needed specially to keep the moderator and monitors in communication.

As the moderator determines the changes required, he or she will communicate them to moderators to pass on to participants.

Many of the injects will be planned in advance. Some of them will only be optional, for use by the moderator if needed.

The injects are designed to simulate the way a real incident would unfold, so as in the real world, they may include incomplete or possibly flawed information about the theoretical incident.

Many exercises simulate media reports as one way to inject new developments. Participants then receive these fake reports, similar to the way that such information is likely to be distributed in a real incident. Other injects will simulate other sources of the information, such as network monitoring tools, suppliers, customers, emergency services, etc.

- *Managing scenario injects effectively requires very effective communication between the moderator and monitors.*
- *The moderator must be able to efficiently digest the incoming information from participants (via the monitors), integrate it into the pre-planned scenario, and decide how next steps should*

unfold. To do that, organizers must prepare a detailed scenario with many paths of possible development, and those paths must accurately predict the actions that participants will take.

- *A software tool can be effective to help moderators juggle this large amount of information, possibilities and decisions.*
- *Injects should simulate real-world communication about an incident*.

As described above in the chapter on *Planning The Exercise*, there are several ways in which the media is of interest to exercise organizers and participants, and the question is what role, if any, should the media play in an exercise.

To avoid confusion or alarm caused by misunderstanding of the actions taken by participants in full-scale exercises, media should usually be notified in advance about the exercise.

During the exercise, the media may want to observe the participants. Since participating organizations generally do not want public scrutiny of their internal operations, especially when they may include vulnerabilities or mistakes that may emerge during the exercise, it is likely that you will want to avoid allowing the media to observe the exercise close up.

On the other hand, allowing the media to understand the exercise at a high level, can help generate public awareness of the risks that are being tested, and also generate good publicity for participating stakeholders.

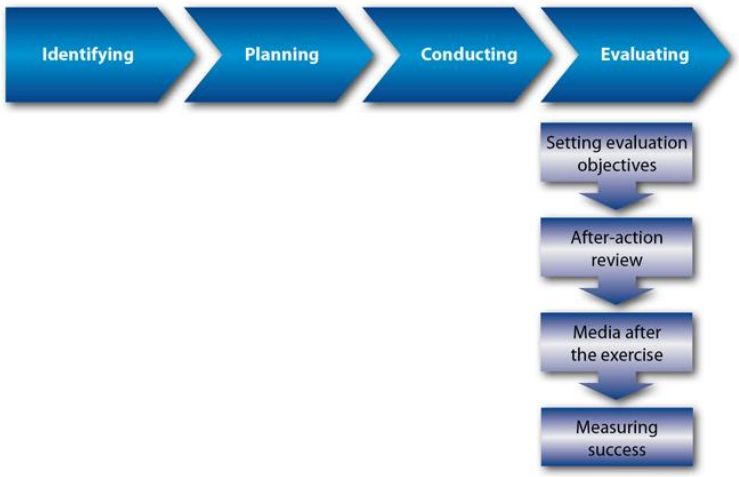
And in many emergencies, the media plays an important role in communicating new information ("breaking news") to the public and to the various organizations involved in emergency response activities. Since media could play a role in some scenarios, you may want to consider inviting some media participation, if it is truly relevant.

- *If your exercise will be operations-based, include public activities, or just take place on a large scale, you should inform the media in advance to avoid confusion or alarm.*
- *You should take advantage of the interest of the media to generate publicity for the initiatives you are undertaking, and for the participating stakeholders.*
- *You should still avoid divulging sensitive information about the actions of participants, such as any weaknesses or mistakes during the exercise.*

Upon completion of the exercise, the organizers should ensure that the exercise is effectively and usefully evaluated. This process is sometimes given insufficient attention, but it is very important, as it is the process that draws conclusions and recommendations for improving resilience plans and ensuring that stakeholders act on these points. Those organisations or individuals participating in the evaluation are having the role of the ‘ .

> *[US] One expert suggested that as much effort should be put into the after-action review as into the pre-exercise planning, while lamenting that that wish will never fully be realized, Still, those who plan an exercise should heed this advice and plan from the start to follow the exercise with a diligent and extended after-action review process.*

The key steps in this phase are shown in the figure below.



The evaluation process is designed to enable all involved to learn lessons from the exercise. These lessons will include observations about areas for improvement within individual organizations and their processes, as well as observations about interdependencies, ways to improve cooperation across organizations, and lessons in various other areas.

The evaluation process should aim to identify these lessons, but to do so, the evaluation process must be designed in advance to collect the necessary information. Sources of information will be discussed further below. Furthermore, to decide what information is needed, the objectives of the evaluation must be clear in advance. Objectives may include, for example, aims to identify:

- The major obstacles to success of the continuity plans tested;
- Skills required for successful implementation;
- Interdependencies and weak links in the chains of communications, coordination, and decisions among participants;
- Developing recommendations to improve in these areas;
- And many other objectives.

In setting these objectives, planners and organizers should consider that the most effective objectives will be Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART). Such objectives will set clear, achievable goals for the evaluation process, help to set the specifications for the types of information that must be collected during and after the exercise, and ensure that clear results emerge that can form the basis of SMART recommendations to stakeholders.

- *Ensure that SMART objectives are set for the evaluation process during the planning phase. That*

Evaluation should be done fairly quickly after the exercise. That pertains to the need to collect thoughts on the exercise from the various participants and role-players, while they are still fresh. It also pertains to the need to develop the evaluation results and communicate them to stakeholders before attention wanders and priorities change. Organizers should take advantage of the motivation and excitement about the exercise to ensure adequate interest is paid to the conclusions and lessons learned.

> *[NO] One expert explained that the general evaluation must happen rather fast. The evaluation report for one previous exercise was delivered about 10 months after the exercise. Memory of the event, and motivation to learn and apply lessons fade. "Act when things are warm," he advised.*

It is critical to plan for the evaluation. During the planning phase, the evaluation measures and process will have been specified in detail, and the organizers and stakeholders will now need to follow through with those plans.

Evaluation should be as inclusive as the planning and execution were. It ensures comprehensive insight into challenges experienced, procedures followed, interdependencies, lessons learned, corrections needed, etc. Additionally, if participants play a part in drawing conclusions and recommendations, they are more likely to implement them. Inclusiveness also ensures consensus on any critical comments in the evaluation and the recommended steps to be taken.

On the other hand, the evaluation process will handle some sensitive information that could reveal confidential company details, dangerous vulnerabilities, or embarrassing weaknesses or errors. Therefore, the evaluation process and outcomes must be handled delicately.

Related to the concern over information embarrassing to participants, many organizers advised strongly that evaluation reports should try to avoid laying blame. Shunning of participants will be a strong disincentive to future collaboration and exercise participation.

- *Ensure a high level of commitment to the evaluation process.*
- *The evaluation process must be planned in advance of the exercise.*
- *The evaluation process should be inclusive, as working with the stakeholders to reach consensus ensures the evaluation conclusions and recommendations will be accepted by stakeholders and gives greater chance the recommendations will be acted upon.*
- *Avoid blaming individual participants or stakeholders, as this will discourage future participation and cooperation in the sector. Keep the conclusions and recommendations constructive and avoid reference to specific organizations in any negative context.*

Evaluations are usually prepared using several different materials. Not all are required, and others may be identified. However, the most common sources mentioned by organizers were:

- Reports from the monitors, possibly consisting of detailed notes about their observations during the exercise, and/or summary reports that they prepare afterward;
- Questionnaires completed by monitors at interim stages and after the exercise;
- Questionnaires completed by participants at interim stages and after the exercise;
- Immediate debriefings (or "hot wash-ups") with participants after each main section of the exercise to gather fresh thoughts on the experience;
- Debriefing sessions/workshops held with participants, monitors, and moderators after the exercise;
- Questionnaires and reports submitted by participant organizations;
- And possibly also technical results from tools that may have been used.

- *Seek information for evaluation from many sources.*
- *Obtain this information at interim periods as well as after completion.*
- *Prepare the materials and the plan for obtaining this information in advance.*

Most evaluation processes focus on and culminate in one or more evaluation reports.

To cope with the issue of sensitive information, evaluation reports will likely need to be carefully worded, avoiding blame, and probably also issued in different versions. For example:

- One unique version might by prepared for each stakeholder—and held confidential to that stakeholder—and this version might hold some detailed observations and advice for a specific organization.
- Another version might be an overall review, reflecting consensus conclusions about broad issues, general areas that need improvement across the sector, and recommendations for improvement. This report will not identify by name any organizations

that may have revealed problems. Such a version would only be issued to the participating stakeholders.

- And a final version might only include general information about the exercise, without identifying names, weaknesses, vulnerabilities or other details, and be issued to the press and the public.

- *Prepare separate reports for separate audiences, tailoring each to the type and amount of information required.*
- *Ensure that sensitive information is only revealed to the company to which it pertains, if necessary at all.*

And finally, it is best to consider the evaluation activities as a useful process, rather than as a means of producing a report.

As with the planning phase, exercise evaluation is a process that generates a large portion of the benefits simply through the process itself, rather than through the result.

- In essence, these stakeholders have just completed a large endeavour together over an extended period of time that may even have lasted two full years. These participants will have grown motivated to see the exercise and to learn the results.
- Once the exercise is completed, it is possible to retain the planning committee(s) for evaluation, discussion of results, discussion of key challenges or problems experienced, review of interdependencies revealed, examination of how participant actions met or diverged from expectations, and preparation of recommended improvements for the overall community of participants.
- Obtaining the evaluation report is an important goal, but planners should also recognize that by ensuring continuing collaboration and developing consensus in preparing the report, they will have achieved and reinforced many of core objectives of conducting the exercise, possibly more so than any final report could achieve.

Most exercise organizers consider the project completed after the evaluation reports are submitted, or perhaps after a brief follow-up procedure to review, validate, or comment on the reports.

Many of these organizers continue the collaborative efforts by quickly moving onto the planning of the next exercise.

evaluation of one exercise, and the planning of the next, as they do not want to lose momentum.

Ongoing collaboration can also be extended in other ways. For example:

- You can establish a committee of stakeholders to prepare the evaluation over a period of time, including a series of meetings and discussions.
- This committee can organize a seminar or workshop to review draft findings and seek input and validation from a wider number of stakeholders and key individuals.
- There can be additional follow-up meetings to review progress in implementing recommendations, or to continue discussion of specific challenges or action plans.

[US] One private-sector expert recommends extending this process by following the evaluation report with a draft action strategy, an action strategy workshop, and then the formulation of ongoing working groups and forums that address specific challenges that the sector should continue to address through collaboration.

Some authorities may also want to include individual follow-up steps with stakeholders to address particular issues or needed improvements. The exercise may reveal specific vulnerabilities or weaknesses at an operator that should be addressed. However, authorities should do so in a constructive and sensitive way. It is important to avoid sharp criticism or penalties in these follow-up discussions, lest all trust, interest in exercises, and willingness to collaborate disappear in an instant.

- *Leverage the evaluation process as a means to generate consensus about next steps the sector stakeholders need to take, and to generate interest and commitment to taking those steps.*
- *Roll over exercise evaluation quickly into planning for the next exercise, in order to maintain momentum and build on the skills and commitment generated in the previous one.*
- *Consider ways to extend collaboration in other ways, through ongoing committees, meetings, or forums for discussion of challenges identified.*

As mentioned above, you may want to include in the evaluation process a public report on the exercise. This report should not identify the detailed findings. Instead, it should include a higher level summary of the objectives, participating sectors, broad benefits of the exercise, and related high-level information.

This public report can be reinforced by additional publicity measures, if desired, such as holding a press conference, publishing documents online, etc.

- *Publish a high-level report for public and media consumption that highlights the objectives, participants and general benefits of the exercise, without revealing details. Avoid revealing negative results, especially about specific participants.*

Generally, each exercise that is performed is a success because all of the participants have learnt something new even if individual elements of the exercise were not successful. Still, it is useful to measure how successful it was, in order to learn lessons that can enable continuous improvement of later exercises.

Measuring the success of an exercise can be broken down into two categories:

1. One can examine whether the exercise achieves the objectives.
2. And one can examine how effective the processes of the exercise were (whether the exercise was planned well, executed well, etc.). For example, an exercise may be run smoothly, but not make much impact on the objectives.

The benefits of exercises range from very specific (a function tested) to very general (increased cooperation on wider resilience initiatives). As such, measuring the success or effectiveness of an exercise also includes a mix of specific and general measurements.

are easier to measure. Some options include:

- Organizers can use questionnaires to stakeholders to gauge their views on the subjects of the exercise at different points before and after the exercise. Measuring their changed views of specific issues can provide concrete evidence of the effectiveness of an exercise.

- Organizers can test the same function multiple times, and compare results to see if improvement occurs. For example, certain types of communication between organizations during an exercise will be repeated in many exercises, even in different scenarios. Organizers can compare results for that function through multiple exercises.
- Some organizers may take a hands-on approach to ensuring that participants address any revealed weaknesses in their continuity plans. As discussed above, authorities who take that approach with voluntary participants will need to be careful not to punish or blame the participant, lest they refuse to participate in future exercises. However, it may be possible to take a constructive approach, offering advice to help improve performance.
- The evaluation may reveal specific areas for improvement, as well as suggesting steps to do so. Organizers can then observe progress in each of these areas by coordinating periodic discussions to review progress, and by testing for some in future exercises.

of exercises are more difficult to measure, though they remain important indicators of success. For example, organizers may want to increase cooperation among sector participants. They may also want to increase awareness of vulnerabilities, interdependencies, and resilience and continuity planning. One indicator of these general benefits could be an increase in enthusiasm (or decreased resistance) for later exercises. Stakeholders may be more enthusiastic for other types of cooperation. Similarly, organizers can observe participation of stakeholders during planning, the exercise itself, and the evaluation for indications of commitment to these issues.

Measuring the effectiveness of the exercise processes can be straightforward. The evaluation process includes the collection of large amounts of information about the exercise, and this can include reviews of the exercise processes themselves. For example, the materials for evaluation (questionnaires to participants and monitors, debriefings, etc.) can include specific questions to learn how satisfied individuals and stakeholders are with the way these processes were carried out. That can yield specific lessons for planning future exercises.

To ensure that lessons are collected and acted upon, organizers can ensure that a separate evaluation document is prepared that focuses on the lessons learned about the exercise management experience. As with the other evaluation processes, clear objectives on what to look for in advance will help organizers to measure success, and of course serve as guidance for the planning process in the first place.

Another effective practice could be to log lessons from each exercise, collecting them as a set of good practices for internal use with each successive exercise. This log also would help to set out the measures to test for in the evaluation of the exercise processes in later exercises.

- *Conduct surveys of stakeholders over time (such as early in planning and then after the exercise) to measure changed perception of such issues as interdependencies, vulnerabilities, preparedness, etc.*
- *Test repeatedly for certain key areas to measure improvement.*
- *Follow-up with stakeholders (as a group or individually) to encourage follow-through with needed improvements.*
- *Include questions in the evaluation process that reveal views on the effectiveness of the exercise processes.*
- *Prepare a separate evaluation of the exercise processes, to help guide future exercise processes.*

With this Guide, ENISA has sought to help authorities in the ICT sector in EU Member States to build expertise in conducting exercises that will help to increase resilience of public eCommunications networks in each country. In addition to this local impact, these skills are also intended to help these authorities as they prepare to participate in transnational exercises in this sector.

There are several reasons for conducting transnational exercises. In particular, the nature of the infrastructure, organizations, and risks are no longer significantly constrained or separated by borders. For example, communications networks; service providers; the users dependent on them; and the threats to these networks and services are all increasingly international and interdependent.

That is not to say that all exercises should be international, only that some probably should be. There appears to be widespread support for international cooperation, and specifically international exercises:

- Interviews with experts broadly supported international cooperation. Many of the experts cited international knowledge-sharing as an important objective that they would like to pursue. This knowledge sharing can be in the form of seminars, discussion forums, research materials, as well as exercises.
- Most of the public authorities and private-sector companies that have participated in several exercises have included international exercises among them. Just a few of these include Germany's BSI, the UK's BIS, France's ANSSI, Hungary's CERT-Hungary, and several others.
- The European Commission has identified a need for much greater cooperation and coordination of efforts across EU Member States in enhancing the resilience of public communications networks.
- The European Commission proposed the creation of the first pan-European exercise by the end of 2010. Member States have supported the objective.

However, even when transnational exercises are desired, there is some question about readiness to conduct them. Interviews with European experts showed some uncertainty still about how such exercises would be conducted effectively.

These sentiments mainly emphasise caution about the skill set needed to hold such an exercise, rather than any opposition to the notion itself. Many of the public and private-sector stakeholders who

would play key roles in such exercises do not yet have substantial experience in doing so. They need experience, in order to develop the skills that will make larger exercises successful.

To develop this skill set, experts generally shared common advice. They recommend building slowly toward full-scale pan-European exercises. Start small, they say, and build the exercise planning and execution skills first, by starting for example with tabletops and other discussion-based exercises. Once experience is gained at the smaller scale, organizers can increase the scale and supplement their exercise plans with larger exercises, even full-scale operational exercises.

In addition to building skills, this gradual approach also helps build the necessary relationships and trust between organizations. That trust is critical for recruiting participants to an exercise. By starting small, the participants can be recruited to lower-cost exercises, demonstrating the benefits, and attracting them to contribute and participate in larger-scale exercises.

Such an approach can be applied within each country, but it also applies to transnational or even pan-European exercises. Even where stakeholders have significant experience with national exercises, they may not have a great deal of experience of working with their counterparts internationally, and they may not have the trusting collaborative relationships that they will need for successful exercises and successful incident response. That is exactly why the transnational or pan-European exercises are planned, but also the reason why initial pan-European exercises will likely need to start small and allow long planning cycles, before pushing ahead with more expansive and ambitious exercises later.

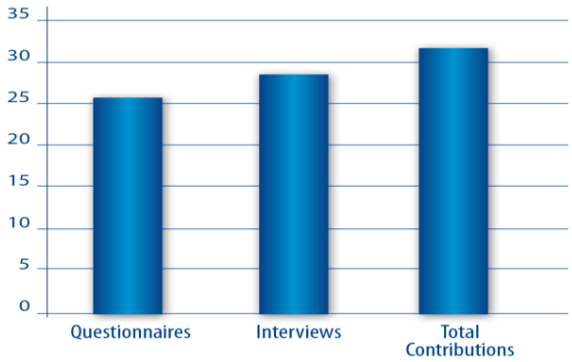
This Guide contains a large amount of information that can be referenced to support organizers and planners through the exercise life-cycle. To help readers to quickly identify the key steps they need to undertake each step of the way, we have prepared the following checklist. This checklist aims to ensure that each major subject and issue has been considered and addressed. Each item consists of many subordinate details, but this checklist should help you to stay on top of the big picture from start to finish, helping you to identify and address the subordinate issues as well.

		Identify clear objectives for the exercise	Organizer
		Identify the measures and groups to test	Organizer
		Choose high-level scenario options	Organizer
		Choose the exercise type, size, geographic scope	Organizer
		Identify key stakeholders	Organizer
		Set a schedule that allows for the complexity of exercise planning and any limitations you have on resources, time, budget, etc.	Organizer and planners
		Include key stakeholders in planning	Organizer
		Conduct meeting to introduce the subjects of resilience, interdependencies, exercises	Organizer and planners
		Conduct meeting to reach consensus on need for exercise	Organizer and planners
		Create realistic scenario with all desired and needed injects (including how they will be injected – e.g. by media)	Planners
		Assign roles for the exercise (monitors, moderator/director, etc.)	Organisers and Planners
		Set objectives for evaluation of the exercise itself, along with how to	Organisers and

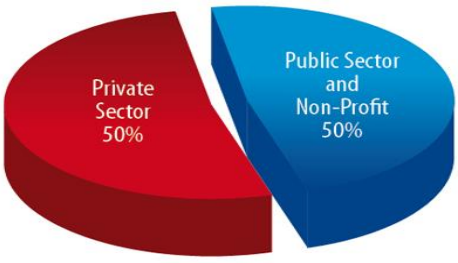
		measure them through questionnaires and exercise results	Planners
		Set objectives for the evaluation of the exercise processes, along with how to measure them through questionnaires and exercise results	Organiser and Planners
		Prepare exercise materials	Planners
		▪ Training/briefing documents	Planners
		▪ Tools for participants/ moderator/ monitors during the exercise	Planners
		▪ Tools/checklists/forms for monitors	Planners
		▪ Survey questionnaires for all involved	Planners
		Train monitors, moderator, others, to perform their duties during the exercise (test runs – exercises of the exercise are advised)	Planners
		Invite desired observers	Planners
		Decide on a media policy	Planners
		Notify media, if relevant	Planners
		Ensure moderator/director and monitors are prepared to execute the scenario	Planners
		Train participants (briefing, their roles, rules of the exercise, etc.)	Planners
		Execute the scenario and injects	Moderator/Director
		Provide injects as guided by moderator/director	Monitors, others
		Observe participants, taking notes on observations, and measuring performance against checklist and guidance from exercise materials	Monitors
		Report participants' decisions, actions and procedures back to the moderator for incorporation into the scenario	Monitors

		Simulate continuity and response procedures as effectively and realistically as possible	Participants
		Complete periodic questionnaires about exercise progress, effectiveness, problems, etc. (such as at end of each day)	Participants, monitors, others
		Complete questionnaires at end of exercise	Participants, monitors, others
		Conduct/participate in debriefings to share experiences and observations	Participants, monitors, others
		Collect required information (questionnaires, completed forms from monitors, etc.)	Evaluators
		Prepare evaluation for individual stakeholders	Evaluators
		Prepare group evaluation for all stakeholders	Evaluators
		Prepare public exercise document for media and public	Evaluators
		Present group evaluation and recommendations to stakeholders	Evaluators
		Follow up with individual stakeholders, if necessary and desired	Evaluators
		Follow up with stakeholder community over time to encourage and check on progress implementing recommendations	Evaluators

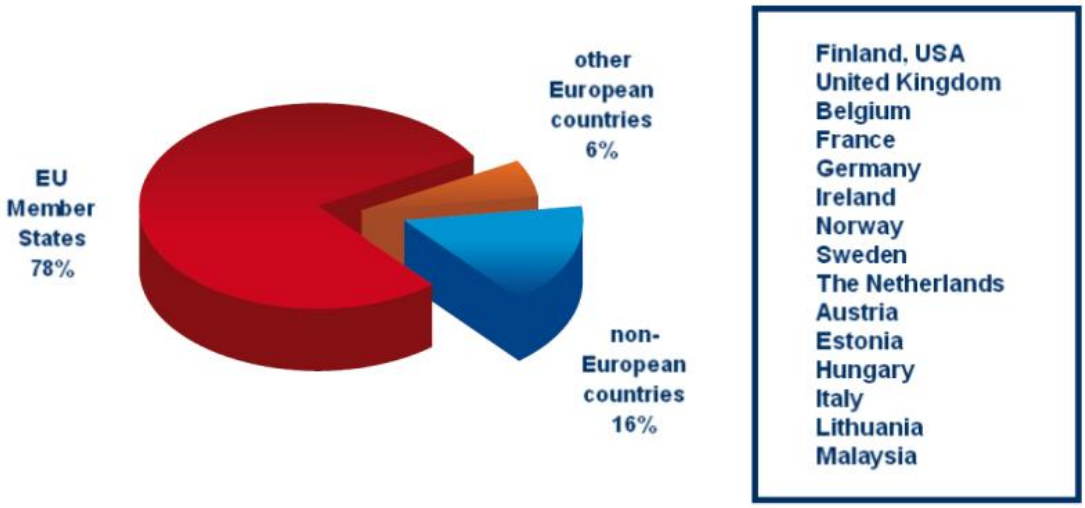
To identify good practices that have been proven effective in organizing exercises on public eCommunications networks, ENISA and IDC collected questionnaires and conducted interviews with experienced exercise organizers and planners across the EU and in other regions of the world. In total, 26 questionnaires were collected, and 29 interviews conducted, totalling responses from 31 different organizations.



Respondents came from diverse perspectives. Of the total, 15 were from public authorities, and 16 from the private sector. Public-sector participants included ministries of communications, national regulatory authorities, European Commission experts, national and specialized CERTs, and others. Private-sector participants included telecoms network operators, technology vendors, consultancies, and others.



Geographically, most of our respondents were located within the EU, where we have covered organizations with headquarters in Austria, Belgium, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, Sweden, the Netherlands, and the United Kingdom. In addition to that we also spoke to organizations with headquarters outside of the EU, mainly in Norway and the USA.



–

- . The French national IT security agency ANSSI is conducting national cyber exercises every 2 to 3 years and assists public agencies in conducting smaller-scale exercises. [http://www.ssi.gouv.fr/]
- (since 2005). The Asia Pacific CERT is coordinating yearly multinational drills focusing on communication and cooperation between national CERTs during emergencies such as DDoS' and other cyber attacks. [http://www.apcert.org/documents/pdf/annualreport2008.pdf]
- (ACID, since 2006). Annual incident multinational drills focused on cooperation during incident handling. Organized by SingCERT.
- . Series of regional (US multi-state) exercises focusing on various aspects of disaster response, usually with 200-300 participants. Topics: terrorist attack, cyber-attack, earthquake, influenza pandemic, recovering supply chains. Carried out in the USA in 2002, 2004, 2006, 2007, and 2008). [http://www.regionalresilience.org/home/BlueCascades/tabid/108/Default.aspx]
- (since 2006). Yearly tabletop exercise to test the functioning of the EU's Emergency and Crisis Coordination Arrangements (CCA) in Brussels. Involves the Presidency, the Member States directly affected by the crisis modelled in scenario, and top Council and Commission officials. Scenarios so far covered a terrorist attack on five cities (2006), a bio-terrorist attack (2007) and a twin storm (2008), always with effects on several Member States. [http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/91480.pdf, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/95958.pdf, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/102939.pdf
- (2006, 2008). National (CS I) and international (CS II) large-scale exercises with participants from public (international, country and state level) and private (companies or sector associations) organizations across multiple sectors. Organized by the US Home Security Department. The exercises tested response to and recovery from cyber-attack on national infrastructure. A sequel, Cyber Storm III, is planned for 2010. [http://www.dhs.gov/files/training/gc_1204738275985.shtm]
- (since 2004). Periodical tabletop exercise of the NEAT (National Emergency Alert for Telecoms) scheme in the UK. Scenarios included bomb attacks (2004), extreme weather (2005), and large-scale regional electricity supply outage (2007).

- (2008, 2009). The Finnish Federation for Communications and Teleinformatics (FiCom) has organized regional exercises focused on cooperation between electricity and telecommunications sectors during failure recovery. Owners and operators of both power supply and eCommunication networks in a selected region participated.
- Norway conducts yearly national emergency preparedness exercises. The 2008 exercise focused on ICT. 30+ participants from private and public organizations in telecom, IT, banking, and finance, energy supply, oil and gas industry, police and justice. Followed by another exercise along the same scenario among the ministries (SNØ 08). Topic: Trojan and DoS attack, attack on power supply network.
- . Series of exercises for general crisis response in Germany (2004, 2005, 2007, and scheduled for 2010 and 2011). Involving federal and state level public agencies and private sector organizations. Topics: technical failures, natural disasters, terrorist threats and attacks, influenza pandemic. [http://www.denis.bund.de/luekex/]
- . The Swedish regulator PTS offers corporate training courses tailored for private companies. The trainings are carried out on the individual companies' premises and include both training sessions and a tabletop exercise. Apart from these, there are also individual courses on crisis management (3 modules per 3 days each). [http://www.pts.se/upload/Faktablad/En/facts-about-training-and-exercises.pdf]
- – . Series of experimental exercises (2000, 2004, 2006) testing communication and technology issues in responding to simulated emergencies;, often with humanitarian relief aspect; particular focusing on civil-military cooperation. Participation voluntary, organized by private subjects in the USA. [http://www.strongangel3.net/]
- (2007, 2009, in 2005 as Samvete). Nationwide eCommunication exercises in Sweden, bi-annual. Involves major operators plus representatives of public administration, IT, energy sector. Topics: weather calamity (2007), terrorist attack (2009). [http://www.pts.se/upload/Ovrigt/Om-PTS/infomaterial/Telo07_eng.pdf, http://www.pts.se/upload/Ovrigt/Om-PTS/infomaterial/pts-telo-09-english.pdf]
- – . Series of nationwide or international exercises involving thousands of top officials from national, state, regional and local government, plus international and private organizations. Topic: responding to simulated terrorist attacks with biological or chemical weapons or radiological dispersal devices (RDDs). Organized by the US Home Security Department in 2000, 2003, 2005, 2007. [http://www.dhs.gov/files/training/gc_1179350946764.shtm]

- (2006). Tabletop simulation of reaction and recovery from electrical transmission system disruptions. Small number of role players interacting with sophisticated software modelling tool and human exercise management. Financed by an EC grant, carried out by a pool of private companies. Main actors modelled were electricity transmission companies, civil protection authorities and national crisis management teams in two fictive countries. [http://vita.iabg.eu/]

- (2008). National exercise in the Netherlands testing response to flooding (river, sea, polder). Wide range of public agencies (ministries, crisis response centres, water boards, police and rescue forces, military support), over 10,000 people exercising during 1 week.

- (2007). Nationwide exercise in the UK for a human flu pandemic. Over 5,000 participants from National Health Service, local authorities, Government departments and private companies (Food, Fuel, Water and Transport sectors) exercised in two stages over three days in January and February 2007. [http://www.cabinetoffice.gov.uk/media/132988/winter_willow_lessons.pdf]

- A number of exercises conducted on national or regional level get less public coverage and therefore will be mentioned briefly.

    - The Norwegian regulator NPT organizes biannual tabletop exercises for eCommunications network and service providers.

    - NPT also takes part in a multi-year cross-sector regional exercise program with the electrical power and public road authorities. This activity plans to organize two or three regional exercises per year.

    - The Finnish Ministry of Defence and Ministry of Transport and Communications organize bi-annual exercises for companies involved in CIIT (operators, broadcasters, manufacturers, maintenance providers), central ministries, and the National Emergency Supply Agency (NESA). The exercises are tabletop and are scheduled for several days each.

    - Since 2008, NESA and the Finnish Communications Regulatory Authority (FICORA) have been organizing Information Security Seminars for business directors, risk assessment directors, security managers and information security managers. There are 1 to 2 seminars held per year.

    - The Cabinet Office hosts a number of examples of British national, local and regional exercises at its 'UK Resilience' pages.

[http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies.aspx#content, http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/regionalcasestudies.aspx]

The German Federal ministry of Interior (Bundesministerium des Innern, or BMI) offers policy guidance and a practical handbook for exercises, available also in English:

- “IT Emergency and Crisis Exercises in Critical Infrastructures”, (December 2008) [http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf],
- with useful "Appendices to the Concept of IT Emergency and Crisis Exercises in Critical Infrastructure," (December 2008) [http://www.bmi.bund.de/cae/servlet/contentblob/560090/publicationFile/27810/kritis_1_eng.pdf]

. ENISA’s website offers an extensive collection of research, recommendations, and good practices on various topics related to network resilience. Sample documents include:

- "Analysis of Member States' Policies and Regulations. Policy Recommendations", (2009) [http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations/at_download/fullReport]
- "Stock Taking of Member States’ Policies and Regulations related to Resilience of public eCommunications Networks," (September 2008) [http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report/at_download/fullReport]
- Set of Good Practice Guides [http://www.enisa.europa.eu/act/res/policies/good-practices-1]

. The key recent documents on the topic of this guide:

- "Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience," Communication from The Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, COM(2009) 149 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT]
- "A Strategy for a Secure Information Society – "Dialogue, Partnership and Empowerment"", Communication from the Commission to the European Parliament, the Council, the European

Economic and Social Committee, and the Committee of the Regions, COM(2006) 251 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT]

. The UK Cabinet Office offers an informative web site on publicly coordinated exercises in the UK and the lessons learned. The site offers, among others:

- "Exercise Planners Guide," (1998) [http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/plannersguide.aspx]
- List of examples with descriptions and lessons learned, if available: [http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/nationalcasestudies.aspx, http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises/regionalcasestudies.aspx]
- The project homepage is [http://www.cabinetoffice.gov.uk/ukresilience/preparedness/exercises.aspx]

As part of the Homeland Security Exercise and Evaluation Program (HSEEP), the US Homeland Security Department has published a number of documents providing guidance on, examples of, and templates for preparation, conduct, and evaluation of exercises. Included are, for instance

- "Homeland Security Exercise and Evaluation Program, Volume II: Exercise Planning and Conduct," (February 2007) [https://hseep.dhs.gov/support/VolumeII.pdf]
- "Homeland Security Exercise and Evaluation Program, Volume III: Exercise Evaluation and Improvement Planning," (February 2007) [https://hseep.dhs.gov/support/VolumeIII.pdf]
- Exercise Evaluation Guides, [https://hseep.dhs.gov/pages/1002_EEGLi.aspx]
- Library of other sample materials [https://hseep.dhs.gov/hseep_vols/default1.aspx?url=home.aspx]
- The project homepage is [https://hseep.dhs.gov/pages/1001_HSEEP7.aspx]

IDENTIFICATION OF THE EXERCISE(S)

Which type of exercise(s) are you (have you been) involved in (e.g. discussion based - seminar, workshop, game-, Operations-Based -drill, functional, full scale, etc.-

What stakeholders are involved (e.g. vendors, owner/operators, public and private customers, emergency management community, etc.),

What is the scope of the exercise, including:

- Geographic scope (regional, country wide, cross country)
- Sectors (e.g. network operators, service providers, power providers, etc.)
- And timing (frequency and duration)

What measures are tested (preparedness measures, policies, procedures, agreements, etc.)? Pls. explain.

ORGANIZATION OF THE EXERCISE(S)

Please describe the planning process, such as:

Who leads the planning process, and who participates? / What is the planning process and duration? / How is the concept of the exercise developed?

Please describe selection of the participants. For example:

ORGANIZATION OF THE EXERCISE(S)

How are stakeholders identified and recruited? / How is trust built between them? / Are there any incentives or assistance in any form (financial, technical)? / What is the involvement of the private sector?

What background information is communicated to the participants (network resilience and other information) before the exercise, how is it prepared and in what format (training seminar, study material, etc.)?

How are media relations handled and what is their role in the exercise?

EVALUATION OF THE EXERCISE(S)

What is the monitoring process that is used for the exercise?

How is the exercise evaluated, what performance indicators are used, and how are gaps identified and solutions recommended?

How does the outcome of the exercise improve the contingency plans and the overall resilience measures of participating organizations? How do you assess this?

How are the results of the exercise communicated to the stakeholders and the media?

CONCLUSIONS AND SUGGESTIONS

What were the major challenges faced in preparing and conducting the exercises?

What recommendations do you have for others who want to prepare similar exercises?

Please tell us if you feel we have missed out any important questions or subject areas which should be addressed when producing the good practice guide.

Short for *robot network*. A collection of compromised computers that are used by some individual or organization (the botnet master) without the awareness of their owners. Any such infected computer is referred to as a 'bot' or 'zombie'. Botnets are mostly used for nefarious purposes such as forwarding spam or malicious software to other computers on the Internet, conducting distributed denial-of-service (DDoS) attacks, committing click fraud, or data security breaches.

Availability of critical business functions to customers, suppliers, regulators, and other entities that must have access to those functions. Business continuity is ensured by a range of means and activities that foster availability and recoverability of services, such as: business continuity planning; guaranteed services and/or supplies from suppliers and subcontractors; internal backup and recovery policies; procedures for change control and project management; and customer support.

Creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. [COM(2004) 702]

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.). [COM(2005) 576].

Also called Computer Security Incident Response Team (CSIRT). A CERT or CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. CERTs provide the necessary services to handle incidents and support their constituents to recover from breaches; most CERTs also provide preventative and educational services. CERTs may be established for groups of stakeholders on national or sub-national levels, or within single organizations. [ENISA WP2006/5.1 (CERT-D1/D2)]

An explicit attempt to render a computer or a network incapable of providing normal services, performed via coordinated attack from multiple locations. DDoS attackers compromise a number of end-hosts (typically using a virus or worm) or routers, and then use those compromised hosts to flood the bandwidth or resources of a targeted system, thus making it unavailable to the intended users. [W3C, Internet Architecture Board, CERT/CC]

Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed [Directive 2002/21/EC] (see below definition on public communication networks).

An event or situation which threatens serious damage to human welfare or to the environment; also an act of war or terrorism which threatens serious damage to the national security. [Emergency Response and Recovery: Non Statutory Guidance Accompanying The Civil Contingencies Act 2004; ver 2, August 2009]

The continuous process by which all individuals, groups, and communities manage hazards in an effort to avoid or ameliorate the impact of emergencies. For the purposes of this guide, emergency management refers to publicly coordinated emergency management and to the authorities which are in charge of it.

The process of immediate reaction to a large scale emergency. For the purposes of this guide, emergency response refers to publicly coordinated emergency response.

Organizations which ensure public safety by addressing different emergencies.

Input from the scenario to the exercise players. Injects represent certain development in the scenario or simply give details on the situation. They may be presented in the form of media reports, messages from public authorities or emergency services, data files from network management tools, etc. Injects are usually prepared in advance, sometimes in variants, and distributed in response to the exercise course upon the decision of the exercise moderator(s).

A unique numeric identifier assigned to computers and other devices participating in a network that is using the Internet Protocol for communication between its nodes.

An organization that provides carrier services in the wired or wireless arena and operates its own network. Examples include fixed and/or mobile telephony companies, Internet Service Providers, wholesale carriers.

An electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. [directive 2002/21/EC].

A cooperative venture between the public and private sectors, built on the expertise of each partner, that best meets clearly defined public needs through the appropriate allocation of resources, risks and rewards. For the purposes of this Guide, private-public partnerships include also activities beyond mere economic contracts, such as CIP projects. [Canadian Council of Public-Private Partnerships, IDC]

The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.

Topic of the exercise, developed into a series of simulated events to which the exercise players have to react. Scenarios may or may not contain detailed injects for the players and may or may not contain variants/alternatives.

– Agence nationale de la sécurité des systèmes d'information [French Network and Information Security Agency, FR]

– Department of Business, Innovation and Skills [UK]

– Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security, DE]

– Computer Emergency Response Team (see the definition above)

– Critical Infrastructure (see the definition above)

– Critical Information Infrastructure (see the definition above)

– Critical Information Infrastructure Protection

– Distributed Denial of Service (see the definition above)

– Information and Communication Technologies

– Internet Protocol

– Information Technologies

– Personal Computer

– Standard Operation Procedures