



Federal Ministry
of the Interior

National Plan

for Information
Infrastructure Protection
CIP Implementation Plan



Appendices to the Concept of IT Emergency and Crisis Exercises in Critical Infrastructures

UP KRITIS
Working Group 1
“Emergency and Crisis Exercises”

www.bmi.bund.de

Contents

A	Appendix: Existing exercise series	3
	A.1 National exercises in Germany	3
	A.1.1 LÜKEX	3
	A.1.2 CYTEX	4
	A.2 National exercises in other countries	5
	A.2.1 INFORMO	5
	A.3 International exercises	6
	A.3.1 CYBER STORM	6
B	Appendix: Role model for CIP exercises	8
C	Appendix: Exercise phases	11
	C.1 Exercise planning	11
	C.1.1 Drawing up the rough outline for the exercise	11
	C.1.2 Drawing up the detailed plan for the exercise	11
	C.1.3 Holding training sessions and informative meetings in advance of the exercise	12
	C.2 Preparing the exercise environment	13
	C.3 Conducting the exercise	14
	C.4 Dismantling the exercise environment	14
	C.5 Evaluation and follow-up	15
D	Appendix: Exercise types	17
	D.1 Tabletop exercises	17
	D.1.1 Objectives, content and scenarios	17
	D.1.2 Requirements, participants and expense	18
	D.2 Communication exercises	19
	D.2.1 Objectives, content and scenarios	19
	D.2.2 Requirements, participants and expense	21
	D.3 Coordination exercise	22
	D.3.1 Objectives, content and scenarios	22
	D.3.2 Requirements, participants and expense	24
	D.4 Extended coordination exercise	25
	D.4.1 Objectives, content and scenarios	25
	D.4.2 Requirements, participants and expense	26

E	Appendix: Resources	28
	E.1 Planning an exercise	28
	E.1.1 Template for capturing the general conditions forming the framework for a CIP exercise	28
	E.1.2 Items included in a rough exercise outline	30
	E.1.3 Scenario catalogue	35
	E.1.4 Guidance on scenario development	37
	E.1.5 Sample schedule for exercise planning and follow-up	39
	E.1.6 Sample exercise script	41
	E.2 Exercise implementation	42
	E.2.1 Exercise log template	42
	E.3 Exercise follow-up and evaluation	43
	E.3.1 Master evaluation form	43
	E.3.2 Template for an external exercise report	44
	E.3.3 Items for inclusion in internal exercise reports	47

Tables

Table 1:	Information distribution checklist	14
Table 2:	Items included in a rough exercise outline	30
Table 3:	Exercise scenarios	35
Table 4:	Example of an exercise script	41

A Appendix: Existing exercise series

Below is a brief outline of exercise series which have already been performed or are currently being conducted on similar or related themes. It also includes some exercises which have only taken place once to date. It starts by listing the exercises which have been performed on a national level in Germany, before moving on to further exercises on a national level in other countries and ending with international exercises.

A.1 National exercises in Germany

A.1.1 LÜKEX

The strategic series of interstate and interdisciplinary crisis response exercises known by the name of LÜKEX (“Länder Übergreifende Krisenmanagement Exercise”) is held regularly about every two years at political and administrative level in the Federal Republic of Germany. The exercises are organised by the Federal Office of Civil Protection and Disaster Assistance (BBK). The following exercises have taken place in this series to date:

LÜKEX 2004

Events organised between	29 November till 1 December 2004
Scenario	Simulation of prolonged hurricane-induced power failure, terrorist threats and attacks
Participants	Eight Federal Ministries, Federal Armed Forces and police forces of the Federal Government and Federal States, the Federal States of Baden-Württemberg, Bavaria, Berlin and Schleswig-Holstein, fire brigades, aid organisations, Federal Agency for Technical Relief, over 100 enterprises, such as utility companies, railway, airport and airlines operators
Implementation	From actual work environments via normal communication channels and controlled via own network

LÜKEX 2005

Events organised between	14 and 15 December 2005
Scenario	Simulated disruption of major events by acts of terrorism, natural disasters and accidents caused by technical mishaps
Participants	Nine Federal Ministries, Federal Armed Forces and police forces of the Federal Government and Federal States, the Federal States of Baden-Württemberg, Brandenburg, Hessen, North Rhine-Westphalia, Lower Saxony and Saxony, fire brigades, aid organisations, Federal Agency for Technical Relief, utility companies, railway, airport and airlines operators
Implementation	From actual work environments via normal communication channels and controlled via own network

LÜKEX 2007

Events organised between	7 and 8 November 2007
Scenario	Simulation of influenza pandemic
Participants	Representatives of several Federal Ministries, all Federal States (seven with a direct involvement, the others with an indirect involvement) and representatives of aid organisations and selected private and public sector organisations and companies; around 3,000 in total
Implementation	From actual work environments via normal communication channels and controlled via own network

To all intents and purposes, LÜKEX exercises also deal with IT issues although the emphasis is clearly on the coordination of the numerous disaster control organisations which, if anything, are confronted with physical problems. Given that there are major areas of interplay and that some of the CIP organisations are involved both in this issue and in IT issues, it is an option to integrate IT aspects in LÜKEX exercises.

A.1.2 CYTEX

The CYTEX (Cyber Terror Exercise) was a one-time event and the first relatively large exercise in Germany on the theme of cyber-terrorism. It was basically a simulation game for AKSIS (Working Group on Infrastructure Protection) which brought together approximately 40 participants from companies and federal agencies.

CYTEX

Events organised between	12 till 14 November 2001
Scenario	Series of targeted internal and external attacks on Berlin's infrastructure
Participants	Representatives of BMI / BSI, BMWi, BMVg / BWB, Federal College for Security Studies, Telekom, DFS, DB, police, THW, E.ON, TÜV, EADS, IABG
Implementation	In prepared joint working environment with own network

CYTEX mainly focused on the response to politically motivated targeted attacks on the IT infrastructure. Supply and transport problems disrupted an international conference in this scenario. The CYTEX exercise is an appropriate model for CIP exercises.

A.2 National exercises in other countries

A.2.1 INFORMO

INFORMO is a one-time exercise devised by the Special Task Force for Information Assurance (Sonia) in Switzerland. The event was organised by the Swiss Federal Chancellery.

INFORMO

Events organised between	13 till 15 June 2001
Scenario	Simulated information security crisis
Participants	Government and canton administrations in Switzerland, Swiss companies; around 150 in total
Implementation	In a civil defence centre

INFORMO was the follow-up exercise to the Strategic Leadership Exercise held in 1997 (SFU 97) which resulted in Sonia being set up as an instrument of crisis management. The Reporting and Analysis Centre for Information Assurance (Melani), which works with the German Federal Office for Information Security (BSI), was also set up to assist with threat detection.

A.3 International exercises

A.3.1 CYBER STORM

Cyber Storm is designed as a series of exercises put on by the USA's National Cybersecurity Division. This is located in the Department of Homeland Security. The effect of the exercise extends far beyond the borders of the USA because it is a simulation game involving the cooperation of many international bodies which are concerned with IT security.

CYBER STORM I

Events organised between	6 till 10 February 2006
Scenario	Simulated attacks on IT of utility companies, IT and telecommunications enterprises, logistics companies, federal and state authorities
Participants	Eight US departments and three US agencies, the US states of Michigan, Montana, New York and Washington, nine IT enterprises, six utility companies, two aerospace companies, MS-ISAC (Multi-State Information Sharing and Analysis Center), interfaces to Australia, Canada, New Zealand and Great Britain; over 300 participants in total
Implementation	At 60 locations in the USA, Canada and Great Britain

CYBER STORM II

Events organised between	10 till 14 March 2008
Scenario	Simulation of a large-scale, coordinated cyber-attack on critical infrastructures carried out by a hypothetical adversary in the pursuit of political and economic goals. It entails serious disruption to the information and communications infrastructure which calls for an internationally coordinated response
Participants	Eight US departments and agencies, nine US states, nine IT enterprises, five countries, 40 private enterprises; several thousand participants in total
Implementation	At 60 locations in the USA, Canada and Great Britain

Cyber Storm is a highly complex exercise which focuses mainly on threats which ensue from a dependency on IT. The focal point of Cyber Storm is

quite definitely in the USA. However, it has always been designed to encourage international collaboration. The first time it only involved institutions in English-speaking countries. However, the focus is set to broaden in the future and might also incorporate Germany's BSI.

B Appendix: Role model for CIP exercises

The roles listed below have been identified as major roles in CIP exercises:

Role	Explanation	BBK equivalent ¹
UP KRITIS Working Group 1	<p>The UP KRITIS partners participating in UP KRITIS Working Group 1:</p> <ul style="list-style-type: none"> • make decisions of general principle on holding the exercises and their framework conditions • decide whether to approve interim and final results in the individual exercise phases • determine the nature and extent of press and public relations work 	Exercise management
Planning team	<p>The planning team works out the details in advance of the exercise. The team draws up the rough outlines and the detailed plans for the exercises.</p>	Steering / control staff
Exercise leader	<p>The exercise leader takes on the role of a coordinator throughout the exercise, including the set-up and dismantling of the exercise environment. This typically includes the following tasks:</p> <ul style="list-style-type: none"> • 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 • Facilitation of tabletop exercises • Coordinating supplies for the exercise participants (e. g. catering) 	Exercise management / head of exercise management staff

¹ Roles allocated by the BBK which are used e. g. for LÜKEX exercises. The role of the exercise management team at the BBK, where it makes fundamental decisions of general principle in the exercise planning and preparation phase, approves results, etc., is assumed in this document by representatives of the UP KRITIS partners in joint talks.

Role	Explanation	BBK equivalent ¹
Exercise leadership team	In complex exercises, it might be necessary for the exercise leader to have some assistance. Together, they make up the exercise leadership team.	Steering staff / exercise control group
Facilitators	<p>The main task of the facilitators is to brief the participants on the initial situation before the exercise and to bring in further events in the course of the exercise. They also have the following tasks:</p> <ul style="list-style-type: none"> • Record direct responses of those taking part in the exercise, e. g. on the telephone • Give expert presentations at relevant points during the exercise if necessary 	Framework management groups
Exercise participants	<p>The exercise participants discuss or enact their response to scenarios or check that technical facilities are functional.</p> <p>Additional tasks are as follows:</p> <ul style="list-style-type: none"> • Attending the exercise briefing session before the actual emergency and crisis simulation begins • If necessary, attending expert presentations which are incorporated into the exercise in order to give the exercise participants the necessary background knowledge • If necessary, issuing status reports to the exercise leaders as required, either at regular intervals or on request • If necessary, completing evaluation forms after the exercise and submitting them to the exercise management team 	Exercising participants
Exercise observers	Exercise observers log the activities performed by the exercise participants. Their records also include, for example, the times achieved and any notable insights, such as unexpected difficulties or room for improvement.	Exercise observers (referees)

Role	Explanation	BBK equivalent ¹
Follow-up team	The follow-up team evaluates the course of the exercise and reports on its findings. It bases its findings on evaluation forms and on the logs written during the exercises.	Steering staff

There can be some overlap in terms of the personnel assuming the various roles. The planning team could double up as the evaluation team, for example, and the exercise leader and the observers could be taken from this team. The only exception is the exercise participants who should not assume any other roles.

C Appendix: Exercise phases

C.1 Exercise planning

The exercise plan is drawn up by the planning team selected by the UP KRITIS partners in liaison with the Single Points of Contact (SPOCs). The team starts by drawing up a rough outline for the exercise. Once the rough outline has been approved, it is fleshed out in detail by the planning team. This detailed plan sets out the procedures for the exercise and all the documents required to put the plan into action.

C.1.1 Drawing up the rough outline for the exercise

The rough outline serves to establish the basics of the exercise. It is based on the general framework specified by the UP KRITIS partners. Items typically included in a rough outline are listed in Appendix E.1.2. Questions and unresolved issues, which have to be clarified in the run-up to the exercise by the UP KRITIS partners, are recorded and resolved separately.

C.1.2 Drawing up the detailed plan for the exercise

The detailed plan comprises a revised and updated version of the rough outline as well as all the necessary technical and organisational details and final planning documents. It thus constitutes the operative document for the performance, evaluation and follow-up of the exercise. It can also serve as a rough guide for the planning of similar exercises in the future.

The detailed plan typically includes the following in addition to the rough outline:

- Exercise documentation/lists
- Presentation documents, handouts for training sessions and informative meetings in advance of the exercise
- Templates for letters of invitation and notification (e. g. background information on the exercise, introductory notes on the nature of the exercise, objectives and, where applicable, rough outline of scenario)
- Press releases
- Explanatory/ Instruction documents for briefing of exercise participants
- Presentation documents, lecture handouts

- Schedules and checklists for preparing the exercise environment, running the exercise and dismantling the exercise environment
- Exercise script for complex exercises with inserted events (see Appendix E.1.6 for a specimen)
- Exercise technical support documents
- Basic documents such as alarm and contingency plans which are relevant for the exercise
- Communication templates (pre-prepared specimen texts for all types of communications, such as e-mail, fax, announcements, etc.)
- Contract documents
- Planning of supplies for exercise participants (e. g. with catering) if the exercise is held outside normal working hours or away from the normal working environment
- Evaluation form for the exercise participants.

C.1.3 Holding training sessions and informative meetings in advance of the exercise

An essential prerequisite for the success of the exercises is that the participating UP KRITIS partners have a comparable level of knowledge. Training sessions and informative meetings are required to achieve the required level of knowledge. In addition to the theory, it is also important to involve the participants in practical sessions where they explore different responses to the crisis (workshops). This increases their appreciation of the measures required to respond to the crisis, making them receptive to specialist knowledge and enhancing their reaction capability. Valuable and interesting information plays a major role in maintaining high interest levels among participants.

The training sessions, informative meetings and workshops are particularly valuable at the start of the exercise cycle.

C.2 Preparing the exercise environment

Before the exercise actually begins, all the necessary foundations must be in place to guarantee that the exercise will proceed in an efficient manner without interruptions. The exercise leader is responsible for preparing the exercise environment. This typically includes the following (as already set out in the exercise plan):

- Making special arrangements and provisions which might be necessary before the exercise can be conducted (e.g. equipping exercise premises with the resources and equipment needed, providing specific exercise environment and conditions)
- Informing institutions and persons which or who have no direct part to play in the exercise but could be directly impacted by the exercise and should be duly informed about the time, duration, content and objectives of the exercise. They should also be given the details of contact persons in the exercise management team whom they can contact should problems arise as a direct result of the exercise
- Immediate neighbours and government bodies, such as the police and fire service, should be informed in due time if there will be potential external effects in order to avoid false alarms
- Informing the media: the media should be notified in advance if the exercise is expected to involve political signals or if the exercise is likely to be evident to those not taking part
- Briefing the exercise participants (exercise participants, facilitators and observers): Table 1 shows who is to be provided with which information. In the case of large-scale exercises it might be necessary to brief the participants in several stages. The participants are usually briefed immediately before the start of the exercise so that the element of surprise can be factored in, as would be the case in a real emergency. Depending on the type of exercise, it may not be necessary to brief all the participants. If the exercise includes the sounding of issuing of an alert, for example, it might only be relevant to brief those who trigger the alert but not those who respond to it since part of the exercise might be to communicate the starting scenario correctly.

Table 1: Information distribution checklist

Briefing content	Exercise participants	Facilitators	Observers
Starting scenario and exercise objectives	Yes	Yes	Yes
Logging requirements and resources	–	Yes	Yes
Exercise scripts	–	Yes	Yes
Exercise period	Yes	Yes	Yes
Exercise conditions and artificial situations	Yes	Yes	Yes
Contact persons in the exercise management team should unforeseen events arise	Yes	Yes	Yes
Evaluation forms	Yes ¹	Yes ¹	Yes ¹

¹ Possibly not until the end of the exercise

C.3 Conducting the exercise

The exercise is held as set out in the plan or the script. The exercise leader is responsible for co-ordinating the various stages of the exercise. He also decides on any departures from the plan and, ultimately, whether to cancel the entire exercise.

The exercise participants should adhere to the exercise conditions and artificial situations in force during the exercise, but not to the point of suppressing their own initiative for taking creative action. Facilitators are intended to insert other events as the exercise progresses, thus keeping the simulation moving and creating elements of surprise. Observers log events during the course of the exercise.

C.4 Dismantling the exercise environment

All the conditions which have been specially set up for the exercise are reverted to their original state, as set out in the plan. All the exercise documents which have been issued (notes, records, logs, etc.) are collected at one central point. The exercise leader is again responsible for these tasks.

C.5 Evaluation and follow-up

The detailed evaluation and follow-up of each exercise are just as important as careful planning beforehand. The evaluation procedure is performed by the follow-up team specified in the exercise plan. The objectives are as follows:

- To check whether the exercise objectives have been achieved
- To identify any need for improvement
- To set an impulse for implementing improvement measures
- To illustrate the success of the exercise (each exercise which is performed is a success because all of the participants have learnt something new even if individual elements of the exercise were not successful)
- To provide a resource base to assist with the planning for the next exercise and to reduce the input required for subsequent exercises.

Tasks typically include the following:

- Send (and if necessary resend) the evaluation form to exercise participants as an editable document with a deadline for its submission
- Analyse the logs and completed evaluation forms: a statistical analysis can be useful depending on the exercise (e. g. number of successful/ abortive contact attempts, runtime distribution, etc.).
The evaluation is a summary of the facts without any assessment
- Issue exercise reports: two reports are issued for every KRITIS exercise:
 - An abridged report for external consumption which is highly anonymised. It is approved for release by the UP KRITIS partners and can then be freely circulated to all exercise participants and organisations taking part in the exercise. It can also be distributed to other bodies subject to the prior express consent of all the UP KRITIS partners taking part in the exercise.
 - A detailed report for internal consumption (its coverage in line with the scope of the exercise). It is also intended to highlight vulnerabilities and suggest improvements. However, this report is also anonymised to preclude any inferences as to where specific vulnerabilities might lie among individual UP KRITIS partners. This internal report is highly confidential and is only issued to a select few who are

jointly and unanimously specified beforehand by the participating UP KRITIS partners.

Items typically included in exercise reports are listed in Appendix E.3.2 (external report) and Appendix E.3.3 (internal report).

- Approval of exercise reports by UP KRITIS partners and expressing thanks to all participants involved parties on completion of the exercise
- Presentation of exercise results at a joint meeting of the UP KRITIS partners including time for discussion and accounts of impressions of participants
- Preparation of press releases, where applicable
- Collation of all available documents as a template for subsequent exercises
- Archiving of all documents at the BSI, having due regard for the high confidentiality requirements of the documents when filing
- Give an impulse for measures designed to bring about improvements, with priority being given to measures based on insights gained in practical exercises as these measures are often fundamental to the successful mitigation of the next crisis. In subsequent exercises, particular attention should always be paid to checking whether action has been taken for purposes of reviewing and documenting improvement and progress. This completes the full exercise cycle.

D Appendix: Exercise types

The following section goes into more detail on the types of exercise envisaged in the policy.

D.1 Tabletop exercises

Tabletop exercises provide an opportunity to jointly develop and review response patterns to a given scenario and to expose interdependencies of operators of critical infrastructures. It is typically a guided discussion with key questions conducive to constructive dialogue and might also incorporate expert presentations to fill in background information on the scenario at issue. It is a theoretical exploration of possible responses to the scenario rather than actual doing.

D.1.1 Objectives, content and scenarios

The objectives of tabletop exercises can be as follows:

- To identify demands on communication structures and precautions to put in place by UP KRITIS partners in emergencies and at times of crisis
- To expose interdependencies and expectations of operators of critical infrastructures
- To raise awareness and create mutual understanding among UP KRITIS partners
- To explore possible reactions and response mechanisms in the context of the UP KRITIS
- To identify vulnerabilities in crisis strategies, contingency plans and in action plans before these are practised or adopted at great expense
- To clarify areas of accountability and responsibility in emergency and crisis responses.

This type of exercise might include the following:

- Familiarisation with a topic
- Exchange of information
- Presentation of the response of an organisation to certain scenarios
- Discussion and investigation of proposed solutions and plans
- Examples illustrating the problem of different interpretations of messages
- Identification of conflicts in terms of accountability or roles.

Tabletop exercises can be used as a “multi-purpose tool” at any level of complexity and regardless of the prior knowledge of the participants. Scenarios of any kind can be treated. The exercise is always announced. Since it is a discussion-oriented exercise, there is no need to consider any interfaces to the outside world.

They do not lend themselves to being combined with other exercises. Their primary role is as a conceptual platform establishing a basis for further exercises. During a tabletop exercise blocks of relevant specialised information can be integrated in the form of lectures.

D.1.2 Requirements, participants and expense

The aspects requiring preparation are the scenarios and content which will be discussed, the order of the meeting and the discussion facilitation methods. This can be handled by a small preparation team. This will usually take between several days and one week, the amount of input corresponds to that required to prepare a relatively large specialised workshop.

The representatives of the relevant UP KRITIS partners should participate in a tabletop exercise along with the SPOCs representing specific sub-sectors. The exercise participants must have prior knowledge of the general structures and procedures in the event of a crisis, both in their own organisations and in the CIP context. A facilitator (exercise leader) and minute-taker (exercise observer) are also required, and possibly speakers for specialised presentations.

Tabletop exercises are held at a central location (conference room) and last for about half a day. The outlay required to run a tabletop exercise (exclud-

ing travel expenses) thus amounts to half as many man-days as participants. The follow-up phase generally takes just a few man-days.

D.2 Communication exercises

Communication exercises are essentially:

- A review of the communication methods and procedures which have been agreed for alerting
- A review of the communication methods and procedures provided for information to be exchanged in emergencies and crises, possible means of communication being e. g. telephone, fax, e-mail, messaging systems, internet portals and/or videoconferencing.

A communication exercise generally starts out as a star-shaped arrangement, with the UP KRITIS partners communicating via the SPOCs with a central location (e. g. the BSI IT Situation and Crisis Response Centre) on all aspects of events related to the crisis (communication in general and in crises outside simulation games, exercises, etc. is set out in the “Concept on Early Warning and Mitigation of IT Crises” (Working Group 2). Other topologies can also be used as the exercise progresses, e. g. conference channels.

D.2.1 Objectives, content and scenarios

The objectives of communication exercises can be as follows:

- To review the documentation and mechanisms required for alerting
- To review the documents, mechanisms and technical systems with reference to communications in emergencies and crises
- To review the adequacy of the accessibility of the points of contact provided
- To practise the methods provided for communication between all involved, including communications in encrypted form if applicable
- To review and, if applicable, evaluate the real alert times
- To improve the skills and knowledge of the personnel involved in handling the above-mentioned documents, mechanisms and systems.

The focuses of the exercise can differ depending on the objectives, e. g.:

- Technical review of primary and alternative communication channels
- Alert procedures
- Communications procedures in emergencies and crises.

The following details might be practised or reviewed:

- Different alert channels and triggers
- Dissemination of information between the participants
- Function of technical communication equipment
- Availability of SPOCs and other units forming part of the alert process run by the operators of critical infrastructures, and availability of crisis response units and control units during and outside normal working hours
- Adherence to the agreed response times
- Completeness and accuracy of contact and alert lists
- Direct deployment in response to the alert, e. g. forming crisis response teams with the UP KRITIS participants
- Function of encryption and authentication procedures used to guarantee secure connections among participants.

Communication exercises are activity-based exercises. A scenario is not always required. If a scenario is used for the exercise then a simple starting situation is sufficient. The situation could be made more complex during the exercise by introducing a failure of the communication equipment. The exercise can be announced or unannounced. If the emphasis is on checking the alert-raising mechanism then the exercise should be unannounced (within a specified period).

The following situations can be introduced to increase the degree of complexity:

- The exercise practises different alert triggers. It might then be necessary to run through chains of command in different directions.
- Alternative communication channels are developed in addition to the standard channels or as an alternative in the case of a notional disruption to the primary channels.
- Complex communication structures are developed, e.g. extensive conference channels.

They may be combined with internal exercises developed by the UP KRITIS partners. This is advisable because in a real crisis it might also be necessary to run through internal alert-raising and communication procedures at the same time with the UP KRITIS partners.

D.2.2 Requirements, participants and expense

Communication exercises assume that coordinated alert plans are in place with current contact details and that the participants have decided on the means and channels of communication which are to be used and that they have made and documented the necessary technical arrangements. If formal logs are to be used, these must be available and flawless in syntax and semantics. The participants must be familiar with them, and all the technical equipment must be in working order.

A small team is adequate for the planning. The time required for planning may be more than one week. The communication relationships which will have to be established in the exercise must be specified and adequately prepared. Once prepared, documents can be reused in subsequent exercises. It might be appropriate to run preliminary internal tests on the communication infrastructure at the UP KRITIS partners in advance of the chosen means of communication are rarely used.

Those participating in the exercise are the users of the means of communication on all sides, i.e. SPOCs or members of the crisis organisation, and possibly technicians who have to set up the equipment specifically in crisis situations. There is also an exercise leader who might also be called on to perform the logging duties at the same time (exercise observation). A communication exercise lasts no more than one day, bringing the total time required for the exercise to a few days taking into consideration the total number of participants. Similarly, the follow-up phase generally requires only a few man-days.

D.3 Coordination exercise

A coordination exercise has two points of focus. First, it serves to review the technical and organisational prerequisites which are fundamental to the efficient execution of all the actions and aspects involved in the crisis (e.g. the BSI IT Situation and Crisis Response Centre). Second, it serves as a practice run for mitigating an emergency or crisis.

A scenario is essential for a coordination exercise. In contrast to tabletop exercises, this scenario is not only discussed but it is enacted with the aid of the available plans and crisis response resources. This involves the entire crisis organisation in the framework of the UP KRITIS. The scenario and subsequent events are discussed and responses decided. However, the responses are not implemented; the world outside the direct CIP crisis organisations is completely regarded as an artificial situation.

D.3.1 Objectives, content and scenarios

The objectives of coordination exercises are as follows:

- To review the readiness of central resources for action in the event of a crisis
- To practise communication processes, decision-making and control systems in crises on the basis of realistic scenarios
- To devise joint solutions and measures for containing and mitigating crises
- To work under crisis conditions and stress
- To review the appropriateness and adequacy of the relevant processes and resources.

Exercises might include the following:

- Manning emergency task force headquarters, crisis response units, etc.
- Bringing alternative premises into service, where available, for the above
- Coordination and communication between the UP KRITIS partners involved
- Running through a sequence of events based on the scenario and exchanging information about progress
- Processing of situational information for presentation to the management level of the participating organisations and possibly joint decision making.

As already mentioned, coordination exercises involve working with a number of artificial situations. They might involve bringing together all the participants at the emergency task force headquarters or the situation centre. This enables the parties to communicate directly with each other, rather than through the communication channels provided, which is a better way to establish the plan of action. It also means that the proceedings can be controlled much more easily. In the long term, however, the participants should eventually be dispersed to their respective places of work, as in a real crisis, and use the various communication channels provided for crisis situations.

One essential aspect of a coordination exercise is to have persons who do not belong to the crisis organisations of the participating bodies to simulate the outside world. They play along with the scenario, coping with subsequent inserted events, and act on the decisions and orders of the exercise participants. They simulate the responses and ongoing scenes in the outside world and report back to the exercise participants. This cycle is repeated several times in the exercise.

In this manner, all conceivable scenarios can be enacted. The exercise is usually announced due to the large number of participants. It can be combined with internal exercises run by the participating organisations. This increases the element of reality. However, the scenarios do need to be discussed and agreed in advance, which can have the disadvantage of losing the element of surprise for the participants. Efforts are therefore also made to integrate coordination exercises in other series of exercises, e. g. LÜKEX. This allows the combined rehearsal of aspects which are relevant to both

disaster control and IT scenarios and is more cost-effective than running separate exercises.

D.3.2 Requirements, participants and expense

The successful execution of coordination exercises is subject to having laid the necessary foundations in terms of organisation, infrastructure and technical requirements. The areas of responsibility of the participants must also be fully defined and well established in their own crisis organisations and communications. This implies that the chain of command is clearly specified and rehearsed and that the participants are duly trained.

Part of the preparatory work is to develop a scenario with numerous inserted events (including the expected responses), e. g. in the form of an exercise script (see Appendix E.1.6). It is advisable to use software tools at this stage to record the scenario and to support the implementation of the exercise. Developing the scenario presupposes a great deal of experience on the part of the relevant persons and requires several man-months in total. These exercises cannot be repeated with the same scenario therefore there is little scope for reusing the preparatory work. If the coordination exercise is integrated in another larger-scale exercise (e. g. LÜKEX), the CIP scenario is subsumed in the wider scenario.

Those taking an active part in the exercise are SPOCs, representatives of the crisis organisations of the relevant UP KRITIS partners, technicians to assist with communications, the exercise management team, facilitators and several observers. A standard exercise lasting between one and several days would require one or more man-months.

This exercise also involves an extensive follow-up process, which involves retracing and evaluating the course of the exercise and suggesting where improvements might be made. These suggestions might equally relate to the structures and resources which were used or to the handling of the crisis itself.

D.4 Extended coordination exercise

The extended coordination exercise is the highest level and has the greatest degree of complexity and reality of all the exercises. The entire response to a crisis is enacted, predominantly in real-time and therefore, where necessary, over a longer period, preferably with all the people who would be implicated in a real crisis.

As with the coordination exercise, a starting scenario is established as a basis and numerous events are inserted as the process evolves. In an extended coordination exercise, however, the outside world is no longer artificially simulated but is incorporated as far as possible. This means that the participating UP KRITIS partners will involve bodies outside the UP KRITIS crisis organisations. Another factor requiring clarification is the extent to which disruption to of IT can be simulated for the purposes of the exercise, e. g. in a test environment. This allows, albeit in a limited context, a realistic testing of events even for technical measures.

D.4.1 Objectives, content and scenarios

The objectives of extended coordination exercises are similar to those pursued in normal coordination exercises. However, there are some additional objectives:

- The interaction of many persons and teams belonging to different organisations
- The review of assumptions, especially with regard to the outside world, the coping mechanisms of those involved, the realistic duration of events, and with regard to general logistics.

Extended coordination exercises allow an to completely test all of emergency and crisis response processes. Examples include:

- Performance of the full range of communications required in the crisis by all organisations involved
- Change of location of persons involved during a crisis while still maintaining contact and staying on task
- Coordinated distribution of critical resources in the event of their scarcity

- Coordinated approach in the event of extensive problems with the IT
- Joint approach to public relations and statements to the media.

Any conceivable crisis situation can basically be enacted as a scenario in an extended coordination exercise. Naturally, there is still a need for artificial situations, however, as events must not be allowed to develop into a real crisis. But it might be possible to replicate a CIP-type event – possibly forming part of the scenario – in a separate exercise environment, providing a realistic opportunity to train the practical problem-solving process.

Extended coordination exercises always have to be announced due to the large number of participants. Given the number of participants and the amount of input required, it is again worth attempting to combine them with other exercises. This applies to internal exercises run by the UP KRITIS partners involved which might overlap with the scenarios rehearsed, and it also applies to exercise series applied across-the-board at national or international level.

D.4.2 Requirements, participants and expense

An extended coordination exercise dictates the clear definition and full establishment of all the crisis organisations of the bodies involved and the communication between them. All the relevant resources are clearly specified and available, the processes pre-tested and the participants duly trained.

As with a normal coordination exercise, a complex scenario is developed featuring events which are inserted along the way. The required number of inserted events may be lower in the extended coordination exercise as there is less simulation and more real enactment of events. However, these inserts still have to be incorporated in the planning and observation, which results in another large increase in the scope of the exercise as compared to a normal coordination exercise. If the extended coordination exercise is integrated in another larger-scale exercise, the CIP scenario is subsumed in the wider scenario. As with the normal coordination exercise, a software tool is advisable to record the scenario and run through the exercise.

A large team is required for the planning. One major requirement is a long process of consultation between the relevant UP KRITIS partners, possibly involving external bodies. This increases the amount of input required and can amount to several man-years. Again, the majority of this work can only be used once.

An extended coordination exercise lasts at least one day but generally, several days. Naturally, the amount of work involved is immense and is in the range of man-years, especially for a full run-through of an entire crisis response process. One option in terms of reducing the amount of input is not to run the entire exercise in real-time but to build in time shifts. The exercise involves the SPOCs, the entire crisis organisations of the relevant UP KRITIS partners as well as technical personnel who can facilitate the realistic enactment of possible IT scenarios and support communications. A number of other people are required for the exercise management team and to act as facilitators and observers.

The follow-up process, comprising logging, evaluation and making suggestions for improvements, is more time-consuming than for a normal coordination exercise. Several man-months will need to be planned for.

E Appendix: Resources

E.1 Planning an exercise

E.1.1 Template for capturing the general conditions forming the framework for a KRITIS exercise

General planning framework for a KRITIS exercise			
Status	<input type="checkbox"/> Draft <input type="checkbox"/> Approved		
Date last revised	dd.mm.yyyy		
Exercise type	<input type="checkbox"/> Tabletop exercise <input type="checkbox"/> Communication exercise <input type="checkbox"/> Coordination exercise <input type="checkbox"/> Extended coordination exercise		
Exercise purpose and objectives			
Exercise scenario			
Participants	Company/author- ity/institution	Name of contact person	Contact details
Announcement	<input type="checkbox"/> Announced exercise <input type="checkbox"/> Unannounced exercise		
Risks			

General planning framework for a KRITIS exercise			
Confidentiality requirements			
Date of exercise			
Duration of exercise			
Required approvals	Approval milestone	Target date	Approval terms
Planning team			
Exercise management team			
Evaluation team			
Rough estimate of financial budget and personnel requirements, assumption of costs and expenses			
Other general conditions			

E.1.2 Items included in a rough exercise outline

Table 2 lists the items typically included in a rough outline with explanatory notes and examples.

Table 2: Items included in a rough exercise outline

Item	Explanatory notes
Name of exercise	<p>(WHAT NAME?) The exercise should have a plausible name which is easily recognisable and which identifies the exercise and, where applicable, its position in a series of exercises, e. g.</p> <ul style="list-style-type: none"> • Coloured ribbon (expressing variety and a connective element) • Gabriel 06 (patron saint of postal and communication workers) • Hermes, Mercury, Wotan = Odin (messengers of the gods) • Argus (Greek mythology, “the all-seeing”, a giant with one hundred eyes, stands for watchfulness) • CIC 06 Communication in Crises
Exercise type	<p>(HOW?) Type of exercise (tabletop exercise, communication exercise, etc.)</p>
Exercise purpose and objectives	<p>(WHY and WHAT FOR?) Formulation of the intention behind the exercise, its individual aims and overall objectives, e. g.:</p> <ul style="list-style-type: none"> • The stated intention of UP KRITIS partners is to check the response times taken to alert the Single Points of Contact (SPOCs) in the event of a crisis by running a communication exercise. <p>An exercise may also have the following objectives, e. g.:</p> <ul style="list-style-type: none"> • To enhance the confidence of those taking action and provide experience • To check documentation (address lists, availability) • To test various communication media (telephone, fax, e-mail) and review the technical communication capability • To review times of availability • To check the response times to an alert

Item	Explanatory notes
Personnel organisation	<p>(WHO and WITH WHOM?)</p> <p>The following are to be specified:</p> <ul style="list-style-type: none"> • Planning team • Exercise leader • Exercise leadership team (where necessary) • Facilitators (where necessary) • Exercise participants differentiated as follows: <ul style="list-style-type: none"> - Key participants (these are the key decision-makers without whom the exercise cannot feasibly be implemented. If a key participant withdraws, the entire exercise is jeopardised) - Other participants • Exercise observers • Follow-up team <p>It might be necessary to clarify the necessity / possibility of external support from a consultancy firm.</p>
Investment	<p>(HOW MUCH?)</p> <p>Estimation of the requirements in terms of finance, personnel and other resources for the preparation, execution and follow-up of the exercise (measures must also be in place to ensure that all those involved have access to the resources required for the planning, preparation, execution and evaluation).</p>
Risk assessment	<p>(WHAT LEVEL OF RISK?)</p> <p>Identification and evaluation of unwanted side effects which could arise in the course of the exercise:</p> <ul style="list-style-type: none"> • Threats and the likelihood of their occurrence • Possible precautions to prevent their occurrence. <p>Examples of risk factors are as follows:</p> <ul style="list-style-type: none"> • Non-availability of participating personnel for operations • Failure of linked IT systems.
Reasons for termination	<p>(WHEN TO CALL A PREMATURE END?)</p> <p>Agreement on the conditions which would necessitate the premature termination of the exercise, e. g.:</p> <ul style="list-style-type: none"> • Occurrence of a real crisis during the exercise, which has to be mitigated as a matter of priority • Unforeseen and unwanted side effects which arise in the course of the exercise and have a major impact • The exercise objectives are obviously not being met • The exercise is called to a premature halt by participants who are playing a key role.

Item	Explanatory notes
Announcement	(WHAT ELEMENT OF SURPRISE?) Specification as to whether the exercise will be unannounced or announced (proposal of dates, where applicable, with several alternatives).
Dates	(WHEN and HOW LONG?) <ul style="list-style-type: none"> • Setting of a date or period (e. g. within a given calendar week) on or within which the exercise is to be held • Determination of the duration of the exercise (depending on the objectives).
Exercise location(s)	(WHERE?) Specification of the location or locations in which the exercise is to be held (ensuring that the locations meet the requirements in terms of their size, equipment, logistics, etc. and are available at the time of the exercise).
Exercise planning	(WHAT PREPARATIONS?) Rough identification of the necessary activities, documents (e. g. detailed plan, exercise script) and milestones (e. g. start of planning, availability of preparatory documents, approvals, training sessions, execution, evaluation, availability of results documents) in the form of a schedule (cf. also Appendix E.1.5).
Course of exercise	(WHAT Course of events?) Planned course and time estimates for the exercise schedule, requirements in terms of facilitators and observers.
Exercise tools	(WHAT KIND OF SUPPORT?) Specification of the IT programs and tools which will be used in planning and executing the exercise. Wherever possible, use should be made of existing tools, e. g. deNIS.
Internal information	(WHAT PRIOR KNOWLEDGE?) Specification as to whether there ought to be a training seminar / information event beforehand to brush up on the methods and revise the procedures already prepared. This might involve an introduction to the specific or general exercise concept and practical execution of the exercise.
External information	(WHOM TO INFORM?) Specification as to who should / must be informed about the exercise besides those directly participating.

Item	Explanatory notes
Exercise conditions and artificial situations	<p>(WHAT TO OBSERVE, WHAT NOT TO DO?)</p> <p>Specification as to whether there should be specific exercise conditions to be observed by the participants during the exercise. These conditions are in part intended to establish a clear relationship between an alert and the exercise, to focus on what is to be practised, to avoid misunderstandings and problems with external parties, to document the exercise more clearly and comprehensibly, etc., e. g.:</p> <ul style="list-style-type: none"> • All communications must be preceded with “EXERCISE EXERCISE EXERCISE” • Documents issued during the exercise must be marked “EXERCISE EXERCISE EXERCISE” • Contact is only permitted with those exercise participants previously determined. External contacts are represented by facilitators. • There is to be no cross-communication between the exercise participants • A copy of each e-mail will be sent to the exercise management team • An e-mail should be sent in preference to using the telephone, or a short report should be written for the exercise observers • If the person attempting to make contact encounters an answering machine or an out-of-office message, the person should follow the instructions given on one communication medium only (to another telephone number or e-mail address) Alternatively: All instructions should be followed • If several points of contacts are given for an organisation/institution/site, these shall be deemed to have been contacted if contact is made with one of the points (assuming that the alert is forwarded internally) • Questions are to be directed to ...@.... <p>Exercise conditions might entail artificial situations for the exercise. This is necessary because it is not possible to genuinely reproduce everything which can happen in emergencies (e. g. fire, failure of ICT systems, data loss, contact with media representatives) or things are not available or possible or should not be simulated.</p>

Item	Explanatory notes
Aspects of confidentiality	<p>(HOW SENSITIVE?)</p> <p>Exercises in the CIP setting generally have high confidentiality requirements as they may reveal critical vulnerabilities and allow security-related insights into the emergency and crisis responses of the participants.</p> <p>It is therefore necessary to adopt appropriate policies for handling information and documents relating to the exercise.</p> <p>Another aspect requiring clarification is the necessity for anonymity and source neutralisation. Source neutralisation means that the exercise management team neutralises all information relating to specific participants (e.g. “one participant was ...”) thus rendering any problems anonymous. It is particularly important when conducting exercises for the first time or across organisations that the participants work together without exposing vulnerabilities and problems to the other participants on the outside (“saving face”). This is why it is advisable to use so-called “no-fault” exercises (~ “nobody did anything wrong / nobody is doing anything wrong”), which do not require any exposure of (internal) problems. On the other hand, it is essential for vulnerabilities and gaps to be revealed in an alert network. It can even be helpful to publicise the respective response times as a kind of a “competition”.</p> <p>Another aspect which might require specification is the communication structure designed to guarantee the required anonymity and source neutralisation, e.g.:</p> <ul style="list-style-type: none"> • In case of express protection of the source: star-shaped communication structure from an arbitration point (only the latter has knowledge of vulnerabilities) • If there are no special requirements: cross-communication between the participants is allowed
Follow-up	<p>(HOW DID IT GO and WHAT NOW?)</p> <ul style="list-style-type: none"> • Clarification as to whether there should be an evaluation form for the exercise participants as a follow-up. What questions should be asked of the participants? • Setting of date for final event / evaluation meeting. <p>Items typically included on an evaluation form are listed in Appendix E.3.1.</p>

E.1.3 Scenario catalogue

The list of possible exercise scenarios in Table 3 is by no means exhaustive. It is meant as a source of ideas for simulation games and exercises. The classification into exercise types is a suggestion only. All the scenarios are primarily intended to focus on their impact on critical IT resources and the consequences arising therefrom.

Table 3: Exercise scenarios

Subject of exercise	Tabletop exercise	Communication exercise	Coordination exercise	Extended coordination exercise
IT				
Failure of central IT assets	X		X	X
Disclosure of critical IT vulnerabilities	X		X	X
Large-scale occurrence of malware with potential to cause great damage	X		X	X
Large-scale unauthorized access to critical IT systems (e. g. through foreign intelligence services)	X		X	X
Massive distributed denial-of-service attacks on several UP KRITIS partners	X		X	X
Attacks with enormous financial backing and technical know-how	X		X	X
Communication				
Failure of central public network infrastructures	X	X	X	X
Prolonged overload of public network structures	X	X	X	X

Subject of exercise	Tabletop exercise	Communication exercise	Coordination exercise	Extended coordination exercise
Security incidents				
Threat of physical or logical attacks on critical ICT facilities	X		X	X
Terrorist attacks on several critical ICT facilities within a short period of time	X		X	X
Environment				
Extreme snowfall / rainfall / storms / flooding in large parts of Germany	X		X	X
Prolonged extreme heat wave in Germany with water shortages / reservoirs drying out	X		X	X
Infrastructure				
Large-scale disruption of power supply	X		X	X
Failure of central information infrastructure locations	X		X	X
People				
Epidemic (measles, gastro-intestinal infections, influenza virus, bird flu, etc.)	X		X	X
Large-scale blockades of urban areas	X		X	X

E.1.4 Guidance on scenario development

Basics

A scenario must always serve the purposes and aims of the exercise. It is advisable to start with straightforward scenarios and to proceed to more complex ones. This allows a steady increase in self-confidence and expertise over the course of several exercises. Different exercise participants can be provided with various scenarios which complement one another in order to stimulate and test their reciprocal communication. The difficulty of a scenario will depend on how often exercises have been organised, how well-trained the team is, and whether it is a repeat exercise. If the participants appear to need more of a challenge, the complexity can be increased by incorporating surprise events.

A repetitive process has proved successful in formulating scenarios, with added value if participants are able to discuss events in several sessions.

Form of a starting scenario

A starting scenario usually takes the following form:

- Compact in formulation
- Highly specific
- Written in the present tense
- Written in short sentences intended to convey emphasis and suspense
- Situation might be set out chronologically (required for events with early warning period)

The starting scenario tends to be shorter with unexpected events (such as a chemical accident or an attack). In some cases it might be appropriate to set the scene in more detail leading up to the event/emergency (school nearby, evening rush hour traffic, etc.) in order to generate more pressure.

What is the best way to write a starting scenario?

It is appropriate to start by asking the following questions and noting down short answers (two to three words):

- What type of event has occurred?
- How rapid, powerful, profound, dangerous is it?
- Where did it happen?
- How was it discovered?
- What action has already been taken?
- What damage has been identified?
- What happened prior to the event? How did it happen?
- What time did it happen?
- Was there any advance warning?
- Does the weather play any particular role?
- What other factors would affect the emergency measures?
- Is there any prediction as to how the situation might develop?

The starting scenario is then basically written by making a sentence out of the key words noted down in each case.

Subsidiary scenes and inserted events

Developing a scenario for an exercise is like writing a play or a film script. While writing the play, the dramaturge breaks it down into acts and scenes. In a similar way, the scenario can be subdivided into scenes and can have various events inserted. Subsidiary scenes and inserts take place after and, in most cases, as a result of the starting scenario. They are to be regarded as events which are meant to prompt the participants to make realistic responses and to take realistic action in order to achieve the objectives of the exercise. A diligent build-up is important in order to achieve a convincing and coherent scenario which is consistent with the objectives of the exercise, rather than a series of disjointed, highly diversified and random events.

What form should inserted events take?

In the case of exercises intended to train the leadership process from the assessment of the situation, appraisal, decision and measures, it is helpful to record the insertions in a detailed list of events, the so-called exercise script (see Appendix E.1.6 for an example).

What is the best way to write insertions?

Each insert is designed to provoke one or more expected reactions by one or more of the exercise participants. There are various ways of developing inserts:

- The first stage is to identify the measures which the participants ought to take. An event is then brought into the overall scenario which is intended to precipitate these measures.
- A list of events which could arise in the specific scenario is drawn up. These events are then paired up with measures which are likely to be taken in this case.
- The events and the expected reactions are planned at the same time.

The following points are subsequently clarified:

- Who would be the most credible person to send a message about the event?
- How would the message be conveyed?
- Who would receive the message? If the recipient is not the decision-maker, how would the message be forwarded?
- Does the message contain all the information required to make a decision?

It is advisable to try out various messages. This will involve speaking to a person who is familiar with the institution concerned and discussing whether the message would result in the expected reaction.

E.1.5 Sample schedule for exercise planning and follow-up

Activity/milestone	Start	Duration	Activity/milestone
M1	dd.mm.yy	–	Submission of general conditions for the exercise/start of work of planning team
A	M1+2W	2W	Prepare rough outline
A	M1+2W	–	Distribute rough outline
A	M1+4W	2W	Review rough outline
A	M1+6W	2W	Incorporate change requests

Activity/milestone	Start	Duration	Activity/milestone
M2	M1 + 8W	–	Approval of rough outline
A	M2 + 1W	1D	Invite participants
A	M2 + 3W	2W	Write exercise script
A	M2 + 3W	2D	Prepare evaluation form
A	M2 + 4W	1D	Send detailed information to participants
A	M2 + 5W	3D	Prepare briefing handouts
M3	M2 + 6W	–	Completion of detailed plan
A	M3 + 1W	1D	Preliminary meeting with exercise leader/observers/facilitators
M4	M3 + 2W	1D	Execution of exercise
A	M4 + 1W	3D	Evaluate questionnaires and exercise logs
A	M4 + 2W	1W	Prepare exercise reports
A	M4 + 4W	2W	Review exercise reports
A	M4 + 6W	2W	Incorporate change requests
M5	M4 + 8W	–	Approval of exercise reports
A	M5 + 1W	1D	Distribute exercise reports
A	M5 + 1W	2D	Prepare concluding presentation
M6	M5 + 2W	1D	Concluding presentation
A	M6 + 1W	1D	Collate and file all exercise documentation
A	M6 + 2W	1D	Follow-up workshop on action taken since the exercise

E.1.6 Sample exercise script

An exercise script can be written in the form of a table, as illustrated in Table 4. The columns listed below are based on the templates used by the BBK with two examples and explanatory notes.

Table 4: Example of an exercise script

Column	Example 1	Example 2
Consecutive number	34	35
Preceding no.	27	34
Subsequent no.	35	65
Date of inserted event	2008.07.17	2008.07.17
Time of inserted event	10:30	10:45
Trigger / inserter	Power station control room	Computer centre control room
In organisation	Utility company	Financial institution
Mode of communication	Telephone call	E-mail
Recipient	Head of crisis squad	Head of computer centre
In organisation	Utility company	Financial institution
Coverage	Town	Company
Event	Disruption of power supply	Activation of emergency power supply
Description	There is a mains fault resulting in a town being cut off from the power supply.	The bank building is experiencing a power outage. The emergency power supply is then switched on in the computer centre.
Expected reaction	Establish alternate connection, notify town council, eliminate the cause of the defect	Contact power supply company
Appendix (Yes/no)	No	No
Author	Lutz Strom	Niklas Bit
Author's e-mail address	lutz.strom@energy.com	niklas.bit@itservice.com

E.2 Exercise implementation

E.2.1 Exercise log template

Basic data

Name of exercise	
Type of exercise	
Start (date, time)	
End (date, time)	
Minute-taker	
Exercise location	
Participants	

Pre-exercise schedule

Action	Start time	End time	Comments (e.g. any problems which have arisen, possible improvements)

Schedule for exercise performance

Action	Start time	End time	Comments (e.g. any problems which have arisen, possible improvements)

Post-exercise schedule

Action	Start time	End time	Comments (e. g. any problems which have arisen, possible improvements)

Reference list of appendices, supporting documents, notes

No.	Brief outline (e. g. system log)

E.3 Exercise follow-up and evaluation

E.3.1 Master evaluation form

Basic data

Name of exercise	
Type of exercise	
Name	
Company/authority/institution	
Organisational unit	
Tel./e-mail	

Questions on the exercise

What was the overall perception of the exercise?	
Were the documents (list of documents) complete and useful?	
Did you learn something that others should know? (Please give details)	
Where is there a need for improvement?	
Any further comments?	

E.3.2 Template for an external exercise report

The items listed below are typically included in an external exercise report (NB: Sample texts are in italics, items in square brackets [] are to be supplied).

UP KRITIS Exercise Report

[Type and name of exercise]

[Date and location of exercise]

Background and basic framework

Type of exercise:

One-day tabletop exercise (similar to a workshop) headed by the head of the BSI IT Emergency and Crisis Response Centre and assisted by a facilitator

Topics covered by exercise:

- *Crisis prevention/contingency planning for operators of critical infrastructures*
- *Measures required to maintain operations in the event of a power failure*
- *Aspects involved in safeguarding IT operations*
- *Telecommunications connections of the BSI IT Situation and Crisis Response Centre and their ability to withstand crises*
- *Alternative site considerations/planning*

Purpose and objectives:

- *To experience the complex interdependency of critical infrastructure operators with a particular focus on ICT*
- *To deduce consequences and crisis response measures in the realm of CIP*

Scenario:

It has been assumed as a starting scenario that ...

Participants:

- Exercise management team:
[Company/authority institution, name (where applicable)]
- Exercise observation:
[Company/authority institution, name (where applicable)]
- Exercise participants:
[Company/authority institution, name (where applicable)]

Exercise input:

Preparation	xx man-days
Implementation	xx man-days
Follow-up	xx man-days

Abridged evaluation of exercise

Implementation:

The atmosphere at the tabletop exercise was “relaxed” and constructive

- 1) *Introduction by leader of crisis management team and facilitator*
- 2) *Identification of interfaces which must be maintained in crises and emergencies*
 - *Business processes which have to be sustained in crises are known*
- 3) *Discussion about handling the threat of power failure*
 - *Generally well-prepared in terms of emergency power supply for 48h in main locations*
 - *Operational capability of central IT is guaranteed*
- 4) *Discussion of managing failure of IT*
 - *Enormous dependency on IT*
- 5) *Discussion about handling failure of communications ...*
 - *...*
- 6) *Summary and concluding session*

Exercise results:

- *The exercise met the objective of increasing awareness among participants*
- *The business processes which must be maintained in crises were discussed*
- *The dependency on internal technology was recognised.*
- *The following measures will help to reduce external dependencies: ...*

Future action:

Check that the agreed measures have been implemented

E.3.3 Items for inclusion in internal exercise reports

The items listed below are typically included in an internal exercise report:

- Management summary (approx. 2 pages)
- Brief description of background, purpose and objectives of the exercise
- Examples illustrating the success of the exercise and the attainment of the purpose and general objectives
- Details of achievement of objectives
- List of participants
- Summary of statistical analyses
- Enumeration of fundamental insights gained during the exercise which are relevant to all participants (e. g. standard times of availability for contact points were not met in many cases, e-mails to generic office mailboxes are answered far more rapidly than e-mails sent to individuals)
- Evaluation from point of view of exercise management team and observers, where applicable
- Recommendations for possible next steps, where applicable, and measures to be implemented to eliminate vulnerabilities “... from the standpoint of the exercise management team and observers”
- Anonymised quotations taken from comments and suggestions (show general trend initially then list all comments as far as possible, especially the negative ones so that everyone can find their own statements, albeit summarised if possible)
- “Lessons learned” for future exercises – what can be improved in the next exercise of the same type, what was missing, what was criticised, where were there unforeseen repercussions?
- Future plans/next steps

Imprint

Published by:

Bundesministerium des Innern
Alt-Moabit 101 D, 10559 Berlin
www.bmi.bund.de

Edited by:

Arbeitsgruppenleitung UP KRITIS, Geschäftsstelle UP KRITIS
(Bundesamt für die Sicherheit in der Informationstechnik)

Design and production:

MEDIA CONSULTA Deutschland GmbH

Status:

December 2008