



Federal Ministry
of the Interior

National Plan

for Information
Infrastructure Protection
CIP Implementation Plan



IT Emergency and Crisis Exercises in Critical Infrastructures

UP KRITIS
Working Group 1
“Emergency and Crisis Exercises”

www.bmi.bund.de

Preface

The vulnerability of modern industrial infrastructures became obvious for the worldwide public no later than with the terrorist attacks in New York, Madrid and London. Of course, there had been attacks on all manner of vital assets in highly developed industrial societies and service economies before 11 September 2001 – we might recall the poison gas attacks in Tokyo in the spring of 1995 – but it was only after New York that non-experts became aware of the importance of functioning transmission links, supply systems, communication channels, etc. – or, more concisely, infrastructure.

In Germany, the course of action taken jointly by government and industry to safeguard infrastructures relevant to the whole of society is one significant effect of this new development. This approach, which is based on the “Public-Private Partnership” model (PPP model), has proven more successful in the long term than separate actions being taken by government and the private sector and is, as a result, a *modus operandi* appreciated both by the public and the private sector and therefore provides resilience in case of crisis situations.

One of the key insights gained by working together has been that the protection of vital infrastructures in our society had been practised in isolation in any given sector. However, it has become apparent that sharing the work involved in critical infrastructure protection (CIP) provides the best chance to serve the society in times of crisis. Needless to say, the PPP approach did not settle overnight like dew on the critical infrastructure field, in contrary a great deal of convincing was required on many fronts before the seed was finally able to bear fruit.

The connecting element in the growing CIP community is the “National Plan for Information Infrastructure Protection (NPSI)” adopted by the Federal Government in June 2005. This Plan acts as a reference framework for information infrastructures, supporting and protecting the various angles in the strategy polygon. As early as August 2005 the Federal Ministry of the Interior (BMI) published as a physical counterpart to the NPSI the Baseline Protection Concept for the “Protection of Critical Infrastructures” as a recommendation for companies, and then started to work at the beginning of 2006 on the CIP Implementation Plan branded as UP KRITIS (this term will be used throughout this document). Following the publication of this plan

in September 2007, work began on fleshing out the theoretical bones of the Implementation Plan. The results of these efforts concerning the IT emergency and crisis exercises are presented in this document.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction and motivation | 5 |
| 2 | Target groups | 9 |
| 3 | Limitations | 10 |
| 4 | Types of exercises | 11 |
| 5 | Exercise scenarios | 15 |
| 6 | Exercise plan | 18 |
| | 6.1 Development and sustainment phase | 18 |
| | 6.2 Strategic CI exercise plan | 18 |
| 7 | Perspective and next steps | 23 |
| | Annex | 24 |
| | Abbreviations | 25 |
| | Glossary | 26 |
| | References | 33 |
| | Participating UP KRITIS partners | 34 |

Figures

| | |
|--|----|
| Figure 1: Development phase exercise plan | 19 |
| Figure 2: Sustainment phase exercise plan | 20 |

Tables

| | |
|--|----|
| Table 1: Exercise and planning input for the different types of exercise | 13 |
| Table 2: Exercise and planning duration for the different types of exercise | 14 |
| Table 3: Frequency of exercise types in development phase | 19 |
| Table 4: Frequency of exercise types in sustainment phase | 20 |

1 Introduction and motivation

Critical infrastructures (CI) are organisations and facilities of major importance for German public life, as defined in the National Plan for Information Infrastructure Protection (NPSI). Even partial failures of or serious problems with these structures in Germany can entail long-term supply shortages, major disturbances in public security or other far-reaching consequences. Another factor to take into consideration is that some sectors classified as critical infrastructures are heavily dependent on each other. Operators of critical infrastructures include government bodies, commercial enterprises and other institutions. They all agree that the protection of critical infrastructures is an important national mission which must be addressed jointly. One particular focus in this context involves safeguarding information infrastructures that are essential for their operation.

In this context and under the aegis of the Federal Ministry of the Interior, the Implementation Plan for Critical Infrastructures, furtheron referred to as UP KRITIS¹, was drawn up as a part of the National Plan for Information Infrastructure Protection. UP KRITIS includes a mission statement. In this statement the parties involved in developing the plan underline the necessity of long-term collaboration and ascertain that concrete measures should be implemented to guarantee an adequate level of protection for critical infrastructures.

One essential measure is the organisation of IT emergency and crisis exercises designed to rehearse the handling of acute threats and critical damage to information infrastructures. These exercises enable the UP KRITIS partners to gain awareness of mutual dependencies, to develop adequate joint policies and action plans for IT emergency and crisis response, and to check and review these regularly. Naturally, the focus of the exercises is not on handling IT emergencies and crises in isolation but on working together across sectors and liaising with public agencies. Taking due account of the responsibilities of the German federal and states administrations, there is a perceived requirement for collaboration with all parties potentially involved right down to local authority level. The structures and processes required to meet this requirement are described in the concept for the “Early Detection and Mitigation of IT Crises”, which was also developed in the context of UP KRITIS.

¹ German title for “Implementation Plan for Critical Infrastructures”, also referred to as “CIP Implementation Plan”: “Umsetzungsplan für Kritische Infrastrukturen”, also referred to as “Umsetzungsplan KRITIS” or “UP KRITIS”.

This concept contains the following sections:

- Descriptions of possible types of exercises
- Recommendations on the regular conduct of exercises.

Participation in CI exercises is voluntary. The UP KRITIS partners decide whether to take part in each scheduled exercise and, if so, to what extent. The objective is to achieve maximum benefit for the participants with minimum input.

Further information on the concept offering specific help with planning and running CI exercises and giving detailed explanations of the types of exercises is available as a separate document entitled “Appendices to the Concept for IT Emergency and Crisis Exercises in Critical Infrastructures”.

This document outlines IT emergency and crisis exercises designed to test collaborative practices as well as mechanisms for dealing with acute threats and critical damage which may affect the information infrastructures. It serves the following purposes:

- Specification and description of possible types of exercise
- Recommendation of regularity with which the exercises should be conducted
- Specification of planning, preparation, implementation, evaluation and follow-up of exercises including specific resources
- Optimisation of input and investment in exercise procedures through consideration of potential integration in other overlapping and complementary crisis exercises, e. g. LÜKEX
- Promotion of collaboration among working group parties in planning the specifics of the exercises
- Recruitment of further CI companies², public authorities and institutions to join the work on UP KRITIS.

Exercise objectives

By simulating IT emergencies and crises when there is no real emergency, it is possible to practice management and response to IT incidents and cri-

² The involvement and assistance of private enterprises which are not classified as belonging to CI sectors is not ruled out.

ses as well as to test the functionality of the relevant facilities and to make improvements on the basis of the insights gained in the exercise.

The UP KRITIS partners already have extensive concepts and measures for individual IT crisis and emergency management, which are trained on a regular basis. However, this is not true to the same extent for cross-sector and interdisciplinary collaboration in the event of IT-relevant emergencies and crises which jeopardise critical infrastructures, nor is it true concerning collaboration with the relevant government bodies. The work done thus far in the context of UP KRITIS does, however, clearly show that such collaboration is appropriate due to the many interfaces and dependencies between the UP KRITIS partners, and provides significant additional benefits for all involved. Exercises provide the opportunity to reveal areas with a need for action and to make and maintain improvements to the IT emergency and crisis response within a secure environment and unaffected by the consequences of a real emergency. Mistakes can be tolerated in exercises. Appraising and learning from these mistakes can help to optimise the response processes.

The following specific objectives can be achieved through exercises:

- The efficiency and operability of existing concepts, structures, measures and means of communication are reviewed on a regular basis. Even if they are painstakingly elaborated, it is highly probable that they will not function as intended in an emergency if they have not been practised beforehand. One reason for this is that they are never or virtually never used outside of IT crises and emergencies.
- The capabilities of all those involved are developed and their confidence to act adequately in emergencies improved. Well-trained personnel also react more appropriately to situations which have not been rehearsed.
- The process also allows the UP KRITIS partners to trust one another in terms of their communications, and valuable contacts are facilitated and consolidated.
- The UP KRITIS partners also gain additional awareness of the necessity for cross-sector collaboration, the mutual dependencies and the necessity for exercises.

- The mutual expectations of the UP KRITIS partners in managing IT emergencies and crises are revealed. If it becomes apparent in exercises that expectations are not being met, resulting vulnerabilities in IT emergency and crisis management strategies can be identified.
- The exercises reveal where and when it might be expedient and necessary to work together in IT emergencies and crises.
- Interdependencies of critical infrastructures across sectors and sub-sectors are identified. Dependencies which have not been previously found can also indicate existing vulnerabilities in the IT emergency and crisis management.
- Experience is gained in liaising with the BSI Situation and Crisis Response Centre.
- The UP KRITIS working group on “Crisis Response and Mitigation” is provided with suggestions on how to develop appropriate structures, concepts and measures for joint IT emergency and crisis mitigation efforts.

In summary, it has to be stated that IT emergency and crisis exercises are a fundamental prerequisite for achieving adequate and optimum response processes. However, it should be emphasised that participation in exercises is voluntary. Each UP KRITIS partner decides whether to take part in any scheduled exercise and, if so, to what extent. Even after a given party has declared its intent to take part in a specific exercise, it can still pull out at any stage of the exercise preparation and implementation, without stating why if the circumstances so dictate.

2 Target groups

This document is primarily intended for the following parties:

- Members of the UP KRITIS working groups: Their task is to raise awareness of the exercise concept in the institutions and companies to which they belong, to adopt a basic administrative framework for exercises, to assist with the planning of exercises, and to act as facilitators with regard to the provision of the resources required for the exercises in their institutions and companies.
- Private sector contacts for critical infrastructures (SPOCs): These are involved in many exercises because of their role (e. g. alert exercises) and therefore have to have an awareness and understanding of the exercises.
- Staff working at the managerial level in public authorities and companies which operate critical infrastructures, work with them, or are involved in their protection: This target group should have a basic knowledge of the reasons for and the objectives of IT emergency and crisis exercises as set out in UP KRITIS. This knowledge is required as the exercises cost time and money and, as such, they have to be agreed with the management.
- All emergency staff leaders, emergency staff members and other potential managers, who might conceivably be implicated, should have advance knowledge of this concept. This also serves to identify potential areas where CI and internal company exercises might be dovetailed and linked up with existing series of exercises, such as LÜKEX.
- Staff who work in the Federal Ministry of the Interior and associated authorities (especially the BSI and BBK) who are au fait with critical infrastructure protection tasks.
- Staff who work for supervisory and regulatory authorities for operators of critical infrastructures (e. g. BaFin and Federal Network Agency): The exercises are a contribution to risk management which is often a legal requirement for companies.
- Representatives of stakeholder groups / business associations of branches of industry which are classed as critical infrastructures.

3 Limitations

The exercises set out in this concept document supplement the disaster control measures and emergency exercises already implemented in Germany. While disaster control measures and emergency exercises place the emphasis on restoring physical infrastructures and coping with physical injuries, the exercise scenarios outlined in this document focus on the information infrastructures which are necessary for the operation of critical infrastructures. One measure which is regarded as necessary is to integrate CI exercises in disaster control and emergency exercises under the aegis of national / public authorities, such as LÜKEX. This integration target is backed up by present concept document.

There is also a separate series of individual exercises run by operators of critical infrastructures. The individual exercises generally focus on internal mechanisms for coping with IT crises and emergencies. The exercises outlined in this document therefore emphasize the overarching cooperation of CI companies and relevant government bodies. Linking CI exercises with internal exercises can be a worthwhile exercise for UP KRITIS partners but is not an essential requirement to the conduct of CI exercises. The decision about a possible link is therefore made on a case-by-case basis by each UP KRITIS partner.

4 Types of exercises

The content and form of exercises can vary greatly depending on their purpose. The first point of differentiation is what occurs in the exercise:

- Discussion-based exercises address possible processes, plans and policies for any given IT crisis on a theoretical level. In the process procedures and possible solutions are presented and discussed. Consequently, these exercises are less about testing existing measures than developing new responses to IT emergencies which are appropriate for managing crisis situations. They lend themselves to introducing new topics,
- Action-oriented exercises (drills) serve to “act out” and rehearse realistic scenarios and to assess processes, plans, concepts, arrangements, etc. They can be a valuable experience for those involved and can also expose deficiencies in planning, loopholes, shortfalls in resources, unassigned responsibilities, etc. As such, they provide a way of increasing the efficiency of those involved in the exercises and ensuring that which has been practised is up to date.

A further reasonable point of differentiation is with respect to the target groups for the exercises. Three levels can be identified in this regard:

- The specific actions and procedures at the implementation level are practised in operational drills. Processes which are clearly organised and, where necessary, supported by technical measures are appropriate for such drills. The participants are employees on the operations side or from emergency teams in the organisations conducting the drills.
- In tactical exercises the main priorities are coordination, collaboration and decision-making, including and especially among different organisations. This is the main focus of this concept. The target group includes the coordination structures provided for the IT crisis.
- The strategic exercises address the management level. The important issue in this case is the general mode of interaction between the organisations involved and the complex decisions associated therewith.

UP KRITIS exercise types

It is also appropriate for the purposes of this concept to mix different approaches with regard to the exercise objectives, exercise input and exercise participants. The following types of exercise ought to be used in the context of UP KRITIS:

- Tabletop exercises are the only discussion-based exercises. They are appropriate for the purpose at both the tactical and the strategic level and can be used as an all-purpose tool to run through any scenario. They are essentially theoretical discussions of sequences of events in an IT emergency / crisis with reference to specific scenarios, where experts and senior staff engage in a joint constructive discussion with a facilitator and a main theme and, where applicable, with a presentation by a specialist on the topic in question.
- Communication exercises are held at all levels. They are used to check whether the relevant people will be available and the relevant procedures will be in place in the event of an alert. They are also used to test the efficiency of the means and methods of communication which are to be used in IT emergencies or crises (or they are used to discuss complex situations with the potential to develop into crises).
- Coordination exercises take place at the operational and tactical level. The senior and staffing structures and the emergency and crisis response units of the organisations involved rehearse their response to a specific scenario without the events actually happening and the measures actually being put in place. The requirements of the central crisis response organisation in terms of infrastructure and technical systems are reviewed at the same time.
- Extended coordination exercises involve additional levels. They simulate conditions which are as realistic as possible, providing scenarios in which all the parties involved can run through their response to a specific IT crisis. Events are enacted as they might actually occur to the greatest possible extent, and adopted measures are actually put into action.

The availability of adequate organisational and technical structures is essential for communicating in crises and managing crises³ for all of the above exercise types with the exception of tabletop exercises. These requirements do not apply to tabletop exercises. Exhaustive descriptions of the individual types of exercise can be found in the separate appendix to this concept document.

Input and duration

The following overview tables Table 1 and Table 2 summarise and contrast the individual types of exercise in terms of their input and duration. The majority of the planning input typically comes from a small team of people. However, the effort and time required for the exercise itself is normally due to the large number of people who are involved in the exercise. The planning input for an individual exercise can be reduced if series of exercises are always performed in the same manner (e. g. raising the alarm).

Table 1: Exercise and planning input for the different types of exercise

| Exercise type | Planning input | Exercise input |
|--------------------------------|-------------------|-----------------------|
| Tabletop exercise | Low | Low |
| Communication exercise | Moderate | Low to moderate |
| Coordination exercise | High to very high | Moderate to very high |
| Extended coordination exercise | High to very high | Very high |

Explanation of input categories:

Low: one week's work for one person

Moderate: several weeks' work for one person

High: several months' work for one person

Very high: years of work for one person

³ The UPKRITIS concept for the "Early Warning and Mitigation of IT crises" contains the outline of the basic structures.

The planning duration for complex exercises with a large number of participants can be more than one year. The work must therefore be started in due time with a view to achieving target deadlines for such exercises. However, the duration of the actual exercise is short to avoid any adverse effects on the UP KRITIS partners as a result of taking staff away from production and administration processes for the exercise. The maximum conceivable duration of a CI exercise would be several days if the situation at issue is a complex IT crisis also possibly involving rehearsals across international networks.

Table 2: Exercise and planning duration for the different types of exercise

| Exercise type | Planning duration | Maximum exercise duration |
|--------------------------------|-------------------|---------------------------|
| Tabletop exercise | Moderate | Very short |
| Communication exercise | Moderate | Short |
| Coordination exercise | Long | Short |
| Extended coordination exercise | Long | Short |

Explanation of duration categories:

Very short: up to one day

Short: between one day and one week

Moderate: several weeks

Long: several months or longer

5 Exercise scenarios

A scenario generally starts with an initial situation leading to a sequence of events to which a response is required by those taking part in the exercise (What if...?). The scenario can include realistic fictitious incidents or real events and provides basic information or suppositions relevant to the exercise. There is a detailed description of the state of affairs which creates the environment leading up to the initial situation for the scenario.

Inserts of smaller details (e. g. a notice, an incoming message, a press release) subsequently add to, expand or alter the scenario, thereby necessitating response and action from those taking part, providing additional information, and test the adaptability and capacity to manage IT emergencies and crises.

Additional assumptions and so-called artificial situations in some cases need to be brought into the scenarios as it is not possible or feasible to simulate all the real events which can occur in IT crises and emergencies (e. g. assuming that the telephone system breaks down although all the telephone sets are working, or all the external contacts are displayed by the exercise leaders).

A general distinction is also drawn between cause and effect scenarios:

- A root cause scenario includes the underlying causes (power failure, virus attack, unauthorised access by hacker, etc.).
- An effect scenario assumes specific failures / damage (e. g. failure of a computer centre) without consideration of the causes.

The type and objective of the exercise will determine which of the two types of scenario would be more appropriate. Causal scenarios are expedient when the objectives of the exercise are to explore root causes, to practise problem-solving or to engage in damage limitation processes with reference to specific causes. Effect scenarios are used when the emphasis is on response processes irrespective of the root cause or when the aim is to explore interdependencies of critical infrastructures.

Seen in the context of this concept, the scenarios must also be designed such that they:

- both seriously affect IT availability which is essential to the operation of the critical infrastructures
- and have the potential to cause serious and, as far as possible, cross-sector impact to critical infrastructures.

In many cases a single event is not sufficient to fulfil the above conditions. As a consequence, it is also advisable to consider scenarios which comprise several (possibly also independent) events which occur at the same time or in close succession in several places (distributed events).

It is helpful to address the communication channels and interfaces first and then to rehearse the scenarios which are deemed to have the highest likelihood of occurrence. However, it should be considered that it is often very difficult to determine the exact degree of probability.

Other factors to be taken into consideration when mapping out scenarios are as follows:

- the exact specification of the resources affected as well as the type and scope of the impact
- the background contexts and objectives of root cause scenarios deliberately caused by persons
- the chronological sequence and geographical spread (in the case of distributed events)

Basic exercise scenarios

Those working on UP KRITIS have agreed on several basic scenarios which appear to be particularly appropriate in the CI environment and which therefore should form the primary focus:

- The loss of supply services which are fundamental to the operation of IT systems, e. g.:
 - a widespread power failure
 - the breakdown of air-conditioning systems in computer centres due to extreme climatic conditions
 - the failure of central control rooms
 - the loss of central communication systems, e. g. core networks, which act as a channel for various services (Internet, telephony, data transfer, ...)
 - extensive loss of operational staff

- Physical attacks intended to take over the IT infrastructure or render it inoperative, e. g.:
 - on computer centres
 - on central hubs
 - on central network connections

- Logical attacks evidently backed up by extensive funds and technical know-how, e. g.:
 - on central hubs
 - large-scale malware attack
 - denial-of-service attacks on critical IT systems
 - targeted, unauthorised access to critical IT systems and misuse of the systems

6 Exercise plan

The UP KRITIS partners agree that the arrangements designed to optimise the response to IT emergencies and crises have to be sustained and continually updated. An appropriate exercise plan contributes greatly to meeting this requirement.

6.1 Development and sustainment phase

The exercise plan is subdivided into a development phase and a sustainment phase. The development phase is concerned with devising exercises with ascending degrees of complexity in order to:

- highlight areas where there is a need for action
- provide a basis for the crisis response and crisis management work in UP KRITIS
- try out new procedures and techniques proposed by the aforementioned working group
- have demonstrated the required ability to respond to the given scenarios for the first time

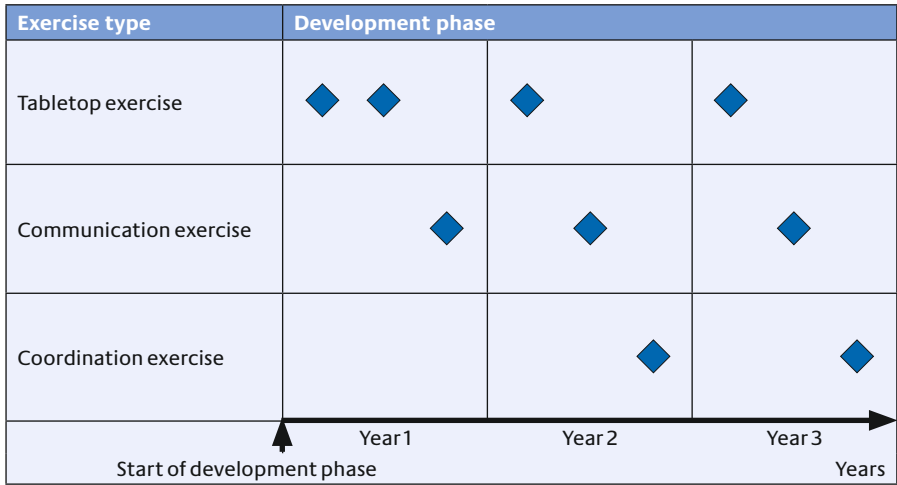
The development phase should be completed within three years.

This is followed by the sustainment phase in which the aim is to guarantee and consolidate the future sustainability of the required response capability. The duration of the sustainment phase is indefinite. However, major changes to the communication structure, exercise participants or other resources may make it necessary to initiate a new development phase.

6.2 Strategic CI exercise plan

The UP KRITIS partners have agreed on an exercise plan for the development and sustainment phase to achieve the objectives set out in the previous sections.

The exercise plan for the development phase is outlined in Figure 1 and described in more detail in Table 3:

Figure 1: Development phase exercise plan**Table 3: Frequency of exercise types in development phase**

| Exercise type | Frequency in development phase | Comments |
|------------------------|--------------------------------|---|
| Tabletop exercise | 4 x | Main focus is working out requirements for the “Crisis Response and Mitigation” working group. Recommended scenarios include e.g. power failure and logic attacks on IT. |
| Communication exercise | 3 x | Requires definition and implementation of the necessary communication structure recommended by the “Crisis Response and Mitigation” working group first. |
| Coordination exercise | 2 x | Requires definition and implementation of the necessary communication structure recommended by the “Crisis Response and Management” working group; if possible, linking up with LÜKEX 2009 and potentially with Cyber Storm 2010. |

The exercise plan for the sustainment phase is set out in a similar form in Figure 2 and in Table 4:

Figure 2: Sustainment phase exercise plan

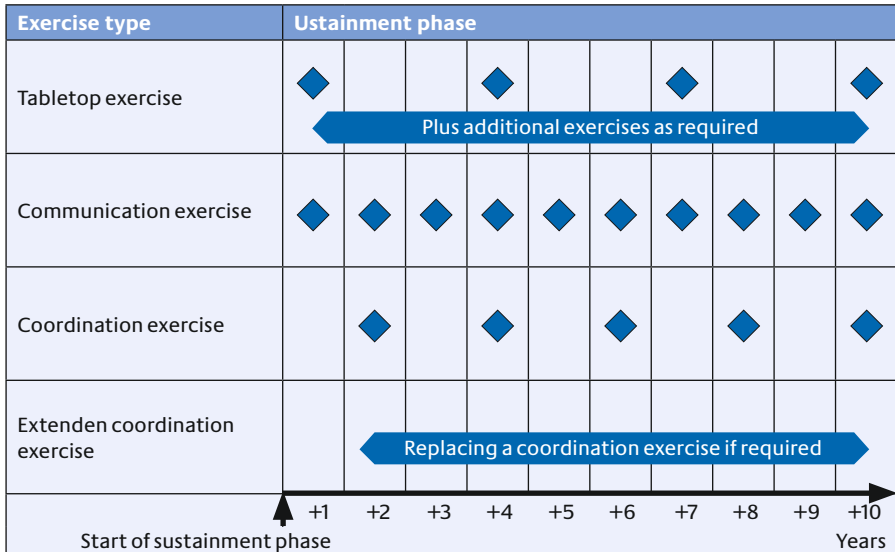


Table 4: Frequency of exercise types in sustainment phase

| Exercise type | Frequency in sustainment phase | Comments |
|--------------------------------|--|---|
| Tabletop exercise | Every three years and additional exercises if required | As and when required, e.g. if new, relevant IT crisis scenarios crop up which would be inadequately served by the existing response mechanisms. |
| Communication exercise | Annually | A fully functional alert system and adequate means of communication are fundamental requirements for every IT emergency and crisis response. |
| Coordination exercise | Every two years | Preferably combined with other national or international exercises, e.g. LÜKEX or Cyber Storm. |
| Extended coordination exercise | As required instead of a coordination exercise | Preferably combined with other national or international exercises, e.g. LÜKEX or Cyber Storm. |

Detailed planning

The strategic exercise plan has to be fleshed out in more detail in the form of an exercise schedule (see separate appendix to this concept document) for each of the exercises listed. It is also envisaged that the UP KRITIS partners will meet regularly in the future to adopt an administrative framework for imminent exercises, to declare their fundamental willingness to participate, and to charge members of the working group and / or external bodies with the performance of further detailed planning. It is essential to ensure that sufficient time is allowed to enable thorough planning of the exercise schedule (see Table 1 in section 4). The planning team tasked and adequately resourced to run the exercise reports to the UP KRITIS partners on its progress and seeks approval at various stages of the work.

The framework conditions which have to be decided on for each scheduled exercise and which form the basis for the initial decision to participate are as follows:

- The objectives and benefits of the exercise (WHAT is to be achieved?)
- The scenario (WHICH situation is chosen?)
- The group of participants (WHO?)
- The time of its performance and the anticipated duration (WHEN?, HOW LONG?),
- Whether it will be announced or unannounced (WHICH ELEMENT OF SURPRISE?)
- The risk involved (WHICH SCALE OF RISK?)
- The confidentiality requirements (HOW SENSITIVE?)

In order to enable planning to proceed, the following parameters also need to be fixed and then fleshed out in more detail:

- The members of the exercise planning team, the exercise leadership and the evaluation team, including external support where applicable (WITH WHOM?)
- The required approvals of interim and final results, such as the exercise schedule, by the UP KRITIS Partners (WHAT FORM OF MONITORING?)
- A rough estimate of the budget and human resources required for the preparation, execution and follow-up of the exercise, as well as the assumption of costs and division of labour (WHO and HOW MUCH?)

Regarding the assumption of costs and division of labour the following principle applies as a general rule:

- BMI and BSI provide support the exercise preparation and follow-up work to a large extent. However, the individual UP KRITIS partners still need to bear the cost of any items or personnel which they require for the preparation and follow-up of the exercises and for internal preparations.
- Each of the UP KRITIS partners is responsible for the expenses incurred to him / his organisation in respect of the execution of the exercise and the costs.

Further explanations on the basic parameters are given in the separate appendix to this concept document.

Integration of new partners

Potential new UP KRITIS partners have the option to join the exercise schedule at a later date. Assistance is offered as required. Participation in tabletop exercises is possible at any time without any further qualifications. The minimum requirements for participation in other types of exercises are integration in the concept for early detection and mitigation of IT crises, and a timely decision to participate in the planning process. New UP KRITIS partners who are participating for the first time in a complex coordination exercise might also have to be given the option of taking part in selected sections of the exercise (e. g. the alert) which are appropriate to their level of integration in UP KRITIS.

7 Perspectives and next steps

The exercises are intended to facilitate, as soon as possible, resilient, cross-sector responses to IT crises in the critical infrastructures. The approach is to begin with simple basic exercises, with the level of complexity and degree of reality being increased gradually. One of the first exercises should serve to verify the efficiency of communication channels and points of contact. This is intended to add much value in the management of critical events through the networking of relevant areas of industry and the administrations of the German Federal Government and the German states. This document serves as a common basis for the drawing up of future exercise schedules and the ensuing activities.

Annex

Abbreviations

| | |
|------------------|---|
| BaFin | Bundesanstalt für Finanzdienstleistungsaufsicht [Federal Financial Supervisory Authority] |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [Federal Office of Civil Protection and Disaster Assistance] |
| BAK | Bundeskriminalamt [Federal Criminal Police Office] |
| BMI | Bundesministerium des Innern [Federal Ministry of the Interior] |
| BSI | Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] |
| CI | Critical Infrastructure |
| CIP | Critical Infrastructure Protection |
| ICT | Information and communication technology |
| IT | Information technology |
| KRITIS | Critical Infrastructures |
| LÜKEX | Länderübergreifende Krisenmanagement Exercise [Interstate crisis management exercise] |
| NPSI | Nationaler Plan zum Schutz der Informationsinfrastrukturen [National Plan for Information Infrastructure Protection] |
| SPOC | Single Point of Contact |
| UP | Umsetzungsplan [Implementation Plan] |
| UP KRITIS | Umsetzungsplan KRITIS [CIP Implementation Plan] |

Glossary

Artificial situations

It is not possible or feasible for an exercise to reconstruct everything which actually happens in crises and emergencies (e. g. fire, loss of ICT systems, data loss, and contact with media representatives). Indeed, there will be some degree of hypothesis and simulation. This is embraced in the notion of artificial situations.

Catastrophe

(Large-scale) events of natural origin which cause damage (earthquakes, storm tides, volcanic eruptions, etc.) or man-made disasters (chemical spillages, plane crashes, attacks, etc.) which put a large number of people in mortal danger or constitute a health hazard for a large number of people, or which threaten to harm the environment or other important interests protected by law, and which cannot be adequately controlled by the means and resources at the disposal of the authorities responsible for averting the danger.

Crisis

A situation which deviates from normal conditions, which develops suddenly or gradually, which carries the inherent threat of injury to life and limb and has the potential to cause damage to major material assets and to seriously threaten the political, social or economic system, and one which necessitates a decision – often from a position of uncertainty without being in possession of the full facts.

Crisis management

Creation of the conceptional, organisational and procedural prerequisites required to manage the abnormal situation which has arisen and restore things to normality as quickly as possible.

Crisis mitigation

The taking of measures aimed at resolving an acute crisis, minimising its repercussions, and restoring things to normality as quickly as possible.

Critical infrastructure

Critical infrastructures are organisations and facilities of strategic importance for the community, the failure or disruption of which would result in long-term supply shortages, major disturbances in public security or other dramatic consequences

In Germany the following areas are classed as critical infrastructures:

- Transport and traffic (aviation, maritime shipping, railways, local transport, inland waterway transport, roads, postal service)
- Energy (electricity, nuclear power plants, mineral oil, gas)
- Hazardous substances (chemicals and biological substances, hazardous materials transportation, armaments industry)
- Information technology and telecommunications
- Finance, banking and insurance (banks, insurance companies, financial service providers, stock exchanges)
- Supply systems (health service, emergency and rescue services, disaster control, food and water supply, disposal)
- Public authorities, government and the judiciary (government institutions)
- Other (media, major research institutions, prominent or highly symbolic buildings, cultural assets)

Drill

A special type of exercise which is action-oriented with the aim to eradicate mistakes and increase efficiency.

Exercise

The term exercise encompasses the simulation of responses to emergencies and crises and the process of checking that emergency and crisis response processes are working when there is no real emergency.

Exercise instructions

Rules and procedures determined prior to the exercise which the participants are required to follow during the exercise.

Exercise leader

An exercise leader is required for the conduct of each exercise. The leader assumes the role of a coordinator throughout the exercise, including the set-up and dismantling of the exercise environment. This typically includes the following tasks:

- 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 course of the exercise or calling a premature halt to the exercise in the event of serious complications which cannot be resolved
- Facilitating tabletop exercises
- Coordinating supplies for the exercise participants (e. g. catering)

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.

Exercise observer

Exercise observers log the activities performed by the exercise participants during the exercise. Their records include the times achieved, for example, and any notable insights, such as unexpected difficulties or room for improvement.

Exercise participants

Exercise participants enact tasks in which they would be implicated in a real emergency as part of their response to an emergency or crisis. Additional activities include:

- Attending the exercise briefing session before the actual emergency and crisis simulation begins
- If applicable, attending expert presentations which are incorporated into the exercise in order to give the exercise participants the necessary background knowledge
- Issuing status reports to the exercise leaders as required, either at regular intervals or on request
- Completing evaluation forms after the exercise and submitting them to the exercise leadership

Exercise script

In complex exercises it is advisable to write down the course of action in a detailed format similar to a film script. The script contains all the events pertaining to the overall exercise scenario and other relevant information, such as the manner of notification and anticipated responses.

Facilitators

The main task of the facilitators is to brief the participants on the initial situation at the beginning of the exercise and to insert in further events in the course of the exercise. They also have the following assignments:

- Record immediate responses of those taking part in the exercise, e. g. on the telephone
- Give expert presentations at relevant points during the exercise if applicable

Follow-up team

The follow-up team is responsible for evaluating the exercises and issuing reports on them. It bases its findings on evaluation forms and on the reports written on the exercises.

| | |
|--|--|
| Information infrastructure | The entirety of IT elements that are part of a given infrastructure. |
| Information technology | Information technology (IT) encompasses all the technical resources used to process or communicate information. Information processing includes acquisition, recording, use, storage, communication, software-controlled processing, internal display and output of data. |
| Insert | Inserts are events (e. g. a notice, an incoming message, a press release) which add to, expand or alter the progression of initial scenarios in exercises, thereby necessitating a response from those taking part — e. g. taking action or obtaining more information — and all designed to assess their adaptability and capacity to cope with emergencies and crises. |
| IT crisis | An IT crisis is said to exist in the context of UP KRITIS if organisations and facilities of importance for the general public experience or might experience failure or disruption directly or indirectly related to IT, which results in long-lasting supply shortages, major disruptions to public security or other dramatic consequences. |
| IT security | IT security denotes a status in which the availability, integrity and confidentiality of information and information technology are protected by appropriate safeguards. |
| Operators of critical infrastructures | Operators of critical infrastructures are private enterprises or public authorities which provide services in the critical infrastructures. |

Planning team The planning team is responsible for the detailed advance planning of exercises. It issues the rough outlines and the detailed plans for the exercises.

Scenario A scenario is a situation or a sequence of events requiring a response from those participating in the exercise (what if...?).

A distinction is drawn between cause and effect scenarios:

- An effect scenario assumes specific failures / damage (e. g. failure of a computer centre) without considering the causes.
- A root cause scenario also includes the underlying causes (power failure, virus attack, unauthorised access by hacker, etc.).

The type and objective of the exercise will determine which of the two types of scenario would be more appropriate. Causal scenarios are expedient when the objectives of the exercise are to explore root causes, to practise problem-solving or to engage in damage limitation processes with reference to specific causes. Effect scenarios are used when the emphasis is on response processes irrespective of the root cause or when the objective is to explore interdependencies of critical infrastructures.

SPOC Single Point of Contact. Firmly established function in a subsector acting as a central communications platform and reporting point (outgoing and incoming) for the companies in the subsector.

**UP KRITIS
partners**

All the public authorities, stakeholder groups/
business associations, companies, etc. which
work together (e. g. in working groups) and
participate in exercises in the context of the UP
KRITIS

References

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Nationaler Plan zum Schutz der Informationsinfrastrukturen [National Plan for Information Infrastructure Protection]. Berlin, 2005

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen [CIP Implementation Plan of the National Plan for Information Infrastructure Protection]. Berlin, 2007

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Konzept zur Früherkennung und Bewältigung von IT-Krisen [Policy Governing the Early Detection and Handling of IT Crises]. Berlin, 2008

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept [Protection of Critical Infrastructures – Baseline Protection Concept]. Berlin, 2005

Bundesministerium des Innern [Federal Ministry of the Interior] (Eds.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement [Protecting Critical Infrastructures – Risk and Crisis Management]. Berlin, 2008

Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] (Eds.): COMCHECK und ALEX – Beschreibungen, Checkliste und Hilfen für Kommunikationsüberprüfungen und Übungen [COMCHECK and ALEX – Descriptions, Checklists and Aids for Communication Checks and Alarm Exercises]. Bonn 2006

Participating UP KRITIS partners

Allianz Deutschland AG
Arcor AG & Co. KG
Bundesamt für Sicherheit in der Informationstechnik
[Federal Office for Information Security] (BSI)
Bundesanstalt für Finanzdienstleistungsaufsicht
[Federal Financial Supervisory Authority] (BaFin)
Bundesverband deutscher Banken
[Association of German Banks]
Commerzbank AG
Deutsche Bank AG
Deutsche Börse Group
Deutsche Bundesbank
Deutsche Postbank AG
Deutsche Telekom AG
DFS Deutsche Flugsicherung GmbH
Dresdner Bank AG
eco e. V. – Verband der Deutschen Internetwirtschaft
[eco – Association of the German Internet Industry]
(E-Plus Group) E-Plus Mobilfunk GmbH & Co KG
European Central Bank
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
[German Insurance Association]
HUK-COBURG
Mineralölwirtschaftsverband
[Association of the German Petroleum Industry]
RWE Aktiengesellschaft
RWE Energy Aktiengesellschaft
SIZ Informatikzentrum der Sparkassenorganisation GmbH
Telefónica O2 Germany GmbH & Co. OHG
Vodafone D2 GmbH

Notes

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 Sicherheit in der Informationstechnik)

Design:

MEDIA CONSULTA Deutschland GmbH

Status:

December 2008