Federal Ministry
of the Interior

National Plan
for Information
Infrastructure Protection
CIP Implementation Plan

CIP Implementation Plan
of the National Plan for Information Infrastructure Protection

www.bmi.bund.de

This page was intentionally left blank.

CIP Implementation Plan
of the National Plan for Information Infrastructure Protection

Contents

1. Introduction and Aims

Critical infrastructures are vital for our society. The dependable provision of the services which these infrastructures convey is a fundamental precondition for our country's economic development, our society's well-being and political stability.

>> Critical infrastructures are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences.[1]

Both the Federal Government and the business community consider the protection of critical infrastructures to be an important national task because national security is increasingly affected by IT security. Germany is taking the required actions to ensure the adequate protection of IT infrastructures. The CIP Implementation Plan [Umsetzungsplan KRITIS] is making an important contribution towards the dependable provision of vital services through appropriate IT protection. The parties involved in its implementation have set themselves the following goal:

>> We are working together in order to describe the competence and know-how of the German business community and the Federal Government in their joint responsibility for IT security within the processes of critical infrastructures. Recommendations and measures are to be put in place in order to enable all operators of critical infrastructures to maintain and further develop a reasonable security level of information infrastructures in general and of IT systems used by business and industry. Long-term cooperation in order to identify and handle IT crises is to be promoted across all sectors and sub-sectors together with the Federal Government.

>> Our goal is to ensure that operators of critical infrastructures actively endorse the common principles and continue to increase the IT security level of critical infrastructures on the basis of the following recommendations.

[1] Definition of critical infrastructures in Germany, see glossary.

1.1 Motivation of the CIP Implementation Plan

Modern information technology is increasingly conquering all aspects of life. Critical infrastructures are also increasingly relying on IT in order to be able to operate, control and monitor processes more effectively and efficiently. This sometimes leads to highly complex IT-based networks and dependencies within and between CIP sectors.

The protection of critical infrastructures hence also calls for adequate protection of information infrastructures. Therefore, the Federal Government has adopted the "National Plan for Information Infrastructure Protection"[2] (NPSI) as its cross-sectoral IT security strategy. The implementation of the NPSI is undertaken in a consensus to integrate the operators' goals as private industry players and the higher-level (safeguarding) interest of the community.

[2] Federal Ministry of the Interior, National Plan for Information Infrastructure Protection, dated June 2005.

The National Plan for Information Infrastructure Protection focuses on protecting information infrastructures as a task of society as a whole which calls for coordinated action supported by all players. The plan sets forth three strategic objectives as follows:

- Prevention: Protecting information infrastructures adequately
- Preparedness: Responding effectively to IT security incidents
- Sustainability: Enhancing German competence in IT security – setting international standards

This concerns, in particular, the federal administration and operators of critical infrastructures. Most critical infrastructures in Germany are operated under private responsibility, i.e. by individual enterprises. IT security has so far been a task that has been largely performed within individual companies and organisations. Although these responsibilities remain unaffected, they need to be supplemented.

The requirements for IT management and IT security management rise with increasing dependencies and a growing cross-enterprise interconnection of IT landscapes and information technologies. For that reason, IT security measures at the companies' and organisations' level are no longer sufficient when it comes to ensuring adequate protection of the information infrastructures in Germany and world-wide. Instead, action is necessary on several levels:

- within companies and organisations in order to take all necessary steps that can be taken in their own responsibility,
- in the sub-sectors whenever the components of critical infrastructures of different companies are closely interlinked and/or interdependent in order to increase reliability through coordinated action,
- across sectors at national level:
  - in order to correctly assess incidents (such as accidents or targeted attacks) in the larger framework,
  - in order to enable a joint and coordinated response to incidents which may occur despite preventive measures,

- in order to jointly adapt measures in response to the latest developments, that will be taken into consideration in future updates of the CIP Implementation Plan,

- at international level in order to ensure the correct evaluation of and adequate response to incidents with consequences that are not limited to national level:
  - within (sub-)sectors together with other businesses,
  - at national level in agreement with those responsible in other countries.

The Federal Ministry of the Interior hence invited representatives of operators of critical infrastructures to take part in the development of the CIP Implementation Plan and to contribute their expertise and experience as well as their knowledge of the specific requirements of the different sectors of critical infrastructures.

This jointly developed Implementation Plan is the basis for the further enhancement of the protection of information infrastructures in the CIP sectors and for achieving a high basic level of IT security.

All the parties involved are aware of their responsibility towards society as a whole.

The CIP Implementation Plan is a major German contribution towards the announced "European Programme for Critical Infrastructure Protection" (EPCIP). Whenever possible, national and international IT security strategies for the protection of critical infrastructures should be reconciled and supplement each other.

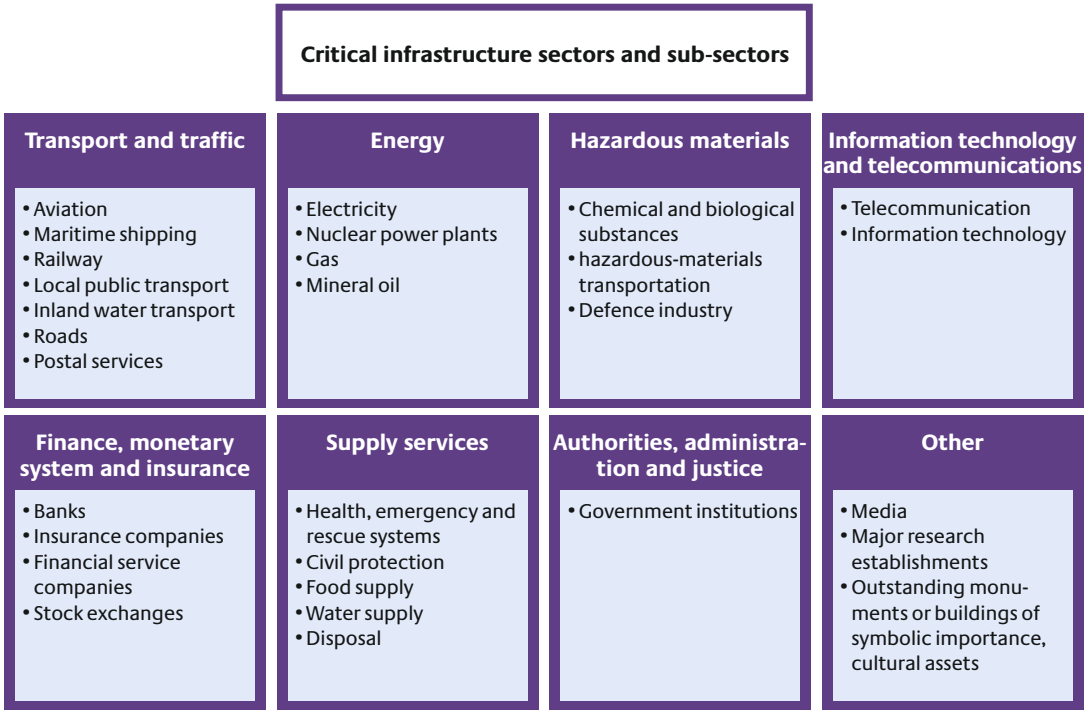
1.2 Addressees

Addressees of the CIP Implementation Plan are generally operators of critical infrastructures in private business. These are companies and organisations from the sectors transport and traffic, energy, hazardous materials, information technology and telecommunications, finance, monetary system and insurance, supply services, and others (media, research facilities, cultural assets). The sectors are broken down into several sub-sectors (see figure 1, page 8).

Due to their paramount importance to society, critical infrastructures require special protection. Terrorist threats, environmental hazards and IT threats must be taken into consideration. The CIP Implementation Plan focuses on information technology and related protective measures in private business. The Federal Government is preparing a separate implementation plan for the federal administration.

The contributing companies consider the concepts and measures described in the following chapter to make sense and be state-of-the-art with respect to protecting information technology. These concepts and measures should be put in place in all CIP areas. The authors of the CIP Implementation Plan consider the jointly developed recommendations as a necessary supplement to the measures which are already in place. These measures should be implemented first and foremost by operators of critical infrastructures in cooperation with the federal administration. To other companies and sectors of industry, it is also recommended to follow suit in order to effectively protect their IT infrastructures.

Figure 1: Structuring of Critical Infrastructures



1.3 Assignment of Tasks in the Implementation of IT Security Measures

The assignment of tasks for the implementation of measures can be described as follows for the different levels:

- Companies: implementation of measures within the respective organisation
- (Sub-)sector level: consideration of aspects beyond company level which concern several companies of a (sub-)sector
- Cross-sector level: implementation of measures which concern several sectors

The operators of critical infrastructures are determined to pursue the measures and to implement the recommendations on the basis of the CIP Implementation Plan. The CIP Implementation Plan is to be updated and adapted to the continuously changing parameters of the security environment under the overall responsibility of the Federal Ministry of the Interior.

2. Starting Situation and Recommendations for the Future

2.1 Introduction

The operators of critical infrastructures in Germany are aware of their responsibility when it comes to providing vital services for the nation. They have hence already taken extensive steps in order to ensure the dependable provision of these services. This chapter describes the tried-and-tested processes and measures which the operators and sub-sectors involved in the preparation of the CIP Implementation Plan are already using as basic IT protection in essential parts. These processes and measures should be implemented in a comparable manner by every operator of critical infrastructures. Furthermore, recommendations are given so that operators can protect their IT infrastructures even better in the future. For other critical infrastructure operators and enterprises not part of a critical infrastructure sector it is suggested that they implement these recommendations on a voluntary basis.

This chapter is broken down into the areas prevention, preparedness, and sustainability to follow the strategic goals of the National Plan for Information Infrastructure Protection. In these sections, the measures and recommendations of the company, (sub-)sector, and cross-sector levels are depicted in different colours.

Company level

The measures and recommendations described on this level are implemented within companies largely without the cooperation of other operators or service providers in other sub-sectors. This level includes forms of cooperation, for example, with (mostly local) rescue services, technical relief organisations, the police, fire brigades, etc. The implementation of the measures and recommendations is a continuous process which includes ongoing monitoring of IT security trends on the part of the operators as well as a quick and effective response to changes.

Sub-sector level

This section describes cooperation between operators and associations within sub-sectors and gives recommendations as to how this cooperation can be improved. The implementation of the measures is designed to help prevent production downtimes or minimise delivery bottlenecks, for example. Cooperation includes the definition of standards and test methods or the execution of large exercises, etc. The given starting situation on sub-sector level was extrapolated from several sub-sectors and does not apply to the same extent to all sub-sectors.

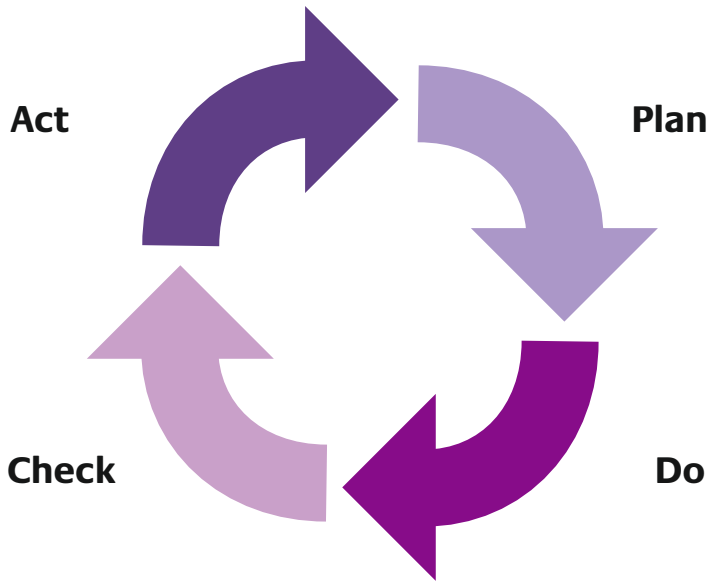
Cross-sector level

The measures and recommendations described for the cross-sector level go beyond cooperation within companies and within sub-sectors. Cooperation partners on this level include, for example, federal or state agencies as well as companies from other (sub-)sectors. This field also covers tasks which public or other neutral agencies fulfil without concrete cooperation with sectors or companies (examples from other areas include travel destination warnings as well as information concerning epidemics or other health risks).

2.2 Prevention

All operators of critical infrastructures admit high importance to preventive measures in order to ward off potential damage to their IT infrastructures and ensure IT security and service availability. The IT security management process as a planned and organised course of action of all those involved in the implementation and maintenance of a reasonable IT security level consists of interlinked individual processes. The IT security management process and all IT security processes are based on the “plan – do – check – act” (PDCA) loop (see figure 2, page 12).

Figure 2: Process loop



The most important individual processes are described below.

As part of the IT security process, critical business processes and their potential risks are identified. Laws, regulations and other conventions to be applied as well as the requirements defined therein are taken into consideration. This serves as a basis for drafting and implementing company-specific IT security concepts. Staff are trained and must commit themselves to abide by the defined measures. Repeated emergency exercises, also in cooperation with external parties, round off the preventive measures. Problems which occur despite all precautions are analysed. The results are used to improve the measures and procedures, so that the risk of recurrence is reduced and damage due to similar future occurrences is limited.

2.2.1 Organisation of IT Security

IT security management and company-wide and nation-wide baseline protection are a high priority for operators of critical infrastructures. Organisational structures ensuring efficient IT security are established within companies. Staff in charge of IT security management have the responsibilities, authority and qualifications necessary to diligently perform their jobs. This includes a general overview of the company and its major tasks as well as thorough methodological knowledge of concepts and procedures in the fields of IT and IT security. Appointing an IT

security officer contributes to defining clear-cut responsibilities. In order to achieve comprehensive security throughout a company or organisation, responsibilities are defined and assigned for all information, applications and IT components.

2.2.2 Critical Business Processes

The operators' aims can only be reached with proper and secure IT use. The identification of critical business processes and the pertinent IT systems is hence very important. These processes are therefore subject to special protection. Dependencies on IT or voice and data networks are identified. Special attention is attached to IT security as early as during the design and development of IT architectures and IT systems for critical business processes. The IT security concepts include suitable measures to address the higher protection requirements of critical business processes. Certified IT systems and IT solutions, if available, are an obvious choice. Technical redundancy and organisational measures ensure the availability of important components. Trustworthiness and security competence are crucial selection criteria whenever external services are used.

Along with processes within their companies, operators of critical infrastructures also analyse interdependencies with external processes with a view to their criticality. These can be external communication services or other externally sourced services. Both traffic of data and goods as well as different transport modes are considered. The analysis focuses on problems which can potentially result from disturbances of the IT infrastructure (both in the organisation's own and in the communication partner's infrastructure).

In view of dynamic IT developments, the risks are subject to permanent change. The current threat situation is continuously examined and evaluated. Appropriate counter-measures are triggered as required.

Recommendations:

- Specifications for IT security requirements for IT system components should be developed and applied.
- Evaluation criteria for assessing the security of IT architectures and IT systems should be applied, further criteria should be developed.
- External service providers should be obliged to fulfil the same security requirements as internal resources when integrated to provide IT (security) services.
- In the long term, certified IT products should be increasingly used considering related cost-to-benefit analysis.
- Certified products should be increasingly used for (sub-)sector-wide critical processes.

2.2.3 IT Security Conceptual Framework

A reasonable degree of IT security can only be achieved with a coordinated set of measures. An overall conceptual framework is required which integrates all areas of IT security and which is implemented on a consistent basis. The operator's IT security guideline defines the IT security targets which are to be aimed at and/or achieved in order to support the performance of business processes to the required extent. The requirements are also a function of the organisation's aims and at times of the aims of its units, too. The company's executive management approves the IT security guideline and puts it into effect. The security guideline is checked and updated on a regular basis.

The IT security concept is orientated towards the requirements of the IT security guideline. National and international laws, regulations, directives and standards also set a framework for security concepts. The systems to be protected are identified. Their security and protection demand is determined in line with potential damage scenarios. Taking the risks identified into consideration, measures are selected and compiled in an IT security concept. The decision as to which concrete measures need to be implemented in view of the risks identified is made in agreement with the executive management. Measures from contingency and crisis management plans are considered within the scope of the IT security concept. The IT security concept is implemented in a clear-cut manner and updated on a regular basis.

A cost-to-benefit analysis forms part of the concept development phase. To this effect, the probability of occurrence and potential damage levels (threat to health and life, material and immaterial losses) are assigned to the identified risks and compared to the estimated costs of effective protection mechanisms. The executive management determines for each and every risk whether and to what extent protection measures have to be implemented. Relevant applications and processes are monitored on operational level in order to quickly identify irregularities.

Operators of critical infrastructures also ensure the physical security of their IT systems. The corresponding measures are already considered in the IT security concept. Additional information and recommendations for physical baseline protection are detailed in the Baseline Protection Concept[3].

The IT security concept is supported through the provision of sub-sector-specific guidelines, directives and procedures.

[3] Federal Ministry of the Interior, Protection of Critical Infrastructures – Baseline Protection Concept.

2.2.4 Maintenance of Critical Business Processes

Within the scope of business continuity management (BCM), critical business processes are protected by preventive measures in such a manner that these processes will not or only temporarily be interrupted even in critical situations and emergencies, in order to ensure the company's economic existence and ward off serious consequences for society. Emergency and crisis management is vital in order to minimise damage and losses in crisis situations and fulfil legal and company-specific requirements. As a precautionary measure following the identification and evaluation of critical business processes, a powerful emergency and crisis management system is set up to systematically prepare for tackling damage incidents and preventing damage from spreading to other parts of the company and/or to other organisations. Company-specific contingency plans are set up which also form the basis for gaming and emergency exercises.

If it is not possible to maintain critical processes for a company in an emergency, sub-sector-internal agreements are in place in order to resume controlled business operations as quickly as possible. Furthermore, agreements exist in many areas on the basis of tried-and-tested concepts which were drafted and coordinated within the sub-sectors in order to maintain the availability of a service on sub-sector level following failure of one provider.

Recommendations:

- Alternative processes should be at hand in order to reduce the consequences for disruptions to critical business processes in a crisis.
- Sufficient capacities of the respective infrastructures (in particular, power supply) should be available within a sub-sector in order to cope with crises and emergencies.
- Furthermore, alternative infrastructures should be available.
- Contingency and crisis plans should be set up on a cross-sector basis to serve as a preparation for crises and as a basis for cross-sector exercises.
- Clear-cut responsibilities should be defined in order to handle crises and emergencies.
- Criteria and responsibilities for the identification of a crisis should be defined.
- Responsibilities should be defined for enforcing contingency and crises plans.
- In the event of resource bottlenecks in a crisis, operators of critical infrastructures should be given preference in order to ensure the efficient resumption of critical business processes.

2.2.5 Implementation of the Security Concepts

The security concepts of operators of critical infrastructures are on principle verifiable and fully implemented. Implementation is subject to regular assessments. The standard requirements for IT security in the fields of availability, integrity and confidentiality at the operator end include, for example, the following:

- analysis of the infrastructure with a view to high availability, implementation of the related technical and organisational measures,
- security classification of documents and information,
- preparation and implementation of concepts for the cryptographic protection of information requiring protection,
- guidelines for the use of new components in existing IT architectures,
- extended rules and checks for access to IT systems and data,
- selection of companies with proven trustworthyness for IT security services.

2.2.6 Security Throughout the Entire Product Lifecycle

Operators of critical infrastructures set up specific requirements for the security and reliability of the products used. These requirements include not just the security features themselves, but also the entire lifecycle. Security is already a central aspect when it comes to defining procurement requirements. This also applies to trouble-shooting, further development and migration to successor products or versions. These requirements must be adhered to no matter whether internal developments, external developments or standard products are concerned.

In order to address the higher security requirements of operators of critical infrastructures, products and components having the appropriate properties must be developed and used. For highly critical components, operator-specific solutions have already been developed and are deployed.

Recommendations:

- Operators of critical infrastructures should define security requirements and cooperate sub-sector-wide when it comes to examining, checking and analysing these requirements.
- Products and components should be developed which correspond to the higher security requirements of operators of critical infrastructures.
- Players at sector and cross-sector levels should increasingly demand and promote the use of certified software.

2.2.7 Training and Awareness Programmes Through Target Group-Specific Information Offers

Staff are called upon to pay attention to their organisation's security and to always act with security in mind. IT users, staff responsible for IT and IT security as well as executives attend suitably designed training and education programmes within the organisation with appropriate curricula and materials in order to attain the required level of IT security expertise.

In order to achieve the highest possible and homogenous education level within the individual critical infrastructure sub-sectors, training materials and concepts are developed and applied on a sub-sector-specific basis. These materials and concepts also lay down the criteria for assessing the success of training measures. Besides an organisation's own staff, customers and partners are another target group for training programmes. Furthermore, the contents is developed in cooperation with educational institutes and universities.

In order to increase awareness with respect to the importance of IT security, operators of critical infrastructures have embarked on cross-sector cooperation with organisations of the public administrations, such as the German Federal Office for Information Security (BSI), the Federal Criminal Police Office, the Federal Network Agency and the specialist ministries in charge. Joint exercises are held, such as the crisis management exercise across federal states, LÜKEX ["Länderübergreifende Krisenmanagement Exercise"].

The public administration provides special and reliable information, such as IT situation reports, travel destination and terror warnings or epidemics information. Manufacturer-neutral aids and guidelines are offered free of charge.

Recommendations:

- IT security qualifications should be added to the profiles of job vacancy publications.
- The development of sub-sector-wide training concepts and information offers should be intensified.
- Operators of critical infrastructures should be increasingly involved in sector-wide and nation-wide as well as international awareness initiatives in order to reduce their security risks.

2.2.8 IT Security Audit

The implementation of the IT security concepts is subject to regular, internal audits. One of the tasks of an audit is an independent check of compliance with legal requirements and the related implementation rules. The tasks of the audit are separated from the IT (security) department. IT security audits and IT audits which are particularly important for IT-based critical business processes are subject to regular audits based on audit plans. The audit results are considered in the ongoing improvement of IT security concepts and the resultant measures.

In some sub-sectors, specific approval and testing rules for IT systems exist. These rules also ensure the operability and security of cross-company processes.

2.2.9 Emergency and Crisis Response Exercises

Emergency and crisis response processes can only be quick and effective if all the parties involved are familiar with the corresponding activities and if exercises are carried out in order to verify their effectiveness. Within organisations, these important processes are exercised on a technical and organisational level.

Exercises on sub-sector level focus, in particular, on:

- whether the agreed communication relations can be established and maintained and
- whether the agreed measures for mutual support and task-sharing are implemented as planned.

The results are evaluated in cooperation with all the partners involved.

Recommendations:

- At company level, the exercises should be carried out using more comprehensive scenarios and also involving external partners.
- Emergency exercises should be carried out with alternating aims and participants.
- Rules for cooperation and interaction with different organisations, such as the police, fire brigade, technical relief organisations, local disaster protection authorities and the Federal Office for Information Security as well as customers and suppliers should be developed and considered.

- Within and across sectors, the regular performance of strategic games, table-top exercises and emergency exercises should be intensified with all relevant public agencies, organisations and external partners in order to be prepared for (sub-) sector-wide and cross-sector crises. These emergency exercises should be developed and evaluated by panels established for this purpose. In this way, optimisation processes can be triggered in a targeted manner, and existing cross-sector dependencies as well as critical shortcomings can be identified and prevention strategies developed.
- In order to effectively tackle crises, issues related to the telecommunications and electricity sectors should be specifically addressed and relevant public organisations and authorities should be involved in the exercises.
- Crises scenarios should be developed, such as power outage in a major city, in order to improve cross-sector coordination, develop suitable cooperation structures and identify existing threats.

2.3 Preparedness

Disruptions in information infrastructures call for a quick and effective response. In addition to the capture and analysis of information, this primarily also means alerting those affected and triggering measures to minimise damage and restore critical business processes. Suitable mechanisms are widely established among operators. IT contingency teams and CERT structures at operators of critical infrastructures deserve special attention in this respect. Crisis and contingency plans as well as measures to ensure permanent reachability of decision-makers and technical personnel are other central components of crisis response. In the case of a disruption in the information infrastructure of an operator, the situation is first analysed internally and suitable counter-measures are taken. In the case of possible external effects, steps are taken within the scope of the sub-sector-specific crisis management in order to maintain the availability of goods and services.

2.3.1 Identification of the IT Security Status

The operators of critical infrastructures have defined and established mechanisms for identifying the security status. The basis for this is the detection, analysis and evaluation of incidents within a company according to defined rules and taking the general security status into consideration. Information is centrally captured and evaluated in order to establish the internal status of the company.

Deviations from the normal status immediately trigger suitable counter-measures. This procedure – including the definition of stage-specific roles and obligations – is documented and available to an operator's units and personnel concerned. The relevant rules are assigned to staff who have been trained accordingly. Deputy rules are in place. Standard mechanisms are defined within companies, setting forth escalation criteria as well as escalation levels.

Besides the internal assessment of the IT status within a company, the higher-level IT security status on sub-sector level is also considered in order to detect potential threats at an early stage. Following their evaluation, the related information is exchanged with other operators within the sector, with the communication paths and contact partners being precisely defined for this purpose. This ensures that suitable preventive action can be triggered throughout the sub-sector at an early stage.

Recommendations:

- On cross-sector level, with the involvement of the federal administration, any information necessary and important for assessing the IT security status should be identified and entered into the appropriate reporting structures.
- Suitable structures should be set up to enable cooperation between all the parties involved, especially with regard to a cross-company situation and analysis centre. This would allow to comprehensively identify, evaluate and process incidents.
- For the situational assessment, an escalation system should be introduced representing the severity of an incident on the basis of escalation stages.

2.3.2 Warning and Alert Mechanisms

Security-critical incidents call for a prompt and adequate response. For this purpose, operators of critical infrastructures have laid down suitable warning and alert procedures which define the units and individuals to be warned or alerted as a function of the incident discovered and the differentiation criteria for warnings and alerts. Besides internal units and staff, external parties are also informed depending on the process involved.

When security-critical incidents are discovered which could have significant consequences for the entire sub-sector, those who may perhaps be concerned are warned or alerted through defined channels.

Recommendations:

- Mechanisms for monitoring and capturing incidents should be established in order to enable a tiered evaluation of the situation.
- Alerts should consist of qualified information concerning the type and extent of the incident in order to be able to forward targeted warnings and alerts.
- The established processes should be broken down into three escalation stages (company-internal, (sub-)sector-internal and cross-sector alerts).

2.3.3 IT Crisis Response

Operators of critical infrastructures lay down adequate responses in crisis response plans in order to tackle IT crises. These plans also cover cooperation with internal and external units in a crisis. Crisis management organisation and the distribution of responsibilities are laid down in a clear-cut manner so that the appropriate action can be triggered and implemented without delay.

Suitable procedures for tackling sub-sector-wide crises are laid down for certain areas. These procedures administer cooperation between operators in order to cope with a crisis. They describe, for example, procedures for coordinating defence measures and for maintaining critical services as well as details of contact partners and communication channels. Guidelines for informing the general public in a crisis are also laid down there.

Recommendations:

- Crisis response processes should also be established on a cross-sector level. Procedures should be defined in this respect in order to ensure smooth cooperation between all the parties involved.
- Contingency concepts for cross-sector IT crises should be developed and implemented.
- These concepts should define units and people to be contacted in a cross-sector crisis as well as reporting channels and escalation levels.
- Across sectors, planned coordination procedures of suitable defence measures should be implemented.
- Exercises should be carried out in order to validate and update existing concepts.

2.3.4 Logging and Monitoring

Operators of critical infrastructures process the information collected on security incidents and remedial measures. Security-relevant incidents must be logged as a precondition for this. Automated records are drawn up especially in critical areas where defined actions related to data and processes are logged (monitoring). The log files enable the detection of irregularities and post-mortem analyses of incidents. They also serve as proof related to incidents. The monitoring function is designed with special consideration of staff co-determination and privacy rights.

2.4 Sustainability

As a precondition for the long-term protection of its national information infrastructures, Germany needs, in addition to political determination and the willingness of all players, to strengthen the country's IT security, technical expertise as well as trustworthy IT services and IT security products. The operators are already making important contributions to this end. Examples include participation in the development of staff training curricula and cooperation in research and development programmes designed to provide more dependable IT systems. On the sub-sector-wide and cross-sector levels, operators of critical infrastructures cooperate with other organisations in order to enforce their joint interests in improving IT security on national and international level.

2.4.1 IT Security Education

Cooperation programmes with educational institutions and universities are in place with which operators are aiming to increase the weight attached to IT security in education and training.

Joint government and industry activities propose curricula for educational institutions and universities, so that future IT users, IT managers, IT security officers and executive staff will deal with the IT security subject in greater depth during their education.

Recommendation:

- Cross-sector IT security training and education initiatives should be launched.

2.4.2 Cooperation in Research and Development

Operators of critical infrastructures cooperate with manufacturers, research institutes and universities in individual subjects. The development of new products and solutions, for example, is supported in order to satisfy the growing demand for IT security.

The industry and business associations of the CI sub-sectors are working together with universities and companies from other sub-sectors in order to promote the development of more dependable IT solutions. The vast potential of knowledge and research capacity available at universities is thereby being exploited in the interest of IT security.

Recommendations:

- IT security should be made an integral part of all research and development projects. Depending on the required security level, products or components from the national crypto-industry should be employed.
- IT security should be considered already during the product planning phase.
- Cooperation between operators of critical infrastructures and the area of "research and development" should be intensified, so that the latest results and innovative products can be put to practical use and trustworthy security products made available.

2.4.3 Cooperation for IT Security

Representatives of operators of critical infrastructures in several sub-sectors have set up working groups to develop solutions for issues of common concern. These working groups address, for example, concrete security issues concerning several operators or the entire sub-sector, as well as IT procedures, business processes and standards.

Many IT security precautions are implemented as insular solutions within companies. Cross-company cooperation, however, would enable the definition of a sub-sector standard. The advantages are obvious, especially in the field of secure communications. Furthermore, synergies can be used even with measures which are fully restricted to internal use within a single company. Security requirements, for example, are the result of joint development and updating, but are implemented on a company-specific level. Furthermore, cooperation platforms have been set up as a means of informal exchange on specific security issues.

Recommendation:

- Cross-sector cooperation on IT security should be intensified and placed on a broader basis.

2.4.4 Enforcement of Interests on a National and International Level

Operators of critical infrastructures have agreed to cooperate in order to enforce their interests related to the protection of critical infrastructures on national and international level. This includes, for example, cooperation in standardisation bodies. Industry associations, public authorities and further institutions are also involved.

Recommendations:

- Activities on national and international level should be bundled and coordinated as a precondition for the secure operation of critical infrastructures.
- Operators of critical infrastructures should intensify their cooperation both within and between (sub-)sectors in order to shape the political will on a national and international basis.
- Cooperation should cross borders. The legal, organisational and technical parameters should be identified and implemented.
- Security aspects should be directly included in product standards with the involvement of public agencies.

2.5 Conclusions

On company level, the essential measures necessary to safeguard a reasonable IT security level are implemented. Emergency and crisis management exercises could be carried out more comprehensively in certain sub-areas.

The intensity of cooperation between operators of critical infrastructures and associations on sub-sector level concerning prevention issues and especially IT crisis response varies from case to case. Measures taken by certain sub-sectors were mentioned as examples. We recommend that comparable measures be implemented by other sub-sectors.

On the cross-sector level, intensive cooperation is already under way in certain areas and has been found to be very valuable especially with a view to enforcing interests on an international level. At national level, cooperation in the field of IT crisis response should also be intensified.

3. Communication

3.1 Introduction

The parties involved in the CIP Implementation Plan consider the expansion of communication – especially with regard to IT crisis prevention and quick response to IT crises – to be a key part of improving IT security in critical infrastructures.

>> An IT crisis in the context of the CIP Implementation Plan exists if a failure or impairment of organisations and facilities of major importance for society with a sustained shortage of supplies, with significant disruptions of public order or with other dramatic consequences occurs or is to be expected as a direct or indirect consequence of IT system conditions.

Prevention and crisis management call for different communication modes:

- **Cause-related communication for the early detection of crises** is used by operators of critical infrastructures in order to report special occurrences in the field of IT security, to improve the assessment of the overall IT security situation and thereby to initiate protective action at an early stage.

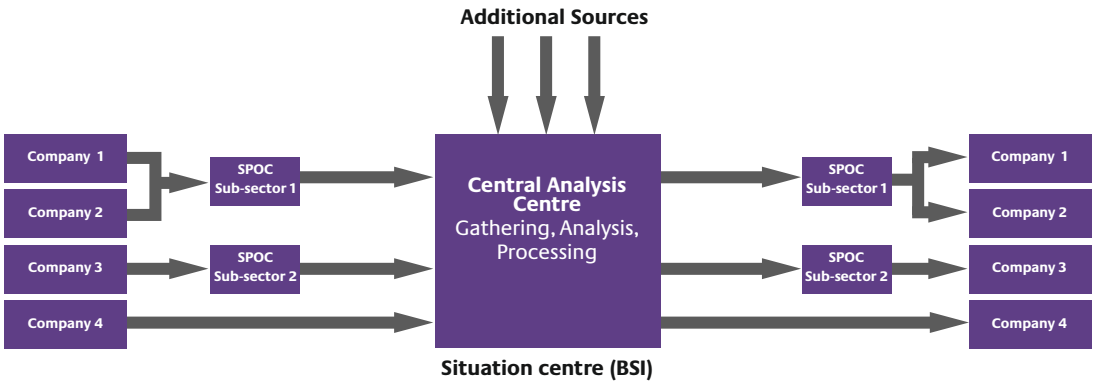
- **Communication for alerting and crisis mitigation** establishes the exchange of information between operators of critical infrastructures and with government agencies in the event of IT security incidents. The consequences of events relevant for IT security are to be minimised, IT crises are to be prevented from spreading, and/or cross-company counter-measures are to be coordinated as quickly as possible.

- Working groups are set up and meetings held within the scope of routine **information exchange and cooperation for crisis prevention.** The exchange of experience and information from the different sub-sectors is aimed to further improve IT security at operators of critical infrastructures. Furthermore, improvements are to be proposed and made available to other operators after IT security incidents have occurred.

For the first two communication modes mentioned above, a mutual exchange of information of the operators of critical infrastructures through single points of contact (SPOCs) with the Federal Office for Information Security will be established (see figure 3). The contact partners in the companies of the respective sub-sectors can be reached via the SPOCs. The SPOCs are to bundle the flow of information on sub-sector level and ensure 24/7 availability. As an interim solution pending the establishment of the SPOCs, direct contact between operators of critical infrastructures and the Federal Office for Information Security will be intensified.

The information gathered will be supplemented and processed by the IT situation centre of the Federal Office for Information Security (in order to generate a national IT security situational picture, for example). These analyses are made available to the operators. The Federal Office for Information Security aims at gaining access to additional information that will serve as a broader basis for evaluating the IT security situation.

Figure 3: Communication structures



3.2 Information Exchange

The security of operators of critical infrastructures can be further enhanced by the targeted forwarding of up-to-date information concerning threats to IT, incidents relevant for IT security and necessary protective action. Communication between government and the business community is of particular importance in order to cope with a crisis. In order to enable this cooperation, measures must be taken in order to ensure the quick and secure flow of information.

The operators of critical infrastructures are already well prepared for crises in internal communications within companies. First communication structures extending beyond the borders of a company in an IT crisis are in place. Sub-sector-internal escalation and reporting channels, also covering public authorities and the police, have already been established in certain sub-areas. Cross-sector communication for IT crisis mitigation is at present still quite rare. Existing communication channels should be used when it comes to expanding and/or intensifying communication between operators of critical infrastructures.

Information is exchanged on a voluntary basis. This requires the definition of clear-cut rules for handling, disclosing and protecting such information and, above all, their sources.

3.2.1 Cause-Related Communication for the Early Detection of IT Crises

Findings with potential consequences for the IT security status or signs of an IT crisis are communicated to the IT situation centre of the Federal Office for Information Security. These include, for example, serious IT attacks against companies or vulnerabilities in critical IT applications not yet communicated unless such vulnerabilities are communicated within the scope of the established CERT structures.

Cause-related communication for the early detection of IT crises supports and supplements the development of a national IT security situational picture by the Federal Office for Information Security. The distribution of this situational picture to the SPOCs and/or operators even further enhances the secure operation of IT in critical infrastructures. Operators of critical infrastructures can thus prepare themselves earlier for potential IT crises.

So far, cause-related communication for the early detection of crises is not yet subject to increased requirements for confidentiality and availability of the means of communication (such as telephone, fax, email). In the medium term, suitable measures should be taken in order to enable the transmission also of sensitive data. Special importance must hence be attached to the development and expansion of suitable communication structures as well as technologies and mechanisms which can be used to this effect. These should be defined and developed in a joint effort. The involvement of operators in the IT situation centre of the Federal Office for Information Security is seen as a long-term goal.

3.2.2 Communication for Alerting and Crisis Mitigation

Quick and coordinated communication is important in an IT crisis in order to enable an early response and to restrict damage. Information concerning extent, duration, reason and/or cause of the incident as well as information on potential consequences for other companies should be communicated. Such information enables companies not yet affected to take the appropriate preparatory action.

The mechanisms of cause-related communication for the early detection of IT crises are only to a limited extent suitable for communications for alerting and crisis mitigation. This communication mode requires the processing of particularly time-critical information. The mechanisms and means of communications must

be upgraded especially with a view to the availability of communication in special crisis situations. The procedures defined in conjunction with the establishment of the SPOCs should be used and/or developed further. The contact partners in the companies should be familiar with suitable IT crisis response procedures and have the required responsibilities.

3.2.3 Information Exchange and Cooperation for Crisis Prevention

The prevention of IT crises to the maximum extent possible and enhanced preparedness for future events call for a continuous exchange of information and cooperation within the scope of workshops and working groups involving operators of critical infrastructures and government agencies. Existing and urgent IT security issues can be discussed there. Post-mortem analyses of past IT crises are carried out, experience is exchanged and possible improvements are developed. Lessons learned can make an important contribution towards the sustainable protection of critical information infrastructures.

3.3 Conclusion and Perspectives for Cooperation

The analysis of existing communication modes shows that company-wide and sometimes even sub-sector-wide structures for exchanging information between operators of critical infrastructures are already in place for both cause-related communication for the early detection of crises and communication for alerting and crisis mitigation. However, there are still no communication structures in place for exchanging information and cooperation for crisis prevention on cross-sector level.

The operators of critical infrastructures support the intensification of communications, especially on cross-sector level, in order to address growing mutual interdependencies. In the medium term, SPOCs are to be expanded and established as central communication nodes of the sub-sectors.

Further joint efforts by all the parties involved are considered to be necessary and important. In a first step, communication processes and technologies are to be specified in more detail, for example. An exchange of information on topical IT security issues and retrospective analyses of IT crises should enhance IT security even further in critical infrastructures. The processes established in this context should be practiced on a regular basis and gradually upgraded.

4. Roadmap for the Future

The recommendations for maintaining and enhancing IT security and for establishing communication structures described in the previous chapters were taken up by those involved in setting up the CIP Implementation Plan, and a decision was made to set up a roadmap for future action.

This roadmap addresses four main subjects as follows:

1. Emergency and crisis exercises
2. Crisis response and management
3. Maintaining critical infrastructure services
4. National and international cooperation

The corresponding working groups were set up in April 2007 with the Federal Ministry of the Interior as the lead organisation. Cooperation between government and the business community is thereby continued and the recommendations will be implemented within a concrete time schedule.

Each working group will be managed by a member of the team in charge of the preparation of the CIP Implementation Plan. Furthermore, representatives from companies, associations and public authorities not yet involved in the preparation of the CIP Implementation Plan are also invited to join the working groups.

The subjects of “emergency and crisis exercises” and “crisis response and management” will be the first to be addressed in more detail.

First results and implementations will be developed by 2008. The results thereby obtained will be used as the basis for the following working group on “maintaining critical infrastructure services” and form an input to “national and international cooperation”.

The working groups will be supported and assisted by the Federal Office for Information Security which will not only be technically involved but will also host the function of central office.

This cross-sector working group concept which is applied for the first time in this form in Germany will essentially contribute towards sustainably ensuring IT security in critical infrastructures.

4.1 Emergency and Crisis Exercises

Emergency and crisis response processes can only be quickly and effectively performed if all the parties involved are familiar with the corresponding activities and if exercises are carried out in order to verify the effectiveness of the processes. Whilst these key processes are already practiced on technical and organisational level within companies, further steps are still necessary on (sub-)sector and cross-sector levels.

The “emergency and crisis exercises” working group was set up in April 2007 in order to implement the recommendations related to this subject.

The activities of this working group focus on the development and implementation of all parameters necessary for planning, performing and evaluating emergency and crisis exercises. Cross-sector IT crisis scenarios are developed which are used as a basis for regular exercises. Existing exercise programmes are considered in this context and potential synergy effects are identified and used. This means that the scenarios developed can, for example, be used as templates for planning LÜKEX exercises (crisis management exercises across federal states). The federal-state and municipal levels may also be involved.

The alternating participants in emergency and crisis exercises are representatives from the different sub-sectors operating critical infrastructures as well as representatives from the relevant government and business organisations.

Common goals of all the parties involved are the identification of cross-sector dependencies and critical shortcomings, the optimisation of crisis response processes as well as the improvement of cross-sector coordination by establishing suitable structures.

This creates, for example, the basis for further work within the scope of the "crisis response and management" working group.

By mid-2008, the working group will deal with the preparations of regular exercises and the related creation of suitable framework conditions, also with the involvement of further participants (besides the Federal Office for Information Security, also the Federal Office for Civil Protection and Disaster Assistance as well as the Academy for Crisis Management, Emergency Planning and Civil Protection). Starting at the end of 2008, the emergency and crisis exercises developed in this way will be carried out with changing goals and participants. The first members of this working group are representatives from Arcor AG & Co. KG, Bayerische Hypo- und Vereinsbank AG, Commerzbank AG, DB Sicherheit GmbH, Deutsche Bank AG, Deutsche Bundesbank, Deutsche Telekom AG, Deutsche Postbank AG, Dresdner Bank AG, Deutscher Sparkassen- und Giroverband e. V., E-Plus Mobilfunk GmbH & Co KG, O2 (Germany) GmbH & Co. OHG, Gesamtverband der Deutschen Versicherungswirtschaft e. V., Mineralölwirtschaftsverband e. V., RWE Energy AG, T-Mobile Deutschland GmbH as well as representatives of the Federal Ministry of Economics and Technology and the Federal Financial Supervisory Authority.

4.2 Crisis Response and Management

Security-critical incidents call for a prompt and adequate response. The operators of critical infrastructures have set up crisis response plans in order to define adequate procedures for their area. Crisis response agreements within and across sub-sectors must be enhanced.

The "crisis response and management" working group kicked off in April 2007 and now works on the cross-sector establishment of suitable crisis response processes, from the IT situation analysis via warnings and alerts right through to coordinated crisis mitigation.

For this purpose, aspects of capturing and evaluating the IT security situation and the related structures for cooperating with the national IT situation and analysis centre are considered.

Processes and technical implementations for warning and alerting functions in the event of serious IT incidents are defined and jointly implemented by the Federal Office

for Information Security and the companies operating critical infrastructures. The establishment of single points of contact on sub-sector level as well as the pertinent definition of reporting structures constitute an important milestone to this end.

The processes required for joint crisis mitigation are identified and integrated into harmonised, cross-sector crisis response concepts. Controlled and prepared communications between all the parties involved are of central importance in order to cope with a crisis in a coordinated manner.

The working group will prepare concepts for cross-sector crisis response and management by mid-2008. The first members of this working group are representatives from Allianz SE, the German Financial Supervisory Authority, the Federal Network Agency for electricity, gas, telecommunications, post and railways, Bundesverband deutscher Banken e. V., Commerzbank AG, Deutsche Bahn AG, Deutsche Bank AG, Deutsche Bundesbank, Deutsche Flugsicherung GmbH, DZ BANK AG Deutsche Zentral-Genossenschaftsbank Frankfurt am Main, Deutscher Sparkassen- und Giroverband e. V., the European Central Bank, E-Plus Mobilfunk GmbH & Co KG, Gesamtverband der Deutschen Versicherungswirtschaft e. V., O2 (Germany) GmbH & Co. OHG, RWE Energy AG, T-Mobile Deutschland GmbH and Vodafone D2 GmbH.

4.3 Maintaining Critical Infrastructure Services

Infrastructure services which are critical for the nation must be protected by preventive measures in order to ensure that such services are not interrupted or on a temporary basis only in critical situations and emergencies and that the company's economic existence continues to be ensured. Serious consequences for the country and its people must be avoided.

For this purpose, critical processes are identified by a working group and more detailed protection concepts and measures will be developed as required. As soon as first results of the "crisis response and management" working group will be available, this working group will be set up and start work in 2008.

Within the scope of preparing protection concepts, ways to ensure the preferential supply of operators of critical infrastructures in cases of resource shortages due to a crisis are also considered in order to ensure that critical processes are maintained or quickly resumed.

4.4 National and International Cooperation

Sustainable advances in the protection of critical infrastructures and IT security require close international cooperation. A host of bodies and international cooperation projects have already been established to this effect in order to develop standards and comprehensive protection strategies.

The activities of the working group which was set up in April 2007 are to result in better coordination and harmonisation of the parties involved in the CIP Implementation Plan. As a first step, information concerning the international CIP activities of the different stakeholders is exchanged to this effect. Tried-and-tested methods and approaches are discussed and joint strategic aims are agreed to. Cooperation projects are to be agreed so that the protection of critical infrastructures on national and international level can be pursued even better.

The aim of the working group is to contribute towards establishing a comparable minimum IT security level in critical infrastructures on an international scale, starting in Europe. The working group will first explore ways to form a common discussion platform for information exchange and subsequently implement appropriate structures. If special issues are to be agreed to, working group meetings will be convened as required and/or sub-working groups established for long-term tasks.

5. Summary and Outlook

Critical infrastructures are vital for our society, their protection is a task that concerns all citizens. A large part of these infrastructures is operated by private business. None of these critical infrastructures can render its services without adequately protected information infrastructures. The operators of critical infrastructures are aware of this. They have hence already implemented a high degree of IT security in the respective companies. However, adequate protection of information infrastructures cannot be achieved by measures which are limited to individual companies and organisations. Parallel, (sub-)sector-wide and cross-sector measures are needed on national and international level.

Operators of critical infrastructures have hence joined forces with the Federal Ministry of the Interior in order to identify the measures needed to protect information infrastructures on the basis of the strategic goals defined in the National Plan for Information Infrastructure Protection, i.e. prevention, preparedness and sustainability. These measures are now compiled in this CIP Implementation Plan. This cooperation reflects the joint responsibility of government and business. It is designed to bundle the know-how of operators and to sustainably strengthen the IT security of critical infrastructures in Germany.

The CIP Implementation Plan is an IT security guideline for operators of critical infrastructures. It aims to assist political decision-making and national and international cooperation. It is recommended to other companies as a guideline for implementing an adequate IT security level.

The situation described in this Implementation Plan reflects the current good practice adopted by operators of critical infrastructures in the field of IT security. This ranges from a consistent IT security organisation in the individual companies to measures for the special protection of critical business processes and the implementation of awareness-raising measures for staff members.

The foundations for the continued reliability of infrastructure services are to be strengthened. The roadmap adopted with the Implementation Plan is to be implemented and updated in a joint effort by operators of critical infrastructures and government agencies in order to meet with growing demands in the future.

The trustworthy and target-oriented cooperation and coordination in crises already in place in individual industries are to be further expanded.

The tried-and-tested partnership between operators of critical infrastructures and the federal administration is given a broader basis with the CIP Implementation Plan.

To this effect, joint working groups will handle the subjects of “emergency and crisis exercises”, “crisis response and management”, “maintaining critical infrastructure services” and “national and international cooperation”.

The CIP Implementation Plan will be updated in view of the continuous further development of the IT landscape. Results from the working groups’ activities and from the implementation of measures and recommendations will be considered in updates of the CIP Implementation Plan.

Public authorities and operators of critical infrastructures cooperate closely in examining the up-to-dateness of measures and recommendations and the resultant amendments. The group of those involved is not limited to the present authors; instead, cooperation with further operators is welcomed.

Comments and suggestions concerning this CIP Implementation Plan are always welcome. Please send your comments and suggestions to the following address:

Federal Ministry of the Interior, Division IT 3
Alt-Moabit 101 D
10559 Berlin, Germany
Telephone: (+49 30) 18 681-0
E-mail: it3@bmi.bund.de

Abbreviations

BCM	Business Continuity Management
BMI	Bundesministerium des Innern (in English: Federal Ministry of the Interior)
BSI	Bundesamt für Sicherheit in der Informationstechnik (in English: Federal Office for Information Security)
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
EPCIP	European Programme for Critical Infrastructure Protection
IT	Information Technology
KRITIS	Kritische Infrastrukturen (in English: critical infrastructures)
LÜKEX	Länderübergreifende Krisenmanagement Exercise (in English: crisis management exercise across federal states)
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen (in English: National Plan for Information Infrastructure Protection)
SPOC	Single Point of Contact
UP KRITIS	Umsetzungsplan KRITIS (in English: CIP Implementation Plan)

Glossary

Federal Administration	Federal ministries and their specialist agencies, such as the Federal Office for Information Security, the Federal Criminal Police Office, the Federal Office for Civil Protection and Disaster Response, the Federal Network Agency (refer to Article 86 of the German Constitution).
Information infrastructure	The entirety of the IT components of an infrastructure is referred to as its information infrastructure.
Interdependency	Interdependency is the complete or partial mutual dependency of several goods or services.
IT security	IT security is the condition where availability, integrity and confidentiality of information and information technology are protected by adequate measures.
Operators of critical infrastructures	Operators of critical infrastructures are private businesses or public authorities delivering services in critical infrastructures.

Critical infrastructure

Critical infrastructures are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences.

In Germany, the following sectors are attributed as critical infrastructures:

- Transport and traffic (aviation, maritime shipping, railway, local public transport, inland water transport, roads, postal service)
- Energy (electricity, nuclear power plants, mineral oil, gas)
- Hazardous materials (chemical and biological substances, hazardous-goods transports, defence industry)
- Information technology and telecommunications (telecommunication, information technology)
- Finance, monetary system and insurance (banks, insurance companies, financial service companies, stock exchanges)
- Supply services (health, emergency and rescue systems, civil protection, food and water supply, disposal)
- Authorities, administration and justice (government institutions)
- Other (media, large research institutes as well as outstanding monuments or buildings of symbolic importance, cultural assets)

IT security guideline

"IT security guideline" is used as a collective term for terms also used by operators of critical infrastructures, such as "information security policy", IT security policy", "IT security strategy", "IT security principles" and "IT security guidelines".

References

Federal Ministry of the Interior (editor): Schutz Kritischer Infrastrukturen – Basisschutzkonzept (in English:Protection of Critical Infrastructures – Baseline Protection Concept). Berlin, 2005.

Federal Ministry of the Interior (editor): Nationaler Plan zum Schutz der Informationsinfrastrukturen (in English: National Plan for Information Infrastructure Protection). Berlin, 2005.

Imprint

Published by:
Federal Ministry of the Interior
Public Relations Division
Alt-Moabit 101 D
10559 Berlin
www.bmi.bund.de

Design:
MEDIA CONSULTA Deutschland GmbH
Anita Drbohlav (original design),
Helmut Spörl, Petra Grampe (editing)

Images :
Bundesamt für Sicherheit in der Informationstechnik (BSI)