WHITE PAPER

Critical infrastructures (KRITIS) and NIS-2 implementation

| A company of the Gretsch-Unitas group

Cutting-edge locking systems

The BKS brand

Security has a name, or to be more accurate, it is a brand. BKS GmbH is a member of the Gretsch-Unitas group. More than a century of experience in manufacturing high-quality locking systems. Ever since the round cylinder was developed in 1938, BKS GmbH has been and remains today one of the leading companies in the field of locking technology and security.

Opening and locking

Locking systems from BKS offer individual and tailor-made solutions and are manufactured in accordance with the highest quality standards. By choosing a BKS master key system, you opt for the most modern locking systems with the most diverse functions and features. You also open up flexible design options for subsequent extensions.

Versatile solutions

Locking systems from BKS offer a variety of solutions for securing individual doors and for planning modern master key systems. Convenience and security can be individually designed and economically implemented with the combination of mechanical and electronic locking systems.

Perfect interplay

Along with the outstanding quality of their mechanical, mechatronic and electronic cylinders, BKS offer a comprehensive range of services in the field of planning, administration and reordering of duplicate or replacement keys and cylinders.

Table of contents

The following themes are hot topics of the industry 04

What are critical infrastructures? 06

Risk management 10

Reporting obligation 13

Emergency and recovery measures 14

Security audits 15

Our solutions/Contact data 16

Copyright notice

Image credits

BKS product and building images: Gretsch-Unitas group
AI-generated: cover image and page 6, 8, 10, 14. AdobeStock: page 4, 12, 16

Publisher

Gretsch-Unitas GmbH
Johann-Maus-Str. 3 I 71254 Ditzingen, Germany
Tel. + 49 71 56 3 01-0 I Fax + 49 71 56 3 01-2 93 I www.g-u.com

The following themes are currently hot topics in every branch of industry

Europe-wide and globally networked processes, as well as the increasing digitalisation of all areas of life and the economy, mean a greater susceptibility to external factors which are frequently beyond our control. This development has made the situation in relation to cyber threats more acute, which has led to new challenges that require a coordinated and innovative response in all EU member states.
The number, scope, complexity, frequency and impact of incidents is increasing and poses a considerable threat to smooth running of businesses and facilities.

The EU NIS-2 Directive (formerly NIS Directive of 2016) which came into force in 2023 sets out the minimum cybersecurity standards in the European Union.

CURRENTLY HOT TOPICS

- Critical infrastructures (KRITIS)
- Implementation of the EU NIS-2 Directive
- BSI Critical Infrastructure Regulation (BSI-KritisV)
- Law on implementation of the NIS-2 Directive and on regulating the main features of the information security management in the federal administration (for short: law on implementation of the NIS-2 Directive)
- KRITIS Umbrella Act (KRITIS-DachG)

The aim is to strengthen resilience and cybersecurity measures in the critical sectors (KRITIS sectors). Resilience (resistivity) generally refers to the ability to protect, react and recover from disruptions, attacks or other unexpected events without lasting adverse effects and adapt to changing conditions.

The focus here is mainly on security incidents in the network or information systems and also the physical security of the infrastructure of these systems and personal security.

These can be summarised in a few points

- Areas of application – definition
- Risk management with technical and organisational security measures to ensure the availability of infrastructures
- Security Incident Management – detection, monitoring and response
- Reporting obligations of security incidents
- Emergency and recovery measures
- Security audits, auditing of security standards, documentation
- Training courses: raising awareness and promoting a security culture

The NIS-2 implementation will affect almost 30,000 companies and other organisations in Germany. Are you as operator, your company or your facilities affected by this?

1.) Areas of application – definition:
The answers to the questions about the definition of the "Areas of application" and "What are critical infrastructures?" can be found in the Act on the German Federal Office for Information Security (BSIG) and Critical Infrastructure Regulation of the German Federal Office for Information Security (BSI-KritisV) in which the nine critical infrastructure sectors are defined. Furthermore, the facilities are defined by the "Law on implementation of the NIS-2 Directive and on regulating the main features of the information security management in the federal administration" ("law on implementation of the NIS-2 Directive") as announced in the German Federal Law Gazette on 05 December 2025.

As a consequence, companies and other organisations will be classified as operators and as facility/facilities in three categories:

- **Operators of critical infrastructures (KRITIS operators)**
- **Facilities of major importance**
- **Important facilities**

Furthermore, **special cases** and **facilities of the federal administration** exist.

In addition, the KRITIS Umbrella Act (KRITIS-DachG), which is expected to come into force in 2026, will strengthen and regulate the resilience and above all the physical security of critical infrastructures in Germany.

The integration of physical security measures in the cyber security strategy as set out in the NIS-2 Directive can improve overall security at companies and strengthen their resilience to a large number of threats.

> *The more exacting requirements arising from the implementation of the NIS-2 Directive and Cyber Security Strengthening Act (IT security, reporting obligation) and from the KRITIS Umbrella Act (resilience) also have an impact on the security requirements of the physical infrastructure.*

In the words of a security advisor:
"IT security does not happen behind the door to a server room, nor is it the responsibility of the cloud provider. The physical security, whose availability and also resilience are based on the risk evaluations, use of sustainable solutions, the implementation, adherence to, checking and adaptation, the reporting obligation through to ongoing further training.
What's more, many companies often underestimate how quickly 'internal' anomalies in a building or property can lead to a chain of events because of the large number of integrated systems. These events can ultimately lead to security incidents and losses leading to delays and adverse economic effects as well as downtimes. The reason is simple: 'It just wasn't on the screen!'

Example: air-conditioning of the UPS control breaks down and, since this is not considered to be particularly important, the problem is only rectified the day after or in the following days.
If by coincidence further problems (factors) arise during this downtime, such as a fault at the local electricity provider, this prompts activation of the emergency standby system (emergency diesel generator). However, before this happens, the uninterruptible power supply (UPS) breaks down completely because the control has overheated.
This results in an downtime throughout the entire company for an extended period."

Operators of critical infrastructures (KRITIS operators)

Your company and other concerned organisations belong to this category if you are an operator of a "critical infrastructure" and facilities, systems or parts in the following areas of industry (KRITIS sectors):

- Energy
- Information technology and telecommunication
- Transport and traffic
- Health
- Water
- Food
- Finance
- Municipal waste disposal
- Social security and basic security benefits for job seekers

These facilities or systems are very important for the functions of the local community because if they did not exist or were restricted, this could lead to significant supply bottlenecks or pose major hazards to public safety.
In addition to the standard threshold value of 500,000 inhabitants to be supplied, further quantitative and qualitative criteria can also be taken into consideration.
This means for your company as operator that the following security measures arise from the implementation of the NIS-2 Directive:

- IT security
- Reporting obligation and
- Systems for attack detection
  KRITIS Umbrella Act (KRITIS-DachG*):
  resilience

Classifications	Facilities	Threshold values
Operators of critical infrastructures (KRITIS operators)	• Energy • Information technology and telecommunication • Transport and traffic • Health • Water • Food • Finance • Municipal waste disposal • Social security and basic security benefits for job seekers	Someone who carries out critical services meet the demands of the general public. Inhabitants to be supplied: ≥ 500,000

*subject to changes in the final KRITIS Umbrella Act, version dated 11/2025

Facilities of major importance

Your company and other concerned organisations or facility/ facilities fall into this category if it/they has/have at least 250 employees or an annual turnover of > €50 m and an annual balance sheet total of > €43 m, offer(s) goods or services and belong(s) to the following sectors:

- Energy sector (electrical power supply, district heating or cooling supply, fuel and heating oil supply, gas supply)
- Transport and traffic (air traffic, rail traffic, road traffic, sea transport)
- Finance sector (banking, financial market infrastructures)
- Health (healthcare provider, EU reference laboratories, pharmaceuticals research/development, pharmaceutics, medical products)
- Water (drinking water supply, wastewater treatment)
- Digital infrastructures (Internet Exchange Points, Cloud service providers, Data centre service providers, Content delivery network providers, Managed services provider, Managed security services provider)
- Space (ground infrastructure for space-based services)

Similarly with at least 50 employees or an annual turnover of > €10 m and an annual balance sheet total of > €10 m

- Publicly accessible telecom services, public telecom networks

Likewise independently of employees, annual turnover/balance sheet total:

- Operators of critical infrastructures
- Qualified trust service provider, Top Level Domain Name Registries or DNS service providers
- Facilities of the federal administration - if also operators of critical infrastructures

This means for your company as facility/facilities that the following security measures arise from the implementation of the NIS-2 Directive:

- IT security
- Reporting obligation

Classifications	Facilities	Threshold values
Facilities of major importance (companies and other organisations)	• Energy • Transport and traffic • Finance • Health • Water • Digital infrastructures • Space	Number of employees: ≥ 250 or Turnover: > €50 m Balance: > €43 m
	• Publicly accessible telecom services • Public telecom networks	Number of employees: ≥ 50 or Turnover: > €10 m Balance: > €10 m
	• Operators of critical infrastructures • Qualified trust service provider • Top-level domain name registries • DNS service provider • Facilities of the federal administration - if also operators of critical infrastructures	Without threshold values

*subject to changes in the final KRITIS Umbrella Act, version dated 11/2025

Important facilities

Your company and other concerned organisations or facility/facilities fall into this category if it/they has/have at least 50 employees or an annual turnover of > €10 m and an annual balance sheet total of > €10 m, offer(s) goods or services and belong(s) to the following sectors:

- Energy sector (electrical power supply, district heating or cooling supply, fuel and heating oil supply, gas supply)
- Transport and traffic (air traffic, rail traffic, road traffic, sea transport, postal and courier services)
- Finance sector (banking, financial market infrastructures)
- Health (healthcare provider, EU reference laboratories, pharmaceuticals research and development, pharmaceutics, medical products)
- Water (drinking water supply, wastewater treatment)
- Digital infrastructures (Internet Exchange Points, Cloud service providers, Data centre service providers, Content delivery network providers, Managed services provider, Managed security services provider)
- Space (ground infrastructure for space-based services)
- Waste treatment
- Production, manufacturing and trading in chemical substances
- Production, processing and sales of food items
- Processing industry/manufacturing of goods (medical products, in-vitro diagnostics, data processing units, electronic and optical products, electrical equipment, mechanical engineering, automobiles and automobile parts, automotive engineering)
- Digital services provider (online marketplaces, online search engines, platforms for social-networking services)
- Research (research facilities, but not educational facilities)

Similarly with less than 50 employees and an annual turnover of ≤ €10 m or an annual balance sheet total of ≤ €10 m

- Publicly accessible telecom services, public telecom networks

Likewise independently of employees, annual turnover/balance sheet total:

- Trust service provider

This means for your company as facility/facilities that the following security measures arise from the implementation of the NIS-2 Directive:

- IT security
- Reporting obligation

Classifications	Facilities	Threshold values
Important facilities (companies and other organisations)	• Energy • Transport and traffic • Finance • Health • Water • Digital infrastructures • Space • Waste treatment • Production, manufacturing and trading in chemical substances • Production, processing and sales of food items • Fabrication industry/manufacturing of goods • Digital service providers • Research	Number of employees: ≥ 50 or Turnover: > €10 m Balance: > €10 m
	• Publicly accessible telecom services • Public telecom networks	Number of employees: < 50 and Turnover: ≤ €10 m or Balance: ≤ €10 m
	• Trust service provider	Without threshold values

*subject to changes in the final KRITIS Umbrella Act, version dated 11/2025

Risk management with technical and organisational security measures to ensure the availability of infrastructures

GEMOS, a physical security information management system, is more than just a technical measure for pooling information.
It organises the central monitoring, processing and visualisation of extensive security information from various industries in an independent risk management system.
GEMOS carries out manufacturer-neutral pooling and integration (notifications and instructions) of various physical security and information systems (GEMOS interfaces), such as:

- Fire detection and extinguishing systems
- Video management systems
- Intrusion detection systems
- Perimeter systems
- Escape door control systems
- Alarm receiving systems
- Transmission systems
- Communications systems
- Personal emergency signal systems
- Voice alarm systems
- Key management systems
- Building automation systems and technical systems (e.g. IT systems) using standard protocols such as BACnet, DALI, EIB/KNX, ESPA, Modbus, OPC, SNMP

With GEMOS access (access control system) you also receive an essential security system element of the NIS-2 requirements, which allows you fast access centrally to all security information on your access points (WHO-WHEN-WHERE/WHERE TO).

› Our products help you maintain the availability of your infrastructures:

- GEMOS (physical security information management system)
- GEMOS access (access control system)

Security Incident Management - detection, monitoring and response

With a GEMOS system, all security information and events such as (faults, alarms and other statuses) of all integrated security and information systems (GEMOS interfaces) are monitored, detected and presented in such a manner that everything can be clearly understood.

The GEMOS system is administered centrally so you can respond directly to security incidents. Here are just a few examples:

- **Video management systems with cameras:**
these systems can analyse live images and detect security incidents immediately. To carry out the monitoring automatically, or allow it to be controlled manually by the operator, GEMOS can immediately trigger the Pan-Tilt-Zoom control (PTZ) of the alarm camera, connection of live images from the periphery camera, start recordings and therefore generate archive images. Intervention personnel can be systematically deployed via the communication systems in response to detected incidents. Furthermore, GEMOS enables alarms, faults or info messages from other physical security and information systems to be connected by activating images which are linked to the alarms.

- **Intrusion detection and perimeter systems and corresponding sensors and detectors:**
these systems prevent unauthorised access and physical security violations. They also detect these types of events simultaneously when they occur. Video surveillance cameras can be connected and integrated into GEMOS which significantly improves the monitoring of security incidents and the ability to respond to these. This also includes the visual representation of arming and disarming of areas and sub-areas in the floor plan, especially in the event of an alarm. The activation and deactivation of sensors and detectors can also be monitored and documented.

- **Fire alarm and extinguishing systems and their detectors:**
these systems detect fire in the early stages, prevent propagation and therefore minimise the potential risks. Selected intervention measures, alerting of emergency personnel, automatic provision of fire-brigade route maps and possible activation of key management systems are smoothly coordinated through their integration into GEMOS in order to respond efficiently to security incidents. Deactivation and activation operations can be time-controlled and carried out manually, including an indication of need and verification by the operator.

- **Transmission systems and alarm receiving systems:**
the transmission of alarm, sabotage, raid, fault, arming/disarming messages for example, as well as maintenance and information messages from external facilities and their hazard detection systems via communication networks, form the core element of an alarm receiving system. The triggering objects can be visually displayed in the floor plan and controlled by selecting preset intervention measures in GEMOS. Measures can be time-dependent and linked to categories to ensure a fast effective response to security incidents.

- **Personal emergency signalling systems and holdup reporting systems:** in addition to the physical protection of critical infrastructures, protection and security of personnel are a major part of the NIS-2 Directive, especially in relation to physical and security-related threats. Automatic triggering of emergency calls by motion or position sensors as well as manual triggering of the emergency call system via panic buttons or mobile alarm devices is monitored so that security incidents can be quickly detected. Localisation functions can be used in combination with GEMOS for display in the floor plan and targeted reactions to intervention effectively implemented in the floor plan.

- **Building automation systems and technical systems:**
the statuses of these systems and facilities, such as temperature, pressure, rotational speed, speed, fill level, meter reading and flap and valve settings are monitored in GEMOS. This information can be categorised as alarm, pre-alarm, fault, maintenance or info messages, for example. GEMOS visualises critical events as digital or analogue value in the floor plan, also defining several threshold areas accompanied by a graphic representation to facilitate accurate detection and monitoring, in order to be able to respond to these events in good time.

- **Communication systems:**
facilitate a smooth exchange of information when detecting and monitoring incidents In combination with GEMOS, this ensures a fast, effective coordinated response to security incidents. Integrating additional CCTV surveillance cameras and other physical security systems achieves a more comprehensive accurate visual overview of the situation.

- **GEMOS access (access control system):**
physical barriers such as fences, gates and security mantraps can prevent unauthorised access, whereas an access control system monitors and controls the access to critical infrastructures. With this system, access can be restricted to authorised personnel by defining physical zones and time frames, mapping access rights and using security passes (such as RFID transponders and cards,

NFC media), PIN codes and biometric scanners. Further typical functions of an access control system can be implemented with the "Dynamic Rights", including bag checks, repeat access block (anti-passback), access sequence control, reporting system, multiple person presence check and exclusion for a specific period of time following multiple failed attempts with two-factor authentication. When this system is integrated into GEMOS and linked to video surveillance cameras with the option of activating lockdown scenarios, this greatly enhances the ability to respond when security incidents occur. This enables direct control of security mantraps, controlled physical access systems, swing and revolving doors and access gates.

Reporting obligations of security incidents

In GEMOS access (access control system) we help you fulfil your reporting obligations in relation to security incidents with comprehensive detailed records of all access attempts and events. Furthermore, change histories and presence lists which can be evaluated during subsequent checks and analyses can be logged in the system.
Comprehensive reporting and action logs are made available in GEMOS (physical security information management system) in order to fulfil reporting obligations in the event of security incidents. Individual monitoring operations of integrated physical security and information systems (GEMOS interfaces) can be specifically set up, configured and, if required, modified using the GEMOS action plan processing.
Furthermore, system and security monitoring logs are available from GEMOS itself and the integrated physical security and information systems (GEMOS interfaces).
These tools can be used to quickly and systematically respond to unusual and unexpected system events and also suspicious activities related to system security.

As authorised GEMOS operator, you therefore have access to the wide range of instruments (reports) which are available to you to meet your reporting obligation in the event of security incidents.

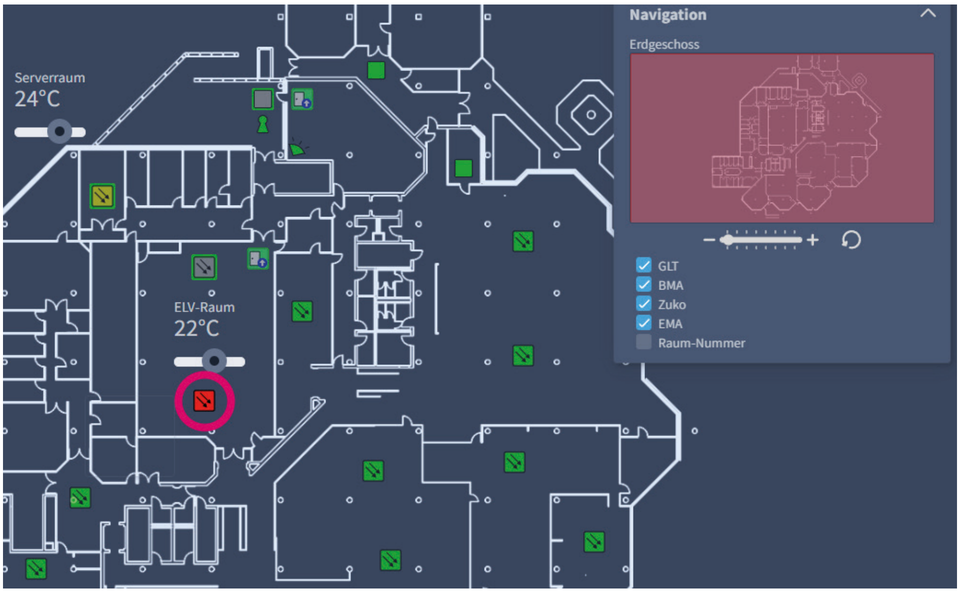
Security incident

(Excerpt from the law on implementation of the NIS-2 DIRECTIVE, definitions)

A security incident shall be considered to be significant if:
a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or
b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.
GEMOS provides you with a complete overview (WHAT-WHEN-WHERE) of all security events. This increases efficiency considerably in terms of monitoring, detecting and reacting to security incidents.

Furthermore, we offer many advanced options in the form of GEMOS modules to satisfy your individual security requirements in every respect.

GEMOS enables a centralised risk management system.



Emergency and recovery measures

Apart from the normal backup options in a GEMOS system, failure safety and immediate recovery are a high priority.
GEMOS - ENTERPRISE ONE SERVER serves as
an optional basis for safeguarding against failure of a GEMOS system. This can be done, for example, by operating two GEMOS servers in hot standby mode. Permanent monitoring ensures that if the server or network communication with the first GEMOS server fails, this is detected and a changeover to the second GEMOS server automatically takes place.
When an individual server fails, this does not result in restrictions or message loss in the GEMOS system. The recovery of normal operation (synchronisation of GEMOS server databases) and reactivation of the first GEMOS server are also supported.

The following basic functions are provided by the GEMOS – ENTERPRISE ONE SERVER:
Real-time data redundancy:

- Message statuses
- Commands/Instructions
- Alarm stack
- Message log

Master data replication:

- Databases
- Files

We recommend for the high availability requirements of a GEMOS 5 system in the sense of the security level "Function must be maintained at all times, 24/7 operation (24 hours a day, 7 days a week)" to use a spatial separation of the GEMOS server. The GEMOS system can consist of physical GEMOS server hardware and/or virtualised GEMOS server environment. There is more to emergency and recovery measures than just a system backup, which is why we offer integrated solutions.

Security audits, auditing of security standards, documentation

GEMOS:

- GEMOS security: configured encryption: TLS cryptologies 1.3 – AES-256 according to BSI (German Federal Office for Information Security)
- Non-platform specific (including administration and storage of imported or generated certificates and the corresponding private codes) – operating systems such as Windows or Linux can be used on servers and workstations.
- Web-based user and operator interface: installations, updating of client software, additional runtime environments at workstations are basically not required.
- All databases are and will remain on the GEMOS servers. No databases (or parts thereof) are located on the workstations.

GEMOS – ENTERPRISE ONE SERVER:

- The exchange of real-time data (message statuses, commands/ instructions, alarm stack, message log) between the GEMOS servers takes place securely via the configurable setting (BSI-compliant (German Federal Office for Information Security)) by means of TLS 1.3 - AES-256 encryption.
- The continuous, automatic and monitored synchronisation of data by means of master data replication (databases and files) between GEMOS servers is carried out securely using a configured setting (compliant with German Federal Office for Information Security) via TLS 1.3 - AES-256 encryption.
- Server independence of the modular GEMOS interfaces to the physical security and information systems
- Rights and roles concept – based on granular GEMOS system architecture
- User authentication – comprehensive support of security settings (password length/validity/ complexity, support for 2-factor authentication using WebAuthn standard of FIDO2/U2F, but also support for Time-based One Time Password und Hash-Based-One-Time-Password)
- Central control via the GEMOS server (installation, configuration, update of GEMOS interfaces and GEMOS modules)

GEMOS access:

- Browser-based operation, no installation of software on the workstations
- Flexible configuration by abstracting the access rights from the room structure (management of room zones and reader groups)
- Encrypted data transmission (with appropriate reader hardware from the card/card reader to the data traffic of the bus communication – bus encoding)

Training courses – raising awareness and promoting a security culture

	Training courses for
GEMOS academy	• Sales/Planner • Technical sales/Customer care • Installer • User/Operator • One-to-one training

Comprehensive seminars and training courses are available to meet the needs of participants. You will be guided on your path to success by our expert product trainers with many years of practical experience. The seminars and training courses are held in German or in English:

- Location-independent online training
- BKS in-house training facilities in Berlin and Offenbach am Main (Germany)
- On-site trainings (certain training content requires pre-arranged and available infrastructure)

We create solutions

The implementation of GEMOS (physical security information management system) and GEMOS access (access control system) in the context of the NIS-2 Directive has many benefits, especially for companies who need or would like to optimise their IT and physical security infrastructure. The specific advantages:

- **Integration of security data**
  GEMOS provides the option of integrating security data from various sources, physical or digital. It can therefore provide a comprehensive picture of the overall security landscape at a company.

- **Centralised administration and monitoring**
  With GEMOS, all security measures can be administered and monitored centrally. This central risk management is decisive for improving coordination during security incidents and ensuring a fast, effective response.

- **Automation and secuity processes**
  Many security processes, including alarm management and escalations, can be automated in GEMOS. This reduces the need for manual interventions and increases efficiency which helps improve continuous monitoring and the ability to respond.

- **Fast response**
  As security data can be integrated and analysed in GEMOS, the response is much quicker in the event of security incidents for minimising the effects of security incidents and ensuring the protection of critical infrastructures.

- **Comprehensive risk analysis and evaluation**
  GEMOS provides advanced tools for carrying out risk analyses and evaluations. This helps companies identify potential weaknesses in their infrastructure and develop suitable measures for minimising risk.

- **Compliance with legal requirements**
  By providing support with monitoring, detecting and reporting security incidents, GEMOS gives companies the support they need to fulfil the compliance requirements. This includes the documentation of incidents and reporting to the relevant authorities.

Sources:

- EU NIS-2 Directive
- EU RCE Directive also known as CER Directive (Critical Entities Resilience Directive)
- BSI Act (BSIG)
- Ordinance for Determining Critical Infrastructures according to the Act on the German Federal Office for Information Security (BSI Critical Infrastructure Regulation – BSI-KritisV)
- Law on implementation of the NIS-2 Directive and on regulating the main features of the information security management in the federal administration
- KRITIS Umbrella Act (KRITIS-DachG)
- openkritis.de

Notes

Gretsch-Unitas GmbH
Baubeschläge
Johann-Maus-Sr. 3
71254 Ditzingen, Germany
Tel. +49 7156 301-0
Fax +49 7156 301-77980

BKS GmbH
Heidestr. 71
42549 Velbert
Germany
Tel. +49 2051 201-0
Fax +49 2051 201-9733

www.g-u.com

11/2025 Printed in Germany

GEMOS

Contact

GEMOS und GEMOS access sales contact
Are you looking for a GEMOS expert contact?
If so, just write to us, we will be pleased to help.
info@bks.de

https://www.bks.de/de-en/kontaktformular

GEMOS - drop in and take a look:

7pxl.de/GEMOS-App/

Securing technology for you

G-U BKS FERCO