Redefining Hosting – Reinventing Security

kyberio.

IT-Security Concept
kyberio GmbH

Security on all Levels:
Physical, Digital, and Organizational

kyberio.

IT-Security
at kyberio

3 lived ISMS: ISO 27001

4 Perfect Add-On: PCI-Certification

5 5-Zone-Security Concept

6 ISMS Excerpt

8 Business and Service Continuity

Certified IT-Security:
Our lived ISMS

Our ISO 27001 certification based on IT Grundschutz from the German Federal Office for Information Security is built on a wide range of precise, practiced guidelines and processes.

The scope of the **BSI ISO 27001** certification covers the data center network in Hanover and its management. It includes all systems and processes required to operate the data center infrastructure, customer management, and providing services for the co-location.

The application of ISO 27001 based on IT Grundschutz from the German Federal Office for Information Security (BSI) includes the objectives and measures from Annex A of ISO 27001 and the associated implementation guidance for commonly accepted procedures from ISO/IEC 27002.

As a prerequisite for certification, Kyberio has undergone a multi-stage audit procedure for the data center and the associated organizational processes. This audit takes place periodically.

The audit primarily covers the following areas:

- Company business requirements
- Technical infrastructure
- Management Responsibility
- Organizational processes
- Risk management
- Data protection

By choosing Kyberio, our customers also improve their security in light of IT security legislation. The requirements regarding data protection and the associated liability risks have become much stricter since May 2018 due to the EU's General Data Protection Regulation. This legal change means even more drastic penalties for breaches of data protection law than the previous Federal Data Protection Act.

Certification provides legal protection and offers many business advantages in conjunction with improved security. To summarize the benefits:

- Improved IT infrastructure security
- Increased security awareness from management to employees.
- Legal protection and reduction of liability risk
- Improved competitiveness
- Cost savings through outsourcing of expensive security-related in-house services
- Creation of trust among customers and the public
- Possibility for the certification of customer applications based on Kyberio's existing certificate.

PCI-DSS v3.2 –
The perfect Add-On

PCI-DSS Standard stands for „Payment Card Industry Data Security Standard.“ The PCI standard corresponds to a set of rules that reflects the security requirements for payment transactions with credit cards. This standard is binding for all companies, institutions, and organizations that process credit cardholder data.

Companies and organizations that process cardholder data (CHD) electronically on a cardholder environment (CDE) must secure this environment against data abuse and unauthorized access following the PCI guidelines to protect its ongoing operation. Furthermore, the standard provides a clear assignment of responsibilities for the different areas and tasks within the CDE. It must be possible to track all access and work steps. An essential part of operating such an environment is physical security and the associated processes to ensure this in data center operations.

These requirements concern 12 areas:

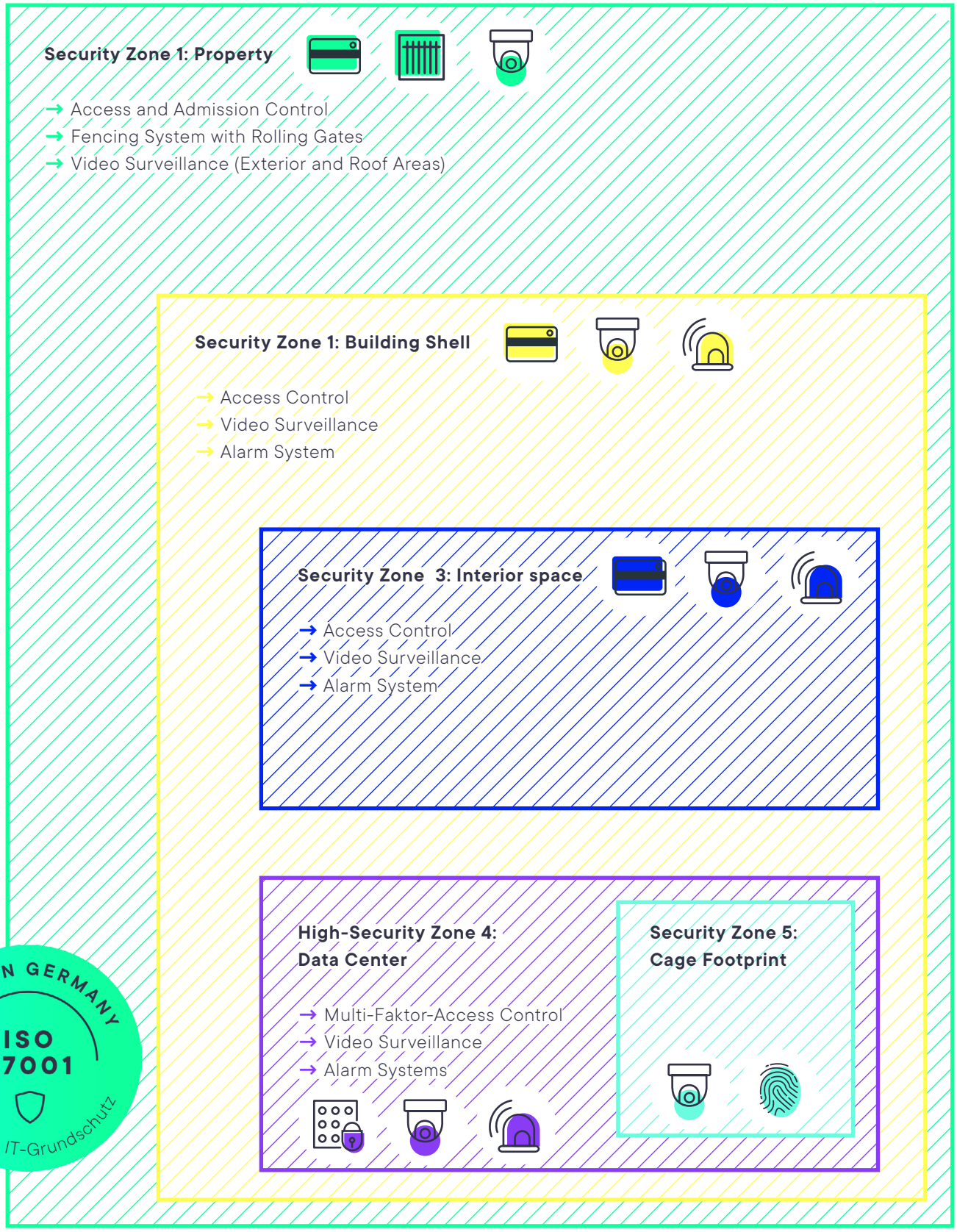
- A firewall concept
- Password security
- Protection of cardholder data
- Data encryption
- Anti-virus software
- Systems and application maintenance
- Access restriction
- User-specific access
- Physical access restriction
- Tracking and monitoring data access
- Regular testing (systems and processes)
- Maintaining an information security policy

Tracking admission and access to the environment is ensured by professional access controls and processes, seamless video surveillance around the clock, logging and exact verification of persons in the data center, data comparison, and plausibility checks.

As a co-location customer in our data center, you benefit from a service that is already PCI-certified by a qualified auditor („QSA“), which extends all the way to your rack cabinet. This certification allows you to concentrate on the compliance of your rack-operated infrastructure and refer to the physical security of your rack based on our certification, which covers essential components of requirements 9 and 12 of the PCI requirements catalog and requirement 11.1 regarding wireless access points. These points are no longer included in your audit as you build your certification on the certified PCI compliance of the data center operator.

E-commerce providers, content providers, institutions, and other organizations that offer services or products or accept donations online by credit card, therefore, have the opportunity to implement this in a PCI-certified data center environment in their own, individually lockable 19“ rack (with 22 or 42 height units). We are happy to provide you with our Attestation of Compliance („AOC“) for this purpose.

5-ZONE-SECURITY CONCEPT



MADE IN GERMANY
ISO 27001
based on IT-Grundschutz

MORE THAN SECURE

5-Zone-Security

People, Technology, Processes

As part of our ISMS, we address multiple topics to ensure the long-term secure operation of our data centers and customer systems.

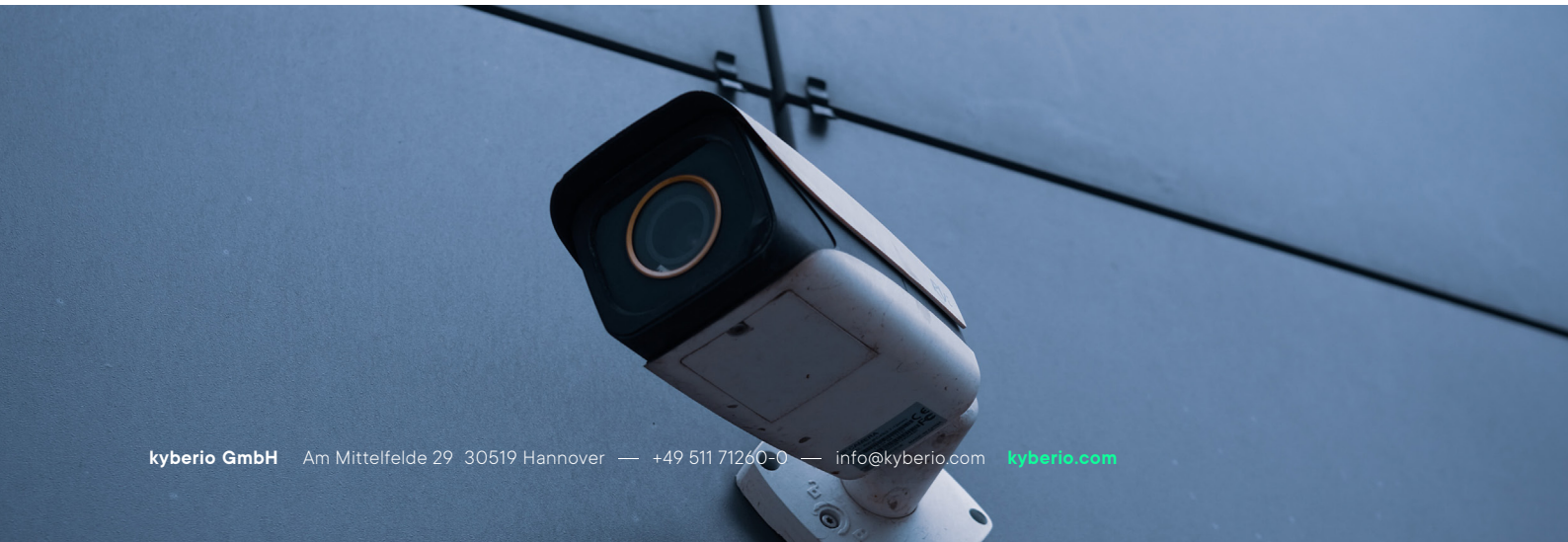
These include, among others:

→ **24/7/365 Staff on Site:** Thanks to our continuously staffed Operation Center on-site, we can respond quickly to any incident and ensure the smooth operation of the data centers.

→ **Perimeter Protection:** The business park on which the data center is located is protected by barred gates, while the data center itself has additional perimeter protection. The gate to the customer parking lot and the building are controlled and monitored by the Operation Center and remain locked to unauthorized persons around the clock.

→ **24h Videosurveillance:** The outside area, all building entrances, and the data center area are monitored around the clock by cameras with motion detection. The live video sequences are transmitted to the Operation Center, where they are reviewed and stored for later review.

→ **Access Control:** Access is only granted after prior registration, in the company of authorized employees, and following the security concept of two-factor authentication (2FA). Authentication is granted with a personalized RFID transponder of the employee („possession“) in combination with the correct entry of the personal PIN („knowledge“).



MORE THAN SECURE

5-Zone-Security

- **Monitoring and Alerting:** The building management system fully integrates into our central monitoring solution and alerting processes. Compliance with defined operating parameters and fault messages are immediately transmitted to the staff on site and our security service providers connected via redundant communication channels. Depending on the message type, the security service provider directly informs the police, fire department, and building services if necessary or first consults with the staff on site.

- **Fire Protection Concept:** Highly sensitive smoke detectors for very early smoke detection (VESDA) are used for early identification and prevention of fires. If further fire detectors (2-line dependency) detect a potential fire, an automatic nitrogen extingu-ishing system (N^2 extinguishing) is triggered after a warning to protect any people in the technical area. At the same time, the fire department, the Operation Center, and the building services are informed, and an emergency plan is activated.

- **Redundant Power Supply:** A battery-supported, uninterruptible power supply (UPS) combined with a diesel emergency power system (EPS) to ensure operation if the public power grid fails. These are scaled so that all components, including air conditioning, can continue operation without restrictions.

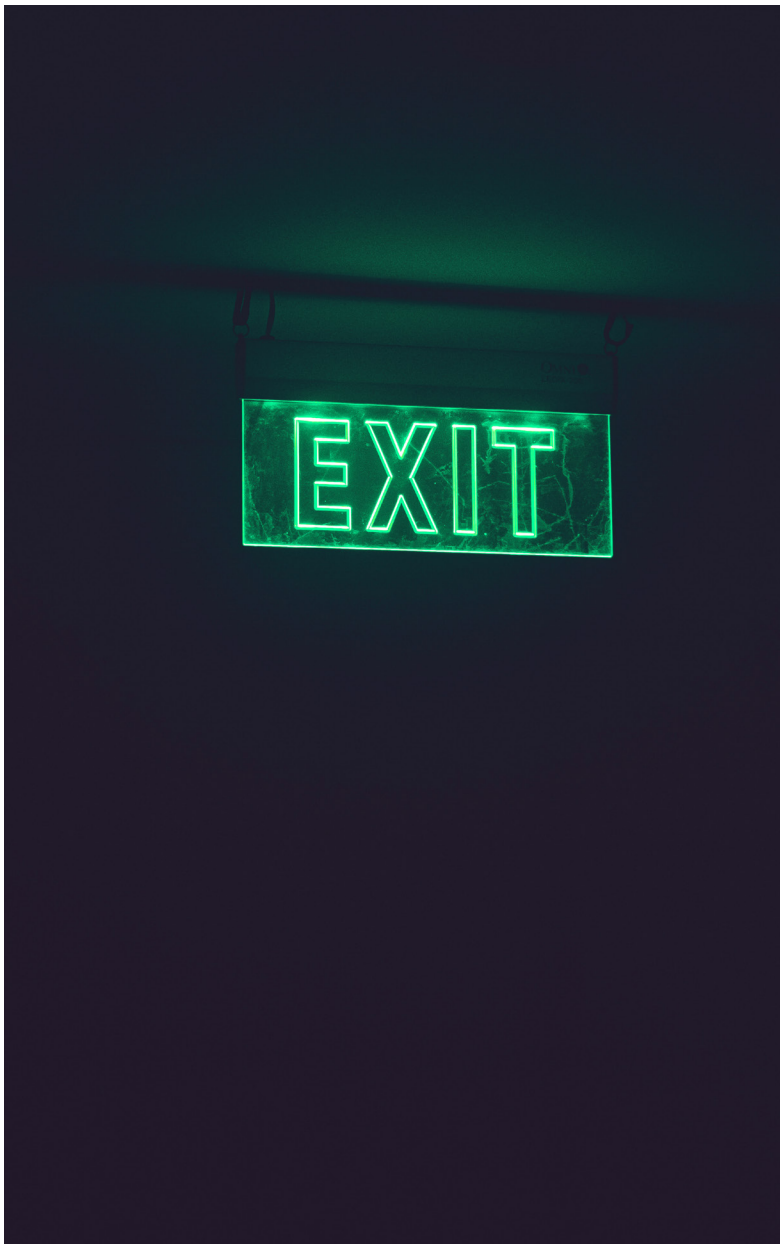
- **Multi-Layered Protection against Cyber Attacks:** Protecting networks and IT systems against cyber attacks is essential; we are constantly adapting it to current threats. We have developed a multi-layered security concept based on D/DOS protection, threat detection (IDS/IPS), next-generation firewalls, malware protection, and tamper-proof backups for our customers and our proprietary systems.

Business and Service Continuity

As part of the ISMS, comprehensive emergency plans strategies and escalation paths have been defined to secure the uninterrupted operation of essential systems even in crisis scenarios (e.g., fire, power outage, or cyberattacks) or at least their restoration as quickly as possible.

In addition to the routine review of the required documentation, processes, and systems, we conduct periodic emergency drills and training sessions with all employees and external service providers (e.g., maintenance companies). Critical systems required for operation (such as our monitoring) are designed redundantly and distributed across our two independent data centers.

All systems are continuously maintained and subjected to regular performance tests (including load transfer from the EPS). Through contractually agreed on-call services with our maintenance companies, we also ensure a rapid response in case of a fault.



Redefining Hosting – Reinventing Security

kyberio.

Questions
and Contact:

Kyberio
Am Mittelfelde 29
30519 Hannover
Phone: +49(0)511 - 71 260 0
Fax: +49(0)511 - 71 260 199
E-mail: sales@kyberio.com
www.kyberio.de

Design by Agentur für Markenschärfung Hannover, Icons: Freepik