As at: November 2026

EXPERT HANDBOOK

KRITIS & PHYSICAL SECURITY

Video Surveillance & Remote Video Monitoring

for critical infrastructure (KRITIS) facilities

SPECIALIST PORTALS AND BRANDS OF SECUCONCEPT

Legal framework: KRITIS Umbrella Act & NIS-2 / BSI Act · GDPR-compliant implementation

Technology & standards · Alarm verification via an alarm receiving and service centre

Cost examples & economics · Checklists for operators

Quality through Trust

SecuConCept · Security – Consulting – Conception · www.secuconcept.de 0800 666 000 4 · vertrieb@secuconcept.de

ABOUT THIS HANDBOOK

Physical protection is mandatory – and plannable

With the KRITIS Umbrella Act (KRITIS-Dachgesetz, in force since 17 March 2026), the physical protection of critical facilities is governed by cross-sector legislation for the first time. In parallel, the revised BSI Act implementing the NIS-2 Directive has applied since 6 December 2025. Video surveillance with professional remote monitoring via an alarm receiving and service centre (ARC) is one of the most effective instruments for securing perimeters, access roads and unstaffed outdoor facilities around the clock – provided that technology, procedures and data protection interlock cleanly.

This handbook is written for executive management, security and facility management, technical management, procurement, and construction and project management in energy, water, healthcare, transport, logistics and other sectors requiring protection. It brings together the legal framework, standards, data protection requirements, cost examples and checklists in a single document.

Contents

1 At a Glance 3

2 The KRITIS Legal Framework 2026 4

3 Video Surveillance in the Resilience Concept 7

4 Technology, Standards and Cyber Security 9

5 Remote Monitoring via the Alarm Receiving Centre 11

6 Data Protection and the GDPR 13

7 Cost Examples and Economics 15

8 Project Checklist for Operators 17

9 Frequently Asked Questions (FAQ) 18

10 Your Partner for KRITIS Security 19

11 Sources, Standards and Legal Status 20

KEY FACTS FOR DECISION-MAKERS

01 At a Glance

The ten most important facts for operators of critical facilities who are planning or modernising video surveillance and remote video monitoring.

1 **The KRITIS Umbrella Act has been in force since 17 March 2026** (BGBl. 2026 I No. 66). It governs the physical protection and resilience of critical facilities in ten sectors.

2 **Specific obligations depend on the KRITIS Ordinance.** Thresholds and effective dates will be set by a statutory ordinance of the Federal Ministry of the Interior (BMI); a ministerial draft has been available since 26 May 2026. The original registration deadline of 17 July 2026 has been repealed.

3 **§ 13 KRITISDachG explicitly names** site perimeter demarcation, instruments for monitoring the surroundings, detection equipment and access controls – the core field of video surveillance.

4 **Incidents must be reported within 24 hours** (§ 18 KRITISDachG); a detailed report follows within one month at the latest. Complete video documentation makes both easier.

5 **Executive management is liable** for implementing and overseeing the resilience measures (§ 20 KRITISDachG).

6 **NIS-2 / BSIG since 6 December 2025:** network cameras, recorders and video management systems are IT systems and belong in the risk management framework under § 30 BSIG.

7 **Data protection remains fully applicable:** KRITIS status establishes a strong legitimate interest, but replaces neither the balancing of interests, transparency nor a data protection impact assessment.

8 **Remote monitoring instead of mere recording:** only live verification at a monitoring centre (ARC) to DIN EN 50518 turns images into a response – with a defined response chain.

9 **Planning to DIN EN 62676-4:** the protection objective for each camera (Detect, Recognise, Identify) determines resolution, lens and position.

10 **Cost-effective:** depending on the site, a remotely monitored perimeter solution often costs only a fraction of 24/7 on-site guarding – but does not replace it in every scenario (see Chapter 7).

Important note on legal validity

This handbook provides professional guidance and is no substitute for legal advice. Legislation, ordinances and official interpretations change – in particular the still-pending KRITIS Ordinance under the KRITIS Umbrella Act. Legal status of research: November 2026. Before taking decisions, check the current position with the BBK, the BSI and your data protection supervisory authority, and involve your data protection officer and, where appropriate, legal counsel. All cost figures are non-binding reference values (net) and do not replace a site-specific quotation.

KRITIS UMBRELLA ACT · BSIG / NIS-2 · HOW THEY INTERACT

02 KRITIS Legal Framework 2026

Two sets of rules interlock for operators of critical facilities: the KRITIS Umbrella Act (KRITIS-Dachgesetz) for physical resilience and the BSI Act for cybersecurity. Video surveillance systems sit precisely at the interface.

2.1 KRITIS Umbrella Act (KRITISDachG)

The Act transposes EU Directive (EU) 2022/2557 (CER Directive). The Bundestag passed it on 29 January 2026 and the Bundesrat approved it on 6 March 2026; it was promulgated on 16 March 2026 and has been in force since 17 March 2026.

Sectors covered (§ 4 in conjunction with Annex 1)

Sectors under the KRITIS Umbrella Act	
Energy	Transport and traffic
Water	Healthcare
Food	Finance[1]
Information technology and telecommunications[1]	Space
Municipal waste disposal[2]	Social insurance and basic social security[2]

[1] For IT/telecommunications and financial undertakings (DORA), the risk-analysis, resilience, verification and reporting obligations largely do not apply, as special regimes take precedence. [2] Here, essentially only the risk-analysis obligation remains. The standard threshold is a supply serving around 500,000 people; the sector-specific values of the KRITIS Ordinance are decisive.

Obligations and deadlines for operators

Obligation	Legal basis	Deadline (from classification as critical)
Registration with the BBK (joint BBK/BSI portal)	§ 8	within 3 months at the latest
Risk analysis and assessment	§ 12	after 9 months; thereafter as required, at least every 4 years
Resilience measures and resilience plan	§ 13	after 10 months
Reporting of significant incidents	§ 18	within 24 h; detailed report within 1 month
Implementation and oversight duty of executive management	§ 20	after 10 months
Fines	§ 24	tiered, up to €1 million

Current status (November 2026)

The fixed registration deadline of 17 July 2026 was repealed by the Act of 21 July 2026 (BGBl. 2026 I No. 221). According to the BBK, there is currently no registration obligation as long as the KRITIS Ordinance is not in force. **Recommendation:** once the Ordinance takes effect, the deadlines run very short. Preparing the risk analysis and protection concept now avoids procurement bottlenecks and time pressure in tendering, permitting and installation.

§ 13 KRITISDachG – resilience measures relating to video surveillance

§ 13 obliges operators to take appropriate and proportionate technical, security-related and organisational measures. One of its objectives is adequate physical protection of the premises. Paragraph 3 lists, by way of example:

- Site protection through **perimeter demarcation** (fences, barriers)
- **Instruments and procedures for monitoring the surroundings** – this covers video surveillance including perimeter detection
- **Detection equipment** and **access controls**
- defined **alarm and response procedures**, personnel security management, training and exercises – explicitly including the staff of external service providers (para. 3 no. 5)

The considerations behind the choice of measures must be documented in a comprehensible manner (§ 13 para. 4). A written security concept with protection objectives, threat analysis and a justification for each camera therefore serves not only as data protection evidence, but also as KRITIS evidence.

2.2 BSI Act under NIS-2 (NIS2UmsuCG)

The NIS-2 Implementation Act recast the BSIG; it has applied since 6 December 2025 without any transition period. Around 29,500 companies fall under BSI supervision as “important” or “particularly important entities” (§ 28 BSIG). The regular registration deadline ended on 6 March 2026 and the grace period granted by the BSI on 31 July 2026; outstanding registrations must still be completed.

- **§ 30 BSIG – risk management:** minimum catalogue of ten measures, including security in procurement and maintenance, access control, cryptography and supply chain security. Video systems, cameras and VMS fall within this scope.
- **§ 32 BSIG – reporting obligations:** early warning within 24 h, report within 72 h, final report within one month.
- **§ 38 BSIG – executive management:** approval and oversight of the measures, training obligation, personal liability.
- **§ 41 BSIG – critical components:** the Federal Ministry of the Interior can prohibit the use of certain components, for instance where the manufacturer is controlled by the government of a third country. Manufacturer selection is thus also a compliance issue (see Chapter 4.3).
- **§ 65 BSIG – fines:** up to €10 million or 2% of worldwide annual turnover (particularly important entities).

2.3 Other relevant regulations

Regulation	Relevance for video & remote monitoring
GDPR / BDSG / state data protection acts	Lawfulness, transparency, retention periods, DPIA – see Chapter 6
§ 34a German Trade Regulation Act (GewO), Security Industry Ordinance	Licensing and qualification requirements for guarding and alarm response personnel
§ 201 German Criminal Code (StGB)	Prohibition of covert audio recording – operate cameras without audio recording
§ 87 para. 1 no. 6 Works Constitution Act (BetrVG)	Works council co-determination for technical monitoring equipment
EU AI Act (EU) 2024/1689	Restrictions on remote biometric identification; prefer analytics without biometrics
Cyber Resilience Act (EU) 2024/2847	Security requirements and update obligations for connected products (staggered application until 2027)
Building regulations / grid operator requirements	Masts, foundations, cable routing, permits in protection zones where applicable

PROTECTION OBJECTIVES · SECURITY CHAIN · LIMITS

03 Video Surveillance in the Resilience Concept

Cameras do not protect – processes protect. Video surveillance only takes effect as a link in a closed security chain of Deter & Delay, Detect, Verify, Respond and Document.

3.1 The security chain

Deter & Delay	Detect	Verify	Respond	Document
Fence, gates, lighting, bollards	Video analytics, thermal imaging, detectors	Live image at the ARC, audio challenge	Response service, police, operator on-call duty	Event log, preservation of evidence, report under § 18

Highlighted in green: core tasks of video surveillance with remote monitoring.

The time budget is decisive: the time an intruder needs to overcome the barriers must be greater than the sum of the detection, verification and response times. Video surveillance cuts detection and verification to seconds; the on-site response time remains a matter of organisation and regional availability.

Worked example: the time budget

Phase	Without remote monitoring	With remote video monitoring
Detection of the intrusion	by chance, often only at the start of the working day	under 10 seconds (perimeter analytics)
Verification	none	30–90 seconds (operator at the ARC)
First countermeasure	none	live audio challenge after around 2 minutes
Arrival of response service / police	hours to days after the offence	within the agreed response time, e.g. 15–30 minutes
Outcome	**damage is discovered after the event**	**offence is disrupted, aborted and fully documented**

The figures are typical practical values, not a guarantee. They show: the longer fence, gates and building shell delay an intruder, the more likely the response arrives while the offence is still in progress. Barriers and remote monitoring must therefore be planned together.

3.2 Typical protection objectives in KRITIS facilities

Facility type	Main risks	Video focus
Substations, grid stations	Sabotage, non-ferrous metal and cable theft, arson	Perimeter detection with thermal imaging, access roads, transformer areas
Waterworks, elevated tanks, pumping stations	Tampering, unauthorised access, vandalism	Entrances, shafts, tank roofs, fences
PV and wind farms, battery storage	Module and cable theft, sabotage, fire	Large-area perimeter, self-sufficient masts, thermal analytics
Hospitals	Assaults, theft, access to technical areas	A&E access route, technical plant rooms, medicine stores (no patient areas)
Logistics, ports, transport hubs	Cargo theft, intrusion, sabotage	Gates, ramps, open areas, licence plate recognition only with a legal basis
Data centres, telecoms sites	Sabotage, unauthorised access, theft of components	Perimeter, airlocks, access control with video verification

Devil's advocate: where video reaches its limits

Video does not replace a barrier: without a fence and delay, any response arrives too late. Analytics generate false alarms from wildlife, weather and vegetation – without calibration and upkeep, acceptance at the monitoring centre declines. Radio and mobile links can be jammed; KRITIS sites need a supervised transmission path with a backup route. And a 24/7 on-site presence remains necessary wherever people must act on site (e.g. access management, fire watch, plant security).

DIN EN 62676 · DETECTION · IT SECURITY

04 Technology, Standards and Cyber Security

The quality of a video surveillance system is decided at the planning stage. The governing standard is the DIN EN 62676 series, “Video surveillance systems for use in security applications”; the VdS guidelines and manufacturers’ specifications apply in addition.

4.1 Resolution levels under DIN EN 62676-4

A protection objective is defined for each camera. This determines the pixel density required at the target location, measured in pixels per metre (px/m) or as the height of a person in the image.

Level	Pixel density	What it achieves	Typical KRITIS use
Monitor	12.5 px/m	Broadly track the movement of people and vehicles	Overview of large open areas
Detect	25 px/m	Establish whether a person is present	Perimeter and fence lines with analytics
Observe	62.5 px/m	Characteristic details, e.g. clothing	Storage and plant areas
Recognise	125 px/m	Recognise a known person	Entrances, gates, security interlocks
Identify	250 px/m	Identify a person beyond doubt	Vehicle entrance control, main entrance
Inspect	1,000 px/m	Finest details, e.g. lettering	Special cases, number-plate and detail images

4.2 Detection technologies compared

Technology	Strengths	Limitations
Thermal imaging camera with analytics	Night vision without lighting, long range, low false alarm rate when correctly calibrated	No identification, higher cost per camera
Day/night camera with IR and AI analytics	Detection and classification of people and vehicles, colour information by day	Limited IR range, more weather-sensitive
PTZ / speed dome	Tracking by the monitoring centre, zoom for verification	Only one field of view at a time; never the sole means of detection
Radar / fence detection (supplementary)	Weather-independent detection, automatic camera slew-to-cue	Additional integration and calibration
Mobile, self-sufficient camera towers, solar/battery	Rapidly available; construction phases, interim protection	Dependent on power and mobile networks, risk of vandalism

4.3 Cyber security of the video system

Networked cameras are a well-known gateway into corporate networks. For operators within the scope of the BSI Act (BSIG), the following measures form part of risk management under § 30 BSIG:

- A dedicated, physically or logically separated video network (VLAN/segmentation, firewall); no direct internet access to cameras
- Encrypted transmission to the ARC (VPN/TLS), authentication with individual credentials, no default passwords
- Firmware and patch management with documented intervals; manufacturer commitments to security updates (Cyber Resilience Act)
- Role and permissions concept in the VMS, logging of access and exports
- Supply chain review: origin, support period and risk assessment of cameras and software – evaluated independently of any manufacturer
- Monitoring of transmission paths (line supervision, backup path via LTE/5G) and tamper alarms on loss of image or camera repositioning

Caution with manufacturers from third countries – especially China

Under **§ 41 BSIG**, the Federal Ministry of the Interior can prohibit the use of critical components – among other grounds, where the manufacturer is directly or indirectly controlled by the government of a third country. A prohibition can also affect components already installed. There is no general BSI "approval list"; the former notification procedure with a manufacturer's guarantee declaration (§ 9b BSIG, old version) was abolished with the new BSIG. The risk of a wrong decision therefore rests with the operator.

Which products count as critical components is laid down by statutory ordinance – to date mainly for telecommunications and, in part, for energy. Video technology is not expressly covered (as at November 2026), but the scope can be extended to all KRITIS sectors. Internationally, developments have moved further: in the USA, the world's two largest Chinese camera manufacturers are on the FCC's "Covered List"; since 16 July 2026 the restriction has also applied to older models that were already authorised.

Recommendation: Document the manufacturer's origin and control risk in the risk analysis. Prefer components with a transparent ownership structure, transparent firmware, long-term support within the EU and no mandatory cloud services in third countries – this avoids a forced replacement during the service life and problems with third-country transfers under Art. 44 et seq. GDPR.

Manufacturer independence as a security factor

SecuConCept maintains no commission or sales relationships with manufacturers. Components are selected solely on the basis of protection objective, IT security, supply chain risk, maintainability and cost-effectiveness – an advantage when you have to justify procurement decisions to supervisory authorities, auditors or executive management.

ARC · ALARM VERIFICATION · RESPONSE

05 Remote Monitoring via the Alarm Receiving Centre

With remote video monitoring, cameras and detectors transmit alarm events together with live and event images to an alarm receiving and service centre (ARC). Trained operators there assess the situation within seconds and trigger the agreed chain of measures.

5.1 How an alarm unfolds

1	**Detection**	Analytics or a detector reports an event in a defined zone (e.g. fence line, vehicle entrance).
2	**Transmission**	The alarm, event sequence and live stream reach the ARC via an encrypted, supervised connection.
3	**Verification**	The operator checks: genuine alarm, nuisance alarm or technical alarm? Camera tracking via PTZ.
4	**Audio challenge**	Optionally via on-site loudspeakers – in practice one of the most effective ways to make intruders abandon the attempt.
5	**Response**	Alerting of the alarm response service, police and the operator's on-call staff in line with the alarm response plan.
6	**Documentation**	A complete event log with timestamps – the basis for reports under § 18 KRITISDachG / § 32 BSIG and for insurers.

5.2 Quality requirements for the ARC and response service

Criterion	Requirement / standard	What to look for
Alarm receiving centre	DIN EN 50518, VdS approval (VdS 3138)	Ask to see the certificate with its scope and validity; redundant operation, emergency power
ARC staff	§ 34a German Trade Regulation Act (GewO), training records	24/7 staffing, four-eyes principle for critical decisions
Alarm response service	§ 34a GewO, DIN 77200 (security services)	Contractually guaranteed on-site response time, key management, knowledge of the site
Alarm response plan	Site-specific, in writing	Escalation levels, contact details, sign-off by the operator, regular updates
Data protection	Art. 28 GDPR	Processor agreement with the ARC and monitoring provider, evidence of technical and organisational measures
Reporting	SLA metrics	Number of alarms, false alarm rate, reaction times, availability – monthly

5.3 Key points for contract and SLA

Remote monitoring services are only as good as the contract behind them. The following points should be governed in measurable terms – they also serve as evidence for supervisory authorities and auditors under § 13 KRITISDachG:

- **Operator reaction time:** the time from alarm receipt to assessment by the operator, with monthly evidence
- **On-site response time:** an agreed maximum travel time per site and rules for exceptions (weather, major incidents)
- **Availability and failure reporting:** monitoring of transmission paths, notification of image or connection loss within minutes
- **Alarm response plan and escalation:** sign-off by the operator, updates whenever staff or phone numbers change, annual exercise
- **Data protection and data access:** processor agreement, storage locations, access rights, release of recordings to authorities
- **Reporting deadlines:** incident reports delivered early enough for the operator to meet the 24-hour report under § 18 KRITISDachG

> **How SecuConCept works**
>
> The alarm receiving centre used is certified to DIN EN 50518 / VdS and built with full redundancy. SecuConCept delivers response services nationwide through vetted specialist companies of its own **SecuNET** partner network – currently more than 350 member companies working to uniform quality requirements. Your contract partner is always SecuConCept: one point of contact, one alarm response plan, one reporting system.

LEGAL BASIS · TRANSPARENCY · STORAGE · DPIA

06 Data Protection and the GDPR

Critical facilities are no exception: video surveillance processes personal data. KRITIS status considerably strengthens the security interest in the balancing test – but the formal requirements of the GDPR remain fully in force.

6.1 Legal basis

Operator	Legal basis	Note
Private companies (e.g. network operators, logistics, private hospitals)	Art. 6(1)(f) GDPR (legitimate interest)	According to the DSK and the Federal Administrative Court, § 4 BDSG does not apply to non-public bodies
Public bodies at federal level	§ 4 BDSG in conjunction with Art. 6(1)(e) GDPR	Justify by reference to the body's tasks and necessity
Municipal and state institutions (e.g. publicly operated municipal utilities, water boards)	The relevant state data protection act	Check the legal form: municipal utilities organised as a GmbH are generally non-public bodies
Employees within the coverage area	Art. 6(1)(f) GDPR or works agreement (Art. 88 GDPR)	Following ECJ C-34/21 (30 March 2023), the reliability of § 26(1) BDSG is disputed

The balancing of interests proceeds in three stages: (1) name the legitimate interest in concrete terms (e.g. protection against sabotage, documented incidents, the statutory resilience obligation); (2) examine necessity – are there milder means that are equally effective?; (3) weigh up the interests of the data subjects, in particular their reasonable expectations (Recital 47 GDPR).

6.2 The key obligations at a glance

Obligation	Provision	Implementation in practice
Transparency / signage	Art. 12, 13 GDPR	Signage placed before people enter the coverage area (DSK template) plus a complete information sheet
Storage limitation	Art. 5(1)(e), Art. 17	DSK default: max. 72 hours; justify longer periods separately (e.g. unstaffed facilities, weekends)
Data protection impact assessment	Art. 35 GDPR	Regularly required for systematic, extensive surveillance; complete before commissioning
Record of processing activities	Art. 30 GDPR	Dedicated entry "video surveillance / remote monitoring" including the ARC as recipient
Processing on behalf of the controller	Art. 28 GDPR	Processor agreements with the ARC, the installer (for remote maintenance) and cloud/VMS providers

Obligation	Provision	Implementation in practice
Technical and organisational measures	Art. 32 GDPR	Encryption, access rights, logging, deletion routines – congruent with § 30 BSIG
Data subject rights	Art. 15–21 GDPR	Define processes for access and erasure requests; mask third parties before releasing footage
Data protection by design	Art. 25 GDPR	Privacy-zone masking, limit the coverage area to your own premises

6.3 Special situations

- **Public space and neighbouring properties:** mask out as a rule. Exception: a narrow strip along the property boundary, where strictly necessary for perimeter protection and duly justified.
- **Employees:** no performance or behaviour monitoring; break, social and sanitary areas are off limits. Where a works council exists, it has co-determination rights (§ 87(1) no. 6 Works Constitution Act (BetrVG)) – conclude a works agreement early.
- **Hospitals:** patient and treatment areas are generally excluded; a person's mere presence there can itself constitute health data.
- **Audio recordings:** prohibited (§ 201 German Criminal Code (StGB)). Loudspeakers for the audio challenge are permitted; microphones are not.
- **Biometrics and AI:** object and movement classification is far less critical than facial recognition. Biometric identification is conceivable only in narrow exceptions under Art. 9 GDPR and the AI Act.
- **Dummy cameras:** camera dummies create a perception of surveillance and may likewise be unlawful; in a KRITIS context they also offer no protective effect.

> **Risk of fines**
>
> Infringements of the GDPR can be penalised with fines of up to €20 million or 4 % of worldwide annual turnover (Art. 83 GDPR). The objections most frequently raised by supervisory authorities: missing or incomplete signage, excessive storage periods, coverage of public areas, and a lack of documentation of the balancing of interests.

GUIDE VALUES · INVESTMENT · OPERATION

07 Cost Examples and Economics

The following examples show typical cost structures. They are intended for budget planning and do not replace a site-specific quotation. All figures are net at 2026 market level; actual costs depend on perimeter length, civil works, infrastructure, protection objective and response distance.

Example A – waterworks / elevated tank, perimeter approx. 400 m (fixed installation)

Item	Qty	Unit price	Total
Security concept, planning, DPIA support	flat rate		€4,500
Thermal imaging camera with perimeter analytics	6	€3,200	€19,200
IR dome camera (identification at the access road)	2	€900	€1,800
Masts, foundations, civil works	flat rate		€12,000
Network (fibre optics, switches), UPS	flat rate		€6,500
Recorder / video management incl. licences	1	€4,800	€4,800
Installation, commissioning, analytics calibration	flat rate		€7,200
Total investment (net)			**€56,000**

Annual operating costs	Calculation	Amount
Remote video monitoring by the ARC (8 channels, analytics-based)	€390 × 12 months	€4,680
Maintenance and inspection (twice a year)	flat rate	€1,800
Alarm responses (assumption: 12 call-outs)	12 × €145	€1,740
Depreciation of investment (5 years, straight-line)	€56,000 ÷ 5	€11,200
Total annual costs		**€19,420**

Equivalent to around €1,618 per month, or around €53 per day, for 24/7 protection of the perimeter.

Example B – solar farm or construction site, 12 months of mobile camera towers

Item	Calculation	Amount
Hire of self-sufficient camera towers incl. monitoring connection	6 towers × €890 × 12 months	€64,080
Transport, set-up, configuration, removal	6 × €450	€2,700
Total cost for the project period (net)		**€66,780**

Mobile solutions are suitable for construction phases, interim protection until a fixed installation is in place, and short-term increases in the threat level. From a service life of around two to three years, a fixed installation is usually more economical – calculate case by case.

Example C – comparison with 24/7 manned guarding

Model	Calculation	Cost per year
Manned guarding 24/7, 1 security officer (assumption €32/h)	8,760 h × €32	€280,320
Video surveillance with remote monitoring (Example A)	see above	€19,420
Hybrid: Example A + mobile patrols (2 checks per night at €28 each)	€19,420 + 365 × 2 × €28	€39,860

> **Devil's advocate: the comparison is not an equation**
>
> The difference of around €260,900 per year between manned guarding and the video model is real, but the services are not identical: a security officer on site can control access, fight fires at an early stage and intervene immediately. Video with remote monitoring excels at large, unstaffed areas, uninterrupted attention and documentation. For many KRITIS facilities, the hybrid model is the strongest solution both professionally and economically. What matters is deriving the choice from the risk analysis under § 12 KRITISDachG.

Cost drivers to clarify early

- Civil works and power supply to masts (often 20–35 % of the investment)
- Network connection: existing fibre-optic infrastructure or mobile radio with a backup path
- Number of detection zones and false-alarm behaviour (vegetation, wildlife, water surfaces)
- Response distance and the agreed on-site response time
- Integration into existing control-room, access-control and alarm systems

FROM RISK ANALYSIS TO ROUTINE OPERATION

08 Project Checklist for Operators

The checklist follows the proven sequence of a KRITIS security project. It serves as a working basis for internal coordination, tendering and evidence towards supervisory authorities and auditors.

Phase 1 – Analysis	
☐	Check applicability: KRITIS Umbrella Act (sector, threshold) and BSI Act (§ 28) – document the result
☐	Risk analysis under § 12 KRITISDachG: threats, vulnerabilities, incident history
☐	Define protection objectives per area (Detect, Recognise, Identify)
☐	Record existing technology, infrastructure and contracts

Phase 2 – Concept	
☐	Security concept with security chain and time budget (barrier vs. response time)
☐	Camera concept to DIN EN 62676-4 with site plan and coverage areas
☐	Data protection: balancing of interests, DPIA, deletion concept, signage, entry in the record of processing activities
☐	Involve the works council and the data protection officer
☐	IT security concept: segmentation, encryption, patch management, supply chain

Phase 3 – Procurement and implementation	
☐	Draft the specification manufacturer-independently (function instead of product)
☐	Request evidence: DIN EN 50518 / VdS, § 34a GewO, references, data processing agreement
☐	Check manufacturer origin and third-country risk (§ 41 BSIG); document support period and data flows
☐	Installation, analytics calibration, test of all alarm paths incl. backup path
☐	Draw up the alarm response plan and have it approved by the operator

Phase 4 – Routine operation and evidence	
☐	Trial operation with false-alarm optimisation (4–6 weeks)
☐	Monthly reporting: alarms, reaction times, availability
☐	Maintenance, firmware updates, annual exercise of the alarm and reporting procedure
☐	Update the resilience plan and risk analysis (at least every 4 years)

SHORT, RELIABLE ANSWERS

09 Frequently Asked Questions (FAQ)

Is video surveillance a legal requirement for KRITIS operators?

No, not explicitly. § 13 KRITISDachG requires suitable and proportionate measures for physical protection and cites instruments for monitoring the surroundings and detection equipment as examples. Whether video is the appropriate instrument follows from the risk analysis.

From when must operators register under the KRITIS Umbrella Act?

No later than three months after classification as a critical facility. Classification depends on the KRITIS ordinance which, to our knowledge (November 2026), is not yet in force. The earlier deadline of 17 July 2026 was repealed.

How long may video recordings be stored?

In the view of the German Data Protection Conference, as a rule up to 72 hours. Longer storage is possible where specifically justified and documented – for instance at unstaffed facilities that are only checked at longer intervals.

What is the difference between video surveillance and remote video monitoring?

Video surveillance records. Remote video monitoring transmits alarms and live images to a permanently staffed monitoring centre, which verifies the situation and triggers the response. Only the monitoring connection prevents offences instead of merely documenting them.

Is a data protection impact assessment required?

For systematic, extensive surveillance – typical of KRITIS perimeters – as a rule yes (Art. 35 GDPR). It must be completed before commissioning.

May cameras cover the pavement in front of the site?

In principle, no. Public areas must be masked out; at most, a narrow strip along the property boundary may be permissible where strictly necessary.

Which certification should the monitoring centre hold?

Certification as an alarm receiving centre to DIN EN 50518, ideally with VdS approval. Ask to see the certificate, its scope and its validity.

What does remote video monitoring cost per month?

Depending on the number of channels, the analytics and the scope of service, typically a few hundred euros per site per month, plus alarm responses. A worked example is provided in Chapter 7.

SECURITY · CONSULTING · CONCEPTION

10 Your Partner for KRITIS Security

SecuConCept combines manufacturer-independent security consulting, security concept design and operational delivery from a single source – nationwide across Germany, personally coordinated.

Consulting	Conception	Security
Risk analysis, applicability checks under KRITISDachG/BSIG, data protection support, tender support	Security concepts to DIN EN 62676-4, perimeter and monitoring concepts, alarm response plans, resilience building blocks	Remote video monitoring, alarm response, site and plant security, mobile patrols, mobile video surveillance & camera towers

Why SecuConCept?

- **SecuNET by SecuConCept:** more than 350 specialised security companies nationwide – regional expertise, scalable project delivery, uniform quality requirements.
- **One contractual partner:** even where SecuNET partners deliver on site, SecuConCept remains your contractual partner and responsible coordinator.
- **Manufacturer-independent:** no commission or sales relationships with manufacturers – the technology follows your protection objective.
- **Certified and field-proven:** redundant alarm receiving centre to DIN EN 50518 / VdS, experience from plant security at major chemical and industrial sites.
- **Sustainably organised:** company-wide electric mobility, our own photovoltaic system and “upgrade instead of replace” for hardware – existing cameras are assessed and, where appropriate, kept in service.

Portals and brands

SecuFokus – SICHERHEIT GEMEINSAM STEUERN. – BY SECUCONCEPT

SecuFokus by SecuConCept – managing security together.
Specialist information and tools that enable operators, partners and service providers to manage security processes jointly and transparently.

CCTV-SECURITY.DE – VIDEOTÜRME | ALARMZENTRALE | ALARMVERFOLGUNG | REALISIERUNG – by SecuConCept

CCTV-Security.de by SecuConCept – specialist portal for video towers, alarm centre services, alarm response and the delivery of video surveillance solutions.

FREE INITIAL CONSULTATION

KRITIS check for your facility

Applicability, protection objectives, video concept and data protection – in one structured meeting with a clear recommendation for action.

0800 666 000 4 (nationwide, free of charge) · **0221 954 917 52** (Cologne)
vertrieb@secuconcept.de · www.secuconcept.de
SecuConCept · Owner: Torsten Bentlage · Adolf-Grimme-Allee 3 · 50829 Cologne, Germany

FOR REFERENCE

11 Sources, Standards and Legal Status

Legal sources

- Act implementing Directive (EU) 2022/2557 and strengthening the resilience of critical facilities (KRITIS Umbrella Act – KRITIS-Dachgesetz) of 11 March 2026, BGBl. 2026 I Nr. 66; § 8 amended by the Act of 21 July 2026, BGBl. 2026 I Nr. 221
- NIS-2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG), in force since 6 December 2025; BSI Act (BSIG), new version
- Regulation (EU) 2016/679 (GDPR); Federal Data Protection Act (BDSG); state data protection acts
- ECJ, judgment of 30 March 2023, C-34/21 (employee data protection)
- Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2024/2847 (Cyber Resilience Act)
- § 34a German Trade Regulation Act (GewO), Security Industry Ordinance; § 87 Works Constitution Act (BetrVG); § 201 German Criminal Code (StGB)
- § 41 BSIG (prohibition of the use of critical components), formerly § 9b BSIG (old version); US Federal Communications Commission (FCC): Covered List under the Secure Equipment Act

Standards and guidelines

- DIN EN 62676 (series) – video surveillance systems for security applications, in particular Part 4: application guidelines
- DIN EN 50518 – alarm receiving centre (ARC)
- VdS 3138 – alarm receiving and service centres; VdS guidelines for video surveillance systems
- DIN 77200 – security services

Official guidance

- German Data Protection Conference (DSK): guidance on video surveillance by non-public bodies (2020) incl. model signage; DSK short paper No. 15
- Federal Office of Civil Protection and Disaster Assistance (BBK): information and FAQ on the KRITIS Umbrella Act – www.bbk.bund.de
- Federal Office for Information Security (BSI): NIS-2 information and reporting/registration portal – www.bsi.bund.de

Legal status and liability: research status November 2026. At that time, the KRITIS ordinance under the KRITIS Umbrella Act was available as a ministerial draft; specific thresholds and deadlines may change. This handbook does not constitute legal advice. Cost figures are non-binding guide values (net) based on typical project assumptions.

© 2026 SecuConCept · Owner: Torsten Bentlage · Redistribution in unaltered form is expressly welcome.