As of: November 2026

SPECIALIST MANUAL

COMPLETE EDITION · FIVE SPECIALIST MANUALS IN ONE VOLUME

Complete Manual of Security Services

The specialist manual for companies, operators and KRITIS

SPECIALIST PORTALS AND BRANDS OF SECUCONCEPT

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

SecuFokus®
SICHERHEIT GEMEINSAM STEUERN.
BY SECUCONCEPT

A Video Surveillance & Video Alarm Monitoring KRITIS · B Alarm Monitoring, Alarm Response & Prevention
C Guarding or Plant Security · D Reception & Gatekeeper Services
E KRITIS: Security Services as an All-in-One Solution? · List of Sources

Quality through Trust

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

ABOUT THIS MANUAL

Five specialist manuals, one volume

Security is created by the interplay of law, technology, the monitoring center and people on site. This complete manual consolidates the five SecuConCept specialist manuals into a single reference work – with continuous chapter numbering, cross-references between the parts and a shared list of sources.

How to use this manual

Part	Topic	Particularly relevant for
A	Video Surveillance & Video Alarm Monitoring for KRITIS	Operators of critical facilities, technical management, data protection
B	Alarm Monitoring, Alarm Response & Prevention	Facility and security management, branch and site managers
C	Guarding or Plant Security	Executive management, plant and site management, procurement
D	Reception & Gatekeeper Services	Office and site management, facility management, data protection
E	KRITIS: Security Services as an All-in-One Solution?	Executive management of KRITIS companies, contracting authorities

- **Chapter numbers** combine part and chapter: **B3** is Chapter 3 in Part B, **B3.6** the section within it.
- **Cross-references** are underlined in green and clickable in the PDF; so are the table of contents and the bookmarks.
- **Each part** opens with a divider page showing its chapters and the related parts.
- **Cost examples** build on one another: the collectively agreed model rate from Chapter C7 is applied in Chapter D8 and Chapter E8.

> **Important notice on legal validity**
>
> This manual provides professional orientation and does not replace legal, tax or procurement advice. Laws, regulations, collective agreements and official interpretations change – in particular the KRITIS Regulation, which had not yet entered into force as of the research date (November 2026). The assignment of individual activities to German security-industry licensing law is decided by the competent trade office (Gewerbeamt). All cost figures are model calculations and non-binding reference values (net) and do not replace a site-specific quotation.

Contents

Part A · Video Surveillance & Video Alarm Monitoring for KRITIS-Relevant Facilities 5

A1 At a Glance 6

A2 The KRITIS Legal Framework 2026 7

A3 Video Surveillance in the Resilience Concept 10

A4 Technology, Standards and Cybersecurity 12

A5 Video Alarm Monitoring via the Monitoring Center 14

A6 Data Protection and the GDPR 16

A7 Cost Examples and Economic Viability 18

A8 Project Checklist for Operators 20

A9 Frequently Asked Questions (FAQ) 21

Part B · Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection 22

B1 At a Glance 23

B2 Hazard Alarm Systems and Monitoring Connection 24

B3 Monitoring Center and Alarm Response 27

B4 The Client's Duties to Cooperate 30

B5 Preventive Hazard Protection 32

B6 Law, Liability and Data Protection 33

B7 Cost Examples and Economic Viability 34

B8 Checklist for Clients 36

B9 Frequently Asked Questions (FAQ) 37

Part C · Security Services in Practice: Guarding or Plant Security 38

C1 At a Glance 39

C2 Guarding and Plant Security 40

C3 Law, Qualifications and Occupational Safety 42

C4 In-House Staff or Service Provider 44

C5 Practice on Site 46

C6 Quality and Contract Award 48

C7 What an Hour of Security Costs 49

C8 Checklist for Clients 51

C9 Frequently Asked Questions (FAQ) 52

Part D · Reception & Gatekeeper Services – Controlled Entry 53

D1 At a Glance 54

D2 Reception, Gatehouse, Factory Gate 55

D3 Access and Entry Control 56

D4 Law and Data Protection at Reception 57

D5 Emergencies, Threats and De-escalation 59

D6 Staff, Quality and Cooperation 60

D7 Technology at Reception 61

D8 Cost Examples and Economic Viability 62

D9 Checklist for Clients 63

D10 Frequently Asked Questions (FAQ) 64

Part E · KRITIS: Security Services as an All-in-One Solution? 65

E1 At a Glance 66

E2 What KRITIS Operators Must Demonstrate 67

E3 What “All-in-One” Means 68

E4 Opportunities of an Integrated Solution 69

E5 Risks and Limits 70

E6 Criteria for a Resilient Model 71

E7 Contract Award: Private and Public 72

E8 Cost Example and Economic Viability 73

E9 Decision Aid and Checklist 74

E10 Frequently Asked Questions (FAQ) 75

SecuConCept: Integrated and Independent 76

List of Sources 77

PART A

Video Surveillance & Video Alarm Monitoring for KRITIS-Relevant Facilities

The legal framework under the KRITIS Umbrella Act and the BSIG, technology and standards, video alarm monitoring via a monitoring center, data protection and cost examples for operators of critical facilities.

CHAPTERS

A1 At a Glance
A2 The KRITIS Legal Framework 2026
A3 Video Surveillance in the Resilience Concept
A4 Technology, Standards and Cybersecurity
A5 Video Alarm Monitoring via the Monitoring Center
A6 Data Protection and the GDPR
A7 Cost Examples and Economic Viability
A8 Project Checklist for Operators
A9 Frequently Asked Questions (FAQ)

RELATED PARTS

Part B Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection – monitoring connection and monitoring center

Part E KRITIS: Security Services as an All-in-One Solution? – legal framework and service-provider model

KEY STATEMENTS FOR DECISION-MAKERS

A1 At a Glance

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

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

2 **Concrete obligations depend on the KRITIS Regulation.** Thresholds and deadlines are set by a statutory regulation 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 was deleted.

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

4 **Incidents must be reported within 24 hours** (§ 18 KRITISDachG); a detailed report follows no later than one month afterwards. Complete video documentation makes both easier.

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

6 **NIS-2 / BSIG since 6 December 2025:** network cameras, recorders and video management are IT systems and belong in the risk management required by § 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 **Monitoring connection instead of mere recording:** only live verification in a monitoring center certified to DIN EN 50518 turns images into a response – with a defined intervention chain.

9 **Planning to DIN EN 62676-4:** the protection objective per camera (detect, recognize, identify) determines resolution, lens and location.

10 **Economical:** depending on the site, a monitored perimeter solution often costs only a fraction of 24/7 on-site guarding – but does not replace it in every scenario (see Chapter A7).

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

A2 The KRITIS Legal Framework 2026

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

A2.1 The 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 KRITISDachG	
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, evidence and reporting obligations largely do not apply, as special rules take precedence. [2] Here, essentially the duty to conduct a risk analysis remains. The standard threshold is a supply of around 500,000 people; the sector-specific values of the KRITIS Regulation 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 needed, 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
Executive management’s duty to implement and supervise	§ 20	after 10 months
Fines	§ 24	graduated, up to €1 million

Current status (November 2026)

The fixed registration deadline of 17 July 2026 was deleted 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 Regulation is not in force. **Recommendation:** the deadlines run very short once it enters into force. Operators who prepare their risk analysis and protection concept now avoid procurement bottlenecks and time pressure during tendering, permitting and installation.

§ 13 KRITISDachG – resilience measures relating to video surveillance

§ 13 obliges operators to take suitable and proportionate technical, security-related and organizational measures. One of the aims is adequate physical protection of the properties. Paragraph 3 names, by way of example:

- Site protection through property perimeter demarcation (fences, barriers)
- Instruments and procedures for monitoring the surroundings – this covers video surveillance including perimeter detection
- Detection devices 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 way (§ 13 para. 4). A written security concept with protection objectives, a threat analysis and a justification for each camera is therefore not only data protection evidence but also KRITIS evidence.

A2.2 The BSI Act after NIS-2 (NIS2UmsuCG)

The NIS-2 Implementation Act recast the BSIG and has applied since 6 December 2025 without any transition period. Around 29,500 companies fall under the supervision of the BSI 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 are part of 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 supervision 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 example where the manufacturer is controlled by the government of a third country. Manufacturer selection is therefore also a compliance issue (see Chapter A4.3).
- **§ 65 BSIG – fines:** up to €10 million or 2 % of worldwide annual turnover (particularly important entities).

A2.3 Other relevant rules

Set of rules	Relevance for video & monitoring connection
GDPR / Federal Data Protection Act (BDSG) / state data protection acts	Lawfulness, transparency, retention periods, DPIA – see Chapter A6
§ 34a GewO (German Trade Regulation Act), Security Guarding Ordinance (BewachV)	Licensing and qualification requirements for guarding and intervention personnel
§ 201 StGB (German Criminal Code)	Prohibition of covert audio recording – operate cameras without audio recording
§ 87 para. 1 no. 6 BetrVG (Works Constitution Act)	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 networked products (phased application until 2027)
Building regulations / grid operator requirements	Masts, foundations, cable routing, permits in protection zones where applicable

Cross-references

- → E2 What KRITIS Operators Must Demonstrate
- → E7 Contract Award: Private and Public

PROTECTION OBJECTIVES · SECURITY CHAIN · LIMITS

A3 Video Surveillance in the Resilience Concept

Cameras do not protect – processes protect. Video surveillance only becomes effective as a link in a closed security chain of deterring, detecting, verifying, responding and documenting.

A3.1 The security chain

Deter	Detect	Verify	Respond	Document
Fence, gates, lighting, bollards	Video analytics, thermal imaging, detectors	Live image in the monitoring center (NSL), live audio challenge	Intervention, police, operator on-call service	Event log, preservation of evidence, report under § 18

Marked in green: core tasks of video surveillance with a monitoring connection.

The decisive factor is the time budget: the time an offender needs to overcome the barriers must be greater than the sum of detection, verification and intervention time. Video surveillance shortens detection and verification to seconds; the intervention time remains a question of organization and regional availability.

Worked example: the time budget

Phase	Without monitoring connection	With video alarm monitoring
Detection of the intrusion	by chance, often only at the start of the working day	under 10 seconds (perimeter analytics)
Verification	not applicable	30–90 seconds (operator in the monitoring center)
First countermeasure	none	live audio challenge after around 2 minutes
Arrival of intervention / police	hours to days after the offence	within the agreed intervention time, e.g. 15–30 minutes
Result	**damage is discovered after the fact**	**the offence is disrupted, aborted and seamlessly documented**

The values are typical practical figures, not a guarantee. They show: the longer fences, gates and the building shell hold an offender up, the more likely the intervention arrives while the offence is still in progress. Barriers and monitoring connection must therefore be planned together.

A3.2 Typical protection objectives in KRITIS facilities

Type of facility	Main risks	Video focus
Substations, grid stations	Sabotage, non-ferrous metal / cable theft, arson	Perimeter detection with thermal imaging, access roads, transformer areas
Waterworks, elevated tanks, pumping stations	Tampering, unauthorized 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	Emergency admission access, technical centers, medication stores (no patient areas)
Logistics, ports, transport hubs	Cargo theft, intrusion, sabotage	Gates, ramps, open areas, licence-plate capture only with a legal basis
Data centers, telecoms sites	Sabotage, access, theft of components	Perimeter, security airlocks, access control with video verification

Advocatus Diaboli: where video reaches its limits

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

DIN EN 62676 · DETECTION · IT SECURITY

A4 Technology, Standards and Cybersecurity

The quality of a video 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 manufacturer specifications apply in addition.

A4.1 Resolution levels under DIN EN 62676-4

A protection objective is defined for each camera. From this follows the required pixel density at the target location, measured in pixels per meter (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	Roughly track movements 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 technical areas
Recognize	125 px/m	Recognize a known person	Entrances, gates, security airlocks
Identify	250 px/m	Identify a person beyond doubt	Access-road control, main entrance
Inspect	1,000 px/m	Finest details, e.g. lettering	Special cases, licence-plate / detail shots

A4.2 Detection technologies compared

Technology	Strengths	Limits
Thermal imaging camera with analytics	Night vision without lighting, 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/vehicles, colour information by day	IR range limited, more weather-sensitive
PTZ / speed dome	Tracking by the monitoring center, zoom for verification	only one field of view at a time; never the sole means of detection
Radar / fence detection (supplementary)	Weather-independent detection, camera slewing	additional integration and calibration
Mobile, self-sufficient camera towers	Quickly available, construction phases, interim protection, solar/battery	dependence on power and mobile network, vandalism risk

A4.3 Cybersecurity of the video system

Networked cameras are a well-known gateway into corporate networks. For operators covered by the BSIG, the following measures are 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 monitoring center (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
- Supervision of the transmission paths (line monitoring, back-up path via LTE/5G) and tamper alarms on image loss or camera displacement

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 reasons, 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 “approved 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 lies with the operator.

Which products count as critical components is determined by a statutory regulation – so far mainly for telecommunications and, in part, for energy. Video technology is not explicitly covered (as of November 2026), but the scope can be extended to all KRITIS sectors. Internationally, developments are further along: 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, previously approved models.

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 in the EU and no mandatory cloud 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 economic viability – an advantage when you have to justify procurement decisions to supervisory authorities, auditors or executive management.

MONITORING CENTER (NSL) · ALARM VERIFICATION · INTERVENTION

A5 Video Alarm Monitoring via the Monitoring Center

With video alarm monitoring, cameras and detectors transmit alarm events together with live and event images to an emergency call and service monitoring center (Notruf- und Serviceleitstelle, NSL). There, trained operators assess the situation in seconds and trigger the agreed chain of measures.

A5.1 Sequence of an alarm

1	**Detection**	Analytics or a detector reports an event in a defined zone (e.g. fence line, access road).
2	**Transmission**	Alarm, event sequence and live stream reach the monitoring center encrypted and supervised.
3	**Verification**	The operator checks: genuine alarm, deceptive alarm or technical alarm? Camera tracking via PTZ.
4	**Audio challenge**	Optionally via on-site loudspeakers – in practice one of the most effective means of aborting an offence.
5	**Intervention**	Alerting of the intervention service, police and the operator's on-call service according to the alarm plan.
6	**Documentation**	Seamless event log with timestamps – the basis for reports under § 18 KRITISDachG / § 32 BSIG and for insurers.

A5.2 Quality requirements for monitoring center and intervention

Criterion	Requirement / standard	What to look for
Alarm receiving center	DIN EN 50518, VdS approval (VdS 3138)	Have the certificate with scope and validity presented; redundant operation, emergency power
Monitoring center staff	§ 34a GewO, training records	24/7 staffing, four-eyes principle for critical decisions
Intervention service	§ 34a GewO, DIN 77200 (security services)	Contractually guaranteed intervention time, key management, site knowledge
Alarm plan	Site-specific, in writing	Escalation levels, contact availability, approval by the operator, regular updating
Data protection	Art. 28 GDPR	Data processing agreement with the monitoring center and connection provider, evidence of TOMs
Reporting	SLA metrics	Number of alarms, false-alarm rate, response times, availability – monthly

A5.3 Key points for contract and SLA

Video alarm monitoring services are only as good as their contractual safeguards. The following points should be governed measurably in the contract – they also serve as evidence towards supervisory authorities and auditors under § 13 KRITISDachG:

- **Response time of the monitoring center:** time from alarm receipt to assessment by the operator, with monthly evidence
- **Intervention time:** agreed maximum travel time per site and rules for exceptions (weather, major incidents)
- **Availability and outage reporting:** supervision of the transmission paths, notification of image or connection loss within minutes
- **Alarm plan and escalation:** approval by the operator, upkeep on staff or number changes, annual exercise
- **Data protection and data access:** data processing agreement, storage locations, access rights, release of recordings to authorities
- **Reporting deadlines:** incident report delivered early enough for the operator to meet the 24-hour report under § 18 KRITISDachG

How SecuConCept works

The alarm receiving center used is certified to DIN EN 50518 / VdS and built redundantly. SecuConCept carries out interventions throughout Germany with vetted specialist companies of its own SecuNET business network – currently more than 350 member companies with uniform quality requirements. Your contractual partner always remains SecuConCept: one point of contact, one alarm plan, one reporting system.

Cross-references

→ B2 Alarm Transmission to DIN EN 50136
→ B3 Monitoring Center and Alarm Response

LEGAL BASIS · TRANSPARENCY · RETENTION · DPIA

A6 Data Protection and the GDPR

Even at critical facilities, video surveillance processes personal data. KRITIS status considerably strengthens the security interest in the balancing exercise – but the formal requirements of the GDPR remain fully in place.

A6.1 Legal basis

Operator	Legal basis	Note
Private companies (e.g. grid operators, logistics, private clinics)	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 of the Federation	§ 4 BDSG in conjunction with Art. 6(1)(e) GDPR	Justify task relevance and necessity
Municipal / state institutions (e.g. municipal utilities as a public enterprise, water boards)	respective state data protection act	Check the legal form: municipal utilities organized as a GmbH are generally non-public bodies
Employees within the coverage area	Art. 6(1)(f) or works agreement (Art. 88 GDPR)	Following ECJ C-34/21 (30 March 2023), the viability of § 26(1) BDSG is disputed

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

A6.2 The central obligations at a glance

Obligation	Rule	Practical implementation
Transparency / information sign	Art. 12, 13 GDPR	Sign placed before entering the coverage area (DSK template) plus a complete information sheet
Storage limitation	Art. 5(1)(e), Art. 17	DSK standard: 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; carry out before commissioning
Record of processing activities	Art. 30 GDPR	Dedicated entry “video surveillance / monitoring connection” including the monitoring center as recipient
Processing on behalf	Art. 28 GDPR	Data processing agreement with the monitoring center, installer (for remote maintenance) and cloud/VMS provider

Obligation	Rule	Practical implementation
Technical and organizational measures	Art. 32 GDPR	Encryption, access rights, logging, deletion routines – congruent with § 30 BSIG
Data subject rights	Art. 15–21 GDPR	Define an access and deletion process; mask third parties before release
Data protection by design	Art. 25 GDPR	Privacy-zone masking, limit the coverage area to the operator's own premises

A6.3 Special situations

- **Public space and neighbouring properties:** mask out as a rule. Exception: a narrow strip along the property line, insofar as strictly necessary and justified for perimeter protection.
- **Employees:** no performance or behaviour monitoring; break, social and sanitary areas are off-limits. Where a works council exists, co-determination applies (§ 87 para. 1 no. 6 BetrVG) – conclude a works agreement early.
- **Hospitals:** patient and treatment areas are regularly excluded; even someone's presence can constitute health data.
- **Audio recording:** not permitted (§ 201 StGB). Loudspeakers for the audio challenge are permitted, microphones are not.
- **Biometrics and AI:** object and movement classification is 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 surveillance pressure and can likewise be unlawful; in the KRITIS context they also provide no protection.

> **Risk of fines**
>
> Infringements of the GDPR can be penalized with up to €20 million or 4 % of worldwide annual turnover (Art. 83 GDPR). The supervisory authorities' most frequent complaints: missing or incomplete signage, excessive retention periods, coverage of public areas and missing documentation of the balancing of interests.

REFERENCE VALUES · INVESTMENT · OPERATION

A7 Cost Examples and Economic Viability

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

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

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

Running costs per year	Calculation	Amount
Video alarm monitoring NSL (8 channels, analytics-based)	390 € × 12 months	4,680 €
Maintenance and inspection (2 × per year)	lump sum	1,800 €
Interventions (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
Rental of self-sufficient camera towers incl. monitoring connection	6 towers × 890 € × 12 months	64,080 €
Transport, set-up, configuration, dismantling	6 × 450 €	2,700 €
Total costs for the project period (net)		**66,780 €**

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

Example C – comparison with 24/7 staffed guarding

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

> **Advocatus Diaboli: the comparison is not an equation**
>
> The difference of around 260,900 € per year between on-site guarding and the video model is real, but the services are not identical: a security officer on site can manage access, fight fires early and intervene immediately. Video with a monitoring connection scores on 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 it 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 infrastructure or mobile radio with a back-up path
- Number of detection zones and false-alarm behaviour (vegetation, wildlife, water surfaces)
- Intervention distance and agreed intervention time
- Integration into existing control, access and hazard alarm technology

FROM RISK ANALYSIS TO REGULAR OPERATION

A8 Project Checklist for Operators

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

Phase 1 – Analysis	
☐	Check applicability: KRITISDachG (sector, threshold) and BSIG (§ 28) – document the result
☐	Risk analysis under § 12 KRITISDachG: threats, vulnerabilities, incident history
☐	Define protection objectives per area (detect, recognize, identify)
☐	Record existing technology, infrastructure and contracts

Phase 2 – Concept	
☐	Security concept with security chain and time budget (barrier vs. intervention 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	
☐	Write the specification independently of any manufacturer (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. back-up path
☐	Draw up the alarm plan and have the operator approve it

Phase 4 – Regular operation and evidence	
☐	Trial operation with false-alarm optimization (4–6 weeks)
☐	Monthly reporting: alarms, response times, availability
☐	Maintenance, firmware updates, annual exercise of the alarm and reporting procedure
☐	Keep the resilience plan and risk analysis up to date (at least every 4 years)

ANSWERED BRIEFLY AND RELIABLY

A9 Frequently Asked Questions (FAQ)

Is video surveillance legally required for KRITIS operators?

No, not explicitly. § 13 KRITISDachG requires suitable and proportionate measures for physical protection and names instruments for monitoring the surroundings and detection devices as examples. Whether video is the appropriate means 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 Regulation, which to our knowledge (November 2026) is not yet in force. The earlier deadline of 17 July 2026 was deleted.

How long may video recordings be stored?

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

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

Video surveillance records. Video alarm monitoring transmits alarms and live images to a permanently staffed monitoring center, which verifies and triggers measures. Only the monitoring connection prevents offences instead of merely documenting them.

Is a data protection impact assessment necessary?

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 premises?

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

What certification should the monitoring center have?

Certification as an alarm receiving center to DIN EN 50518, ideally with VdS approval. Have the certificate, its scope and its validity presented to you.

What does video alarm monitoring cost per month?

Depending on the number of channels, analytics and scope of services, typically a few hundred euros per site and month plus interventions. A worked example can be found in Chapter A7.

PART B

Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection

Hazard alarm systems and transmission paths, monitoring center and intervention, domiciliary and access rights, the client's duties to cooperate, and prevention.

CHAPTERS

B1 At a Glance
B2 Hazard Alarm Systems and Monitoring Connection
B3 Monitoring Center and Alarm Response
B4 The Client's Duties to Cooperate
B5 Preventive Hazard Protection
B6 Law, Liability and Data Protection
B7 Cost Examples and Economic Viability
B8 Checklist for Clients
B9 Frequently Asked Questions (FAQ)

RELATED PARTS

Part A Video Surveillance & Video Alarm Monitoring for KRITIS-Relevant Facilities – video alarm monitoring
Part C Security Services in Practice: Guarding or Plant Security – intervention officers in practice
Part D Reception & Gatekeeper Services – Controlled Entry – remote gate service and access

KEY STATEMENTS FOR DECISION-MAKERS

B1 At a Glance

The ten most important facts for operators who want to connect hazard alarm systems to a monitoring center, commission alarm response or improve their prevention.

1 **The standards base is clear:** DIN VDE 0833 (hazard alarm systems), DIN EN 50131 (intruder and hold-up alarm systems, Grades 1–4), DIN EN 50136 (alarm transmission), DIN EN 50518 (alarm receiving center).

2 **Grade and class determine the system:** the police recommend Grades 2 to 4 for intruder alarm systems; insurers frequently require VdS-approved systems of classes A, B or C.

3 **Fire alarm systems connected to the fire service** run via the alarm transmission system of the local concession holder in accordance with DIN 14675 – not via a private monitoring center.

4 **Transmission paths age:** the 2G networks will be switched off from 2028. Transmission devices with a GSM-only back-up path must be upgraded in good time.

5 **Alarm response is an intervention service under DIN 77200-1:** agreed measures in reaction to a non-routine event within a defined period.

6 **Security officers have no police powers:** they act on the basis of delegated domiciliary rights and the rights available to every citizen – and without special traffic privileges.

7 **Nothing works without the client's cooperation:** an up-to-date alarm plan, reachable contact persons and trained employees are the most effective remedies against false alarms.

8 **False alarms cost money:** depending on the federal state, fees for police call-outs may be charged; courts have confirmed, for example, 120 € per unjustified alarm.

9 **Prevention first:** mechanical resistance, organization and visible checks prevent offences – alarm and intervention technology limits the damage.

10 **Insurance cover depends on policy obligations:** anyone who fails to arm an agreed intruder alarm system risks reduced payouts (§ 28 VVG, German Insurance Contract Act).

SYSTEM TYPES · GRADES AND CLASSES · CONNECTION TARGETS · TRANSMISSION

B2 Hazard Alarm Systems and Monitoring Connection

Hazard alarm systems (GMA) detect intrusion, hold-up, fire or technical faults and report them to a permanently staffed point. Which point that is, and which requirements apply, depends on the type of report.

B2.1 System types at a glance

System type	Typical reports	Governing rules
Intruder alarm system (EMA)	Opening, climb-through, movement, glass breakage, tampering	DIN EN 50131, DIN VDE 0833-1/-3, VdS 2311
Hold-up alarm system (ÜMA)	Silent alarm, threat, personal emergency signal	DIN EN 50131, DIN VDE 0833-3, ÜEA guideline
Fire alarm system (BMA)	Smoke, heat, manual call points, extinguishing-system activation	DIN EN 54, DIN VDE 0833-2, DIN 14675
Technical alarms	Temperature, water, power failure, cooling, gas	Manufacturer specifications, site-specific definition
Video and perimeter alarms	Fence detection, video analytics, tampering	DIN EN 62676, see Part A

B2.2 Grades under DIN EN 50131 and VdS classes

The DIN EN 50131 series divides intruder and hold-up alarm systems into four grades. In Germany, DIN VDE 0833-1 and -3 supplement it; for insurance-relevant systems, guideline VdS 2311 with classes A to C additionally applies.

Grade	Risk / field of use	VdS class (approx.)	Note
Grade 1	low risk	–	not recommended by the police
Grade 2	low to medium risk, residential, small commercial	Class A	minimum standard for a monitoring connection
Grade 3	medium to high risk, commercial, warehouses	Class B	frequent insurance requirement
Grade 4	high risk, banks, high-value warehouses, special sites	Class C	inspection four times a year

The mapping of grades to VdS classes is an approximation; the insurance contract, the installer's certificate and the planning in the individual case are decisive.

B2.3 Where is the system connected to?

Target	For which reports	Prerequisites
Private emergency call and service monitoring center (NSL)	Intrusion, hold-up, technical, video, faults, armed/disarmed supervision	Contract, alarm plan, key deposit; monitoring center to DIN EN 50518 / VdS 3138
Police (hold-up / intruder alarm system with direct connection)	Hold-up and selected intrusion reports	ÜEA guideline, generally Grade 3 or 4, application and acceptance; varies greatly by region
Fire service (via concession holder)	Fire reports from fire alarm systems required under building law	DIN 14675, fire alarm and alerting concept, fire service connection conditions, key depot

Fire alarm systems: fire service first, monitoring center in addition

Fire reports from fire alarm systems required under building law go via the transmission device to the alarm transmission system of the local concession holder, directly to the fire service. Before installation, a fire alarm and alerting concept under DIN 14675 must be agreed with the fire service. Following a decision of the Federal Cartel Office, the concession may now only cover the receiving equipment at the fire service; the transmission device and transmission path can be chosen freely in open competition.

A private monitoring center can additionally take over fault and status reports and, in the event of fire, organize keys, briefing of the fire service and follow-up – but it does not replace the fire service connection.

B2.4 Alarm transmission to DIN EN 50136

The transmission path is the invisible link of the security chain: if it fails unnoticed, the best system is ineffective. DIN EN 50136-1 distinguishes single-path transmission (SP 1 to SP 6) and dual-path transmission (DP 1 to DP 4). The higher the category, the shorter the supervision intervals and the faster an outage is detected.

Category	Principle	Typical use
SP 1 – SP 3	one transmission path, longer supervision intervals	Residential, small commercial (Grade 2)
SP 4 – SP 6	one transmission path with close supervision	Commercial premises with higher risk
DP 1 – DP 4	primary and back-up path, e.g. fixed IP line plus mobile radio	Grades 3 and 4, branch networks, KRITIS
BMA to the fire service	at least SP 6 or DP 3	per DIN 14675 / connection conditions

B2.5 Fast fault detection

Older dial-up connections need 10 to 15 seconds to establish a connection. Modern, permanently supervised IP connections detect failure or sabotage of the control panel or the transmission device considerably faster; according to the guidance from VdS and BHE, the monitoring center should be informed after no more than 180 seconds. Existing systems should be upgraded to this standard.

2G switch-off: check existing systems now

Telekom intends to switch off its 2G network by 30 June 2028, Vodafone in September 2028 and Telefónica at the end of 2028. Vodafone will keep 2G coverage running for critical applications such as older alarm systems until the end of 2030. Transmission devices whose back-up path only supports GSM will thus lose their second path – often unnoticed until an emergency.

Recommendation: take stock of existing systems, plan transmission paths with LTE/5G and IP, and combine the upgrade with maintenance that is due anyway. The 3G network was already switched off in 2021.

Upgrade instead of replace

Changing the transmission path rarely requires replacing the entire intruder alarm system. Often, swapping the transmission device or adding a module is enough. SecuConCept first checks existing systems for continued use – this saves costs and resources and reduces the ecological footprint.

Relevance to KRITIS

For operators of critical facilities, § 13 of the KRITIS Umbrella Act explicitly names detection devices, access controls and defined alarm procedures as resilience measures. Monitoring connection, alarm plan, intervention and prevention are thus part of the statutory evidence. Details are provided in Part A of this manual, in particular Chapter A2 and Chapter A5.

DIN EN 50518 · DIN 77200-1 · ALARM PLAN · RESPONSE ON SITE

B3 Monitoring Center and Alarm Response

All reports converge in the emergency call and service monitoring center (NSL). It assesses, decides and alerts – around the clock, following an alarm plan agreed with the client.

B3.1 Alarm handling sequence

1	**Receipt**	The report arrives at the monitoring center with site, detector group and timestamp, and is acknowledged.
2	**Assessment**	The operator checks the type of report, its history and, where available, video or audio verification.
3	**Call-back / code word**	Contact with the site or authorized call-back persons; request for the agreed code word.
4	**Alerting**	Intervention service, police or fire service according to the alarm plan; contact persons informed in parallel.
5	**Support**	Guidance of the intervention officer, comparison of the situation, further alerting if required.
6	**Completion**	Log, call-out report, restoration of the armed state, report to the client.

B3.2 Report types and response

Report	Typical response of the monitoring center
Intrusion alarm	Verification, alarm response, immediate police alert where an offence is indicated
Hold-up / silent alarm	no call-back to the site, immediate police alert
Tampering / line fault	Call-back, technical service, alarm response in case of suspicion
Technical alarm	Contact person or on-call service according to the alarm plan, specialist firm if required
Arming supervision	System not armed at the agreed time: call-back, on-site check if required
Disarming outside the agreed times	Code word request, alarm response in case of discrepancy

B3.3 Quality criteria of a monitoring center

- Certification as an alarm receiving center to DIN EN 50518, ideally with VdS approval to VdS 3138
- Redundant technology, emergency power, permanent staffing and a documented fallback solution
- Trained staff with a licence and qualification under § 34a GewO
- Data processing agreement under Art. 28 GDPR and traceable logging
- Monthly reporting: alarms, response times, false-alarm rate, availability

The alarm plan – the most important document

For each type of report, the alarm plan defines who is informed in what order, which measures the monitoring center takes, which code word applies and where keys are kept. It is approved by the client and updated whenever staff or phone numbers change. An outdated alarm plan is the most frequent cause of delayed responses.

B3.4 Alarm response under DIN 77200-1

DIN 77200-1 (current edition 2022-10) describes minimum requirements for security service providers. It distinguishes stationary services such as the alarm-station service and mobile services such as patrol, inspection and intervention services. The intervention service comprises agreed measures in reaction to a special, non-routine event within a defined period. The intervention officer is the extended arm of the monitoring center; every alarm response must be treated as a potential genuine alarm.

B3.5 Procedure on site

1	**Approach**	Confirmation of the assignment to the monitoring center, approach in compliance with road traffic law.
2	**Arrival**	Self-protection, external check, recognize traces without destroying them.
3	**Situation assessment**	Where offenders may be inside: do not enter, request the police, keep the site under observation.
4	**Internal check**	Only if the situation is unremarkable: take the key, walk the site, establish the cause.
5	**Securing**	Emergency closure, reset and re-arm the system, guard the site until damage is repaired if necessary.
6	**Report**	Call-out report with times, findings and photos to the monitoring center and the client.

B3.6 Rights and limits of the intervention officer

Private security officers have no sovereign powers. They act on the basis of the domiciliary rights delegated by the client and the so-called everyman's rights:

- Self-defence and defence of others (§ 32 StGB) and justifying necessity (§ 34 StGB)
- Provisional arrest when an offender is caught in the act (§ 127 para. 1 StPO) – to be interpreted narrowly, proportionate means only
- Defence of possession and self-help under §§ 859, 229 BGB
- Enforcement of domiciliary rights, e.g. ordering a person to leave and issuing a banning order in the client's name

Domiciliary and access rights – what applies during a call-out

Domiciliary rights (Hausrecht): they belong to the owner or possessor and derive from ownership and possession (§§ 858 et seq., 903, 1004 BGB). The security service can only exercise them if the client delegates them – preferably in writing, with a clear description of the premises and powers (e.g. issuing banning orders, directing persons off the premises). Anyone who stays despite being told to leave may be committing trespass (§ 123 StGB); the offence is only prosecuted upon a criminal complaint, which the entitled party must file.

Right of way in the civil-law sense: if the access route crosses third-party land – for instance in business parks, rented premises or plant sites with several users – the intervention officer needs a secured right of access, e.g. from an easement (§ 1018 BGB), the lease or an agreement with the landowner. The security service may not restrict the rights of third parties (neighbours, co-users); domiciliary rights end at the boundary of the client's property.

Right of way in road traffic: private security services have no special or priority rights under §§ 35, 38 StVO (German Road Traffic Regulations) – no blue lights, no siren, no exemptions from speed limits. The intervention time must therefore be agreed realistically according to distance and traffic conditions.

Practice: the delegation of domiciliary rights, access and locking authorizations (barriers, gates, codes) and the contact persons of landowners belong in the alarm plan, in writing.

B3.7 Key and access management

- Deposit in the certified key safe of the intervention station or in a key depot close to the site
- Sealed, coded key pouches without the site address; removal and return are logged
- Regular function checks of keys and codes, immediate notification of lock changes

Cross-references

→ C5 Rights of Security Officers in Practice
→ D4 Domiciliary Rights and Identity Cards at Reception
→ D7 Remote Gate Service

CLIENT · EMPLOYEES · INSTRUCTION · AVOIDING FALSE ALARMS

B4 The Client’s Duties to Cooperate

The best monitoring center can only respond as well as the information it receives. A large share of all false alarms and delayed call-outs has organizational causes at the site – and can be avoided through clear cooperation.

B4.1 The client’s duties to cooperate

Cooperation	Why it matters
Approve the alarm plan and keep it up to date	Wrong or outdated numbers delay every response
Name at least two reachable authorized call-back persons	Decisions on site need a responsible person
Hand over keys, codes and access authorizations	Without access, the intervention ends at the door
Delegate domiciliary rights in writing	Legal certainty for the intervention officer’s measures
Report changes to the site (conversion, change of tenants, storage)	Detectors may be obscured or need realignment
Announce maintenance and inspection work in advance	Avoids false alarms and unnecessary call-outs
Announce deviating working hours and special openings	Otherwise disarming is treated as a suspicious event
Commission maintenance to DIN VDE 0833	Operator duty, often an insurance requirement
Review call-out reports and have defects remedied	Recurring causes are only eliminated this way

B4.2 Cooperation of employees

Employees arm and disarm the system, open doors and windows and are often the first on site. They therefore need short, regularly repeated instruction:

- **Arming:** close windows, doors and gates beforehand, clear movement areas, do not place objects in front of detectors
- **Codes and code word:** do not pass on personal codes; know the code word the monitoring center asks for on call-back
- **Report operating errors immediately:** anyone who triggers an alarm by mistake calls the monitoring center at once – this saves a call-out
- **Hold-up and emergency situations:** know and use the silent alarm, do not endanger yourself, do not negotiate with offenders
- **New employees:** instruction before keys or codes are first issued; delete the codes of departed staff immediately

B4.3 Frequent causes of false alarms and countermeasures

Cause	Countermeasure
Operating errors when arming or disarming	Instruction, blocking lock or forced-sequence interlock, clear operating guide
Open windows, doors, gates when arming	Closure supervision, checklist at the exit
Animals, heating air, balloons, decorations	Have detector selection and alignment reviewed
Construction work, dust, humidity	Report works in advance, have detectors covered, check after completion
Outdated or dirty detectors	Maintenance to DIN VDE 0833, replacement instead of permanent stopgaps

Insurance: take policy obligations seriously

Many commercial insurance policies make the existence and arming of an intruder alarm system a policy obligation. If it is breached intentionally or through gross negligence – for instance because the system was not armed or not maintained – the insurer can reduce or entirely refuse its payout under § 28 VVG. The monitoring center's arming logs are important evidence in the event of a claim.

Data protection and co-determination

Alarm plans contain names and telephone numbers; arming logs show who entered or left the site and when. Employees must be informed in accordance with Art. 13 GDPR. If behaviour or performance can be inferred from the data, an existing works council has a co-determination right (§ 87 para. 1 no. 6 BetrVG) – a short works agreement creates clarity.

Cross-references

- → C5 Cooperation in Site Protection
- → D6 Cooperation at Reception

DETER · DETECT · ORGANIZE

B5 Preventive Hazard Protection

The best alarm is the one that is never triggered. Preventive hazard protection combines mechanical resistance, organizational rules and visible presence – and is what makes alarm technology and intervention effective in the first place.

B5.1 Principle: mechanics, electronics, organization

Police crime-prevention advice follows the principle that mechanical protection holds the offender up while electronic alarm technology detects him. Only when the resistance lasts longer than alerting and intervention take is an offence prevented rather than merely reported. The police crime prevention advisory centers provide free, manufacturer-neutral advice; SecuConCept complements this with a site-specific overall concept covering monitoring connection, intervention and prevention from a single source.

Resistance class DIN EN 1627	Offender type and approach	Typical use
RC 2	Opportunist offenders with simple tools	Residential, offices, side entrances
RC 3	Offenders with additional tools, e.g. crowbars	Commercial premises, warehouses, rear sides of branches
RC 4 – RC 6	Experienced offenders with power tools	High-value warehouses, technical rooms, special sites

B5.2 Building blocks of prevention

Building block	Content
Vulnerability analysis	Walk-through by day and night, offender’s perspective, assessment of entrances, lighting, sight lines
Security concept	Protection objectives, mix of mechanics, technology and organization, responsibilities
Patrol and inspection service	Irregular checks at varying times, visible presence, defect reports
Locking and opening service	Controlled locking, arming and logging in the evening
Access and key management	Authorizations on a need basis, loss process, regular clean-up
Lighting and grounds	Motion-activated lighting, clear sight lines, no climbing aids on facades
Emergency and crisis management	Alarm and emergency plans, contact persons, exercises, debriefing
Fire-protection prevention	Fire safety rules, fire protection assistants, fire watches during hot work

§ 34A GEWO · FALSE-ALARM FEES · GDPR

B6 Law, Liability and Data Protection

Monitoring connection and alarm response touch on trade, police, civil and data protection law. These points should be governed by contract.

B6.1 Trade law

- Security companies need a licence under § 34a GewO (German Trade Regulation Act); their employees are recorded in the security guard register and, depending on the activity, require instruction or an expert-knowledge examination before the Chamber of Industry and Commerce (IHK).
- The Security Guarding Ordinance (BewachV) governs, among other things, liability insurance, service instructions and the duty to carry identification.

B6.2 False alarms and fees

Whether and in what amount the police or fire service charge fees for false alarms is governed by state law or municipal fee schedules. The Federal Administrative Court considers reasonable fees for a police call-out caused by an alarm system to be permissible. The Administrative Court of Neustadt confirmed 120 € for an unjustified alert by an intruder alarm system; an alarm counts as unjustified if the police cannot establish any cause. Fire services usually charge for false alarms based on time, personnel and vehicles. In Baden-Württemberg, around 29,500 fire service call-outs were classified as false alarms in a single year.

B6.3 Liability and contract

- Set out in writing the scope of services, intervention time, key liability, liability limits and third-party damage during emergency openings
- The monitoring center is responsible for handling and alerting, not for the functioning of the system at the site
- Request evidence of the service provider’s business liability and key insurance

B6.4 Data protection

Topic	Implementation
Roles	The monitoring center and intervention service generally act as processors: data processing agreement under Art. 28 GDPR
Scope of data	Only the necessary contact data in the alarm plan; codes and code words kept separately and protected
Retention periods	Delete alarm logs and call-out reports after the agreed period; exceptions for damage events and proceedings
Video, audio and technology	Verification only for alarm checking; encrypted transmission, role-based and logged access

REFERENCE VALUES · INVESTMENT · OPERATION

B7 Cost Examples and Economic Viability

The examples show typical cost structures for budget planning and comparison. All values net, 2026 market level; actual costs depend on site size, grade, transmission path, distance to the intervention station and scope of services.

Example A – warehouse and office building, 1,500 m², intruder alarm system Grade 3 / VdS Class B

Item	Quantity	Unit price	Total
Vulnerability analysis and planning	lump sum		1,200 €
Intruder alarm panel with operating unit	1	2,400 €	2,400 €
Motion detectors	24	95 €	2,280 €
Opening and closure supervision	12	65 €	780 €
External sounder with strobe light	1	450 €	450 €
Transmission device IP/LTE, dual path	1	650 €	650 €
Installation and commissioning	lump sum		3,800 €
Acceptance and installation certificate	lump sum		450 €
Total investment (net)			**12,010 €**

Running costs per year	Calculation	Amount
Monitoring connection to NSL incl. arming supervision	49 € × 12 months	588.00 €
Key deposit	15 € × 12 months	180.00 €
Mobile tariff for back-up path	9.90 € × 12 months	118.80 €
Maintenance to DIN VDE 0833	2 × 290 €	580.00 €
Alarm response (assumption: 6 call-outs)	6 × 95 €	570.00 €
Depreciation of investment (10 years, straight-line)	12,010 € ÷ 10	1,201.00 €
Total annual costs		**3,237.80 €**

Equivalent to around 270 € per month or just under 9 € per day for protecting the entire site.

Example B – what false alarms cost and what prevention saves

Item	Before (12 false alarms)	After (3 false alarms)
Alarm response at 95 € each	1,140.00 €	285.00 €
Police fee at 120 € (assumption: 4 and 1 case)	480.00 €	120.00 €
Internal effort (1.5 h at 45 € per false alarm)	810.00 €	202.50 €
Costs per year	**2,430.00 €**	**607.50 €**

One-off outlay for employee instruction and detector optimization (assumption): 750 €. Savings in the first year: 1,822.50 € − 750 € = 1,072.50 €, from the second year onwards 1,822.50 € annually.

Example C – preventive mobile patrols in addition to the monitoring connection

Item	Calculation	Amount
Night check on every day of the year	365 × 22 €	8,030 €
Additional daytime check at weekends	104 × 22 €	2,288 €
Mobile patrols per year		**10,318 €**

> **Advocatus Diaboli: cheap monitoring is paid for dearly**
>
> Low monthly prices for the monitoring connection say little about the service. What matters are the certification of the monitoring center, the agreed intervention time, the qualification of the response officers, key liability and reporting. An offer without a binding intervention time or without evidence of DIN EN 50518 is not comparable – and, in the event of a claim, often not insurance-proof either.

FROM ANALYSIS TO REGULAR OPERATION

B8 Checklist for Clients

The checklist is suitable for internal coordination, tendering and evidence towards insurers, supervisory authorities and auditors.

Phase 1 – Analysis	
☐	Define protection objectives, assets and risks per site; check insurance requirements
☐	Vulnerability analysis with a walk-through by day and night
☐	Record existing systems: grade/class, age, transmission path, 2G dependence
☐	Clarify connection targets: NSL, police, fire service via concession holder

Phase 2 – Concept and contract award	
☐	Security concept combining mechanics, alarm technology, organization and intervention
☐	Specification with intervention time, reporting and liability
☐	Request evidence: DIN EN 50518 / VdS 3138, § 34a GewO, insurance, data processing agreement
☐	Clarify access and rights of way across third-party land

Phase 3 – Commissioning	
☐	Define and approve the alarm plan, code word and authorized call-back persons
☐	Hand over keys, codes and access authorizations with a log
☐	Delegate domiciliary rights in writing
☐	Instruct employees, provide data protection information and a works agreement where applicable
☐	Carry out a test alarm across all transmission paths

Phase 4 – Regular operation	
☐	Update the alarm plan on every change, review at least annually
☐	Maintenance to DIN VDE 0833 and checking of the transmission paths
☐	Evaluate the monthly reporting, eliminate recurring false alarms
☐	Repeat instruction annually and for new employees

ANSWERED BRIEFLY AND RELIABLY

B9 Frequently Asked Questions (FAQ)

What is the difference between monitoring connection and alarm response?

The monitoring connection links the hazard alarm system to a permanently staffed monitoring center that assesses reports. Alarm response is the on-site call-out that the monitoring center triggers according to the alarm plan.

Can I connect my fire alarm system to a private monitoring center?

Fire alarm systems required under building law must be connected to the fire service via the concession holder. A private monitoring center can additionally supervise faults and organize keys and briefing during a call-out.

How quickly is the intervention officer on site?

That depends on distance, traffic conditions and the contract. Security services have no special rights in road traffic; reputable providers agree a realistic, measurable intervention time per site.

May the intervention officer detain an offender?

Only within the scope of the everyman's rights, in particular the provisional arrest of an offender caught in the act under § 127 StPO, and with proportionate means. Self-protection and alerting the police take priority.

Who pays in the event of a false alarm?

Call-outs of the intervention service are billed according to the contract. Fees of the police or fire service are governed by state law or municipal bylaws and are generally charged to the operator of the system.

Will my alarm system still work after the 2G switch-off?

If the transmission device uses GSM only, no longer reliably. Have the transmission path checked now – often a module or device swap is enough.

What cooperation is expected from us?

An up-to-date alarm plan, reachable contact persons, handed-over keys and codes, domiciliary rights delegated in writing, maintenance work announced in advance and instructed employees.

Do we need a new alarm system for the monitoring connection?

Usually not. Existing systems can often be connected with a new transmission device, provided grade and condition match the risk.

PART C

Security Services in Practice: Guarding or Plant Security

Distinguishing guarding from plant security, § 34a GewO and qualifications, in-house staff or service provider, practice on site, and how an hourly rate is calculated.

CHAPTERS

C1 At a Glance
C2 Guarding and Plant Security
C3 Law, Qualifications and Occupational Safety
C4 In-House Staff or Service Provider
C5 Practice on Site
C6 Quality and Contract Award
C7 What an Hour of Security Costs
C8 Checklist for Clients
C9 Frequently Asked Questions (FAQ)

RELATED PARTS

Part B Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection – rights and domiciliary rights during call-outs
Part D Reception & Gatekeeper Services – Controlled Entry – reception and gatehouse
Part E KRITIS: Security Services as an All-in-One Solution? – integrated service-provider model

KEY STATEMENTS FOR DECISION-MAKERS

C1 At a Glance

The ten most important facts for everyone who commissions, organizes or restructures security services.

1 **Guarding protects premises, plant security protects operations:** plant security is more deeply embedded in a site's processes, hazard-protection and emergency organization.

2 **In-house staff need no licence under § 34a GewO:** guarding your own company with your own employees is not commercial guarding.

3 **External service providers always need one:** a licence for the company, instruction (40 hours) or an expert-knowledge examination for the employees, and entry in the security guard register.

4 **DGUV Regulation 23** governs aptitude, service instructions, site induction and equipment – and prohibits instructions that conflict with the security assignment.

5 **Collectively agreed wages are universally binding:** in 2026, basic hourly wages range from roughly 15 to 19 euros depending on state and activity – well above the minimum wage of 13.90 euros.

6 **A reputable hourly rate is therefore usually around double the collectively agreed wage.** Offers far below that are a warning sign.

7 **A 24/7 post comprises 8,760 hours a year** and needs around five to six full-time staff including leave, sickness and training.

8 **Beware of disguised contracting:** anyone who gives direct instructions to external security officers risks unlawful temporary agency work.

9 **Quality is measurable:** with a clear specification, performance metrics, patrol records, audits and a permanent site supervisor.

10 **The strongest model is often hybrid:** in-house plant security management with operational knowledge, operational services delivered by a qualified provider.

TERMS · DISTINCTION · SERVICE TYPES

C2 Guarding and Plant Security

In everyday language, guarding, site protection and plant security are often used interchangeably. For planning purposes the distinction pays off: it determines tasks, qualifications, integration into operations – and therefore the costs.

C2.1 The difference at a glance

Feature	Guarding / site protection	Plant security
Protection objective	Buildings, grounds, physical assets	The entire operation: people, plant, processes, know-how
Typical sites	Offices, residential complexes, warehouses, construction sites, vacant properties	Industry, chemicals, energy, logistics centers, KRITIS
Integration	Assignment with clearly delimited tasks	Part of the operating organization, close coordination with plant management, HSE and the plant fire brigade
Depth of tasks	Checks, presence, reporting, first measures	Access, plant traffic, material and vehicle checks, emergency and incident organization
Qualification	Instruction or expert knowledge under § 34a GewO	additionally certified plant protection officer, fire protection, hazardous-substances knowledge, first aiders
Organization	predominantly external service providers	in-house staff, service provider or a hybrid model

C2.2 Service types under DIN 77200-1

DIN 77200-1 (edition 2022-10) describes minimum requirements for security service providers and distinguishes stationary and mobile security services as well as the event security service.

Service	Content	Typical use
Dedicated guarding / site protection service	permanent presence at one site, patrol rounds, reports	Industry, administration, construction sites
Reception and gate service	Access, visitor and key management, telephone	Company headquarters, factory gates
Inspection service	Checks at defined points and times	Vacant properties, technical areas
Mobile patrol service	several sites in rotation, irregular checks	Business parks, branch networks
Intervention service	Response to alarms within an agreed period	Sites with a monitoring connection
Event service	Admission, stewarding, fire protection	Trade fairs, company events, events

C2.3 Typical tasks in plant security

- **Access and plant traffic:** ID and visitor management, contractor checks, truck processing, traffic control within the plant
- **Material and vehicle checks:** outgoing goods, spot checks under a works agreement, load and seal checks
- **Hazard protection:** fire-safety rounds, first aid, support for the plant fire brigade, guiding emergency services in
- **Incident and emergency organization:** alerting, evacuation, cordoning, situation reports to plant management
- **Technology:** operating hazard management, video, access control and the control room

> **From practice**
>
> In industrial plant security – especially in the chemical industry – the security service is part of the operational hazard-protection organization. Anyone working there must know the plant, escape routes, assembly points and alarm levels. This operational knowledge is the real added value of plant security – and it only develops through permanent teams, thorough site induction and regular exercises.

§ 34A GEWO · SECURITY GUARD REGISTER · DGUV REGULATION 23

C3 Law, Qualifications and Occupational Safety

Anyone who commercially guards the lives or property of others is subject to German security licensing law. Different rules apply to in-house staff – but occupational safety and qualification remain mandatory in both cases.

C3.1 Who needs what?

Situation	Licence § 34a GewO	Qualification of the employees
In-house plant security / own gatehouse	not required	no statutory requirement under § 34a; qualification based on the risk assessment and DGUV Regulation 23
External site and plant security	company needs a licence	at least instruction (40 hours) at the IHK
Patrols in public traffic areas or in areas with actual public traffic	required	expert-knowledge examination
Protection against shoplifters, door supervision at discotheques	required	expert-knowledge examination
Managerial roles at refugee shelters and access-protected major events	required	expert-knowledge examination

Certain vocational and advanced qualifications replace instruction or the expert-knowledge examination, for example the qualified security specialist or service officer (Fachkraft / Servicekraft für Schutz und Sicherheit), the certified protection and security officer (Geprüfte Schutz- und Sicherheitskraft), the certified plant protection officer (Geprüfte Werkschutzfachkraft) and the master craftsman for protection and security (§ 8 BewachV).

C3.2 Qualification levels at a glance

Level	Qualification	Typical role
Basic	Instruction under § 34a GewO (40 hours)	Site protection, gatehouse, plant security (external)
Advanced	Expert-knowledge examination under § 34a GewO	Mobile patrols, events, shift and team leadership
Further training	Certified protection and security officer (IHK), certified plant protection officer	Site supervision, qualified plant security
Apprenticeship	Service officer (2 years) or specialist for protection and security (3 years)	Plant security, control room, future leadership
Management	Master craftsman for protection and security, plant security master	Plant security management, branch and area management

C3.3 Security guard register and reliability

Since 1 June 2019, the nationwide security guard register (§ 11b GewO) has recorded security companies and their employees. Before deployment, the authority checks reliability; on duty, guards carry an ID card and a name badge or identification number. Clients should have the registration of the deployed staff confirmed.

C3.4 Occupational safety: DGUV Regulation 23

The accident prevention regulation “Guarding and security services” applies to all guarding and security work protecting people and physical assets – regardless of whether in-house staff or a service provider is deployed. Key points:

- Aptitude and capability of the deployed staff, documented
- Written service instructions and regular briefing, including on confrontations, hold-ups, fire protection and first aid
- Site induction before the first assignment, equipment e.g. with powerful torches
- Prohibition of intoxicating substances on duty
- No client instructions may be followed that conflict with the security assignment

> **Securing lone working**
>
> Night duty and patrol rounds frequently take place alone. Based on the risk assessment, a personal emergency signal system may be required; DGUV Rule 112-139 describes selection, operation and operating instructions. For in-house plant security staff, the company itself bears this responsibility; with a service provider it lies with that provider as employer – coordination about hazards at the site remains a duty of both parties (§ 8 ArbSchG, German Occupational Safety Act).

MAKE OR BUY · HYBRID MODEL · DISGUISED CONTRACTING

C4 In-House Staff or Service Provider

The question “in-house plant security or external service provider?” is not purely a cost question. What matters are operational knowledge, resilience against absences, flexibility, management effort and liability.

C4.1 Comparison of the models

Criterion	In-house plant security	External service provider	Hybrid
Operational knowledge	very high	depends on team continuity	high, through in-house management
Absence, leave, sickness	own risk	contractually with the provider	with the provider
Recruitment and training	own effort	service provider	mostly the service provider
Flexibility for extra demand	low	high	high
Management and control	own line management	via the provider’s site supervisor	in-house plant security management steers
§ 34a GewO	not required	required	for the external part
Collective agreements and labour law	company or industry agreement of the operation	security services collective agreement	mixed

C4.2 The hybrid model

In many industrial and KRITIS operations a division of labour has proven itself: an in-house plant security or security management function knows the operation, sets standards and is the contact for plant management and authorities. The operational service – gatehouse, patrols, control room, peak loads – is delivered by a qualified service provider who compensates for absences and keeps staff available. Operational knowledge stays in-house without the company having to run a complete security business.

Avoiding disguised contracting

If external security staff are managed like your own employees – given direct instructions, placed in your own duty rosters or integrated into your operating organization – the service contract can turn into covert temporary agency work. Without a licence under the Temporary Employment Act, the consequences can be a deemed employment relationship with the client, fines and back-payments of social insurance contributions.

Keeping the contract clean: describe services and outcomes in the contract, not individuals’ working hours. Professional requirements flow in via the service instructions issued by the provider. Operational requests are routed through the provider’s site supervisor – not directly to individual security officers.

C4.3 When which model fits

- **External service provider:** sites without special process hazards, fluctuating demand, several sites, construction sites, vacant properties
- **In-house plant security:** very high requirements for operational knowledge and confidentiality, large sites with a plant fire brigade and their own control room
- **Hybrid:** industry, chemicals, energy, logistics centers and KRITIS facilities needing in-house steering and flexible delivery

C4.4 Decision matrix

Rate each criterion for your site from 1 (low) to 5 (high) and multiply by the weighting. High scores on the first three criteria argue for in-house steering, high scores on the last three for a service provider – if both groups score high, the hybrid model is usually the best choice.

Criterion	Key question	Weighting
Operational knowledge	How strongly does security depend on process and plant knowledge?	×3
Confidentiality	How sensitive are know-how, access and information?	×2
Hazard protection within operations	Is the service part of fire protection, incident and emergency organization?	×3
Fluctuating demand	Are there peaks, projects, construction sites or seasonal loads?	×2
Absence risk	How critical would an unstaffed post be?	×3
Management capacity	Are in-house resources for recruitment, training and rostering lacking?	×2

SERVICE INSTRUCTIONS · PATROLS · CHECKS · DOCUMENTATION

C5 Practice on Site

You recognize good security services not by the uniform but by clear procedures, traceable documentation and staff who know their site.

C5.1 From assignment to ongoing service

1	**Site survey**	Walk-through, protection objectives, risks, interfaces with technology, the plant fire brigade and building services.
2	**Service instructions**	Tasks, patrol plan, reporting channels, conduct in emergencies, powers – issued by the provider, agreed with the client.
3	**Site induction**	Every security officer before their first duty: grounds, technology, escape routes, contact persons, danger points.
4	**Familiarization**	Accompanied duties, especially for the gatehouse, control room and plant security tasks.
5	**Regular operation**	Duty roster, shift handover, patrol rounds, reports, defect notifications.
6	**Review**	Regular site visits, audits, performance metrics, updating of the service instructions.

C5.2 Patrol rounds and documentation

- **Digital guard tour monitoring:** checkpoints via NFC or QR code document the time and place of every round
- **Irregular times and routes:** predictable rounds are an open book for offenders
- **Defect reports with photos:** open doors, defective lighting, fire loads, damaged fences
- **Logbook and shift handover:** seamless handover of incidents, keys and open items
- **Monthly report:** events, defects, metrics and recommendations for the client

C5.3 Checks of people, bags and vehicles

Checks when leaving the plant premises are common in plant security but legally sensitive. Security officers have no search powers; checks take place on the basis of domiciliary rights, employment contract provisions and – where a works council exists – a works agreement, since gate checks concern the order of the operation (§ 87 para. 1 no. 1 BetrVG). No search may be carried out against the will of the person concerned; where a criminal offence is concretely suspected, the police are called in.

Rights of security officers

Private security officers have no sovereign powers. They act with the domiciliary rights delegated by the client and the everyman's rights: self-defence and defence of others (§ 32 StGB), necessity (§ 34 StGB), provisional arrest of an offender caught in the act (§ 127 para. 1 StPO), and defence of possession and self-help (§§ 859, 229 BGB). Domiciliary rights should be delegated in writing and the premises precisely described.

C5.4 The client's cooperation

- Name a permanent contact person and route requests via the provider's site supervisor
- Communicate changes to buildings, uses, access authorizations and technology in good time
- Inform employees about the security service's tasks and powers – this increases acceptance and effectiveness
- Work through defect reports from the reports promptly and give feedback

Cross-references

→ B3 Info box on domiciliary and access rights
→ B4 The Client's Duties to Cooperate

SPECIFICATION · PERFORMANCE METRICS · COLLECTIVE-WAGE COMPLIANCE

C6 Quality and Contract Award

Security services are still too often awarded on the lowest hourly rate. The result is high staff turnover, changing faces and declining operational knowledge – the exact opposite of security.

C6.1 Building blocks of a good tender

Building block	What matters
Specification	Protection objectives, tasks, times, qualifications, equipment, interfaces – referencing DIN 77200-1
Personnel	Share of permanently assigned staff, familiarization concept, substitution rules, language skills
Evidence	Licence under § 34a GewO, security guard register, liability and key insurance, certificates
Collective agreements and wages	Commitment to collectively agreed wages, disclosure of wage groups, rules on subcontractors
Evaluation	Best-bidder principle: weight concept, quality and references, not just the price
Start	Trial phase with defined metrics and acceptance

C6.2 Performance metrics for regular operation

Metric	What it tells you	Target direction
Staffing rate	How many planned hours were actually worked?	100 %
Patrol completion	How many checkpoints were reached at the planned time?	as close to 100 % as possible
Team continuity	Share of permanently assigned, inducted staff	high
Response time	Time to action for events and alarms	contractually defined
Defect rate	reported and resolved defects	track resolution
Complaints	Feedback from employees, visitors, contractors	low, with evaluation

> **Advocatus Diaboli: subcontractor chains**
>
> An offer calculated below collectively agreed wage levels usually only works with subcontractors, overlong shifts or missing absence reserves. For the client this creates quality risks and – where staff are integrated into the operation – legal risks as well. Have subcontractors named and approved in writing before deployment, and demand the same evidence as from the main contractor.

COLLECTIVELY AGREED WAGES · HOURLY RATE · 24/7 POST · MAKE OR BUY

C7 What an Hour of Security Costs

An hourly rate is more than the wage. The following model calculation shows how a collectively compliant charge rate is built up – and why offers far below it can hardly be reputable.

C7.1 Collectively agreed wages 2026 – examples

Region / activity	Basic hourly wage 2026
North Rhine-Westphalia, gate service (from 1 February 2026)	15.11 €
Baden-Württemberg, site protection / dedicated guarding	15.14 €
Baden-Württemberg, mobile patrol and intervention service	16.30 €
Baden-Württemberg, certified protection and security officer	18.40 €
Hesse, range across twelve wage groups	15.15 € – 19.08 €
Statutory minimum wage (2027: 14.60 €)	13.90 €

C7.2 Model calculation of the charge rate (basis: gate service, NRW)

Component	Assumption	Amount per hour
Basic hourly wage	NRW 2026 collective agreement	15.11 €
Night, Sunday and public-holiday supplements	Ø 10 %	1.51 €
Subtotal wage		16.62 €
Non-productive time: leave, sickness, public holidays	22 %	3.66 €
Subtotal		20.28 €
Employer social-insurance contributions	21 %	4.26 €
Subtotal staff costs		24.54 €
Training, equipment, uniforms, insurance	6 %	1.47 €
Subtotal		26.01 €
Administration, operations management, control room, risk and profit	18 %	4.68 €
Net charge rate		**30.69 €**

Model calculation with typical overhead rates; actual values depend on the collective-agreement region, wage group, deployment times, qualification and scope of services. Each line builds on the previous subtotal.

C7.3 Example: a 24/7 post – service provider or in-house staff

Model	Calculation	Costs per year
Service provider at the model rate	8,760 h × 30.69 €	268,844 €
In-house staff: 5.5 full-time employees	5.5 × 42,000 € gross × 1.21	279,510 €
In-house staff incl. training, equipment, management (+8 %)	279,510 € × 1.08	301,871 €

Assumptions: 8,760 hours per year, around 1,600 productive hours per full-time employee, 42,000 € annual gross including supplements, 21 % employer contributions. Recruitment, absence management and replacement after resignations are not yet included for in-house staff.

Advocatus Diaboli: the price is not the comparison

Arithmetically, the two models are close together. The difference is made by factors no table shows: who bears the absence risk during a flu wave? Who recruits after resignations? How quickly can the service be doubled when the situation escalates? And how much operational knowledge is lost when staff change constantly? These questions decide the model – not the hourly rate alone.

Cross-references

- → D8 The Model Rate Applied: Reception and Gatehouse
- → E8 The Model Rate Applied: KRITIS Annual Package

FROM NEEDS ANALYSIS TO REGULAR OPERATION

C8 Checklist for Clients

The checklist is suitable for internal decision papers, tenders and the annual review.

Phase 1 – Needs and model	
☐	Define protection objectives, risks and tasks per site; guarding or plant security?
☐	Derive staffing needs from coverage times (24/7 post = 8,760 hours)
☐	Model decision: in-house staff, service provider or hybrid – assessing absence risk and operational knowledge
☐	Clarify co-determination: involve the works council on checks and technology

Phase 2 – Tender and contract award	
☐	Specification based on DIN 77200-1 with metrics and a trial phase
☐	Evidence: § 34a GewO, security guard register, insurance, collective-wage compliance, subcontractors
☐	Best-bidder principle: weight concept, quality, references and price
☐	Draft the contract as a service or works contract, cleanly separated from staff leasing

Phase 3 – Start	
☐	Site survey, service instructions, site induction for every security officer
☐	Delegate domiciliary rights in writing, hand over keys and authorizations with a log
☐	Define contact persons and the communication channel via the site supervisor
☐	Inform the company’s employees about the security service’s tasks

Phase 4 – Regular operation	
☐	Evaluate the monthly report and metrics, work through defects
☐	Regular audits and unannounced checks
☐	Update the service instructions on changes and at least annually
☐	Conduct joint exercises for emergencies, evacuation and incidents

ANSWERED BRIEFLY AND RELIABLY

C9 Frequently Asked Questions (FAQ)

What is the difference between guarding and plant security?

Guarding protects buildings, grounds and physical assets. Plant security is embedded in a company's organization and additionally handles access, plant traffic, checks and operational hazard-protection tasks.

Does our in-house plant security need a licence under § 34a GewO?

No. Guarding your own company with your own employees is not commercial guarding. Occupational safety, qualification based on the risk assessment and DGUV Regulation 23 still apply.

What qualification do external security officers need?

At least the 40-hour instruction under § 34a GewO. For certain activities, such as patrols in public traffic areas, the expert-knowledge examination is mandatory. Higher qualifications replace both.

How many employees does a 24/7 post need?

A round-the-clock post comprises 8,760 hours a year. Including leave, sickness and training, around five to six full-time staff are needed.

Why do hourly rates differ so widely?

Because collective-agreement region, wage group, supplements, absence reserve, training and management are calculated differently. Offers well below the collectively agreed level point to gaps in wages, absence reserves or quality.

May security officers check bags?

Only on the basis of domiciliary rights and company rules, and with a works agreement where a works council exists. A search against the person's will is not permitted.

May we give the security officers instructions directly?

Professional requests yes, but via the provider's site supervisor. Direct instructions and integration into your own organization can lead to covert temporary agency work.

What is a hybrid model?

An in-house plant security or security management function steers, while a service provider delivers the operational service. Operational knowledge stays in-house; absences and peaks are borne by the provider.

PART D

Reception & Gatekeeper Services – Controlled Entry

Zone concept and visitor process, identity cards and data protection at reception, emergencies and de-escalation, technology and the remote gate service.

CHAPTERS

D1 At a Glance
D2 Reception, Gatehouse, Factory Gate
D3 Access and Entry Control
D4 Law and Data Protection at Reception
D5 Emergencies, Threats and De-escalation
D6 Staff, Quality and Cooperation
D7 Technology at Reception
D8 Cost Examples and Economic Viability
D9 Checklist for Clients
D10 Frequently Asked Questions (FAQ)

RELATED PARTS

Part B Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection – monitoring center and remote gate service

Part C Security Services in Practice: Guarding or Plant Security – hourly rate and personnel

KEY STATEMENTS FOR DECISION-MAKERS

D1 At a Glance

The ten most important facts for everyone building, commissioning or improving a reception or gatekeeper service.

1 **Reception is service and security at once:** every person who gets in unchecked bypasses all the other protective measures in the building.

2 **An external gatehouse with access control is guarding within the meaning of § 34a GewO:** the staff need at least the 40-hour instruction.

3 **Your own employees at reception are not guarding someone else's building** – § 34a GewO does not apply to them. Training and briefing are still necessary.

4 **The identity card is not a deposit:** requiring it to be handed over is unlawful under the German Identity Card Act.

5 **Copies of the ID card are only permitted with the holder's consent,** must be recognizable as copies and are almost never necessary at reception.

6 **Open visitor lists are a data protection violation:** every subsequent guest sees the names and companies of the previous ones.

7 **A zone concept defines who may move where** – reception enforces it, technology supports it.

8 **In an emergency, reception is the contact point** for the fire service and ambulance service and keeps the overview of which guests are in the building.

9 **Nothing works without cooperation:** hosts register visitors, collect them and accompany them; employees wear their badges visibly.

10 **Not every door needs round-the-clock staffing:** a staffed daytime reception with a remote gate service via a monitoring center can be considerably cheaper.

TASKS · DISTINCTION · SERVICE PROFILES

D2 Reception, Gatehouse, Factory Gate

Reception, gatehouse and factory gate share the same core task – controlled entry – but have different focuses. A reception that is merely friendly gets bypassed; one that only checks puts guests off. Professional staff combine both – based on service instructions that state unambiguously who may pass unaccompanied.

D2.1 Three deployment forms compared

Feature	Reception / front desk	Gatehouse	Factory gate
Typical location	Company headquarters, administration, office building	Company grounds, public authority, clinic	Industry, logistics, chemicals, energy
Focus	Guests, service, representation	Access, keys, checks	People and vehicle traffic, material
Depth of checks	Identity, registration, badge	Authorization, zones, keys	Badges, loads, contractors, plant traffic
Staffing	usually weekdays, daytime	often in shifts	frequently around the clock
Requirements	Service, languages, IT	Checks, technology, de-escalation	Plant security knowledge, hazardous substances, emergencies

D2.2 Tasks at a glance

Area	Typical tasks
Access	Check identity, verify authorization, issue and retrieve visitor badges, prevent tailgating
Visitors	Process pre-registrations, inform hosts, look after the waiting area, organize escorts
Contractors and suppliers	Check the order, verify safety briefings, assign work areas, direct deliveries
Post and parcels	Acceptance, visual inspection, forwarding, handling of suspicious items
Keys and badges	Issue, return, log, blocking on loss
Service	Telephone, meeting rooms, taxis, lost property, information
Security	Watch the hazard alarm technology, patrol rounds, alerting, first measures in an emergency

ZONE CONCEPT · VISITOR PROCESS · CONTRACTORS · POST

D3 Access and Entry Control

Entry control does not begin at the front desk but with a concept: who may go where, when, and accompanied by whom?

D3.1 The zone concept

Zone	Examples	Access
Public	Forecourt, foyer up to the front desk	everyone
Semi-public	Meeting rooms in the reception area, canteen	registered guests, possibly unaccompanied
Internal	Offices, production areas, warehouses	employees; guests only when accompanied
Security-critical	Server rooms, technical centers, laboratories, cash offices	individually authorized persons, logged

D3.2 The visitor process

1	**Pre-registration**	The host registers the visit with name, company, time and destination area – via form or visitor management.
2	**Arrival**	Greeting, comparison with the registration, checking identity by having an ID shown – not copied, not retained.
3	**Badge and guidance**	Issue a visitor badge with validity; notes on safety, the photography ban and conduct in an emergency.
4	**Collection**	The host collects the guest in the reception area; without collection there is no access to internal zones.
5	**Escort**	Guests move in internal zones only when accompanied; passing on the badge is prohibited.
6	**Sign-out**	Badge return, sign-out, deletion of the data after the defined period.

D3.3 Contractors, suppliers and post

- **Contractors:** check the order and contact person, evidence of the safety briefing, work permit for special work, tool and material list where needed
- **Suppliers:** fixed delivery zone and times, no through-access to internal areas without clearance, drivers stay with the vehicle or are accompanied
- **Post and parcels:** central acceptance, visual check for anomalies (missing sender, unusual weight, leakage, wires, odours)
- **Suspicious item:** do not open, do not move, leave and secure the room, alert the police via 110

§ 34A GEWO · DOMICILIARY RIGHTS · IDENTITY CARD · GDPR

D4 Law and Data Protection at Reception

Security licensing law, domiciliary rights and data protection meet at reception. The most important rules are simple – but frequently violated in everyday practice.

D4.1 Do reception staff need a qualification under § 34a GewO?

Situation	Requirement
Your own employees at reception or the gatehouse	not guarding within the meaning of § 34a GewO; training based on the risk assessment
External provider, pure service reception without control tasks	classification case by case by the trade office
External provider, gatehouse or reception with access control	licence for the company, instruction (40 hours) for the employees
Entry control at access-protected major events in a managerial role	expert-knowledge examination

D4.2 Domiciliary rights

Domiciliary rights allow the holder to decide on entry and continued presence – including refusing entry to individual persons or issuing a banning order. Reception exercises them on the holder's behalf; for external providers they should be delegated in writing. Banning orders are documented, with a photo only where clearly necessary, and kept in a protected list that is reviewed regularly.

Identity card: showing yes, surrendering no

No deposit: under § 1 para. 1 sentence 3 of the German Identity Card Act (PAuswG), the holder may not be required to deposit the card or otherwise give up possession of it. "Swapping" ID cards for visitor badges is therefore unlawful.

Copies only by way of exception: a copy may only be made by the holder or with the holder's consent and must be clearly and permanently recognizable as a copy (§ 20 para. 2 PAuswG). Under the principle of data minimization, having the card shown and noting the name is almost always sufficient at reception.

Practice: suitable deposits for visitor badges are a small cash deposit, a business card or simply collection by the host.

D4.3 Data protection for visitor data

Topic	Rule
Visitor list	Never display openly; individual entry on screen or on separate sheets
Scope	Only necessary data: name, company, host, times; no ID numbers without a specific reason
Retention period	Deletion after the defined period once the purpose is fulfilled; document exceptions for security incidents
Information	Privacy notices under Art. 13 GDPR at reception or in the invitation
Photos on visitor badges	Only where there is a justified security need and a deletion concept
Video surveillance in the foyer	Signage, balancing of interests; do not permanently cover the reception staff's workstation

D4.4 Bag and body checks

Reception and gate staff have no search powers. Checks are only possible voluntarily or on the basis of clear entry conditions; anyone who refuses can be excluded under domiciliary rights. For employees, the works agreement and co-determination apply (§ 87 para. 1 no. 1 BetrVG). Where a criminal offence is suspected, the police are called in.

Cross-references

- → B3 Info box on domiciliary and access rights
- → A6 Data Protection in Video Surveillance

EVACUATION · EMERGENCY SERVICES · DIFFICULT SITUATIONS

D5 Emergencies, Threats and De-escalation

When something happens, reception is the place where all information converges – and where the fire service, ambulance service and police arrive first.

D5.1 Reception's tasks in an emergency

1	**Alert**	Call 112 or 110, trigger the internal alarm chain, inform the monitoring center.
2	**Direct**	Keep access clear for emergency services, secure lifts and access routes, keep onlookers away.
3	**Inform**	Brief the emergency services: situation, route, keys, fire alarm system layout cards.
4	**Keep the overview**	Provide the list of guests and contractors present for the roll call at the assembly point.
5	**Document**	Record times, measures and persons involved; refer media enquiries to the responsible office.

D5.2 Difficult visitors and threat situations

- **De-escalation:** stay calm, keep your distance, use names, listen, offer clear alternatives, do not let yourself be provoked
- **Self-protection:** the desk as a distance zone, keep the escape route behind the workstation clear, no dangerous objects within reach
- **Silent alarm:** hold-up or emergency button connected to the monitoring center or police; practise triggering it regularly
- **Second person:** for known conflict situations (dismissals, social-welfare offices, clinics) staff reception with two people or keep a security officer in the background
- **Aftercare:** document the incident, consider a banning order, relieve those affected and offer support where needed

> **Practice makes safe**
>
> Reception staff should practise evacuation, briefing the fire service and triggering the silent alarm at least once a year – together with the fire protection officers and building services. After every exercise, the lessons learned belong in the service instructions.

REQUIREMENTS PROFILE · METRICS · THE CLIENT'S TASKS

D6 Staff, Quality and Cooperation

At reception, every person represents the company to the outside world. Selection, familiarization and team continuity determine whether reception is perceived as professional – and whether it works in an emergency.

D6.1 Requirements profile

Competence	Content
Service	Demeanour, communication, telephone, dealing with VIP guests
Language	confident German, English or further languages depending on the site
Security	Access rules, spotting anomalies, alerting, first aid
Technology	Visitor management, access control, hazard alarm technology, video
Conflict skills	De-escalation, enforcing rules without escalation
Legal matters	Domiciliary rights, data protection, limits of powers; instruction under § 34a GewO where required

D6.2 Performance metrics

Metric	What it tells you
Waiting time at reception	How quickly are guests greeted and handed over to their hosts?
Badge return rate	How many visitor badges come back at the end of the day?
Pre-registration rate	How many visits are registered in advance?
Findings	Tailgating, unauthorized access attempts, open doors
Team continuity	Share of permanently assigned, familiarized staff

D6.3 Cooperation of the client and employees

- Hosts register visits, collect their guests, accompany them and sign them out again
- Employees wear their badges visibly, do not hold doors open for strangers and report lost badges immediately
- HR reports joiners and leavers promptly so that authorizations are created or blocked
- Managers back reception when rules are enforced – including towards their own staff
- The client keeps access rules, the banning-order list and contact persons up to date and steers via the provider's site supervisor

VISITOR MANAGEMENT · ACCESS CONTROL · REMOTE GATE SERVICE

D7 Technology at Reception

Technology relieves reception of routine and creates records – but it does not replace human judgement.

Technology	Benefit	What to look for
Visitor management software	Pre-registration, invitation with QR code, badge printing, attendance list	Deletion periods, roles, privacy notices
Self-service terminal	fast registration at high visitor volumes	alternative route via staffed reception
Access control	Authorizations by zones and times, logging	Blocking process on loss, co-determination
Single-person entry	Turnstiles, security interlocks against tailgating	Accessibility, escape routes, fire protection
Hold-up and emergency button	silent alarm to the monitoring center or police	regular function testing
Remote gate / video intercom	Access outside staffed hours via a monitoring center	clear rules, verification, intervention time

Tailgating – the most frequent gap

Most unauthorized entries happen not through force but through politeness: someone holds the door open. Single-person entry systems such as turnstiles or interlocks help, but they do not replace the attentiveness of reception and clear rules for employees. Addressing strangers in a friendly way (“Can I help you?”) prevents more than any barrier.

Biometrics only with a sense of proportion

Facial recognition or fingerprints at reception process special categories of personal data (Art. 9 GDPR). For visitors they are practically never necessary; for employees they come into consideration only with voluntary consent and an equivalent alternative. A badge, PIN or accompanied access is sufficient in almost every case.

Cross-references

→ B3 Monitoring Center and Alarm Response
→ A5 Video Alarm Monitoring via the Monitoring Center

ROUND-THE-CLOCK PRESENCE · DAYTIME RECEPTION WITH REMOTE GATE

D8 Cost Examples and Economic Viability

The examples show typical orders of magnitude based on the collectively derived model rate from Part C, Chapter C7 (30.69 € net per hour of gate service).

Example A – presence around the clock

Item	Calculation	Costs per year
Reception weekdays 7 a.m.–7 p.m. (12 h × 250 days = 3,000 h)	3,000 h × 33.50 €	100,500.00 €
Gate service outside reception hours	5,760 h × 30.69 €	176,774.40 €
Total	**8,760 h**	**277,274.40 €**

Example B – daytime reception plus the SecuConCept remote gate service

Item	Calculation	Costs per year
Reception weekdays 7 a.m.–7 p.m.	3,000 h × 33.50 €	100,500 €
Remote gate via the monitoring center (assumption: flat rate)	1,250 € × 12 months	15,000 €
Technology: video intercom, remote opening (assumption)	18,000 € ÷ 5 years	3,600 €
Total		**119,100 €**

Difference to Example A: 277,274.40 € − 119,100 € = 158,174.40 € per year. Intervention call-outs outside staffed hours are billed additionally according to the contract. The rate of 33.50 € for reception service with service and language requirements is an assumption.

> **Advocatus Diaboli: the remote gate does not fit everywhere**
>
> The combined model only pays off if there is little people and vehicle traffic outside office hours. With shift operation, regular night deliveries, plant security tasks or sensitive sites, the person who reacts on site, checks and guides emergency services in an emergency is missing. The decision therefore belongs in the risk analysis – not in the cost calculation alone.

FROM CONCEPT TO REGULAR OPERATION

D9 Checklist for Clients

The checklist supports planning, tendering and the annual review of reception and gatekeeper services.

Phase 1 – Concept	
☐	Define the zone concept: public, semi-public, internal, security-critical
☐	Determine staffed hours and model: presence, remote gate or a combination
☐	Describe the processes for visitors, contractors, suppliers and post
☐	Data protection: scope of data, deletion periods, notices under Art. 13 GDPR, no ID card as a deposit

Phase 2 – Contract award and start	
☐	Specification with service and security requirements, languages and metrics
☐	Evidence: § 34a GewO for access control, insurance, collective-wage compliance
☐	Service instructions, delegation of domiciliary rights, banning-order list, contact persons
☐	On-site familiarization, technology training, emergency briefing

Phase 3 – Regular operation	
☐	Evaluate metrics monthly: waiting time, badge returns, findings
☐	Regularly remind employees of the badge rule and the tailgating rules
☐	Practise evacuation and the silent alarm at least annually
☐	Delete visitor data on schedule, review the banning-order list regularly

ANSWERED BRIEFLY AND RELIABLY

D10 Frequently Asked Questions (FAQ)

May reception retain a visitor's identity card as a deposit for the visitor badge?

No. Under § 1 para. 1 sentence 3 of the German Identity Card Act, requiring the card to be deposited is not permitted. The card may be shown but not retained.

May we copy or scan visitors' ID cards?

Only with the holder's consent and as a recognizable copy – and only if it is necessary. For normal visitor reception this is almost never the case.

Does our receptionist need instruction under § 34a GewO?

Your own employees do not. External staff who carry out access control need at least the 40-hour instruction.

Is a visitor list at reception permitted?

Yes, but not openly displayed. Each guest may only see their own data; the data are deleted once the purpose is fulfilled.

May we check visitors' bags?

Only voluntarily or as a condition of entry. A search against the person's will is not permitted; anyone who refuses can be denied entry.

What should we do about a suspicious postal item?

Do not open it, do not move it, leave and seal off the room, alert the police via 110 and document the course of events.

Is a remote gate service worthwhile?

If there is little traffic outside office hours, it can cut costs considerably. With shift operation or sensitive sites, on-site presence usually remains necessary.

Who is responsible for tailgating?

Everyone: reception watches out for it, technology makes it harder, and employees do not hold doors open for strangers. Without clear rules for your own staff, every control remains incomplete.

PART E

KRITIS: Security Services as an All-in-One Solution?

What KRITIS operators must demonstrate, opportunities and risks of an integrated model, criteria, procurement law and an integrated cost example.

CHAPTERS

E1 At a Glance
E2 What KRITIS Operators Must Demonstrate
E3 What “All-in-One” Means
E4 Opportunities of an Integrated Solution
E5 Risks and Limits
E6 Criteria for a Resilient Model
E7 Contract Award: Private and Public
E8 Cost Example and Economic Viability
E9 Decision Aid and Checklist
E10 Frequently Asked Questions (FAQ)

RELATED PARTS

Part A Video Surveillance & Video Alarm Monitoring for KRITIS-Relevant Facilities – the KRITIS legal framework in detail
Part C Security Services in Practice: Guarding or Plant Security – make or buy
Part B Monitoring of Hazard Alarm Systems, Alarm Response and Preventive Hazard Protection – monitoring center and intervention

KEY STATEMENTS FOR DECISION-MAKERS

E1 At a Glance

The ten most important points for executive managers and security officers in KRITIS companies.

1 **The KRITIS Umbrella Act has been in force since 17 March 2026.** According to the BBK (as of October 2026), the KRITIS Regulation with the thresholds is not yet in force – preparation should nevertheless start now.

2 **§ 13 requires a mix of measures:** site protection, monitoring of the surroundings, detection, access control, emergency and crisis management, personnel security – explicitly including the staff of external service providers.

3 **The considerations must be documented.** A unified concept with end-to-end documentation makes the evidence towards the authority considerably easier.

4 **Interfaces are a risk:** with six service providers and the operator, there are arithmetically 21 interfaces. Each can cost time in an emergency.

5 **All-in-one reduces interfaces** – but can create a concentration risk if the partner has no redundancy of its own.

6 **Consulting and delivery from one source require transparency:** the protection concept must be driven by the risk, not by the provider's own service catalogue.

7 **Manufacturer independence is the precondition** for an all-in-one partner not creating technical dependency.

8 **Public contracting authorities must in principle divide contracts into lots under § 97a GWB;** a single award is permissible on technical or economic grounds with a documented justification.

9 **A network model** – one contractual partner, many regional specialist companies – combines unified steering with SME-based delivery on site.

10 **The decision belongs in the risk analysis under § 12 KRITISDachG:** which model actually increases resilience?

KRITIS UMBRELLA ACT · BSIG · THE CONTRIBUTION OF SECURITY SERVICES

E2 What KRITIS Operators Must Demonstrate

The KRITIS Umbrella Act does not oblige operators of critical facilities to buy individual products but to run a verifiable overall system. This is exactly where the question of the right service-provider model starts.

E2.1 Obligations and the contribution of security services

Obligation	Rule	Contribution of security services
Risk analysis and assessment	§ 12 KRITISDachG	On-site threat and vulnerability analysis, offender's perspective, situational picture from incidents
Resilience measures and resilience plan	§ 13 KRITISDachG	Perimeter protection, video, detection, access control, personnel, alarm and response procedures
Personnel security incl. external service providers	§ 13 para. 3 no. 5	Security guard register, site-specific vetting, training, team continuity
Reporting of significant incidents	§ 18 KRITISDachG	Seamless event logs, initial report within hours
Approval and supervision by management	§ 20 KRITISDachG	Reporting, metrics, audits
Risk management incl. supply chain	§ 30 BSIG	IT security of video and alarm technology, secure monitoring center connection

E2.2 What a "mix of measures" means in practice

§ 13 para. 3 KRITISDachG names, by way of example, site protection through property perimeter demarcation, instruments for monitoring the surroundings, detection devices, access controls, risk and crisis management, and appropriate security management with regard to employees, including the staff of external service providers. These measures interlock: a camera without a monitoring center, a monitoring center without intervention or a gatehouse without current access data fulfils the purpose only in part. The core question is therefore not "who supplies what?" but "who is responsible for everything working together?"

> **Current status**
>
> The KRITIS Umbrella Act has been in force since 17 March 2026. The statutory regulation that uses thresholds to determine which facilities are critical was, according to the BBK, not yet in force in October 2026; there was therefore not yet any registration obligation. After classification the deadlines are short: registration after three months, risk analysis after nine, resilience measures after ten months. Operators who clarify their service-provider model now avoid time pressure in procurement and implementation. The legal framework is covered in detail in Chapter A2.

SERVICE BUILDING BLOCKS · ORGANIZATIONAL MODELS

E3 What “All-in-One” Means

“All-in-one” is understood very differently – from the facility-services group that supplies security on the side to the specialized security partner with a network. For KRITIS operators the precise distinction pays off.

E3.1 Service building blocks

Building block	Content
Consulting and concept	Risk analysis, protection objectives, security and resilience concept, tendering support
Security technology	Video, perimeter detection, intruder and hold-up alarm technology, access control – planning, installation, maintenance
Monitoring center	Monitoring connection, alarm verification, remote gate service, fault supervision, event documentation
Staffed security	Plant and site protection, reception and gatehouse, mobile patrol and intervention services, fire watches
Mobile solutions	Self-sufficient video towers for construction sites, interim protection and escalating situations
Emergency and crisis	Alarm and emergency plans, exercises, support during the event, debriefing
Evidence	Reports, metrics, audit documentation for authorities, insurers and executive management

E3.2 Organizational models compared

Model	Principle	Strengths	Weaknesses
Individual awards	a separate contract per service	Specialization, competition per trade	many interfaces, coordination rests with the operator
Facility package	security as part of a building-services contract	one framework contract, bundling effects	security often a side service, little KRITIS depth
General contractor with own staff	one provider delivers everything itself	unified management	dependency, regional gaps, possible manufacturer lock-in
Network model	one contractual partner steers specialized companies	one responsibility, regional strength, scalability	requires unified standards and tight steering

INTERFACES · RESPONSE TIME · EVIDENCE

E4 Opportunities of an Integrated Solution

The greatest advantage of an integrated model lies not in the price but in responsibility: one party vouches for the security chain being closed in an emergency.

E4.1 Fewer interfaces

Between n parties there are arithmetically n × (n − 1) ÷ 2 possible interfaces. Each stands for coordination, handovers and questions of responsibility – and, in the event of an incident, for possible delays.

Constellation	Parties	Possible interfaces
Operator and one integrated partner	2	1
Operator and three service providers (e.g. technology, monitoring center, personnel)	4	6
Operator and six service providers	7	21

With an integrated partner the internal interfaces do not disappear – but they are managed where the professional competence lies, not by the operator.

E4.2 Further advantages

- **Closed alarm chain:** detection, verification, intervention and documentation follow one shared alarm plan
- **Faster reporting:** a unified event log makes the 24-hour report under § 18 KRITISDachG easier
- **End-to-end evidence:** concept, measures, training and metrics are available in one structure (§ 13 para. 4)
- **Unified personnel security:** the same requirements for vetting, training and induction for all deployed staff
- **Scalability:** escalating situations, construction phases and new sites are covered from one source
- **Relief for the operator:** less contract, invoicing and coordination effort

> **Practical example: the alarm at 3:12 a.m.**
>
> Perimeter analytics report a person at the fence of a pumping station. In the single-award model, provider A's monitoring center checks the image, tasks provider B's intervention service and informs the operator, who calls provider C's maintenance service about a damaged camera location. In the integrated model these steps run according to one alarm plan, with one log and one contact person – the operator receives a complete report in the morning.

ADVOCATUS DIABOLI · COUNTERMEASURES

E5 Risks and Limits

Resilience means that one failure does not become a total failure. An all-in-one model can contradict exactly this principle – if it is not built accordingly.

E5.1 The main risks and how to counter them

Risk	What it consists of	Countermeasure
Concentration risk	If the partner fails, technology, monitoring center and personnel are gone at once	Redundant monitoring center, fallback concept, regional substitute staff, emergency handover
Dependency (lock-in)	Switching becomes expensive or technically impossible	open interfaces, manufacturer independence, data sovereignty with the operator, exit clause
Conflict of interest	The consultant preferentially recommends its own services	risk-based justification for each measure, transparency, second opinion for large investments
Quality in side services	“Can do everything” does not mean “can do everything well”	Metrics per service area, evidence from the specialist companies, audits
Opaque subcontractors	Unclear who actually works on site	Naming and approval of all subcontractors, identical evidence obligations
Loss of knowledge at the operator	In-house security competence withers	a designated responsible person, regular reports, joint exercises

> **Advocatus Diaboli: a contract is not a resilience concept**
>
> Awarding all security services to one partner does not mean the responsibility has been handed over. Under § 20 KRITISDachG, executive management remains responsible for implementation and supervision. An all-in-one contract is only a gain if the operator actively manages it, the performance is measurable and a plan exists for what happens if the partner itself fails.

E5.2 When all-in-one is not the best choice

- When the operator already has a strong in-house security organization with its own monitoring center and only adds individual services
- When individual trades are highly specialized, such as fire alarm systems with fire-service connection or nuclear-sector requirements
- When the provider cannot demonstrate redundancy or offers technology from only one manufacturer
- When no viable justification for a single award exists under procurement law

HOW OPERATORS RECOGNIZE QUALITY

E6 Criteria for a Resilient Model

The following criteria separate a viable integrated model from a bundle that only comes from a single source on paper.

1	**Redundancy**	Fallback monitoring center or redundant operation, substitute staff per region, documented emergency handover if the partner fails. Have the redundancy demonstrated to you.
2	**Manufacturer independence**	No commissions from manufacturers, open protocols and interfaces, technology remains operable with other partners.
3	**Data sovereignty**	Concepts, plans, access credentials, video and event data belong to the operator and are handed over in full at the end of the contract.
4	**Transparency**	Every measure is justified from the risk analysis; subcontractors are named and approved.
5	**Personnel security**	Security guard register, site-specific vetting to the operator's requirements, training and team continuity – including at subcontractors.
6	**Measurability**	Metrics per service area: response times, availability, staffing rate, patrol completion, defect resolution.
7	**Certification**	Alarm receiving center to DIN EN 50518, services to DIN 77200-1, occupational safety to DGUV Regulation 23.
8	**Exit capability**	Termination and transition rules, handover plan, the partner's duty to cooperate in a change.

The operator's cooperation

Even the best integrated model needs an active operator: a designated responsible person, up-to-date alarm and access data, notification of changes to plant and personnel, participation in exercises, and evaluation of the reports. Professional requests run via the partner's project or site supervisor – direct instructions to individual security officers are to be avoided, to rule out covert temporary agency work.

Cross-references

→ B3 Quality Criteria of a Monitoring Center
→ C6 Quality and Contract Award of Security Services

LOT PRINCIPLE · SINGLE AWARD · FRAMEWORK CONTRACTS

E7 Contract Award: Private and Public

Many KRITIS operators – municipal utilities, water boards, municipal clinics – are public contracting authorities. For them, “all-in-one” is first of all a question of procurement law.

E7.1 The lot principle

Public contracts must in principle be divided into partial and specialist lots to take account of SME interests. With the Act to Accelerate the Award of Public Contracts, this principle was transferred from § 97 para. 4 GWB (Act against Restraints of Competition) into the new § 97a GWB as of 1 July 2026; the exception for economic or technical reasons was retained word for word.

E7.2 When a single award can be justified

- **Technical reasons:** services are so closely interlinked that separate awards would endanger functionality – for instance detection, verification and intervention in one alarm chain
- **Special risk potential:** case law has recognized high risk potential and endangerment of the overall service as justification (Munich Higher Regional Court, Verg 10/18)
- **Economic reasons:** disproportionate coordination effort or significant extra costs from dividing into lots
- **Documentation:** the justification must address the specific individual case and be placed in the award file; administrative convenience is not enough

> **SMEs despite a single award**
>
> In a single award, public contracting authorities can oblige the contractor to give particular consideration to the interests of small and medium-sized enterprises when awarding subcontracts (§ 97a para. 5 GWB). A network model with regional, SME specialist companies fulfils this objective structurally.

E7.3 Private operators

Private operators are free in how they structure contracts. Framework contracts with unified standards and metrics have proven effective, in which individual service areas are priced, measured and, if necessary, terminated separately. In this way the operator combines the advantages of a single source with the ability to make targeted adjustments.

REGIONAL WATER UTILITY · INTEGRATED SERVICE PACKAGE

E8 Cost Example and Economic Viability

The example shows a typical integrated annual package. The inputs come from the model calculations in A7, B7, C7 and D8; all values net and non-binding.

Example: main plant and twelve outlying facilities

Service	Calculation	Costs per year
Gate service at the main plant, weekdays 6 a.m.–6 p.m.	3,000 h × 30.69 €	92,070 €
Remote gate at the main plant outside staffed hours	1,250 € × 12 months	15,000 €
Video alarm monitoring of all 13 sites	13 × 390 € × 12 months	60,840 €
Night patrols at 4 priority facilities	4 × 365 × 22 €	32,120 €
Intervention (assumption: 40 call-outs)	40 × 145 €	5,800 €
Maintenance of video and alarm technology	13 × 900 €	11,700 €
Concept, resilience-plan support, exercises	lump sum	12,000 €
Annual package, total		**229,530 €**

Equivalent to 19,127.50 € per month. Not included: investment in security technology, fencing and construction works, and special services during escalating situations.

Where the economic advantage lies

- Less coordination for the operator: one contract, one invoice, one reporting system instead of six
- No duplicated effort: monitoring center, intervention and technology use the same site data and alarm plans
- A needs-based mix: personnel where it is necessary; technology and the remote gate service where they suffice
- Framework-contract conditions: bundling several services and sites improves the terms

> **Advocatus Diaboli: integrated does not automatically mean cheaper**
>
> Individual services can be cheaper under individual awards, because specialist providers price their own trade sharply. The advantage of the integrated model lies in lower interface costs, faster response and simpler evidence – effects that appear in no single line item. Therefore compare total costs including your own steering effort, not hourly rates.

FOUR STEPS TO THE RIGHT MODEL

E9 Decision Aid and Checklist

The checklist guides the decision and is suitable as the basis for a paper to executive management.

Step 1 – Starting position	
☐	Check applicability under the KRITISDachG and BSIG; plan for the deadlines from the entry into force of the KRITIS Regulation
☐	Record existing contracts, technology, monitoring centers and personnel services; check terms and notice periods
☐	Document interfaces and known gaps from incidents and exercises

Step 2 – Assessment	
☐	Risk analysis under § 12 as the basis: which measures are needed, which dependencies arise?
☐	Compare models: individual awards, package, general contractor, network model
☐	Assess the concentration risk: what happens if the partner fails?
☐	For public contracting authorities: division into lots or a documented justification of the single award

Step 3 – Contract award and contract	
☐	Specification with metrics per area, redundancy and exit provisions
☐	Evidence: § 34a GewO, DIN EN 50518, DIN 77200-1, insurance, subcontractors
☐	Secure data sovereignty, open interfaces and handover obligations by contract

Step 4 – Steering	
☐	Designate a responsible person at the operator; evaluate reports and metrics monthly
☐	Joint exercises for incidents, reporting under § 18 and failure of the partner
☐	Keep the resilience plan and risk analysis up to date, review the model regularly

ANSWERED BRIEFLY AND RELIABLY

E10 Frequently Asked Questions (FAQ)

Does the KRITIS Umbrella Act prescribe a particular security provider or a particular model?

No. It requires suitable and proportionate measures and their comprehensible documentation. How the operator organizes them is left to the operator.

Can I transfer responsibility for resilience to a service provider?

The implementation yes, the responsibility no. Under § 20 KRITISDachG, executive management remains responsible for implementation and supervision.

Isn’t an all-in-one provider a concentration risk?

It can be. What matters are redundancy, open interfaces, data sovereignty with the operator and a plan for the partner’s failure.

May public KRITIS operators award security services as a single contract?

In principle the lot principle under § 97a GWB applies. A single award is permissible where technical or economic reasons require it and this is concretely documented.

How are the staff of external service providers vetted?

Security officers are recorded in the security guard register and checked for reliability. § 13 KRITISDachG additionally requires appropriate security management for employees, including external service providers.

Does one provider make it cheaper?

Not necessarily per individual service, but frequently in the overall view – through less coordination, faster response and simpler evidence.

What is a network model?

One contractual partner takes on responsibility and steering; regional specialist companies deliver to unified standards. This creates local proximity and consistent quality.

SECURITY · CONSULTING · CONCEPTION

SecuConCept: Integrated and Independent

SecuConCept combines manufacturer-independent consulting, security conception and operational delivery – as one contractual partner with a Germany-wide network.

Consulting

Applicability checks, risk analysis, model decision, tendering support

Conception

Security and resilience concepts, alarm and emergency plans, metrics and evidence

Security

Video and alarm monitoring, remote gate service, intervention, plant and site protection, reception, mobile patrols, video towers

Why SecuConCept?

- **SecuNET network model:** more than 350 specialized companies throughout Germany – one contractual partner, regional delivery, uniform quality requirements.
- **SecuNET for business clients:** business clients with an exclusive commitment to SecuConCept receive a personal key account manager and 24-hour support.
- **Redundant monitoring center:** certified alarm receiving center to DIN EN 50518 / VdS with a redundant monitoring-center structure – for monitoring connections, verification and the remote gate service.
- **Manufacturer-independent and experienced:** no commissions from manufacturers, “upgrade instead of replace” for existing technology, practical knowledge from plant security at major chemical sites.

Specialist portals and brands

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

CCTV-Security.de by SecuConCept – specialist portal for video towers, the alarm center, alarm response and implementation.

SecuFokus®
SICHERHEIT GEMEINSAM STEUERN.
BY SECUCONCEPT

SecuFokus by SecuConCept – Managing Security Together.
Specialist information and tools for operators, partners and service providers.

FREE INITIAL CONSULTATION

A Security Check for Your Company

Video, alarm monitoring, personnel, reception or a complete KRITIS concept – in a structured appointment with a clear recommendation for action.

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

LEGAL FOUNDATIONS · STANDARDS · CASE LAW · ONLINE SOURCES

List of Sources

Consolidated list for all parts. The letters in brackets show in which parts a source is used. Research status and retrieval of the online sources: November 2026.

Acts and regulations

- KRITIS Umbrella Act (KRITISDachG) of 11 March 2026, BGBl. 2026 I No. 66; amendment of § 8 by the Act of 21 July 2026, BGBl. 2026 I No. 221 (A, B, E)
- BSI Act as amended by the NIS-2 Implementation and Cybersecurity Strengthening Act, in force since 6 December 2025, in particular §§ 28, 30, 32, 38, 41, 65 (A, E)
- Regulation (EU) 2016/679 (GDPR); Federal Data Protection Act (BDSG); state data protection acts (A, B, D)
- German Trade Regulation Act (GewO), in particular § 34a and § 11b; Security Guarding Ordinance (BewachV) (A, B, C, D, E)
- German Identity Card Act (PAuswG), in particular § 1 para. 1 sentence 3 and § 20 para. 2 (D)
- Act against Restraints of Competition (GWB), § 97 para. 4 and § 97a as applicable from 1 July 2026 (E)
- Temporary Employment Act (AÜG); Occupational Safety Act, in particular § 8; Working Hours Act; Minimum Wage Act (C, E)
- Works Constitution Act (BetrVG), § 87 para. 1 nos. 1 and 6 (A, B, C, D)
- Criminal Code (StGB) §§ 32, 34, 123, 201; Code of Criminal Procedure (StPO) § 127 (A, B, C, D)
- Civil Code (BGB) §§ 229, 858 et seq., 903, 917, 1004, 1018; Road Traffic Regulations (StVO) §§ 35, 38 (B, C, D)
- Insurance Contract Act (VVG) § 28 (B)
- Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2024/2847 (Cyber Resilience Act) (A)

Case law

- ECJ, judgment of 30 March 2023 – C-34/21 (employee data protection) (A)
- Federal Administrative Court (BVerwG), judgment of 23 August 1991 – 8 C 37.90 (fees for police call-outs after alarm activation) (B)
- Administrative Court of Neustadt an der Weinstraße: fee of 120 € for an unjustified alert by an intruder alarm system (B)
- Munich Higher Regional Court (OLG München), decision of 25 March 2019 – Verg 10/18 (single award in cases of high risk potential) (E)
- Federal Procurement Chamber (VK Bund), decision of 26 February 2024 – VK 2-11/24 (justification of a single award) (E)

Standards and sets of rules

- DIN EN 62676 (series) – video surveillance systems for use in security applications, in particular Part 4 (A)
- DIN EN 50518 – alarm receiving center; VdS 3138 – emergency call and service monitoring centers (A, B, D, E)
- DIN EN 50131 (series) – intruder and hold-up alarm systems; VdS 2311 – planning and installation of intruder alarm systems (B)
- DIN EN 50136-1/-2 – alarm transmission systems and equipment (B)
- DIN VDE 0833-1/-2/-3 – hazard alarm systems; DIN 14675 – fire alarm systems; DIN EN 54 (B)
- DIN EN 1627 – burglary resistance of doors, windows and closures (B)
- DIN 77200-1:2022-10 – security services (A, B, C, D, E)
- DGUV Regulation 23 “Guarding and security services”; DGUV Rule 112-139 “Personal emergency signal systems” (C, D, E)
- Guideline for hold-up and intruder alarm systems with connection to the police (ÜEA guideline) (B)

Authorities, associations and guidance

- Federal Office of Civil Protection and Disaster Assistance (BBK): information and FAQ on the KRITIS Umbrella Act, as of October 2026 (A, E)
- Federal Office for Information Security (BSI): NIS-2 information and registration portal (A)
- German Data Protection Conference (DSK): guidance on video surveillance by non-public bodies; short paper No. 15 (A)
- Federal Network Agency and network operators: switch-off of the 2G networks (B)
- BHE / VdS: guidance on the defeat of intruder alarm panels and transmission devices; connection of fire alarm systems (B)
- IHK fact sheets on distinguishing instruction from the expert-knowledge examination in the guarding trade (C, D)
- Universally binding wage and remuneration collective agreements for security services 2026, including NRW, Baden-Württemberg, Hesse (C)
- US Federal Communications Commission (FCC): Covered List (A)

Online sources

Part	Source
A	Wikipedia: Kritis-Dachgesetz https://de.wikipedia.org/wiki/Kritis-Dachgesetz
A	coredinate: KRITIS-Dachgesetz und Sicherheitsdienst https://coredinate.de/blog/kritis-dachgesetz-sicherheitsdienst
A, E	datenraume.de: KRITIS-Dachgesetz 2026 https://datenraume.de/blog/kritis-dachgesetz/
A	DSN Group: NIS-2-Umsetzungsgesetz in Kraft https://www.dsn-group.de/datenschutz-notizen/das-nis-2-umsetzungsgesetz-ist-in-kraft-getreten-welche-schritte-sind-nun-erforderlich-4457509
A	Axians: NIS2UmsuCG – aktueller Stand https://www.axians-secure.de/blog/nis2-umsetzungsgesetz-nis2umsucg
A	PwC Legal: DSK-Orientierungshilfe Videoüberwachung https://legal.pwc.de/de/news/fachbeitraege/datenschutzkonferenz-veroeffentlicht-orientierungshilfe-zur-videoueberwachung
A	OpenKRITIS: Garantieerklärung § 9b BSIG https://www.openkritis.de/betreiber/komponenten_garantieerklaerung.html
A	OpenKRITIS: Kritische Komponenten https://www.openkritis.de/betreiber/kritische-komponenten.html
A	BDEW/VKU: Positionspapier zu § 41 BSIG https://www.bdew.de/media/documents/BDEW_VKU_Positionspapier_41_BSIG_NIS2-UmsuCG_Kritische_Komponenten_1.pdf
A	ictally: FCC Camera Ban 2026 https://ictally.com/resources/blog/fcc-chinese-camera-import-ban-nashville
B, C	DIN Media: DIN 77200-1:2022-10 https://www.dinmedia.de/de/norm/din-77200-1/348823032
B	BHE: Aufschaltung von Brandmeldeanlagen https://www.bhe.de/_Resources/Persistent/d/4/9/9/d49991c5c03ba5fe5262346a3f8250efc96e3fd7/leseprobe_10_kapitel_aufschaltung-von-brandmeldeanlagen-1.pdf

Part	Source
B	BHE: Aufschaltung von BMA auf die Feuerwehr https://www.bhe.de/_Resources/Persistent/b/2/c/8/b2c81ae48267cb526313291896282f8ed52f8ac5/2019-10-21_aufschaltung_von_bma_auf_feuerwehr.pdf
B	VdS/BHE: Überwindung von EMA-Zentralen https://www.VDS.de/fileadmin/Website_Content_Images/VdS_Publikationen/Rundschreiben_Security/30-03-2021_Infopapier_Ueberwindung_EMZ.pdf
B	BHE: Einbruchmeldetechnik https://www.bhe.de/_Resources/Persistent/d/5/d/b/d5db10152a56aff56a99c0945df2e5e546ad346d/Leseprobe%20_2.4_Kapitel_Einbruchmeldetechnik.pdf
B	Bundesnetzagentur: 2G-Abschaltung https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Breitband/2GAbschaltung/artikel.html
B	Verbraucherzentrale: 2G-Abschaltung https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/2gabschaltung-was-damit-auf-verbraucherinnen-zukommt-114129
B	LTO: VG Neustadt zur Fehlalarm-Gebühr https://www.lto.de/recht/nachrichten/n/vg-neustadt-kioskbesitzer-muss-fuer-polizeieinsatz-nach-fehlalarm-bezahlen/print.html
B	anwalt24: BVerwG 8 C 37.90 https://www.anwalt24.de/urteile/bverwg/1991-08-23/bverwg-8-c-3790
B, C	bpb: Private Sicherheitsdienste https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/571071/private-sicherheitsdienste/
B	Nordkurier: Fehlalarme der Feuerwehren https://www.nordkurier.de/panorama/wenn-feuerwehren-umsonst-ausruecken-4579918
C	IHK Köln: Erlaubnis nach § 34a GewO https://www.ihk.de/koeln/hauptnavigation/recht-steuern/bewachungsgewerbe-erlaubnis-nach-34a-gewo-5224494
C	IHK Rostock: Abgrenzung der Tätigkeiten nach § 34a https://www.ihk.de/rostock/aus-und-weiterbildung/weiterbildung/sachkundepruefung/abgrenzung-taetigkeiten-34a-6822272
C	IHK Bonn: Merkblatt Unterrichtung https://www.ihk-bonn.de/fileadmin/dokumente/Downloads/Weiterbildung/Weiterbildungspruefungen/Merkblatt-Unterrichtung_im_Bewachungsgewerbe.pdf
C	DGUV Vorschrift 23 https://publikationen.dguv.de/widgets/pdf/download/article/1105
C	Zoll: Lohntarifvertrag Sicherheit NRW https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/Arbeit/sicherheit_lohntarifvertrag_nrw_20250211.pdf?__blob=publicationFile&v=2
C	BDSW: Allgemeinverbindlichkeit Baden-Württemberg 2026 https://www.bdsw.de/images/tarifvertraege/ave/2026/AVE_BW_LTV_2026_0908.pdf
C	Hessische Landesregierung: Entgelttarifvertrag allgemeinverbindlich https://landesregierung.hessen.de/presse/entgelttarifvertrag-fuer-beschaeftigte-in-sicherheitsbranche-allgemeinverbindlich
C	Bundesregierung: Mindestlohn steigt https://www.bundesregierung.de/breg-de/suche/mindestlohn-steigt-2391010

Part	Source
D	Gesetze im Internet: § 20 PAuswG https://www.gesetze-im-internet.de/pauswg/__20.html
D	Bundestag WD 3-041-19: Ausweis-Scans https://bundestag.de/resource/blob/645674/0204d86f6cff7fd920d54703d7ea874b/WD-3-041-19-pdf-data.pdf
D	GIGA: Personalausweis kopieren https://www.giga.de/ratgeber/specials/personalausweis-kopieren-wie-geht-das-ist-das-erlaubt
D	Dr. Datenschutz: Besuchermanagement im Unternehmen https://www.dr-datenschutz.de/besuchermanagement-im-unternehmen/
D	IHK: Merkblatt Unterrichtung im Bewachungsgewerbe https://www.ihk.de/blueprint/servlet/resource/blob/4244936/9eab9ad2cecb3148f3b13fe41114d836/ihk-merkblatt-unterrichtung-bewachungsgewerbe-72018-data.pdf
D	IHK Hannover / DIHK: Unterrichtung oder Sachkundeprüfung https://www.hannover.ihk.de/blueprint/servlet/resource/blob/5294910/c65a3da3c4cc2401b390efef2cc615b8/merkblatt-up-oder-skp-dihk-data.pdf
E	noba-experts: KRITIS-Dachgesetz, Stand Oktober 2026 https://www.noba-experts.de/wissen/themen/kritis-dachgesetz
E	CMS: KRITIS-Verordnung https://cms.law/de/deu/legal-updates/kritis-verordnung-was-betreiber-kritischer-anlagen-jetzt-wissen-muessen
E	gesetze.legal: § 13 KRITISDachG https://gesetze.legal/bund/kritisdachg/13
E	Lobbyregister: BDSW-Stellungnahme zur Zuverlässigkeitsüberprüfung https://www.lobbyregister.bundestag.de/media/67/e9/612529/Stellungnahme-Gutachten-SG2509080026.pdf
E	cosinex: Gesamt- vs. Losvergabe, § 97a GWB https://blog.cosinex.de/2018/09/13/gesamt-vs-losvergabe-wie-begruendet-man-eine-gesamtvergabe-rechtssicher/
E	vergabeblog: OLG München Verg 10/18 https://vergabeblog.de/2019-07-01/hohes-risikopotential-rechtfertigt-gesamtvergabe-olg-muenchen-beschl-v-25-03-2019-verg-10-18/
E	vergabeblog: VK Bund VK 2-11/24 https://vergabeblog.de/2024-06-10/gesamtvergabe-von-leistungen-auf-eine-gute-begruendung-kommt-es-an-vk-bund-beschl-v-26-02-2024-vk2-11-24/
E	lxgesetze: § 97a GWB https://lxgesetze.de/gwb/97a

Legal status and liability: research status November 2026. This manual does not constitute legal advice. Cost figures are model calculations and non-binding reference values (net).

© 2026 SecuConCept · Owner: Torsten Bentlage · Distribution in unchanged form is expressly welcome.