As of: November 2026

TECHNICAL MANUAL

KRITIS & INTEGRATED SECURITY

Security Services as an All-in-One Solution?

For Critical Infrastructure (KRITIS) Operators: Opportunities, Limits, Decision

SPECIALIST PORTALS AND BRANDS OF SECUCONCEPT

KRITIS Umbrella Act & BSIG: what operators must demonstrate

One provider for everything – interfaces, concentration risk, procurement law

Criteria for a resilient model · Cost example · Decision guide

Quality through Trust

SecuConCept · Security – Consulting – Conception · www.secuconcept.de

0800 666 000 4 · vertrieb@secuconcept.de

ABOUT THIS MANUAL

One Provider for Everything – Solution or Risk?

Operators of critical facilities will in future have to plan, implement and demonstrate their resilience holistically: risk analysis, physical protection, personnel, alarm and reporting procedures, exercises. Many are therefore asking whether a single security partner for consulting, technology, monitoring center and personnel is a better choice than a patchwork of individual contracts.

The honest answer is: it depends on how the model is built. This manual shows what all-in-one can deliver in the KRITIS environment, where it creates risks that contradict the very principle of resilience, how public contracting authorities must proceed under procurement law – and by which criteria operators can recognize a resilient model.

Contents

1 At a Glance 3

2 What KRITIS Operators Must Demonstrate 4

3 What “All-in-One” Means 5

4 Benefits of an Integrated Solution 6

5 Risks and Limitations 7

6 Criteria for a Resilient Model 8

7 Procurement: Private and Public 9

8 Cost Example and Economic Viability 10

9 Decision Guide and Checklist 11

10 Frequently Asked Questions (FAQ) 12

11 SecuConCept: Integrated and Independent 13

12 Sources and Legal Status 14

KEY MESSAGES FOR DECISION-MAKERS

01 At a Glance

The ten most important points for executive management 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 ordinance containing the thresholds is not yet in force – preparation should nevertheless begin now.

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

3 **The considerations must be documented.** A unified concept with consistent end-to-end documentation makes it considerably easier to demonstrate compliance to the authority.

4 **Interfaces are a risk:** with six service providers plus the operator, there are arithmetically 21 interfaces. In an emergency, each one can cost time.

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

6 **Consulting and implementation from a single source** require transparency: the protection concept must be driven by the risk, not by the provider's own service catalog.

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

8 **Public contracting authorities** must, as a rule, divide contracts into lots under § 97a GWB (German Act against Restraints of Competition); a single-source award is permissible on technical or economic grounds with documented justification.

9 **A network model** – one contractual partner, many regional specialist firms – combines unified control with implementation by regional SMEs on site.

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

> **Important note on legal validity**
>
> This manual provides professional orientation and is no substitute for legal or procurement advice. At the time of research (November 2026), the KRITIS ordinance was not yet in force; thresholds and deadlines may change. All cost figures are model calculations and non-binding reference values (net).

KRITIS UMBRELLA ACT · BSIG · CONTRIBUTION OF SECURITY SERVICES

02 What KRITIS Operators Must Demonstrate

The German KRITIS Umbrella Act (KRITISDachG) does not oblige operators of critical facilities to buy individual products, but to maintain a verifiable overall system. This is exactly where the question of the right service-provider model begins.

2.1 Obligations and the contribution of security services

Obligation	Legal norm	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 (3) no. 5	Guard register (Bewacherregister), site-specific vetting, training, team continuity
Reporting of significant incidents	§ 18 KRITISDachG	Complete incident logs, initial report within hours
Approval and oversight by executive management	§ 20 KRITISDachG	Reporting, key performance indicators, audits
Risk management incl. supply chain	§ 30 BSIG (German BSI Act)	IT security of video and alarm signaling technology, secure monitoring-center connection

2.2 What "mix of measures" means in practice

§ 13 (3) KRITISDachG lists, by way of example, physical protection through property perimeters, instruments for monitoring the surroundings, detection equipment, access controls, risk and crisis management, and appropriate security management with regard to employees, including the personnel of external service providers. These measures interlock: a camera without a monitoring center, a monitoring center without response capability, or a gatehouse without up-to-date access data serves its purpose only in part. The core question is therefore not "Who supplies what?" but "Who is responsible for making everything work together?"

> **Current status**
>
> The KRITIS Umbrella Act has been in force since 17 March 2026. The statutory ordinance that uses thresholds to determine which facilities are critical was, according to the BBK, not yet in force in October 2026; a registration obligation therefore did not yet exist. Once a facility has been classified, 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.

SERVICE MODULES · ORGANIZATIONAL MODELS

03 What “All-in-One” Means

“All-in-one” is understood in very different ways – 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 is worth making.

3.1 Service modules

Module	Scope
Consulting and conception	Risk analysis, protection goals, security and resilience concept, tender support
Security technology	Video, perimeter detection, intrusion and hold-up alarm systems, access control – design, installation, maintenance
Monitoring center	Alarm monitoring, alarm verification, remote gatehouse, fault monitoring, incident documentation
Manned guarding	Plant and site security, reception and gatehouse, mobile patrol and alarm response services, fire watches
Mobile solutions	Self-sufficient video towers for construction sites, interim protection and heightened threat situations
Emergency and crisis	Alarm and emergency plans, exercises, support during incidents, follow-up
Evidence and records	Reports, KPIs, audit documents for authorities, insurers and executive management

3.2 Organizational models compared

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

INTERFACES · RESPONSE TIME · EVIDENCE

04 Benefits of an Integrated Solution

The greatest advantage of an integrated model lies not in the price but in the responsibility: one party ensures that the security chain is closed when it matters.

4.1 Fewer interfaces

Between n parties there are arithmetically n × (n − 1) ÷ 2 possible interfaces. Each one stands for coordination, handovers and questions of responsibility – and, in 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 expertise lies, and not by the operator.

4.2 Further advantages

- **Closed alarm chain:** detection, verification, response and documentation follow one common alarm plan
- **Faster reporting:** a unified incident log makes the 24-hour report under § 18 KRITISDachG easier
- **End-to-end evidence:** concept, measures, training and KPIs are available in a single structure (§ 13 (4))
- **Unified personnel security:** the same requirements for vetting, training and briefing apply to all deployed staff
- **Scalability:** heightened threat situations, construction phases and new sites are covered from a single source
- **Less burden on the operator:** less contract, invoicing and coordination effort

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

DEVIL'S ADVOCATE · COUNTERMEASURES

05 Risks and Limitations

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

5.1 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 lost at the same time	Redundant monitoring center, fallback concept, regional replacement 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	Consultant preferentially recommends the provider's own services	risk-based justification for every measure, transparency, second opinion for major investments
Quality in secondary services	"Can do everything" does not mean "does everything well"	KPIs per service area, credentials of the specialist firms, audits
Non-transparent subcontractors	Unclear who actually works on site	Naming and approval of all subcontractors, identical evidence obligations
Loss of expertise at the operator	In-house security competence withers away	own responsible person, regular reports, joint exercises

Devil's advocate: a contract is not a resilience concept

An operator who awards all security services to one partner has not handed over the responsibility. Under § 20 KRITISDachG, executive management remains responsible for implementation and oversight. 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.

5.2 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 needs to add individual services
- When individual trades are highly specialized, such as fire alarm systems connected to the fire department or nuclear-related requirements
- When the provider cannot demonstrate redundancy or offers technology from only one manufacturer
- When there is no sustainable justification for a single-source award under procurement law

HOW OPERATORS RECOGNIZE QUALITY

06 Criteria for a Resilient Model

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

1	**Redundancy**	Fallback monitoring center or redundant operation, replacement 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 data, video and incident 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**	Guard register, site-specific vetting to the operator's specifications, training and team continuity – including at subcontractors.
6	**Measurability**	KPIs per service area: response times, availability, staffing rate, patrol completion, defect resolution.
7	**Certification**	Alarm receiving center per DIN EN 50518, service delivery per DIN 77200-1, occupational safety per DGUV Regulation 23.
8	**Exit capability**	Termination and transition rules, handover plan, partner's duty to cooperate in a changeover.

Operator involvement

Even the best integrated model needs an active operator: a designated responsible person, up-to-date alarm and access data, notification of changes to facilities and personnel, participation in exercises, and evaluation of the reports. Technical matters are routed through the partner's project or site manager – direct instructions to individual security officers should be avoided in order to rule out covert temporary agency work (Arbeitnehmerüberlassung).

LOT PRINCIPLE · SINGLE-SOURCE AWARD · FRAMEWORK CONTRACTS

07 Procurement: Private and Public

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

7.1 The lot principle

Public contracts must, as a rule, be divided into partial and specialist lots in order to take the interests of small and medium-sized enterprises into account. With the Act to Accelerate the Award of Public Contracts, this principle was moved on 1 July 2026 from § 97 (4) GWB into the new § 97a GWB (German Act against Restraints of Competition); the exemption for economic or technical reasons was retained word for word.

7.2 When a single-source award can be justified

- **Technical reasons:** services are so closely interlinked that a separate award would jeopardize functionality – for example detection, verification and response within one alarm chain
- **Particular risk potential:** case law has recognized high risk potential and the jeopardizing of the overall service as justification (OLG München, Verg 10/18)
- **Economic reasons:** disproportionate coordination effort or significant additional costs if the contract is divided into lots
- **Documentation:** the justification must address the specific individual case and be recorded in the procurement file; administrative convenience is not sufficient

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

7.3 Private operators

Private operators are free in how they structure their contracts. Framework contracts with uniform standards and KPIs have proven effective, in which individual service areas are priced, measured and, where necessary, also 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

08 Cost Example and Economic Viability

The example shows a typical integrated annual package. The rates are taken from the model calculations in the other SecuConCept manuals; all values are net and non-binding.

Example: main plant and twelve outstations

Service	Calculation	Cost per year
Gatehouse service at the main plant, weekdays 6 a.m.–6 p.m.	3,000 h × 30.69 €	92,070 €
Remote gatehouse for 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-time mobile patrols at 4 priority facilities	4 × 365 × 22 €	32,120 €
Alarm response (assumption: 40 call-outs)	40 × 145 €	5,800 €
Maintenance of video and alarm signaling technology	13 × 900 €	11,700 €
Concept, resilience-plan support, exercises	flat rate	12,000 €
Total annual package		**229,530 €**

Equivalent to 19,127.50 € per month. Not included: investment in security technology, fencing and construction works, and additional services in heightened threat 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, alarm response and technology use the same site data and alarm plans
- **Needs-based mix:** personnel where it is necessary; technology and remote gatehouse where they suffice
- **Framework-contract terms:** bundling several services and sites improves the conditions

> **Devil's advocate: integrated does not automatically mean cheaper**
>
> Individual services can be cheaper when awarded separately, because specialist providers price sharply in their own trade. 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 management effort, rather than hourly rates.

FOUR STEPS TO THE RIGHT MODEL

09 Decision Guide and Checklist

The checklist leads through the decision and is suitable as the basis for a proposal to executive management.

Step 1 – Starting position	
☐	Check whether you fall under the KRITISDachG and BSIG; plan for the deadlines that start when the KRITIS ordinance enters into force
☐	Record existing contracts, technology, monitoring centers and guarding services; check contract 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 necessary, which dependencies arise?
☐	Compare models: individual contracts, package, general contractor, network model
☐	Assess the concentration risk: what happens if the partner fails?
☐	For public contracting authorities: division into lots or documented justification of a single-source award

Step 3 – Award and contract	
☐	Service specification with KPIs per area, redundancy and exit provisions
☐	Evidence: § 34a GewO (German Trade Regulation Act), DIN EN 50518, DIN 77200-1, insurance, subcontractors
☐	Contractually secure data sovereignty, open interfaces and handover obligations

Step 4 – Ongoing management	
☐	Designate a responsible person at the operator; evaluate reports and KPIs 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

10 Frequently Asked Questions (FAQ)

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

No. It requires suitable and proportionate measures and their verifiable 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 oversight.

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 failure of the partner.

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

As a rule, the lot principle under § 97a GWB applies. A single-source award is permissible if technical or economic reasons require it and this is specifically documented.

How is the personnel of external service providers vetted?

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

Does a single provider make it cheaper?

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

What is a network model?

One contractual partner assumes responsibility and overall control; regional specialist firms implement to uniform standards. This creates local proximity and consistent quality.

SECURITY · CONSULTING · CONCEPTION

11 SecuConCept: Integrated and Independent

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

Consulting

Applicability check, risk analysis, model decision, tender support

Conception

Security and resilience concepts, alarm and emergency plans, KPIs and compliance evidence

Security

Video and alarm monitoring, remote gatehouse, alarm response, plant and site security, reception, mobile patrols, video towers

Why SecuConCept?

- **SecuNET network model:** more than 350 specialized firms nationwide – one contractual partner, regional implementation, uniform quality requirements.
- **SecuNET for corporate clients:** corporate clients with an exclusive commitment to SecuConCept receive a personal key account manager and 24-hour support.
- **Redundant monitoring center:** certified alarm receiving center per DIN EN 50518 / VdS with a redundant monitoring-center structure – for alarm monitoring, verification and remote gatehouse services.
- **Manufacturer-independent and experienced:** no commissions from manufacturers, “upgrade instead of replace” for existing technology, practical expertise 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, 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

KRITIS model check for your company

Applicability, existing contracts, interfaces and the right service-provider model – 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 Köln

FOR REFERENCE

12 Sources and Legal Status

Legal foundations

- KRITIS Umbrella Act (KRITISDachG) of 11 March 2026, Federal Law Gazette (BGBl.) 2026 I No. 66, in particular §§ 8, 12, 13, 18, 20
- German BSI Act (BSIG) as amended by the NIS2 Implementation Act, in particular §§ 30, 32, 38
- German Act against Restraints of Competition (GWB), § 97 (4) and § 97a as in force from 1 July 2026
- § 34a GewO (German Trade Regulation Act), Security Guard Ordinance (BewachV); Temporary Agency Work Act (AÜG)

Case law and authorities

- OLG München (Munich Higher Regional Court), decision of 25 March 2019 – Verg 10/18 (single-source award in cases of high risk potential)
- VK Bund (Federal Public Procurement Tribunal), decision of 26 February 2024 – VK 2-11/24 (justification of a single-source award)
- Federal Office of Civil Protection and Disaster Assistance (BBK): information on the KRITIS Umbrella Act, as of October 2026

Standards

- DIN EN 50518 (alarm receiving center); DIN 77200-1:2022-10 (security services); DGUV Regulation 23
- Other SecuConCept manuals: Video Surveillance & Video Alarm Monitoring for KRITIS · Alarm Monitoring, Alarm Response & Prevention · Security Services in Practice · Reception & Gatehouse Services

Legal status and liability: Research status November 2026. The KRITIS ordinance was not yet in force at that time. This manual does not constitute legal or procurement advice. All cost figures are model calculations and non-binding reference values (net).

© 2026 SecuConCept · Owner: Torsten Bentlage · Distribution in unaltered form is expressly encouraged.