Dallmeier

incl. project checklists
and worldwide CRITIS
legal framework
(a.o. EU directives NIS-2 and RCE)

CYBERSECURE VIDEO TECHNOLOGY

FOR CRITICAL INFRASTRUCTURES AND OTHER ESSENTIAL AND IMPORTANT ENTITIES

BEST PRACTICES GUIDE

For decision makers of CRITIS operators and entities
for physical and digital security managers
for planners, installers and system integrators
for authorities and politicians

MADE IN GERMANY

See more.

CONTENT

Scope of this guide: CRITIS legal framework, country-specific scope and objective 2

1 CRITIS: target of attach and object of global security policy 4
1.1 The CRITIS resilience triangle 5
1.1.1 Conventional and physical threats 6
1.1.2 Cyber threats 6
1.1.3 Investors and producers from third countries 10

2 Staff shortages jeopardise security and business continuity 16
2.1 Automation via video technology as a way out and an opportunity 17

3 Critical infrastructures 22
3.1 Legal framework Germany 22
3.1.1 Classification of critical infrastructures 22
3.1.2 Competent supervisory authority BSI, laws and regulations 24
3.1.3 Legal brief overview 27
3.2 Legal framework Europe 36
3.3 Legal framework international (non-EU) 51

4 Which “stumbling blocks” are to be expected in a CRITIS video project? 56
4.1 Costs: justify and argue 56
4.2 Infrastructure: collecting plans and information 58
4.3 Environmental protection and landscape: respect sensitivities and pay attention to the appropriate technology 60
4.4 Team members and project participants 61

5 No fear of data protection – top priority cybersecurity 62
5.1 Initial or beginner’s mistake: data protection as the “enemy” 62
5.2 Video monitoring in accordance with GDPR and the obligatory notice board 64
5.3 The better the image quality, the better the purpose fulfilment 67
5.4 Educating helps against resistance 68
5.5 Privacy & Security by Design 69
5.6 Cybersecurity priority: weakest link in the supply chain decides 70
5.7 What does manufacturer ethics have to do with data protection and data security? 75

6 Public & press: a communication concept helps 77
6.1 Closing know-how gaps and involving the public 77
6.2 Instead of “cold shoulder”: rather show understanding 78

7 Technology and financial decisions 79
7.1 How many cameras for which area? 80
7.2 What actually is “minimum resolution” and how much do I need? 81
7.3 The camera challenge: large areas, long distances 82

7.4 The software challenge: large selection, many functions 84
7.5 Best-of-breed or all from one source or both? 86
7.6 Planning is good – planning in 3D is (even) better 89
7.7 Artificial intelligence: between hype and smart assistance system 91
7.8 Economic efficiency: “tell me, how much is one of these cameras?” 101
7.9 Not the cheapest, but the most economical offer 101
7.10 Tenders: seperate lots with expensive interdependencies 104

8 The right partner 105

9 Questionnaire for your own preparation 106
9.1 Political, organisational and legal conditions 109
9.2 Operational conditions 110
9.3 Infrastructures & synergies 110
9.4 Technology decisions & cost consideration 111
9.5 Check of the manufacturer regarding data protection, data security, ethics and AI 113

10 Support for your CRITIS project 118

11 Collection of additional information 119
Critical Infrastructures (CRITIS) 119
Data protection, data security, information security, IT and cybersecurity 124
Artificial intelligence, video analysis and co. 125
Video technology and video planning 125
Tendering & economy 126

11/2024 . V1.0.0

EDITORIAL

Dear Reader,

Thank you for your interest in our best practices guide.

In many countries around the world, the term, scope and regulation of “classic” critical infrastructures is becoming increasingly broad. Broader in the sense of the economic sectors, institutions and companies affected as well as in the sense of the state-legal regulation of the content of these companies. In addition to cybersecurity, physical security and resilience are also increasingly being regulated. The term “Critical infrastructures” – or “CRITIS” – describes the critical, particularly vital and therefore also particularly ”attack-prone” organisations of an economy – in the truest and extended sense of the word. With regard to the notation, for the sake of simplicity, we will continue to speak of CRITIS or the extended CRITIS affected group or “CRITIS and essential and important entities” in the following.

With regard to the threat situation of CRITIS, for example, in Germany in 2023 a special situation report by the Federal Office for Information Security showed that Germany’s “high-value targets” could increasingly become the target for politically motivated cyberattacks. Similar reports of digital or physical attacks on CRITIS could also be read in many other countries around the world. In the wake of these rapidly changing threat scenarios, security, protection and resilience of CRITIS encompasses much more than cybersecurity, to reiterate. Conventional physical threats as well as geopolitical risks coming from the changing dynamics with investors and manufacturers from authoritarian states create a novel situatin for many.

As a security company with experience around security and CRITIS since 1984, we hear about related problems and issues in almost all CRITIS surveillance projects – whether in decision-making, licensing, public discussion, planning, technology development, or in the field of security.
This is also understandable in many respects: in contrast to their usual routine tasks, many critical infrastructure managers may only carry out a video project once or twice in their professional lives.

Nevertheless, other CRITIS operators and CRITIS managers have already gained a lot of experience. So, as a manufacturer and Dallmeier Group with a large number of CRITIS projects, we thought: Let’s gather this experience and make it available to all interested parties.

The result is a practical guide for those involved in the decision-making process, for experts from the fields of “physical corporate security”, “IT and information security” and “data protection”, for those responsible for resilience and risk, for those responsible for related fields, for the tendering authorities involved, for planners and specialist installers, for supervisory and responsible authorities and for executive and legislative policy-makers.

We hope you will find this document helpful and interesting information to assess, plan, decide on and successfully implement video surveillance projects in CRITIS and essential and important entities.
I hope you enjoy reading it.

Jürgen Seiler,
Head of Business Development CRITIS, Dallmeier

PS: If you have any ideas, criticism or feedback for us, we happily receive your e-mail to critis@dallmeier.com

SCOPE OF THIS GUIDE: CRITIS LEGAL FRAMEWORK, COUNTRY-SPECIFIC SCOPE AND OBJECTIVE

History and scope of application
First of all, an important note on the genesis, the country of origin and – in relation to the global CRITIS legal framework – the relevance and the "country-specific, geographical scope" of this practical guide.

This practical guide was originally written for a German audience. In the German-language version (download here if you are interested), chap. 3 on the CRITIS legal framework focuses specifically on Germany and expands on the European Union (EU).

This English-language practical guide is more broadly defined by the CRITIS legal framework and is applicable worldwide. As a general and universal compendium, it also covers international issues and regulatory aspects.

From the perspective of your respective "CRITIS country", the country-specific CRITIS laws are of course to be found out and observed in detail and independently when affected.

For comparability, understanding and your own classification, we have decided to list helpful references and information on German and EU-wide legislative CRITIS regulation in chap. 3, also in this international, English-language version of the practical guide. All other chapters of this Practical Guide apply worldwide, of course, regardless of country and language version.

Data protection/GDPR
The provisions of the EU General Data Protection Regulation (in chap. 5) can be used as a data protection reference or comparative "highest data protection benchmark" regardless of country. The data protection provisions of the EU GDPR even apply directly to controllers or processors in non-EU countries in certain cases. These cases are defined in Article 3(2) of the GDPR "Territorial Scope", according to which it is not the location of the data processing that is decisive, but rather the orientation of the data processing towards the EU or towards EU citizens or data subjects located in the EU (market location principle). What the framework of this guide does not allow for: Individual country-specific regulations on CRITIS and data protection. Our core competence is primarily not laws, but increasing the physical security and resilience of our customers through forward-looking and cyber-secure video surveillance technology "Made in Germany / Made in Europe".

Global challenges and widening the definition of "CRITIS"
A modern economy is vitally dependent on intact and resilient infrastructures in both the physical and digital spheres for its functioning, for the creation of prosperity and growth, but also for its adaptability to changing economic and geopolitical conditions. Critical infrastructure facilities and the companies that are otherwise important for a national economy are faced with a multitude of challenges not only in their economic activities, but also in the practical implementation of "secure processes". The network character of these processes on a worldwide level, as well as the increasing digitalisation of all economic sectors, leads to an increased vulnerability to external, often uncontrollable influencing factors. Information and security technology in critical plants and important, system-relevant companies plays a central role in this. Their own functional, data- and cybersecurity and resilience is also the basis for the security

of supply of an economy, from electricity and water supply, medical care, food supply and its transport, to the disposal of municipal waste.

In many countries around the world, the concept, scope and regulation of "classic" critical infrastructures is becoming increasingly broad. Broader in the sense of the economic sectors, institutions and companies affected as well as in the sense of the state-legal regulation of the content of these companies. In addition to cybersecurity, physical security and resilience are also increasingly being regulated.

EU RCE and NIS-2: "critical facilities", essential and important entities

In Europe, for example, resilience and physical security will be regulated for the first time by the EU RCE Directive adopted in December 2022 and the national implementation laws (deadline October 2024). In terms of scope and quantitative impact, the new EU NIS-2 Directive, which was also adopted in December 2022, will regulate not only the classic CRITIS operators ("operators of critical facilities" – 1st category), but also other essential (2nd category) and important (3rd category) companies, entities and institutions from certain other economic sectors (e.g. manufacturing industry or hazardous materials industry or postal and courier services) with regard to network and information security.

The entire security chain is only as strong as its weakest link

For the use of video technology in CRITIS, this means in concrete terms: The overall cybersecurity and vulnerability of CRITIS depends not only, but also on the cybersecurity of the video products. In Europe, the new EU NIS-2 Directive justifiably takes this important security link between the CRITIS operator or the essential and important entity and the manufacturer/supplier into regulatory account in Article 21 on "Risk management measures in the area of cybersecurity": In Article 21 letter (d), it explicitly requires "security in the supply chain".

1 CRITIS: TARGET OF ATTACH AND OBJECT OF GLOBAL SECURITY POLICY

Critical infrastructures have always and since the beginning of 2022 increasingly been targets of attack and the subject of global security policy.

The spy balloon launched over the USA in February 2023 may be seen as a symbol of the heightened global geopolitical security awareness and the associated awareness and sensitivity. According to a newspaper report in the Washington Post in February 2023 ("Chinese balloon part of vast aerial surveillance programme, U.S.") says China has used spy balloons on several occasions to spy on military and critical facilities of other states that are important for national security.

In Europe, at the latest since the physical sabotage attacks on the Nord Stream pipelines in autumn 2022 or most recently the sabotage attacks in France on the railroads and digital infrastructure shortly before the Olympic Games 2024, CRITIS protection gained increased attention: among CRITIS operators, the population, but also in politics. As a result, the CRITIS legislative process in Europe (and in Germany) accelerated.

For European CRITIS operators and other essential and important facilities, two directives were adopted in December 2022, which the 27 EU states must transpose into national laws by October 2024:

- NIS-2: Network and Information Security 2 Directive
  DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union
- RCE: Resilience of Critical Entities Directive (in German-speaking countries often CER: Critical Entities Resilience)
  DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities
- More on this in chap. 3.2

With this, the European legislators made it clear: CRITIS are industrial sectors that the state must protect and regulate more intensively and holistically through special measures – classically "physical" as well as digitally "cyber-technical".

Similar legal tendencies for the regulation of critical infrastructures can be observed worldwide. Please find out the corresponding national regulations for your country and project and observe them if you are affected or if your customers are affected.

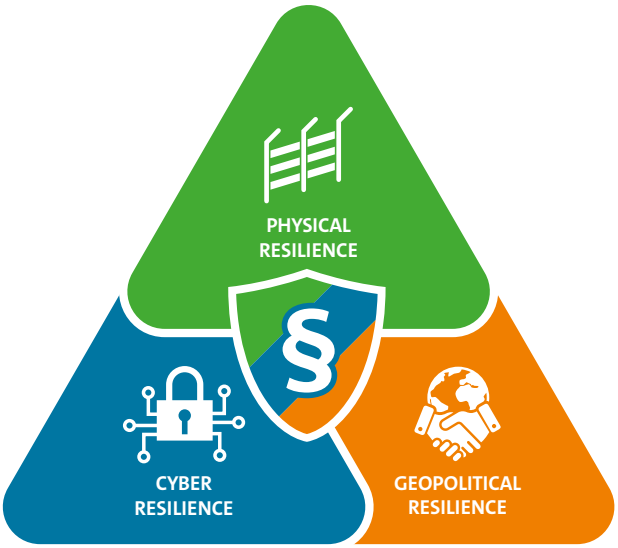
At the international level, NATO and the EU agreed in January 2023 on closer cooperation to protect critical infrastructure, especially against the backdrop of risks posed by "authoritarian actors".

It is about national and international legal sovereignty

The terrible geopolitical escalation in February 2022 openly demonstrates to the global community that critical infrastructures, first and foremost energy supply, information technology and telecommunications as well as transport and traffic, in addition to their actual functional-technical tasks, also acquire geostrategic, geopolitical and security policy significance. Peace and the rule of law are suddenly no longer a matter of course for industry, especially critical infrastructure. They seem to be mutually dependent. The technical and geopolitical integrity of critical infrastructures become "bargaining chips" for peace and the rule of law in the world. Critical infrastructures are therefore not only about technological and digital sovereignty, but also about the economic and political sovereignty of each individual country or of communities of states such as the European Union.

> *"You can never solve problems*
>
> *with the same mindset that created them."*
>
> **Albert Einstein,** physicist

1.1 THE CRITIS RESILIENCE TRIANGLE



The CRITIS resilience triangle
(with accompanying, governmental regulation)

In the spirit of Einstein's demand, we as the manufacturer Dallmeier want to set a good example and speak in the following not of the CRITIS threat triangle, but with a positive mindset of the CRITIS resilience triangle.

With this practical guide and our video solutions, we contribute to more CRITIS security and protection and to problem solving with regard to all dimensions of the resilience triangle, in the spirit of Einstein's admonishing words. And of course in the sense of all CRITIS operators.

Adjacent graphic highlights the resilience to the individual "threats" and "risks".

Conclusion:
The sectors “state and administration” and “media and culture” are not subject to regulation by the BSIG.

Which organisations and companies (“size classes”) fall under regulated CRITIS?
After the BSIG was passed, the question was raised in many places as to which companies actually belong to the operators of critical infrastructure within the meaning of the BSIG.

The ultimately regulated critical infrastructures and the ultimately regulated organisations and enterprises shall be determined in more detail by **statutory order** pursuant to section 10(1) BSIG.

This legal ordinance is called: BSI Criticality Ordinance
“Ordinance on the Designation of Critical Infrastructures under the BSI Act”, in short BSI (DE) Critical Infrastructure Ordinance (BSI-CRITISV) (DE).

The BSI Criticality Ordinance defines thresholds to be exceeded (type of “size classes”), installations, operators, coverage levels and the question “what are critical services”.

If the defined thresholds and criteria are reached or exceeded, the statutory reporting and verification obligations of the BSIG apply to CRITIS operators.

The BSI recommends the CRITIS Implementation Plan (“UP CRITIS”) as a freestyle
Even if the facilities fall below the threshold values of the BSI Critical Infrastructure Ordinance, the BSI recommends (voluntary) participation in the UP CRITIS. The UP CRITIS (UP stands for implementation plan) is a public-private cooperation between operators of critical infrastructures, their associations and the responsible government agencies.

3.1.2 COMPETENT SUPERVISORY AUTHORITY BSI, LAWS AND REGULATIONS

The following information is current as of September 2024.

The Federal Office for Information Security (BSI)

- Year 1991
- BSI according to website: The Federal Office for Information Security (BSI) is the federal government’s cybersecurity authority and the shaper of secure digitalisation in Germany.
- BSI acc. to §1 BSIG (DE): The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) is a higher federal authority in the portfolio of the Federal Ministry of the Interior, for Construction and Home Affairs. It is the central agency for information security at the national level.

The BSI Act (BSIG)

- Year 2009 (since then amended several times, especially 2015/2021 and scheduled for 10_2024)
- Act on the Federal Office for Information Security (BSI)
- BSIG originally only regulated the establishment and tasks of the Federal Office for Information Security
- The BSIG is the "authoritative CRITIS law", i.e. it defines security in the information technology of critical infrastructures, especially in sections 8a ff (DE).
- The BSIG defines the security requirements for the operators of the CRITIS and NEW since 2022 also optionally the security requirements for manufacturers/suppliers of critical components ("Lex Huawei").
- An amendment of the BSIG is planned for October 2024, by the NIS-2 Implementation and Cybersecurity Strengthening Act (NIS-2 UmsuCG).
- The law in detail: BSI Act/BSIG (DE)

The IT Security Act 2.0 (IT-SiG 2.0)

- Year 2021, entered into force in May 2021
- Second Act on Increasing the Security of Information Technology Systems
- The law in detail: IT Security Act 2.0 (DE)

The CRITIS Regulation 2.0

- Year 2021
- Ordinance on the Designation of Critical Infrastructures under the BSI Act
- BSI Criticism Ordinance – BSI-CRITISV
- The BSI Criticality Ordinance 2.0 concretises the statements of the IT Security Act 2.0 and the BSI Act and defines threshold values, facilities and specifications ("Who belongs to CRITIS?").
- The law in detail: BSI CritisV (DE) (2.0)

The European Union's RCE Directive on Critical Infrastructure Resilience

- December 2022: MEPs approve new rules to protect essential infrastructure
- Official document DIRECTIVE (EU) 2022/2557 "On the resilience of critical entities" (RCE) (Language selection page / English version PDF)
- RCE = Resilience of critical entities
- CER = Critical entities reslilience) (*)
- EU states must transpose RCE into national law by October 2024 in Germany with the CRITIS Umbrella Act
- More information under chap. 3.2 or online here

(*) CER often used as an abbreviation in the German-speaking world

The NIS-2 Directive of the European Union

- Official document DIRECTIVE (EU) 2022/2555 "On measures for a high common level of cybersecurity across the Union" (NIS-2) (Language selection page / English version PDF)
- EU states must transpose NIS-2 into national law by October 2024 (deadline);
- In Germany by NIS-2 Implementation and Cybersecurity Strengthening Act (NIS-2UmsuCG).
- More information further down under chap. 3.2 or online here

NIS-2 Implementation and Cybersecurity Strengthening Act (NIS-2UmsuCG)

- July 2024: Governement Draft (PDF / DE / 22.07.2024)
- BMI Press release on the government draft (DE)
- The NIS-2UmsuCG is an amending law that restructures, amends and supplements the articles of various other laws – primarily the BSI Act (New)
- BSI Act (new): Law on the Federal Office for Information Security and on the security of information technology of entities
- Scheduled for Oct 2024, now delayed until March 2025 – according to government's current plans

CRITIS Umbrella Act

- December 2022: Federal government adopts the key points of the CRITIS umbrella law
- Website BMI: Cornerstones for the CRITIS Umbrella Act (original wording PDF / DE)
- December 2023: Draft Version (PDF / DE) CRITIS-Dachgesetz – CRITIS-DachG – des Bundesministeriums des Innern und für Heimat: Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen – (German version).
- Scheduled for Oct 2024, now delayed
- NEW: The Federal Office of Civil Protection and Disaster Assistance (BBK) becomes the national competent supervisory authority for resilience and physical protection of critical facilities

Tip and recommendation:
A very good independent, neutral and low-threshold information platform on all regulatory issues related to CRITIS is "OpenCRITIS" (mainly in german, some presentations in english)

3.1.3 LEGAL BRIEF OVERVIEW

The following information is current as of September 2024.

THE CURRENT LEGAL FRAMEWORK

BSI ACT (BSIG)
(NEW CONTENTS AND UPDATES, APPLY FROM MAY 2021)

Obligations for CRITIS operators:

- Attack detection
- Critical components
- New reporting requirements
- Immediate registration

More companies affected:

- CRITIS Sector Waste Management
- Companies in the special public interest
- Lower thresholds
- More facilities

More powers for the BSI:

- Central Reporting Office
- Deeper investigations
- Protection of the federal networks
- More staff

Sanctions and consumer protection:

- Higher penalties for operators
- More possible infringements
- New quality labels

TO-DO LIST FOR CRITIS OPERATORS SINCE 05_2021

Existing CRITIS operators:

- Attack detection SIEM SOC **(from May 2023)**
- Check new CRITIS facilities
- Examine lower thresholds
- New reporting obligations to the BSI

New operators & disposers:

- Identify CRITIS facilities
- Register as a CRITIS with the BSI
- Implement cybersecurity
- Reporting obligations to the BSI

All CRITIS operators and essential and important entities:

- Prepare for EU regulation (NIS-2 / RCE Directive)
- In Germany: prepare for the CRITIS umbrella law, especially with regard to physical protection measures
- In Germany: prepare for the NIS-2 Implementation and Cybersecurity Strengthening Act (NIS-2UmsuCG) or the new, amended BSIG, including a requirement for “security in the supply chain”

This and other more detailed information can be found on OpenCRITIS.

11 COLLECTION OF ADDITIONAL INFORMATION

CRITICAL INFRASTRUCTURES (CRITIS)

Laws/legislation/institutions/definitions

Germany:

- BSI: BSI is the Federal Cybersecurity Authority and the chief architect of secure digitalisation in Germany
- The BSI operates on the basis of various (special) legal regulations and ordinances at national and European level
- Definition "What are Critical Infrastructures" according to BSI?
- BBK: Federal Office for Civil Protection
- Legal Ordinance "Ordinance on the Designation of Critical Infrastructures under the BSI Act", in short BSI Critical Infrastructure Ordinance (BSI-CRITISV) , german
- Act on the Federal Office for Information Security (BSI Act – BSIG)
- § 9b BSIG: Prohibition of the use of critical components (german)
    - "Lex Huawei" / Security requirements for manufacturers/suppliers of critical components / Third-country risk (german)
- Second act on increasing the security of IT systems (German IT Security Act 2.0)
- Foreign Trade and Payments Act (AWG)
- Foreign Trade and Payments Act, Section 4, (1) Nr 4, Restrictions and obligations to act to protect public security and external interests
- Foreign Trade and Payments Ordinance (AWV)
- Foreign Trade and Payments Ordinance, Section 55, Scope of application of the cross-sectoral assessment
- Foreign Trade and Payments Ordinance, Section 55a, (1) No. 1 Likely effect on public order or security,
- Supply Chain Act (German: Lieferkettensorgfaltspflichtengesetz (LkSG)), literally Obligation to Exercise Due Diligence in the Supply Chain Act or German: Lieferkettengesetz in short)
- Critis Umbrella Act (CRITIS-DachG)
    - expected first half of 2025