BLACK CELL
Protecting critical infrastructures

WHITEPAPER

GERMANY'S NIS2 IMPLEMENTATION

Requirements under the NIS2UmsuCG and BSIG

Created by

Béla Droppa | Compliance

March 2026

TABLE OF CONTENTS

01

ABOUT BLACK CELL

Black Cell is a European cybersecurity company focused on protecting critical infrastructures and the organizations that support them. Our business units cover SOC, Integration, Offensive Security, Cloud Security, Compliance, and ESM (Enterprise Security Monitoring). We take a customer first approach that starts with listening, then shaping solutions to fit the way our clients operate.

Our teams are adaptable and draw on deep knowledge across industries and technologies, from IT and Cloud to ICS/OT. We engage for the long term, providing continual support, service improvement, and measurable outcomes over the lifecycle of the relationship. Clients rely on us to connect regulatory requirements with technology choices and to guide organizational transformation that sticks.

We combine architecture, implementation, and managed operations to close gaps quickly and build sustainable capability. Local presence in Central Europe matters to us, with teams in Budapest and Frankfurt am Main that understand the regional context. This proximity helps us respond faster, coordinate with partners, and keep stakeholders aligned. Above all, we aim to be a trusted partner who strengthens resilience today and prepares you for what comes next.

DISCLAIMER

The information provided in this document is for general guidance only and is used at your own risk. No contractual or advisory relationship is created between Black Cell and any person accessing or using this document or any part of it. Black Cell accepts no liability for any actions, decisions, or consequences arising from the use of this material.

References to third-party sources are included where appropriate. Black Cell is not responsible for the content, accuracy, or availability of external sources, including websites mentioned in this publication.

CONTACT

Béla Droppa
CEO
bela.droppa@blackcell.io

COPYRIGHT NOTICE

02

OVERVIEW

2.1. EXECUTIVE OVERVIEW

Germany’s implementation of the NIS2 Directive is no longer a matter of speculation. With the entry into force of the NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (hereinafter referred to as the NIS2UmsuCG) and the revised BSI-Gesetz (hereinafter referred to as BSIG) in December 2025, cybersecurity obligations for affected organizations are now binding, enforceable, and subject to active supervision by the Federal Office for Information Security (BSI).

The scope of regulation has expanded well beyond the traditional KRITIS landscape. Alongside operators of critical infrastructures, a significant number of essential and important entities across sectors such as energy, transport, finance, health, digital infrastructure, manufacturing, food production, and digital services are now covered. In total, this affects tens of thousands of organizations operating in Germany.

The BSIG is built around three core obligations:

- Mandatory registration;
- Incident reporting;
- Risk management implementation and documentation.

These requirements apply continuously and must be demonstrable at any time. Organizations that were already in scope when the law entered into force were required to complete registration by 5 March 2026, while newly affected entities must register at the BSI within three months of becoming subject to the law.

A central focus of the framework is incident preparedness and response. Essential and important entities must be able to detect, assess, and report significant security incidents within strict statutory deadlines. For KRITIS operators, the bar is higher. They are required to operate continuous, automated attack detection and response capabilities that reflect the state of the art and are proportionate to the potential impact of service disruption.

Compliance is monitored through a graduated audit and enforcement regime. KRITIS operators must regularly provide evidence of compliance through audits at least every three years. Essential entities may be subject to risk-based audits ordered by the BSI, while important entities can be audited where there are indications of non-compliance. Rather than prescribing a fixed audit standard, the law focuses on whether measures work in practice and whether management oversight can be demonstrated.

Where deficiencies are identified, the BSI has a broad enforcement toolkit. This includes remediation orders, follow-up evidence requests, recipient-facing notifications, and escalation to sector authorities. Continued non-compliance can lead to coercive payments of up to EUR 100,000 per measure and administrative fines of up to EUR 10 million or 2 percent of global annual turnover for particularly important entities.

This whitepaper explains who is affected by Germany's NIS2 implementation, outlines the concrete obligations introduced by the NIS2UmsuCG and the BSIG, and shows how organizations can align governance, technology, and operations to meet regulatory expectations and reduce enforcement risk.

2.2. NIS2 REQUIREMENTS AT A GLANCE

2.2.1. WHO IS IN SCOPE

- Operators of critical infrastructures (KRITIS)
- Essential entities (besonders wichtige Einrichtungen)
- Important entities (wichtige Einrichtungen) across sectors including energy, transport, finance, health, digital infrastructure, manufacturing, food, and digital services.

2.2.2. WHAT IS MANDATORY

- Registration with the Federal Office for Information Security (BSI)
- Implementation and documentation of proportionate cybersecurity risk management measures
- Incident detection, assessment, and reporting within statutory deadlines
- Management approval, oversight, and cybersecurity training
- For KRITIS operators: continuous, automated attack detection and response capabilities

2.2.3. KEY DEADLINES

- Registration within three months of becoming subject to the law
- Early incident warning within 24 hours
- Incident notification within 72 hours
- Final incident report within one month
- KRITIS audits at least every three years

2.2.4. HOW COMPLIANCE IS VERIFIED

- Mandatory audits for KRITIS operators
- Risk-based audits for essential entities
- Event-driven audits for important entities
- Evidence-based supervision focused on operational effectiveness and management oversight

2.2.5. WHAT NON-COMPLIANCE CAN COST

- Coercive payments of up to EUR 100,000 per enforcement measure
- Administrative fines of up to EUR 10 million or 2% of global annual turnover
- Mandatory public or recipient-facing notifications
- Escalation to sector authorities and potential management-level consequences

2.3. WHO IS AFFECTED BY GERMANY'S NIS2 IMPLEMENTATION?

With the entry into force of the NIS2UmsuCG in December 2025, Germany has significantly expanded the scope of organizations subject to statutory cybersecurity obligations. The core material requirements are now set out in the revised BSIG.

The law distinguishes between three main groups of affected organizations:

- Operators of critical installations (KRITIS);
- Size-based essential and important entities;
- Size-independent special categories of entities.

Organizations falling into any of these categories are subject to registration, risk management, and incident reporting obligations under the BSIG.

To support organizations in assessing whether they fall within scope, the Federal Office for Information Security (BSI) provides an official online assessment tool ("NIS2-Betroffenheitsprüfung"). While this tool is helpful for initial orientation, the legal classification ultimately follows the statutory criteria set out in the BSIG.

2.3.1. KRITIS

Operators of critical infrastructures remain fully within scope under the German cybersecurity framework. Their classification continues to follow the established KRITIS methodology, based on critical services, sectors, and sector-specific thresholds defined in the BSIG and related ordinances.

KRITIS sectors include, among others, energy, information technology and telecommunications, transport and traffic, health, water, food, finance and insurance, and municipal waste management. For KRITIS operators, the NIS2UmsuCG reinforces existing obligations and introduces additional requirements, particularly in relation to continuous attack detection, reporting, and oversight.

2.3.2. SIZE-BASED ESSENTIAL AND IMPORTANT ENTITIES

Beyond KRITIS, the BSIG introduces two new categories of regulated entities based primarily on sector and company size:

- Essential entities (besonders wichtige Einrichtungen)
- Important entities (wichtige Einrichtungen)

Classification is determined by a combination of sector assignment and enterprise size, in line with the thresholds defined in the law. As a general rule, large enterprises are those with at least 250 employees or an annual turnover exceeding EUR 50 million and a balance sheet total exceeding EUR 43 million. Medium-sized enterprises are those with at least 50 employees or an annual turnover and balance sheet total exceeding EUR 10 million.

Essential entities typically operate in sectors listed in Annex I of the NIS2 framework, such as energy, transport, finance, health, water, digital infrastructure, and space. Important entities generally operate in Annex II sectors, including postal and courier services, waste management, chemicals, food production and distribution, manufacturing, digital services, and research.

When assigning an organization to a sector, minor or negligible business activities may be disregarded if they are not material to the overall operation.

2.3.3. SIZE-INDEPENDENT SPECIAL CATEGORIES

Some entities fall within scope regardless of their size due to the nature of their services. These include in particular:

- **Qualified trust service providers (qTSPs)** within the meaning of the eIDAS Regulation. These entities are classified as essential entities under German law.
- **Top Level Domain (TLD) registries and DNS service providers**, whether authoritative or recursive, provided they offer services to third parties. Root name servers are excluded.
- **Public electronic communications networks and services**, which are subject to specific treatment and cross-references within the BSIG and related telecommunications legislation.

Additional provisions apply to public authorities and bodies of the federal administration, which are regulated separately under the NIS2UmsuCG.

2.4. REGISTRATION OBLIGATION

Organizations classified as essential or important entities under the BSIG are subject to a mandatory registration obligation with the Federal Office for Information Security (BSI) pursuant to §33 BSIG. This obligation has been legally binding since the entry into force of the NIS2UmsuCG on 5 December 2025.

Registration must be completed within three months of an organization becoming subject to the law. For organizations that were already within the scope of the BSIG on the date the NIS2UmsuCG entered into force, this resulted in a registration deadline of 5 March 2026. The same three-month period applies to newly established entities and to existing organizations that fall into scope at a later point due to changes in size, sector classification, or legal status.

The purpose of the registration is to enable the BSI to exercise its supervisory, coordination, and incident-handling functions under the German cybersecurity framework.

2.4.1. INFORMATION TO BE PROVIDED DURING REGISTRATION

During registration, organizations must submit a defined set of information to the BSI. This information can and should be prepared in advance, as it is largely static and organizational in nature. Required details include, in particular:

- Name, legal form and registration identifiers of the entity
- Address of the registered office and relevant operational locations
- Contact details, including general contact information and designated points of contact
- Assignment to the relevant sector or sectors as defined in the statutory annexes

- A list of EU Member States in which the entity provides covered services
- Identification of the competent federal and state supervisory authorities, where applicable

The BSI may request updates to the registration data if material changes occur. Organizations are therefore required to ensure that registered information remains accurate and up to date.

2.4.2. ADDITIONAL REGISTRATION REQUIREMENTS FOR KRITIS OPERATORS

Operators of critical infrastructures are subject to enhanced registration requirements beyond the standard information obligations. In addition to the general registration data, KRITIS operators must provide detailed information on the critical installations they operate.

This includes, among other elements:

- The type of critical service provided
- Classification of the installation within the KRITIS framework
- Public IP address ranges associated with the installations
- Location of the installations and relevant supply metrics

These additional details enable the BSI to assess systemic risks, coordinate sector-specific oversight, and respond effectively in the event of significant incidents affecting critical services.

2.4.3. 24/7 CONTACT POINT (KONTAKTSTELLE)

KRITIS operators are required to designate and maintain a permanently reachable contact point, available 24 hours a day and 7 days a week, and to submit the corresponding contact details to the Federal Office for Information Security (BSI). This contact point must be capable of immediate communication with the BSI, particularly in the context of incident reporting, threat warnings, and crisis coordination.

In addition to organizational availability, the BSIG requires that the contact point be supported by continuous, automated attack detection and response capabilities at both the technical and procedural level. These capabilities must enable timely detection, assessment, escalation, and handling of security incidents.

Organizations may therefore satisfy the legal requirements for the 24/7 contact point either through an internal SOC or by outsourcing these functions to a qualified SOC service provider.

2.5. WHICH SECURITY MEASURES DO I HAVE TO IMPLEMENT?

Essential and important entities are required to implement appropriate, effective, and proportionate technical and organizational measures to manage risks to the security of their network and information systems. These obligations are set out in §30(2) BSIG, which transposes the minimum security requirements of Article 21 of the NIS2 Directive into German law.

The measures must be designed to prevent, detect, and respond to security incidents and to ensure the availability, authenticity, integrity, and confidentiality of information systems and services. While the law allows for proportionality based on the size, sector, and risk exposure of an organization, the core requirement areas apply to all entities within scope.

At a minimum, organizations must address the following areas:

1. **Risk management and governance:**
   - Implementation of systematic risk analysis, information security concepts, and documented policies that define objectives, responsibilities, and controls.
2. **Information security incident management:**
   - Capabilities to detect, assess, respond to and learn from security incidents, including defined processes, roles, and escalation paths.
3. **Business continuity and crisis management:**
   - Measures to ensure operational resilience, including backup and recovery capabilities, crisis response structures, and continuity planning for critical services.
4. **Supply chain security:**
   - Risk management for security-relevant aspects of relationships with direct suppliers and services providers, including contractual, technical, and organizational controls.

5. **Secure acquisition, development and maintenance of systems:**
    - Security measures throughout the lifecycle of information systems and components, including vulnerability handling and coordinated vulnerability disclosure.
6. **Effectiveness assessment of security measures:**
    - Procedures to evaluate whether implemented measures are effective, including monitoring, testing, and internal review mechanisms.
7. **Basic cyber hygiene and training:**
    - Role-appropriate security awareness measures, training progams and exercises to ensure that personnel understand and apply security requirements.
8. **Cryptography and encryption:**
    - Policies and operational procedures governing the appropriate use of cryptographic mechanisms, including encryption at rest and in transit and secure key management.
9. **Human resource security and access control:**
    - Personnel security measures, access control policies with a focus on privileged access and complete, up-to-date inventories of assets and processes.
10. **Secure communication and authentication:**
    - Use of secure communication channels, protected emergency comms, and modern authentication mechanisms such as MFA or passwordless.

2.5.1. PROPORTIONALITY AND DIFFERENTIATION BETWEEN ENTITIES

The principle of proportionality is explicitly codified in §30(1) BSIG. Essential and important entities are required to implement appropriate, proportionate and effective technical and organizational measures, taking into account their individual risk situation.

When assessing proportionality, §30(1) BSIG requires organizations to consider, in particular, the extent of their risk exposure, their size, the costs of implementation, as well as the likelihood and severity of security incidents and their potential societal and economic impact. The proportionality assessment must be documented.

While essential entities are generally expected to demonstrate a higher level of formality, documentation, testing, and management oversight than important entities, the scope of required risk management areas does not differ between the two categories. All entities within scope must address the minimum measures listed in §30(2) BSIG, with the depth and maturity of implementation scaled according to proportionality.

2.5.2. SECURITY DETECTION AND RESPONSE @ KRITIS

Operators of critical infrastructures are subject to additional security requirements beyond the baseline obligations applicable to essential entities. These requirements are set out explicitly in §31 BSIG and apply to information technology systems that are essential for the operation of critical services.

KRITIS operators are required to implement continuous, automated attack detection and response capabilities. These measures must enable the timely detection of security incidents, support their assessment and prioritization, and allow for effective containment and mitigation. The objective is to minimize the impact of security incidents on the availability, integrity, and confidentiality of critical services.

The law requires that detection and response measures reflect the state of the art and be proportionate to the potential impact of a disruption. When assessing proportionality, the implementation costs must be reasonable in relation to the potential damage resulting from an outage or compromise of the critical service.

In practice, compliant implementations typically include continuous monitoring of relevant telemetry, centralized log collection and correlation, endpoint and network-based detection capabilities, and clearly defined incident response processes. These capabilities must operate on a 24/7 basis and be supported by organizational procedures, escalation paths, and documentation that enable effective incident handling and regulatory reporting.

Black Cell supports KRITIS operators in meeting these requirements through its Security Operations Center (SOC) and Managed Detection and Response (MDR). By providing continuous monitoring, automated detection, structured incident response, and defined escalation and communication workflows, Black Cell enables organizations to fulfil the statutory expectations of §31 BSIG. This includes support for timely incident assessment, containment, documentation, and reporting to the BSI.

Detection and response capabilities may be operated internally or outsourced to a qualified external service provider. Where services are outsourced, KRITIS operators remain responsible for ensuring that the implemented measures meet the statutory requirements and that incidents can be reported to the BSI without delay in accordance with the applicable reporting obligations.

2.6. WHAT HAPPENS IN CASE OF AN INCIDENT?

Essential and important entities are subject to mandatory incident reporting obligations under §32 BSIG. These obligations apply when a security incident has a significant impact on the provision of the services covered by the law.

The purpose of incident reporting is to enable the Federal Office for Information Security (BSI) to assess the situation, coordinate response activities where necessary, and support the mitigation of cross-sectoral or cross-border risks.

2.6.1. REPORTABLE INCIDENTS

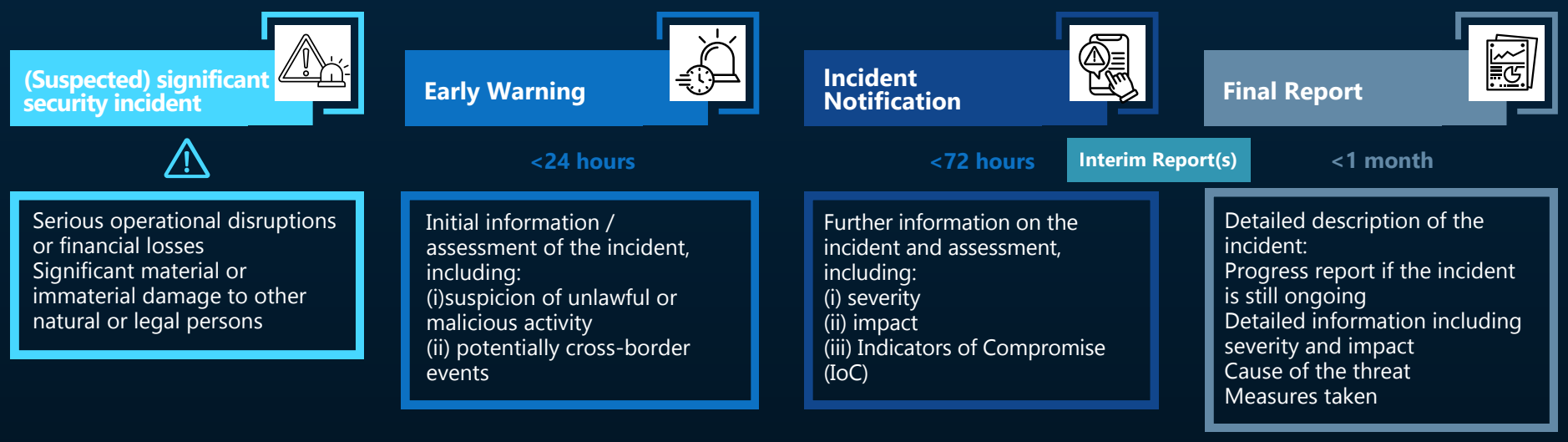
A reportable security incident is an event that compromises the availability, integrity, authenticity, or confidentiality of network and information systems and has a significant operational impact. When assessing whether an incident is reportable, organizations must consider factors such as the number of affected users, the duration of the incident, the geographical spread, and the extent of service disruption.

2.6.2. THREE-STAGE REPORTING PROCESS

The BSIG establishes a three-stage reporting regime, which must be followed once an organization becomes aware of a reportable incident:

1. **Early Warning (within 24 hours):** An initial notification must be submitted to the BSI within 24 hours of becoming aware of the incident. This early warning must indicate whether the incident is suspected to have been caused by unlawful or malicious actions and whether it may have cross-border relevance.

2. **Incident Notification (within 72 hours):** A more detailed incident report must be provided. This report must include an initial assessment of the incident, its severity and impact, and the mitigation measures taken or planned.
3. **Final Report (within one month):** A final report must be submitted no later than one month after the initial notification. This report must contain a comprehensive description of the incident, its root causes, and the measures implemented to prevent recurrence.



2.6.3.ORGANIZATIONAL AND TECHNICAL PREREQUISITES

To comply with the incident reporting obligations, organizations must have both the internal processes and the technological capabilities to detect, assess, and report security incidents. In practice, incident reporting is typically embedded within an Information Security Management System (ISMS), which defines detection thresholds, escalation criteria, internal decision-making processes, and reporting workflows. Detection and response technologies, such as log correlation, endpoint and network monitoring, and incident response tooling, support the timely identification and analysis of incidents and provide the evidence required for BSI reporting.

2.6.4. RECIPIENT-FACING NOTIFICATION OBLIGATIONS

In addition to reporting obligations towards the Federal Office for Information Security (BSI), essential and important entities may be required to inform their service recipients about significant security incidents based on §35 BSIG.

If a significant security incident could disrupt the provision of services, the BSI may require the affected entity to promptly inform its service recipients about the incident. The form of notification may include direct communication with affected recipients or public information measures, such as notices published on the organization's website.

The purpose of recipient-facing notification is to enable users and customers to assess potential impacts on their own operations and to take appropriate protective measures where necessary.

2.6.4.1. ADDITIONAL OBLIGATIONS FOR SPECIFIC SECTORS

For certain sectors, including finance, social security, digital infrastructure, ICT services, and digital services, the BSIG provides for an additional notification obligation. If a significant cyber threat arises that could materially affect service recipients, entities in these sectors must notify both the BSI and their service recipients of the threat and, where appropriate, recommend measures to mitigate potential risks.

This additional obligation applies only where the interests of the service recipients outweigh the interests of the entity. The assessment must take into account potential harm to recipients, the urgency of the situation, and the risk of further escalation.

Recipient-facing notifications do not replace the statutory incident reporting obligations towards the BSI and must be coordinated to ensure consistency, accuracy, and compliance with applicable confidentiality and security requirements.

2.7. WHAT IS THE ROLE OF MANAGEMENT BODIES?

Now that registration, risk management, and incident reporting obligations are clear, the question arises: **who is ultimately responsible for ensuring compliance?**

According to §38 of the BSIG, the responsibility lies with the management bodies of essential and important entities. Management bodies are required to approve the risk management measures implemented pursuant to §30 BSIG and to oversee their effective execution. While operational tasks may be delegated within the organization or to external service providers, the overall responsibility for implementation and oversight remains with the management body.

If management bodies fail to meet these obligations, they may be held liable towards their organization for damages caused by negligent breaches of duty, in accordance with the applicable corporate law provisions.

In addition, §38(3) BSIG introduces a mandatory training obligation for members of management bodies. They must participate in training measures to acquire the necessary knowledge and skills to identify and assess risks, understand risk management practices in IT security, and evaluate how these risks affect the services provided by the organization. This includes taking part in cybersecurity awareness exercises and role-based training designed to build a strategic understanding of cybersecurity and its relevance to business operations.

2.8. $5(0 $1' $725< $8' ,76 3/$11(' "

1 RZ WKDW UHJLVWUDWLRQ ULVN P DQDJHP HQW LQFLGHQW UHSRUWLQJ DQG P DQDJHP HQW UHVSRQVLELOLWLHV DUH FOHDU WKH TXHVWLRQ DULVHV KRZ FRP SOLDQFH Z LWK WKHVH REOLJDWLRQV LV YHULILHG DQG HQIRUFHG LQ SUDFWLFH

7KH 1,6 8P VX&* HVWDEOLVKHV D JUDGXDWHG DXGLW DQG HQIRUFHP HQW IUDP HZRUN WKDW HQDEOHV WKH) HGHUDO2 IILFH IRU,QIRUP DWLRQ 6HFXULW\ %6, WR VXSHUYLVH FRP SOLDQFH DQG WR WDNH FRUUHFWLYH DFWLRQ Z KHUH GHILFLHQFLHV DUH LGHQWLILHG 7KH VFRSH DQG LQWHQVLW\ RI RYHUVLJKW GHSHQG RQ Z KHWKHU DQ RUJDQL]DWLRQ LV FODVVLILHG DV D . 5,7,6 RSHUDWRU DQ VHUYLFH SURYLGHU 7KLUG3DUW\ RU RWKHU

.5,7,6 $8',76 (9(5< <($56

2 SHUDWRUV RI FULWLFDOLQIUDVWUXFWXUHV DUH VXEMHFWHG P DQGDWRU\ SHULRGLF HYLGHQFH REOLJDWLRQV 8QGHU † %6,* . 5,7,6 RSHUDWRUV P XVW GHP RQVWUDWH WKH LP SOHP HQWDWLRQ RI WKH UHTXLUHG ULVN P DQDJHP HQWDQG VHFXULW\ P HDVXUHV E\ P HDQV RI VHFXULW\ DXGLW LQVSHFWLRQV RU FHUWLFDWLRQV

7KHVH DXGLW P XVWEH VXEP LWWHG WR WKH %6, DW D WLP H GHWHUP LQHG E\ WKH DXWKRULW\ QR HDUOLHU WKDQ WKUHH \HDUV DIWHU LQLWLDO FODVVLILFDWLRQ DV D . 5,7,6 RSHUDWRU DQG VXEVHTXHQW HYHU\ WKUHH \HDUV 7KH DXGLWUHVXOW P XVWLQFOXGH LQIRUP DWLRQ RQ LGHQWLILHG VHFXULW\ GHILFLHQFLHV 7KH %6, P D\ UHTXHVWDFFHVV WR WKH XQGHUO\LQJ GRFXP HQWDWLRQ DQG P D\ UHTXLUH WKH VXEP LVVLRQ RI D UHP HGLDWLRQ SODQ DQG HYLGHQFH WKDWFRUUHFWLYH DFWLRQV KDYH EHHQ LP SOHP HQWHG

7KH %6, LV HP SRZHUHG WR GHILQH SURFHGXUDO HYLGHQWLDU DQG RUJDQL]DWLRQDO UHTXLUHP HQWV IRU DXGLW DQG DXGLWRUV WKURXJK SXEOLF QRWLFH 7KLV HQVXUHV D FRQVLVWHQW DSSURDFK DFURVV VHFWRUV

$8' ,76)25 (66(17,$/ (17,7,(6

(VVHQWLDO HQWLWLHV DUH VXEMHFW WR D ULVN-EDVHG VXSHUYLVRU\ UHJLPH XQGHU † %6,* 7KH %6, PD\ UHTXLUH HVVHQWLDO HQWLWLHV WR FRPPLVVLRQ LQGHSHQGHQW DXGLWV LQVSHFWLRQV RU FHUWLILFDWLRQV WR YHULI\ FRPSOLDQFH ZLWK REOLJDWLRQV UHODWLQJ WR ULVN PDQDJHPHQW PHDVXUHV LQFLGHQW UHSRUWLQJ DQG PDQDJHPHQW WUDLQLQJ

6XFK PHDVXUHV PD\ JHQHUDOO\ EH RUGHUHG IURP WKUHH \HDUV DIWHU WKH ODZ HQWHUHG LQWR IRUFH 7KH %6, PD\ UHTXHVW DXGLW UHVXOWV VXSSRUWLQJ GRFXPHQWDWLRQ DQG LQIRUPDWLRQ RQ LGHQWLILHG GHILFLHQFLHV :KHUH VKRUWFRPLQJV DUH LGHQWLILHG WKH DXWKRULW\ PD\ UHTXLUH WKH VXEPLVVLRQ DQG LPSOHPHQWDWLRQ RI D FRUUHFWLYH DFWLRQ SODQ DQG HYLGHQFH RI UHPHGLDWLRQ

:KHQ GHFLGLQJ ZKHWKHU DQG KRZ WR H[HUFLVH LWV VXSHUYLVRU\ SRZHUV WKH %6, WDNHV LQWR DFFRXQW IDFWRUV VXFK DV WKH HQWLW\·V ULVN H[SRVXUH VL]H DQG WKH SRWHQWLDO VRFLHWDO RU HFRQRPLF LPSDFW RI VHFXULW\ LQFLGHQWV

$8',76 $1' 683(59,625< 0($685(6)25 ,03257$17 (17,7,(6

,P SRUWDQW HQWLWLHV DUH VXEMHFW WR D OLJKWHU VXSHUYLVRU\ UHJLPH XQGHU † %6,* $XGLWV RU LQVSHFWLRQV DUH JHQHUDOO\ LQLWLDWHG RQO\ ZKHUH WKHUH DUH LQGLFDWLRQV RI QRQ-FRPSOLDQFH ZLWK REOLJDWLRQV UHODWLQJ WR ULVN PDQDJHPHQW LQFLGHQW UHSRUWLQJ RU PDQDJHPHQW WUDLQLQJ

,Q VXFK FDVHV WKH %6, PD\ DSSO\ HQIRUFHPHQW LQVWUXPHQWV VLPLODU WR WKRVH XVHG IRU HVVHQWLDO HQWLWLHV LQFOXGLQJ UHTXHVWV IRU HYLGHQFH DQG UHPHGLDWLRQ PHDVXUHV 7KLV DSSURDFK UHIOHFWV WKH SULQFLSOH RI SURSRUWLRQDOLW\ ZKLOH HQVXULQJ WKDW VLJQLILFDQW FRPSOLDQFH JDSV FDQ EH DGGUHVVHG

2.9. THE BSI'S ENFORCEMENT TOOLBOX

The legislation establishes an enforcement framework that is designed to be effective, escalatory, and evidence-based. Compliance is not assessed as a one-time exercise, but as an ongoing obligation that must be demonstrable at any point in time.

The Federal Office for Information Security (BSI) acts as the competent supervisory authority and is empowered to verify compliance, identify deficiencies, and enforce corrective action. The intensity of supervision and enforcement depends on whether an organization qualifies as a particularly important entity, an important entity, or an operator of critical installations (KRITIS).

2.9.1. HOW ENFORCEMENT MAY BE TRIGGERED IN PRACTICE

Enforcement measures are typically initiated when there are indications of non-compliance. Such indications may arise from incident notifications, missing or incomplete registrations, audit findings, supervisory reviews, or information obtained through the BSI's own supervisory activities.

The law does not require a major incident to occur before enforcement becomes relevant. Deficiencies in documentation, incomplete implementation of risk management measures, or failure to demonstrate management oversight are sufficient to justify supervisory action.

Once such indications exist, the BSI is legally entitled to move from observation to formal enforcement.

2.9.2. PRACTICAL ENFORCEMENT MEASURES AVAILABLE TO THE BSI

The BSIG provides the BSI with a graduated toolbox of enforcement measures, allowing it to react proportionately and escalate only where necessary.

In practice, this means that the BSI may:

- require organizations to commission independent audits, inspections, or certifications to verify compliance with statutory obligations,
- request audit results, supporting documentation, and underlying evidence, including documentation used during internal assessments,
- require the submission of a remediation plan if deficiencies are identified and demand proof that corrective measures have been implemented,
- issue binding orders to implement specific risk management measures or to remedy identified shortcomings within a defined timeframe,
- ·require recipient-facing notifications or public disclosure of violations where legally justified, and
- escalate unresolved cases to the competent sector authority, which may temporarily suspend authorizations or restrict management activities as a last resort.

These measures are not theoretical. The law explicitly allows the BSI to combine documentation requests, audits, remediation orders, and follow-up evidence checks until compliance is restored.

2.9.3. CONSEQUENCES OF CONTINUED NON-COMPLIANCE

If an organization fails to comply with BSI orders or statutory obligations despite deadlines, the BSIG provides for administrative coercive measures and financial sanctions.

If an organization does not comply with statutory obligations or BSI orders within the specified deadlines, the BSI may apply administrative coercive measures to enforce compliance. These include coercive payments (Zwangsgelder) of up to EUR 100,000 per enforcement measure. These payments are not punitive in nature but may be imposed repeatedly until compliance is achieved.

2.9.3.1. ADMINISTRATIVE FINES: CONCRETE FINANCIAL EXPOSURE

Beyond coercive measures, the BSIG introduces a comprehensive fine regime that applies to violations such as:

- failure to implement required risk management measures,
- failure to document compliance,
- late, incomplete, or missing incident reports,
- missing or incorrect registrations,
- failure to provide audit evidence, or
- refusal to cooperate with supervisory measures.

The law defines explicit upper limits, depending on the classification of the entity. For particularly important entities, fines may reach:

- up to EUR 10 million, or
- up to 2 percent of global annual turnover for organizations with a worldwide turnover exceeding EUR 500 million.

For important entities, fines may reach:

- up to EUR 7 million, or
- up to 1.4 percent of global annual turnover for organizations with a worldwide turnover exceeding EUR 500 million.

The turnover used for these calculations is the global group turnover of the preceding financial year, and the law explicitly allows the authority to estimate turnover if precise figures are unavailable.

2.9.4. PUBLIC DISCLOSURE AND REPUTATIONAL IMPACT

In addition to financial penalties, the BSIG authorizes the BSI to require the public disclosure of violations. This may include orders to publish information about compliance failures or to notify service recipients and affected parties.

While the law does not mandate automatic publication, it explicitly permits such measures as part of enforcement. For regulated or customer-facing organizations, the reputational consequences of public disclosure may significantly exceed the direct financial impact of fines.

2.9.5. MANAGEMENT-LEVEL CONSEQUENCES

Non-compliance under the BSIG is not limited to organizational liability. If an organization persistently fails to comply with enforcement orders, the BSI may escalate the matter to the competent sector authority. As a last-resort measure, this authority may:

- temporarily suspend regulatory approvals or authorizations, or
- temporarily prohibit members of the management body from exercising their function.

In parallel, the BSIG explicitly preserves management liability under corporate law. Management bodies that fail to implement or oversee required cybersecurity measures may be held personally liable for damages caused by negligent breaches of duty.

2.9.6. AUDIT METHODOLOGY

While the BSIG clearly mandates audits and evidence-based supervision, it does not prescribe a single, fixed audit methodology. There is no mandatory checklist, no universal certification scheme, and no predefined scoring model embedded in the law.

Instead, the law deliberately grants the BSI flexibility. Audits may take the form of security audits, technical inspections, or certifications, and the BSI may define procedural requirements, evidentiary expectations, and auditor qualifications through public notices.

What is clear, however, is what audits must be capable of verifying. Any audit or inspection must allow the BSI to assess whether:

- risk management measures required by law exist, are implemented, and are proportionate,
- KRITIS-specific obligations, including attack detection requirements, are fulfilled where applicable,
- incident detection, reporting, and handling processes are operational and documented,
- management bodies have approved, overseen, and are trained in cybersecurity risk management, and
- previously identified deficiencies have been remediated effectively.

In practical terms, this means that audits will focus less on formal compliance statements and more on traceable evidence, operational maturity, and the ability to demonstrate that measures work in practice.

03

BLACK CELL'S OFFERINGS

To support organizations in meeting the risk management and technical requirements of the NIS2UmsuCG, Black Cell provides tailored services and solutions that align with the regulation's core obligations. These offerings help streamline compliance, strengthen cybersecurity posture, and ensure readiness for audits and incident response.

The following examples illustrate how regulatory requirements under the BSIG can be mapped to operational capabilities. They are not exhaustive and do not replace a legal assessment.

#	NIS2 measure	Technology stack	Value added
1	Risk management and governance	ISMS.online GRC for accelerating ISO 27001 compliance with prebuilt frameworks (DORA, ISO, GDPR), integrated dashboards and risk management tools	ISMS design & ISO/IEC 27001 gap/implementation; risk methodology (ISO 27005), SoA & policy stack; sectoral risk and regulatory profiles (e.g., financial services, aviation, manufacturing, pharma among others)
2	Information security incident management	Splunk Enterprise, Microsoft Sentinel, Elastic and Black Cell's proprietary Enterprise Security Monitoring	SIEM implementation, SOC as a Service, mini SOC based on M365 XDR, IR playbooks, threat hunting, CTI, End-to-End incident management

#	NIS2 measure	Black Cell technologies	Black Cell services
3	Business continuity and crisis management	Arrow Cloud Backup for M365 for daily, automated backups with ransomware protection, granular restore options, and compliance-tested recovery for critical enterprise data	BCMS / BIA / BCP-DRP design, DR exercises (TTX), crisis communications; SOC support for business continuity
4	Supply-chain security	Access scoping via Entra ID/PIM, Privileged Identity and Account Management with CyberArk	Supplier due-diligence, contractual security clauses, annual reviews, incident response coordination
5	Secure acquisition, development and maintenance of systems	Black Cell leverages Rapid7 Nexpose, Invicti, Burp Pro, Tenable Nessus, and Checkmarx for proactive vulnerability detection, penetration testing, and secure code analysis, delivering assessments and remediation guidance across diverse IT environments	Vulnerability assessments (active/passive, MITRE ATT&CK-based), continuous vulnerability management with M365 XDR
6	Effectiveness assessment of security measures	ISMS.online for GRC purposes, PowerBI and SIEM dashboards for reporting	Internal audits (technical and compliance), control maturity reviews, KPI dashboards, pre-assessment for certification

#	NIS2 measure	Black Cell technologies	Black Cell services
7	Basic cyber hygiene and training	Black Cell Academy for modular, role-based InfoSec e-learning tailored for NIS2, DORA, and ISO 27001 compliance, enhancing cybersecurity awareness across all organizational levels	Awareness & role-based trainings, phishing/TTX; hygiene baselines via Compliance & SOC
8	Cryptography and encryption	Sophos and Palo Alto firewalls for encrypting data in transit via SSL/TLS inspection, IPSec VPNs, and secure tunneling	Black Cell provides deployment, policy configuration, certificate management, and monitoring for Sophos and Palo Alto Network firewalls
9	Human resource security and access control	Entra ID with PIM secures privileged access, ISMS.online inventories assets and processes, CyberArk manages credentials and enforces least privilege across hybrid environments	Black Cell supports JML (Joiners, Movers, Leavers) and IAM design, access review scheduling, Entra ID/PIM deployment, ISMS asset inventory structuring, and CyberArk implementation
10	Secure communication and authentication	Entra ID supports MFA, continuous authentication, and passwordless login via FIDO2 keys; secure communications enforced through TLS, VPN, and conditional access across hybrid infrastructures	Black Cell deploys FIDO2 key infrastructure, configures Entra ID policies, monitors authentication events, and secures communication channels

3.1. MANAGED DETECTION AND RESPONSE AS AN OPERATING MODEL FOR KRITIS-OPERATORS

Operators of critical installations are subject to heightened security requirements under the NIS2UmsuCG. In addition to the general risk management obligations applicable to particularly important entities, KRITIS operators must implement advanced security detection and response capabilities for the information technology systems that are essential to the operation of critical services.

The BSIG does not require KRITIS operators to build and operate all detection and response capabilities internally. Detection and response functions may be operated internally or provided by qualified external service providers, provided that the statutory requirements are met.

MDR services are therefore a legitimate and widely applicable operating model for KRITIS operators. MDR services typically combine continuous monitoring, automated detection, structured incident handling, and defined escalation processes in order to meet the legal expectations of §31 BSIG.

Where detection and response capabilities are outsourced, responsibility remains with the KRITIS operator. The operator must ensure that the chosen service model provides sufficient visibility, documentation, and control to demonstrate compliance during audits and supervisory reviews.

3.1.1. OUTSOURCED SOC

For organizations requiring comprehensive, multi-source detection and response, Black Cell offers a Full SOC stack that combines Managed SIEM (such as Microsoft Sentinel, Splunk or Elastic) with endpoint detection and response (XDR/EDR) and, where needed, network or OT monitoring capability.

This setup enables 24/7 monitoring, advanced correlation, and guided incident response across IT and OT environments. Telemetry is collected from Microsoft 365, endpoints, servers, firewalls, cloud, and OT/ICS sources, with detection rules mapped to MITRE ATT&CK and tailored to client threat models based on industry and size, among other factors. Incident response is governed by operational runbooks and strict notification SLAs, ensuring rapid escalation and crisis communication. Threat intelligence is integrated through regular trend analysis and hunting, while all activities are documented to support BSI reporting and KRITIS audit requirements. This approach is ideal for organizations needing broad log correlation, long-term analytics, and robust evidence for regulatory proofs.

3.1.2. MINI SOC

For organizations seeking a rapid, cost-effective solution (especially those standardized on Microsoft 365) Black Cell provides a mini SOC that leverages Microsoft 365 Defender's native XDR capabilities without the need for a full SIEM rollout. This solution unifies endpoint, email, identity, and cloud telemetry, correlating alerts into single incidents with actionable response options. Investigation and remediation performed by Black Cell SOC handles commodity threats, by relying on operational playbooks, incident response, and notification SLAs to ensure 24/7 coverage. Threat intelligence is incorporated through custom detection rules and periodic briefings, and all incident evidence is structured for BSI-ready reporting. While this approach is best suited for Microsoft-centric environments and offers fast deployment with lower complexity, it can be extended with targeted connectors or upgraded to a full SOC as needs evolve. For many organizations, the mini SOC provides a state-of-the-art, continuously automated detection and response capability that meets the legal expectations for KRITIS under §31 BSIG.

04

SOURCES

- https://www.recht.bund.de/bgbl/1/2025/301/VO.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-meldeprozess.pdf?__blob=publicationFile&v=3