BLACK CELL
Protecting critical infrastructures

WHITEPAPER

THE CURRENT STATE OF NIS2 IMPLEMENTATION IN GERMANY

Assessing Progress and Challenges in Germany's NIS2 Implementation

Created by

Béla Droppa | Compliance

September 2025

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 organisational 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 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

© 2025 Black Cell Magyarország Ltd. & Black Cell Germany GmbH
All rights reserved. This publication may be freely distributed in its complete and unaltered form for informational purposes. However, reproduction, modification, or extraction of any part of this document (by any means, including electronic, mechanical, photocopying, or recording) is strictly prohibited without prior written permission from Black Cell.

02

OVERVIEW

In April, we briefly looked at how NIS2's transposition was progressing in Germany and emphasized the importance of early preparation for affected organizations. The Member State transposition deadline of 17 October 2024 passed nearly a year ago. Since Germany has not yet enacted a law, organizations should not expect any grace period once the bill is adopted.

Several developments have shaped the current situation. A draft bill was published in late June, followed by the government's proposal titled NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in late July 2025. The Bundestag held its first debate shortly after, and further discussions are now underway in parliamentary committees, led by the Interior Committee. Based on the legislative timeline, the bill is expected to be passed by the end of 2025 or early 2026.

This Black Cell Compliance whitepaper focuses on the requirements outlined in the NIS2UmsuCG, which is expected to apply to around 30,000 companies once adopted. The bill introduces three main categories of obligations:

- Registration;
- Incident reporting;
- Risk management implementation and documentation.

In the sections that follow, we explore these obligations and suggest practical steps organizations can begin evaluating to prepare for compliance with the NIS2UmsuCG.

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

Germany's NIS2 draft expands the scope well beyond classic KRITIS to cover both "besonders wichtige Einrichtungen" (essential entities) and "wichtige Einrichtungen" (important entities), primarily determined by company size and sector. In the current German drafts, enterprises in Annex 1 sectors are "besonders wichtig" (essential), while enterprises in Annex 2 sectors are "wichtig" (important). As a rule of thumb, thresholds follow the EU sizecap: ≥250 employees (or >€50m revenue and >€43m balance sheet) for large; ≥50 employees (or >€10m revenue and >€10m balance sheet) for medium enterprises.

Organisations falling into one of the following three categories must perform a NIS2 impact assessment (BSI online tool "NIS2-Betroffenheitsprüfung" is helpful determining applicability):

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

2.1.1. KRITIS

Independently of NIS2's size logic, existing KRITIS operators remain in scope under the KRITIS methodology (critical services, sectoral thresholds). KRITIS sectors under §2(10) BSIG include Energy; IT & Telecommunications; Transport & Traffic; Health; Water; Food; Finance & Insurance; and Municipal Waste Management.

2.1.2. SIZEBASED “EINRICHTUNGEN” (ENTITIES)

These include the following:

- Annex I sectors (typically “besonders wichtig” for large enterprises): Energy; Transport & Traffic; Finance; Health; Water; Digital Infrastructure; Space.
- Annex II sectors (typically “wichtig” for medium/large enterprises): Post & Courier; Waste Management; Chemicals (production/manufacture/trade); Food (production/processing/distribution); Manufacturing/Processing of goods; Providers of Digital Services; Research.

When assigning an entity to an Annex I/II type, negligible business activities may be disregarded relative to the overall business.

2.1.3. SIZE-INDEPENDENT (SPECIAL) CATEGORIES

Some entities will fall under the scope of the NIS2UmsuCG regardless of their size:

- **Qualified trust service providers (qTSPs)** as defined under eIDAS Art. 3(20). These are explicitly included and classified as “besonders wichtige Einrichtungen” (essential entities).
- **Top Level Domain (TLD) registries and DNS service providers** whether recursive or authoritative, provided they serve third parties (excluding root services).
- **Public telecommunications networks and services**, which are addressed separately in the German drafts with dedicated thresholds and treatment.

Additional requirements for supervisory authorities and governmental entities are outlined in the government bill.

2.2. REGISTRATION OBLIGATION

If your organization is classified as an essential or important entity under the NIS2UmsuCG, it must register with the Federal Office for Information Security (BSI) within three months of becoming subject to the legislation, as outlined in §33 of the draft bill.

During registration, the following information must be submitted. These details can be prepared in advance:

- Name, legal form and registration number of the entity;
- Address and contact details including email addresses, public IP ranges and telephone numbers;
- Relevant sector(s) listed in Annex 1 or 2, and list of EU Member States in which the organisation provides these services;
- The federal and state supervisory authorities responsible for the registered activities.

2.2.1. 24/7 CONTACT POINT (KONTAKTSTELLE)

If your organization operates critical infrastructure, additional registration details are required beyond the standard information. These include the type of critical service provided, public IP ranges of the installations, installation category, supply metrics, and the physical location of each installation.

KRITIS entities must also maintain a 24/7 reachable contact point, with contact details submitted to the BSI. This contact point must be supported by continuous, automated attack detection at both the technological and process level. Organizations can meet this requirement either through an in-house Security Operations Center (SOC) or by outsourcing to a qualified SOC provider.

2.3. WHICH SECURITY MEASURES DO I HAVE TO IMPLEMENT?

In accordance with the requirements in §30 of the NIS2UmsuCG subject to the essential and important entities, at least the following risk management and preventive measures shall be implemented:

1. Risk management: risk analysis and information technology security concepts, policies.
2. Information security incident management: capability to detect, triage, respond to and learn from incidents.
3. Operational resilience: business continuity during crises by appropriate backup and recovery capabilities and crisis management.
4. Supply chain security: risk management for security related aspects of relationships with critical suppliers and services providers.
5. Security measures for the acquisition, development and maintenance of information technology systems, components and processes, including management and disclosure of vulnerabilities.
6. Procedures for assessing the information security risk management's effectiveness.
7. Basic cyber hygiene and training: role-appropriate security awareness raising through trainings and exercises.
8. Cryptography and encryption: policies and operational procedures for appropriate use of cryptography, including encryption at rest and in transit and key management.
9. Human resource security and access control: personnel security, access control (especially privileged access) and complete, current asset and process inventories.
10. Secure communication channels and modern authentication measures: secured voice, video and text, and secure emergency communications; MFA and continuous authentication methods.

2.3.1. PROPORTIONALITY AND SCOPE

The draft bill adopts the minimum measures required by NIS2 and introduces proportionality by differentiating requirements based on the type of entity. Essential entities should expect more formal processes, more frequent testing, and deeper documentation. However, the ten core measure areas apply to all organizations within the scope of the NIS2UmsuCG.

2.3.2. SECURITY DETECTION AND RESPONSE @ KRITIS

According to §31 of the NIS2UmsuCG, IT systems that are essential to the operation of critical infrastructure must implement additional security measures beyond the baseline for essential entities. These measures are considered proportionate if their cost is reasonable compared to the potential impact of an outage.

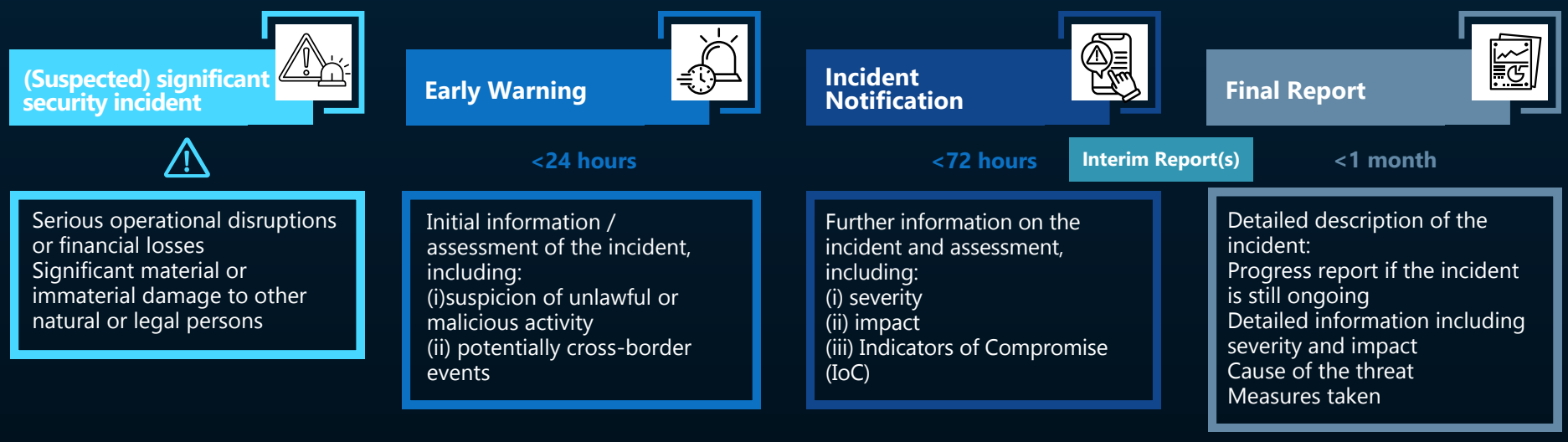
KRITIS operators are required to deploy continuous, automated attack detection technologies. This includes solutions such as SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), and NSM (Network Security Monitoring). These tools must monitor operational parameters, detect threats, and support timely mitigation.

2.4. WHAT HAPPENS IN CASE OF AN INCIDENT?

If your organisation is classified as an essential or important entity under the NIS2UmsuCG, and a cyber incident occurs that significantly impacts service delivery, you are required to inform the Federal Office for Information Security (BSI). The current reporting process is described on the BSI's dedicated subpage.

The reporting obligation consists of three stages:

1. **Early Warning:** Within 24 hours after becoming aware of the incident, an initial notification must be submitted. This should indicate whether the incident is suspected to be caused by unlawful or malicious acts, or if it may have cross-border implications.
2. **Incident Notification:** Within 72 hours, a more detailed report must follow. This should include an initial assessment of the incident, its severity, actual or potential impact, and any mitigation measures taken.
3. **Final Report:** Within one month after the initial notification, a final report must be submitted. This should contain a detailed description of the incident, root cause analysis, and the measures implemented to prevent recurrence.



To meet the incident reporting obligations under the NIS2UmsuCG, affected organizations must have both the internal processes and the technological capabilities to detect, assess, and report security incidents. These requirements can be fulfilled through the implementation of an Information Security Management System (ISMS), which defines incident management workflows and, through risk management activities, guides the selection of appropriate detection and response technologies.

2.4.1. RECIPIENT-FACING NOTIFICATION OBLIGATIONS

Under §35 of the NIS2UmsuCG, if a significant security incident could disrupt services, the BSI may require essential and important entities to promptly inform their service recipients. This can be done via direct communication or public notices, such as updates on the organization's website.

In certain sectors (finance, social security, digital infrastructure, ICT services, and digital services) there is an additional duty. If a major cyber threat arises, entities must notify both the BSI and their service recipients about the threat and recommend protective measures. These obligations apply only when the recipients' interests outweigh those of the entity.

2.5. 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 NIS2UmsuCG, management bodies are required to implement risk management measures and oversee their execution. If they fail to meet this obligation, they may be held liable to their organization for damages caused by negligence.

In addition, management bodies must participate in training to gain 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 to build strategic understanding of cybersecurity.

2.6. ARE MANDATORY AUDITS PLANNED?

Several EU Member States require organizations affected by NIS2 to undergo mandatory audits months after becoming subject to the legislation. This can increase compliance costs and shift focus toward audit readiness rather than meaningful, risk-based improvements in cybersecurity. Without proper oversight, organizations may treat compliance as a checkbox exercise, similar to what has happened under GDPR.

2.6.1. KRITIS AUDITS EVERY 3 YEARS

The BSI has introduced a structured approach to oversight. Organizations operating critical infrastructure must demonstrate the implementation of risk management and preventive measures outlined in §30. This must be done within three years of initial or renewed classification as a KRITIS operator, and then every three years. These organizations must submit audit, inspection, or certification results, including details of any identified security deficiencies. The BSI may also request additional documentation, such as proof of corrective actions.

2.6.2. AUDITS FOR ESSENTIAL AND IMPORTANT ENTITIES

Essential entities may be required to undergo audits, inspections, or certifications conducted by independent bodies. These are intended to verify compliance with risk management and security obligations, starting three years after the law comes into effect. If an organization fails to comply, the BSI may take further action. This includes publishing violations, suspending authorizations, or prohibiting management from continuing in their role. These measures can also be triggered by requests from other EU Member States.

Important entities, such as medium-sized companies in critical sectors, are subject to the same measures if there are clear signs of non-compliance.

2.6.3. AUDIT METHODOLOGY

The BSI plans to publish the audit methodology, evidence standards, and auditor requirements on its website. While these details are still pending, organizations with a functioning ISMS will be well-positioned to meet audit requirements and provide the necessary documentation.

An ISMS ensures that information security risk assessment and treatment is performed across various levels of the enterprise with constant management oversight and engagement in important decisions. Operating on a continuous Plan-Do-Check-Act (PDCA) loop, management plans the scope, policies, risk criteria, security objectives and risk-treatment plans; the organization then does by implementing and operating preventive and reactive controls, assigning roles, training staff, and managing third-party and change processes to execute the chosen treatments.

An essential part of the ISMS is the continuous monitoring (of risks, information security objectives, preventive or reactive controls, and incidents) supplemented by KPIs, logging, testing, and internal audits to check control effectiveness and compliance. The results of monitoring activities and internal audit directly feed into management's planning through management review, driving the act phase: corrective and preventive actions, re-evaluation of residual risks, and updates to policies, objectives, treatment plans and architectures: ensuring continual improvement of the ISMS.

With their extensive documentation requirements, these processes will ensure the presence of necessary audit evidence for BSI and the auditors.

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.

#	NIS2 measure	Black Cell technologies	Black Cell services
1	Risk management (risk analysis, security concepts, policies)	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	Incident handling (detect, triage, respond, learn)	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 & 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 (supplier relationships)	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/ maintenance & vulnerability handling/disclosure	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 evaluation (assess control effectiveness)	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 & 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 & encryption (policies/procedures)	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	HR security, access control & asset management	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 design, access review scheduling, Entra ID/PIM deployment, ISMS inventory structuring, and CyberArk implementation
10	MFA / continuous authentication & secure communications	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 FOR KRITIS-OPERATORS

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.

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.

04

SUMMARY

The NIS2UmsuCG will bring major changes to how organizations in Germany approach cybersecurity and compliance. The law significantly expands the scope of regulated entities beyond the current KRITIS organisations, introduces clear requirements for registration, incident reporting, and risk management, and sets higher expectations for management involvement and audit readiness.

Organizations should not wait for the law to be finalized before taking action. Early steps such as setting up an ISMS, reviewing incident response plans, gathering registration information, and making sure management is engaged will make compliance smoother and help reduce regulatory non-compliance risks.

Black Cell, as a European end-to-end cybersecurity provider offers practical support and proven solutions to help organizations meet these new requirements, from initial assessments to ongoing monitoring and audit preparation.

05

SOURCES

- https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html#nis2betreiber
- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html
- https://www.bundestag.de/dokumente/textarchiv/2025/kw37-de-informationssicherheitsmanagement-1107418
- https://bundestagszusammenfasser.de/details?docid=889
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-meldeprozess.pdf?__blob=publicationFile&v=3