RAPID7

SOLUTION BRIEF

SUPPORTING GERMAN NIS2 COMPLIANCE WITH RAPID7

In Germany, the NIS2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) marks a fundamental shift in how cybersecurity is regulated and operationalised. Implemented through a major overhaul of the BSI Act (BSIG), it moves beyond traditional compliance models to treat cybersecurity as an ongoing, risk-based discipline rather than a one-time exercise.

As digital infrastructure becomes critical to both economic stability and national security, recent cyber incidents have exposed the fragility of interconnected systems. In response, Germany's NIS2 implementation significantly expands both the scope of regulated organisations and the depth of required security measures, increasing coverage from approximately 4,500 to around 30,000 entities.

At its core, the law requires organisations to implement "state-of-the-art technical and organisational measures" (§30 BSIG) to manage cybersecurity risks. This includes not only preventative controls, but also continuous monitoring, incident detection, response, and recovery capabilities.

NIS2UmsuCG establishes a new operating model for cybersecurity in Germany:

- Continuous risk management, rather than periodic compliance.
- Real-time detection and structured incident reporting, with strict timelines.
- End-to-end security across the lifecycle, including supply chains.
- Executive accountability, elevating cybersecurity to a board-level responsibility.

The impact is substantial:

- A significantly broader range of industries and organisations are now in scope.
- Organisations face stricter obligations, increased regulatory oversight, and greater leadership accountability.
- The law extends into key sectors through updates to legislation such as the Energy Industry Act (EnWG) and the Telecommunications Act (TKG).

As regulators converge on this model, Rapid7's platform uniting Exposure Management and Continuous Threat Exposure Management (CTEM) with detection, response, and MDR is uniquely positioned to help organisations operationalise compliance within Germany's NIS2 framework, turning regulatory requirements into continuous, risk-driven security outcomes.

Ultimately, Germany's implementation transforms NIS2 into a highly enforceable national framework, elevating cybersecurity to a core business risk across the German economy

Who is affected?

The law largely abolishes the previous distinction between "KRITIS" (Critical Infrastructure) and "Non-KRITIS" in its old form, replacing it with a broader categorization. Companies are generally affected starting from 50 employees or €10 million annual turnover if they operate in one of the regulated sectors.

Companies must independently verify whether they are affected (there is no notification from the authorities).

Two categories apply:

CATEGORY	CRITERIA	SECTORS (EXAMPLES)
Essential entities	• Large enterprises (≥ 250 employees or > €50m turnover) • Sectors with high criticality • Regardless of size: e.g., DNS providers, critical telecom providers	Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking Water, Waste Water, Digital Infrastructure, ICT Service Management (B2B), Space, Public Administration.
Important entities	• Medium-sized enterprises (50–249 employees, > €10m turnover) in sectors of high criticality • Large and medium enterprises in other critical sectors	In addition to the above: Postal/Courier Services, Waste Management, Chemicals, Food, Manufacturing (e.g., Machinery, Vehicles, Electrical), Providers of Digital Services (Marketplaces, Search Engines), Research.

Key obligations

1. Risk management (state-of-the-art controls)

Companies must implement **technical and organisational measures (TOMs)**, including:

- Risk analysis and security frameworks.
- Incident management.
- Business continuity (backup, disaster recovery, crisis management).

- Supply chain security.
- Secure development and maintenance.
- Encryption and cryptography.
- Cybersecurity training (including management).
- Multi-factor authentication (MFA).

2. B. Incident reporting (strict timelines)

Significant incidents must be reported to the BSI using a 3 phased approach:

- **24h →** Early warning.
- **72h →** Initial assessment.
- **1 month →** Final report.

3. C. Registration duty

Affected companies must register with the BSI and designate a point of contact.

Management liability ("c-level issue")

This is one of the most significant changes. Cybersecurity is now a **board-level responsibility:**

- Executives are **personally accountable.**
- Responsibility **cannot be delegated.**
- Mandatory **management training.**
- Potential **personal liability** (including financial recourse).

Sanctions

Fines have been massively increased and aligned with GDPR levels:

- **Essential entities:** up to €10M or 2% global turnover.
- **Important entities:** up to €7M or 1.4% global turnover.

How Rapid7 solutions supports German NIS2 compliance

Similar to GDPR, compliance with Germany's NIS2 Implementation Act (NIS2UmsuCG) will require organisations to deploy a combination of cybersecurity capabilities to meet the law's broad and enforceable requirements.

At Rapid7, our solutions are designed to support organisations in addressing the core obligations defined under the German BSI Act (BSIG) - particularly around risk management, incident detection and response, and continuous security monitoring.

The table below illustrates how Rapid7 can support your compliance efforts.

NIS2 OBLIGATION	RELEVANT RAPID7 SOLUTION	HOW RAPID7 HELPS FULFILL IT
Risk analysis	Exposure Command • Vulnerability management and cloud security	Exposure Command directly supports the technical component of the NIS2 risk analysis requirements by providing data and context driven insights into exposures, focusing on active risk rather than just vulnerability severity.
Incident management	• InsightIDR (SIEM/XDR) • MDR service	Detection and response: InsightIDR acts as the central nervous system for logging and alerting. It detects anomalies and potential breaches in real-time. If you lack internal staff, Rapid7's Managed Detection and Response (MDR) service provides 24/7 monitoring and response, directly covering the "handling security incidents" mandate.
Business continuity (crisis management)	Incident response (IR) retainer	Crisis Support: While NIS2 mandates backup and disaster recovery, Rapid7's IR retainer fulfills the incident response and crisis management requirements, ensuring a battle-tested recovery path after a disruption.
Supply chain security	• Surface Command • Cloud security	External visibility: Surface Command provides visibility into your digital supply chain by identifying 'shadow' assets and external dependencies that could serve as entry points, helping you validate the security posture of third-party connections. Cloud security ensures that public cloud environments (often interconnected with third parties) remain secure and compliant.
Security in acquisition, development & maintenance	Exposure Command • Application security and cloud security	Secure by design: Application security (DAST) tests web applications for vulnerabilities during development (DevOps integration). Cloud security scans cloud infrastructure as code (IaC) to ensure new systems are secure before they are deployed ("shift left").
Cryptography and encryption	Exposure Command • Vulnerability management and cloud security	Policy auditing: These tools do not perform encryption, but they audit it. They scan your network and cloud specifically to flag unencrypted data stores, weak SSL/TLS certificates, or legacy protocols, ensuring your encryption policy is actually enforced. Rapid7 helps identify where encryption is missing or misconfigured, allowing you to prove to auditors that your 'state-of-the-art' encryption policies are being technically enforced.
Cybersecurity training	• Advisory services • Tabletop exercises	Management training: Rapid7 offers tabletop exercises that simulate a breach. This specifically targets the management and executive level (as required by NIS2) to train them on decision-making during a crisis.
Multi-factor authentication (MFA)	InsightIDR	Verification: InsightIDR ingests authentication logs (from Okta, AD, etc.) to monitor MFA usage. It can alert you if administrators are logging in without MFA or if there are bypass attempts, proving to auditors that MFA is being enforced.

Modern cybersecurity legislation such as NIS2 - and its national implementations, including Germany's NIS2UmsuCG - no longer rewards checkbox compliance. Instead, it demands continuous awareness, prioritized risk reduction, and demonstrable response capability. Compliance is no longer a point-in-time exercise - it is the outcome of a mature, continuously operating security program.

Organizations that treat compliance as a byproduct of strong security, rather than the end goal, will be best positioned to succeed. Rapid7's Command Platform is designed with this principle at its core, enabling organizations to operationalize NIS2 requirements through unified visibility across hybrid environments, threat-informed risk prioritization, and integrated detection and response capabilities.

Central to this approach is the shift toward Continuous Threat Exposure Management (CTEM). Rather than relying on periodic vulnerability scans or static reports, Rapid7 provides the real-time telemetry and

context needed to continuously understand and reduce the attack surface. This is particularly relevant under frameworks like NIS2UmsuCG, where organizations must demonstrate to regulators such as the BSI that they are actively and continuously managing cyber risk - not just documenting it. Compliance is no longer a report generated once a year - it becomes a living, measurable process, visible through ongoing risk insights and operational dashboards.

This approach has been recognized by industry analysts, with Rapid7 named a Leader in the 2025 Gartner® Magic Quadrant™ for Exposure Assessment Platforms, underscoring its strength in helping organizations operationalize CTEM at scale.

As regulatory expectations continue to evolve, Rapid7 remains committed to aligning its platform with emerging standards, providing customers with compliance-aligned capabilities and policy frameworks that accelerate both time-to-compliance and measurable risk reduction.

Ultimately, the shift underway is not just regulatory - it is operational and strategic. Organizations that embed continuous risk management into their security programs will not only meet obligations under NIS2 and NIS2UmsuCG, but also build the resilience and trust required to operate confidently in an increasingly complex threat landscape.

If you would like to find out more on how Rapid7 can support your NIS 2 compliance please visit: https://www.rapid7.com/products/command/exposure-management/ or contact your local Rapid7 representative or partner.

ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our website, check out our blog, or follow us on LinkedIn or X.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**