ManageEngine

A quick guide to the NIS2UmsG

The NIS2 Implementation Act (NIS-2-Umsetzungsgesetz, NIS2UmsG) is Germany's transposition of the EU NIS 2 Directive, enacted as a rewritten Act on the Federal Office for Information Security (BSIG). It sets cybersecurity risk management, reporting, and governance duties for essential and important entities, supervised by the Federal Office for Information Security (BSI).

Sl.no	Requirement area	Articles	Controls required
1	Governance & accountability	§ 30(1), § 38	• Adopt a risk management policy • Document compliance • Management approves and oversees measures • Complete management training
2	Risk analysis & asset management	§ 30(2) Nr. 1, 9	• Maintain a system and asset inventory • Run risk analysis • Classify and manage assets • Set access control policies
3	Access control & authentication	§ 30(2) Nr. 9–10	• Enforce role-based access • Deploy MFA • Govern privileged access • Secure the identity life cycle
4	Threat detection & monitoring	§ 30(2) Nr. 2, § 31(2)	• Centralize log collection • Run attack detection systems • Detect anomalies continuously • Monitor cloud and hybrid systems
5	Incident handling & response	§ 30(2) Nr. 2	• Detect and triage incidents • Contain and remediate threats • Track response times • Maintain response playbooks
6	Incident reporting	§ 32(1)	• Send a 24-hour early warning • Submit a 72-hour notification • File a one-month final report • Record indicators of compromise
7	Business continuity & supply chain	§ 30(2) Nr. 3–4	• Automate backup and recovery • Test disaster recovery • Assess supplier security • Govern third-party access
8	Effectiveness, hygiene & evidence	§ 30(2) Nr. 5–7, § 39	• Manage vulnerabilities • Assess control effectiveness • Enforce cyber hygiene • Maintain audit evidence

The NIS2UmsG and ManageEngine

ManageEngine offers solutions that help organizations govern access, detect threats, and evidence compliance. AD360, ManageEngine's IAM solution, and Log360, its SIEM solution, together cover identity governance, authentication, logging, threat detection, and incident response. With them, you can implement the controls required under the NIS2UmsG.

How can ManageEngine help you implement the NIS2UmsG?

Multi-factor authentication

Enforce risk-scored MFA across roughly 20 methods, including FIDO2 and biometrics, at login to Active Directory, VPN, and applications.

Helps with § 30(2) Nr. 10.

Role-based access governance

Grant access by role, group, or attribute and govern privileged accounts from a central console.

Helps with § 30(2) Nr. 9.

Access certification

Review and validate user entitlements through recurring certification campaigns.

Helps with § 30(2) Nr. 6, Nr. 9.

Attack detection and analytics

Detect threats with over 2,000 ATT&CK-mapped rules, correlation, and UEBA anomaly detection across live systems.

Helps with § 31(2), § 30(2) Nr. 2.

File integrity monitoring

Detect unauthorised change, deletion, or corruption of files on monitored systems.

Helps with § 30(2) Nr. 5.

Centralized log management

Collect, parse, and retain logs from on-premises, cloud, and outsourced systems.

Helps with § 30(2) Nr. 1, Nr. 4.

Incident response automation

Contain threats automatically by disabling accounts, quarantining endpoints, and blocking IP addresses.

Helps with § 30(2) Nr. 2.

Incident reporting and timelines

Assemble severity, impact, and indicators of compromise to meet the 24-hour, 72-hour, and one-month deadlines.

Helps with § 32(1).

Backup and recovery

Back up and restore Active Directory, Entra ID, and Microsoft 365 from automated, secure copies.

Helps with § 30(2) Nr. 3.

For more information, contact sales@manageengine.com