ManageEngine

A quick guide to the KRITIS-Dachgesetz

Germany's federal law on the physical resilience of critical installation

The KRITIS-Dachgesetz (KRITIS Umbrella Act) transposes Directive (EU) 2022/2557 into German law, requiring operators of critical installations in ten sectors to strengthen the physical resilience of the services on which national supply security depends.

Sl.no	Requirement area	Section	Controls required
1	Identification and registration	§ 5, 8	• Confirm sector, critical service, and supply-grade threshold • Register with the BBK and keep particulars current
2	Risk analysis and assessment	§ 11, 12	• Ingest national risk analyses into operator assessments • Run operator risk analysis every four years • Assess cross-sector dependencies and reassess
3	Prevention and physical protection	§ 13(1)	• Harden perimeter and deploy monitoring and detection • Enforce access controls and secure logical access with MFA
4	Personnel security	§ 13(3)	• Screen personnel and govern external-provider access • Provision on lifecycle and train and exercise staff
5	Response and continuity	§ 13(1), (3)	• Maintain crisis and alarm procedures with backup power • Identify alternative supply chains and recover
6	Resilience plan and evidence	§ 13(4), 16	• Document measures, rationale, and audit-ready evidence • Support audits and inspection, and remediate deficiencies
7	Audit, logging & oversight	§ 18	• Detect incidents and report to the BBK within 24 hours • Update ongoing reports and submit a detailed report in one month
8	Governance and data handling	§ 20, 23	• Assign management oversight of resilience measures • Enforce need-to-know access to personal data

Source: www.gesetze-im-internet.de/kritisdachg/KRITISDachG.pdf

The KRITIS-Dachgesetz and ManageEngine

ManageEngine offers solutions that help operators govern access and monitor activity and evidence compliance for the identity and IT dimensions of the KRITIS-Dachgesetz. AD360, ManageEngine's IAM solution, secures authentication, least-privilege access, and recovery of the identity layer. Log360, its SIEM solution, delivers detection, incident response, retention, and audit-ready evidence. Together they help operationalize the parts of the act that touch identity, monitoring, and reporting, alongside the physical measures operators supply separately.

How can ManageEngine help you implement the KRITIS-Dachgesetz?

Registration data management

Maintain authoritative operator, contact, and responsible-person records, and alert on changes that trigger updates.

Helps with § 8(1), § 8(6).

Operator risk analysis

Monitor baseline behavior, score users and entities based on risk, and correlate events to inform the four-yearly assessment.

Helps with § 12(1).

Adaptive authentication

Enforce risk-scored MFA and conditional access on machine, VPN, and application logons at critical installations.

Helps with § 13(1) No. 1–2.

Access governance

Automate lifecycle provisioning and enforce least-privilege access for staff and external service providers.

Helps with § 13(3) No. 5.

Incident response

Trigger containment playbooks and guided investigation automatically when an alert fires.

Helps with § 13(1) No. 3.

Identity-layer recovery

Back up and restore directory objects and roll back unauthorized changes to speed service restoration.

Helps with § 13(1) No. 4.

Audit trails & evidence

Retain time-stamped, searchable records and export audit-ready reports for verification and inspection.

Helps with § 16(2)–(4).

Incident reporting support

Detect and time-stamp incidents in real time and assemble the evidence for 24-hour and one-month reports.

Helps with § 18(1)–(2).

Management oversight

Provide approval workflows and dashboards that evidence resilience measures are implemented and overseen.

Helps with § 20(1), § 23(1).

For more information, contact sales@manageengine.com