ManageEngine

Your 2026 guide to IT-Grundschutz

Complying with the BSI IT-Grundschutz Compendium

AD360 | Log360



www.manageengine.com

Table of Contents

Introduction 3

Compliance levels and requirements 4

- Chapter I: Security management (ISMS) 5
- Chapter II: Organisation and personnel (ORP) 5
- Chapter III: Concepts and approaches (CON) 6
- Chapter IV: Operations (OPS) 7
- Chapter V: Detection and response (DER) 7

How ManageEngine can help 9

- Security management, organisation, and personnel 9
- Operational concepts and controls 12
- Detection, response, and systems 16

Conclusion 19

Introduction

The IT-Grundschutz Compendium is the methodology and catalogue of security requirements issued by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI) for protecting information, IT systems, and the business processes that depend on them. First established in the mid-1990s and revised continually, the compendium reflected in this guide is the edition finalised on 1 February 2021, comprising 97 modules and 47 elementary threats. It applies to public authorities and private organisations of every size and sector.

The framework emerged from a recognition that inadequately protected information is an underestimated risk, one capable of becoming an existential threat to an organisation. Rather than requiring every institution to perform a full risk analysis from first principles, the BSI performed that analysis in advance and packaged it into reusable modules covering everything from server rooms and cloud services to awareness training and industrial control systems. The modules are refreshed regularly to reflect new technologies and attack methods.

Compliance carries value beyond the regulatory obligation. Because IT-Grundschutz aligns with the ISO 27000 family, organisations that implement it gain a structured route toward ISO 27001 certification on the basis of IT-Grundschutz, along with a holistic security posture spanning governance, operations, systems, networks, and physical premises. The sections that follow describe the framework's structure, walk through its principal layers, and set out how ManageEngine AD360 and Log360 help organisations operationalise its technical requirements.

Compliance levels and requirements

The compendium organises its 97 modules using a layer model that separates process modules (which apply across an information domain) from system modules (which apply to specific objects). Ten layers span both families, and within every module the requirements fall into three categories—basic, standard, and increased protection needs—allowing organisations to scale effort to the sensitivity of what they protect.

IT-Grundschutz at a glance

— APPLICABLE REGION —

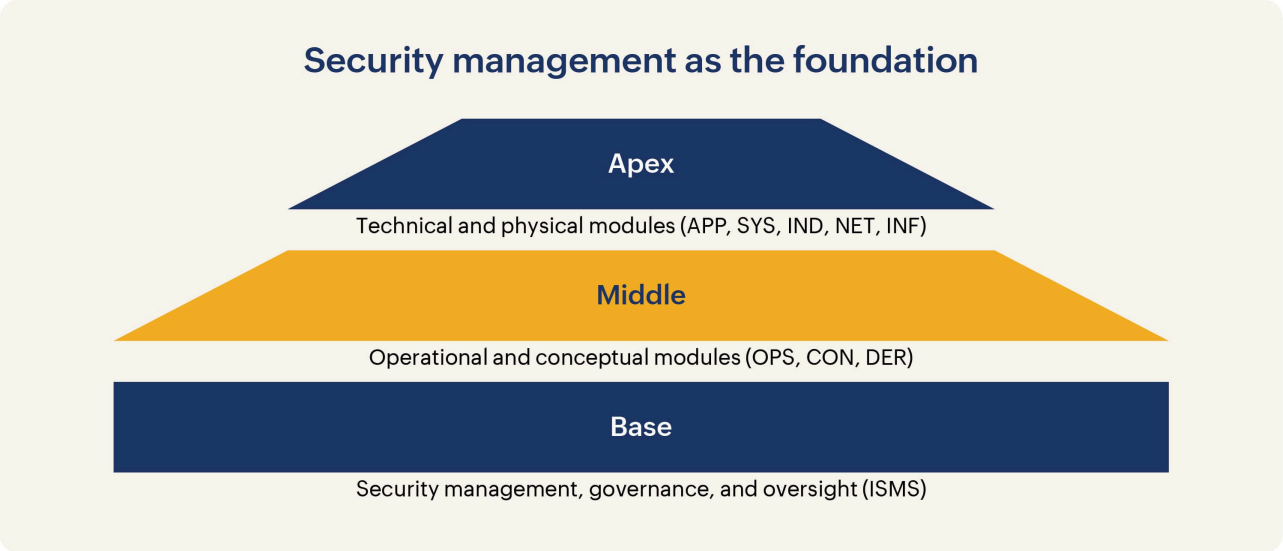
GERMANY

used internationally, published in English

Issuing authority German Federal Office for Information Security (BSI)	**Applicable industries** Public authorities and private organisations of all sizes and sectors organisations of all sizes and sectors	**Effective edition** Final draft, 1 February 2021	**Revisions** Revised continually since the mid-1990s; most recent is the 2021 edition
Total modules 97 modules across 10 layers	**Elementary threats** 47	**ISMS** The information security management system which forms the governance foundation	**ORP** Organisation and personnel, including access and awareness
CON Cross-cutting concepts such as cryptography, data protection, and backup	**OPS** Day-to-day operations, administration, logging, and cloud usage	**DER** Detection of and response to security-relevant events	**APP / SYS / IND / NET / INF** System layers for applications, systems, industrial tech, networks, and infrastructure

Chapter I: Security management (ISMS)

The information security management system (ISMS) layer sets the governance foundation the rest of the framework rests upon. It defines how an information security management system is planned, steered, and maintained, and it is deliberately compact because its role is direction and accountability rather than technical control. Without a functioning management system above them, the technical modules lack coherence.



Chapter II: Organisation and personnel (ORP)

This layer addresses the organisational and human dimensions of security, where many incidents originate. It defines organisational responsibilities, governs the personnel lifecycle from onboarding to departure, builds a culture of awareness, and controls who may access which resources. Identity and access management (IAM) sits at its centre.

The four pillars of the ORP layer

Organisation
Rules, responsibilities, and segregation of duties

Personnel
Secure onboarding, role change, and offboarding

Awareness and training
Building staff as a line of defence

Identity and access management
Governing who accesses what, and how

Chapter III: Concepts and approaches (CON)

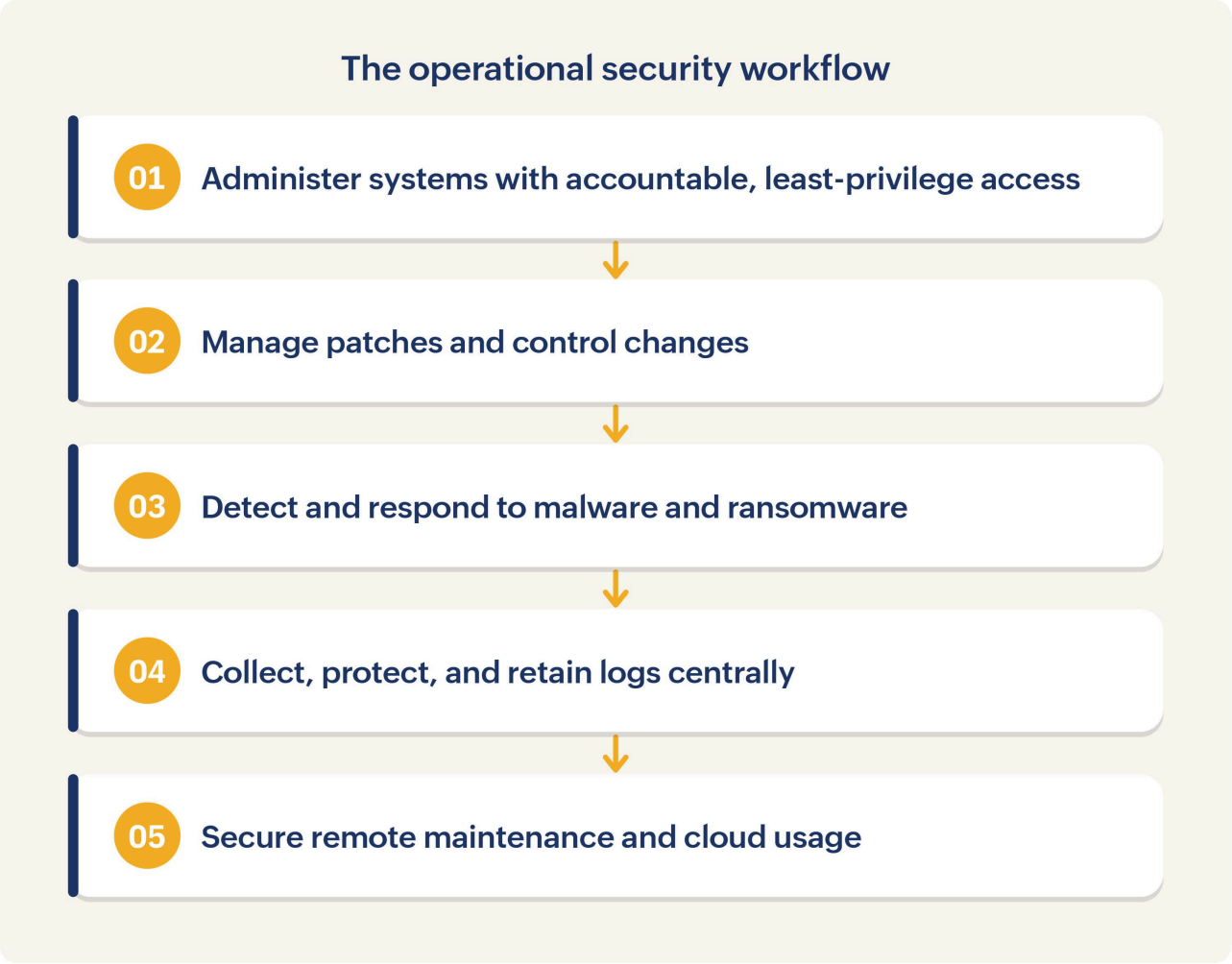
The CON layer holds the cross-cutting concepts an organisation defines once and applies everywhere, so that individual systems inherit consistent rules. It spans cryptography, data protection, backup, secure deletion, and secure development, among others, and it prevents each system from reinventing foundational controls.

Selected CON modules and their focus

Module	Focus
Crypto concept	Consistent application of encryption across the domain
Data protection	Locating, classifying, and controlling personal data
Backup concept	Ensuring data can be restored after loss or attack
Deleting and destroying data	Secure, non-recoverable disposal
Web application development	Building software securely from the outset

Chapter IV: Operations (OPS)

The OPS layer governs how to keep systems running securely once deployed. It covers - the routine security work that shapes most operational activity, including proper administration, patch and change management, protection against malware, logging, remote maintenance, and cloud usage.



Chapter V: Detection and response (DER)

The DER layer covers preparing for, detecting, and responding to security incidents. Its modules move from detecting security-relevant events, through structured incident handling and IT forensics, to cleaning up after extensive incidents and conducting audits and revisions. Treating detection and response as its own layer reflects that prevention alone is never sufficient.

The operational security workflow



How ManageEngine can help

Below are the substantive technical modules of IT-Grundschutz and how ManageEngine AD360 and Log360 help operationalise them. Each module is presented as a self-contained card—the module reference, the requirement in paraphrased form, and the Log360 and AD360 capabilities that satisfy it—each with a one-sentence mapping back to the module. Purely physical, industrial-hardware, and policy-only modules are not shown, as no software control operationalises them.

Security management, organisation, and personnel

Article	Requirement	How ManageEngine helps
ISMS.1	**Security management** Operate a functioning information security management system, including monitoring of the security process, review of policies, and management-level reporting.	**Log360** **Compliance dashboards and report templates** Supply management with continuous visibility of the security posture through prebuilt audit templates and dashboards, supporting the monitoring this module requires. **Real-time violation alerting** Notify responsible roles when a policy or control deviation occurs, operationalising the ongoing oversight the security process demands. **AD360** **Identity governance reporting** Provide management-level reports on identities and access that feed the security-process review this module obliges organisations to perform.

Article	Requirement	How ManageEngine helps
ORP.1	**Organisation** Assign responsibilities, access rights, and segregation of duties across the organisation so that no individual holds	**AD360** **Role-based access control** Enforce the access-rights assignment the module requires

Article	Requirement	How ManageEngine helps
	conflicting privileges.	by binding permissions to defined roles rather than individuals. **Multi-level approval workflows** Separate request from approval so segregation of duties is enforced procedurally, matching the conflicting-privilege prohibition this module sets. **Access certification** Recertify entitlements periodically to keep the assignment of access rights aligned with organisational responsibilities over time.

Article	Requirement	How ManageEngine helps
ORP.2	**Personnel** Handle the joiner-mover-leaver lifecycle securely, provisioning access on hire and revoking it promptly on role change or departure.	**AD360** **Automated identity lifecycle management** Provision accounts upon hire and deprovision them upon departure automatically, closing the access-revocation gap this module addresses. **HCM-driven automation** Trigger the lifecycle from the authoritative HR source so role changes propagate to access without manual delay. **Orchestration templates** Apply consistent provisioning rules across directories and applications, ensuring personnel access matches assigned function.

Article	Requirement	How ManageEngine helps
ORP.4	**Identity and access management** Administer identities and access rights, enforce strong or	**Log360** **Logon and privileged-access auditing**

Article	Requirement	How ManageEngine helps
	multi-factor authentication (MFA), and review granted access on a regular basis.	Record logon activity and privileged-account use, providing the evidence base for the regular access review this module obliges organisations to conduct. **AD360** **Adaptive MFA** Require a risk-scored second factor—biometrics, FIDO2, or hardware token—at login to Active Directory, VPN, and applications, delivering the strong authentication this module mandates. **MFA-secured single sign-on (SSO)** Centralise authentication under audited identities so access to enterprise resources is both SSO and MFA protected. **Self-service password management** Enforce password-complexity policy and let users reset credentials safely, supporting the identity-administration obligation. **Identity lifecycle and RBAC** Administer identities and bind access to roles, directly operationalising the access-rights management this module requires. **Access certification and identity analytics** Recertify access and flag anomalous entitlements, satisfying the regular-review element of this module.

Operational concepts and controls

Article	Requirement	How ManageEngine helps
CON.2	**Data protection** Protect personal data, including knowing where such data resides and controlling access to it.	**Log360** **Sensitive data discovery** Locate personal data across servers, endpoints, and cloud repositories, satisfying the know-where-data-resides requirement this module sets. **Data classification** Tag data by sensitivity so proportionate protection is applied to the personal data this module obliges organisations to safeguard. **File access auditing** Record who accesses protected data, operationalising the access-control element of the data-protection obligation. **Data leak prevention** Block unauthorised exfiltration of personal data via endpoint, email, and USB channels.

Article	Requirement	How ManageEngine helps
CON.3	**Backup concept** Back up data regularly so it can be restored after loss, corruption, or a security incident.	**AD360** **Active Directory backup and recovery** Back up Active Directory and Entra ID and restore objects and attributes after deletion, misconfiguration, or ransomware, covering the identity infrastructure the backup concept this module requires.

Article	Requirement	How ManageEngine helps
CON.6	**Deleting and destroying data** Delete data and media securely so information cannot be reconstructed after disposal.	**Log360** **File-activity and deletion auditing** Record and alert upon deletion events, providing the accountable evidence that the secure-disposal this module requires has occurred.

Article	Requirement	How ManageEngine helps
OPS.1.1.2	**Proper IT administration** Administer IT systems accountably, restricting and monitoring privileged administrative activity.	**Log360** **Privileged-user activity monitoring** Track privileged sessions and flag anomalous administrator behaviour, delivering the monitoring of privileged activity this module requires. **Active Directory change auditing** Audit changes to directory objects with who-did-what detail, supporting accountable administration. **AD360** **Non-invasive delegation** Let technicians perform tasks without standing privilege, restricting administrative access as this module obliges. **Approval workflows and request repository** Route sensitive actions through approval and record them, providing the accountability this module demands.

Article	Requirement	How ManageEngine helps
OPS.1.1.3	**Patch and change management** Track and control changes to systems and detect	**Log360** **Change auditing and correlation** Audit and alert on changes to

Article	Requirement	How ManageEngine helps
	unauthorised or unmanaged changes.	directory objects, files, and monitored configurations, detecting the unauthorised changes this module requires organisations to catch.

Article	Requirement	How ManageEngine helps
OPS.1.1.4	**Protection against malware** Detect and respond to malware, including ransomware, on systems and data stores.	**Log360** **Threat intelligence** Match activity against malicious IP, URL, and domain feeds to surface the malware indicators this module obliges organisations to detect. **Correlation and user and entity behavior analytics (UEBA)** Detect ransomware behaviour through file-activity monitoring and anomaly detection, exposing attacks that signatures alone would miss. **Automated response** Isolate affected systems or halt encryption automatically when malware is detected, delivering the response element of this module.

Article	Requirement	How ManageEngine helps
OPS.1.1.5	**Logging** Collect, protect, and retain log data recording security-relevant events, centrally.	**Log360** **Centralised log management** Collect logs from across the network into a single store, satisfying the central-collection requirement thismodule sets. **Tamper-proof storage and retention** Protect logs against alteration and retain them for a configurable period, meeting the protection and retention obligations.

Article	Requirement	How ManageEngine helps
		Searchable archive Make the retained log data searchable for review and investigation, operationalising the accessibility this module implies.

Article	Requirement	How ManageEngine helps
OPS.1.2.5	**Remote maintenance** Control remote access used for maintenance with strong authentication and logging of remote sessions.	**Log360** **Remote logon auditing** Audit remote logon events and generate alerts upon anomalous remote access, delivering the session-logging this module requires. **AD360** **MFA for VPN and RDP** Enforce MFA on remote-access channels, providing the strong authentication this module mandates for maintenance access. **Adaptive access policies** Evaluate metadata like IP, geolocation, and device before granting remote access, restricting maintenance sessions to approved conditions.

Article	Requirement	How ManageEngine helps
OPS.2.2	**Cloud usage** Use cloud services securely, monitoring cloud access, configuration, and data movement.	**Log360** **Cloud security monitoring** Audit cloud logons and configuration changes, delivering the visibility over cloud access this module requires. **Cloud access security broker (CASB) and shadow-IT discovery** Detect unsanctioned cloud

Article	Requirement	How ManageEngine helps
		applications and track data uploads and downloads, operationalising the data-movement monitoring this module sets.

Detection, response, and systems

Article	Requirement	How ManageEngine helps
DER.1	**Detecting security-relevant events** Detect events that may indicate a security incident, systematically, across systems and networks.	**Log360** **Real-time correlation engine** Analyse collected events against MITRE-mapped detection rules to surface the security-relevant events the module obliges organisations to detect. **UEBA anomaly detection** Baseline normal behaviour and flag deviations such as unusual logons or privilege abuse, catching events rules alone would miss. **Threat-intelligence matching** Correlate activity with global threat feeds to expose indicators of compromise as events occur.

Article	Requirement	How ManageEngine helps
DER.2.1	**Security incident handling** Respond to, contain, and resolve security incidents through a structured process with accountability for resolution.	**Log360** **Incident management console** Track incidents from detection to resolution with assigned ownership, delivering the accountability this module requires. **SOAR playbooks** Automate containment actions such as disabling accounts or isolating endpoints, operationalising the structured

Article	Requirement	How ManageEngine helps
		response this module prescribes. **ITSM integrations** Route incidents into service management software so each resolution is recorded and auditable.

Article	Requirement	How ManageEngine helps
DER.2.2	**Provisions for IT forensics** Prepare for forensic investigation, preserving tamper-evident evidence and reconstructing event twwimelines.	**Log360** **Tamper-proof log archive** Preserve an immutable, searchable record of events, providing the tamper-evident evidence the module requires for forensics. **AI-generated incident timelines** Reconstruct how an incident unfolded through generated timelines and process-lineage visuals, satisfying the timeline-reconstruction element.

Article	Requirement	How ManageEngine helps
DER.3.1	**ww** Audit and review regularly to verify that security controls are effective and being followed.	**Log360** **Audit reports and log search** Supply compliance report templates and searchable logs as the audit evidence this module obliges organisations to produce. **AD360** **Access certification and identity reports** Verify through recertification and identity reporting that access remains appropriate, supporting the control-effectiveness review this module requires.

Article	Requirement	How ManageEngine helps
SYS.1.1	**General server / OS auditing** Operate servers securely, logging security-relevant events and monitoring access and changes at the operating-system level.	**Log360** **Server and OS log collection** Collect Windows event logs and Unix syslog then audit logons and account changes, delivering the OS-level logging this module requires. **File integrity monitoring (FIM)** Detect unauthorised modification of critical system and configuration files on monitored servers.

Article	Requirement	How ManageEngine helps
APP.2.2 / NET	**Directory service and network monitoring** Operate the directory service and network devices securely, auditing changes and monitoring traffic for anomalies.	**Log360** **Real-time directory change auditing** Audit changes to GPOs, OUs, ACLs, and privileged group memberships in real time, protecting the directory that governs access. **Network device log analysis** Ingest firewall, router, and switch logs and correlate network events to surface the traffic anomalies this modules require organisations to monitor. **AD360** **Directory administration and recovery** Manage and back up the directory for recovery, supporting secure operation of the service that governs access.

Conclusion

IT-Grundschutz endures because it converts the demanding task of securing information into something structured and repeatable, packaging the BSI's own risk analysis into modules organizations can adopt directly. Its holistic scope—spanning governance, operations, systems, networks, and physical premises—is what makes a disciplined approach so valuable, and its alignment with ISO 27001 gives compliance an internationally recognized endpoint.

The technical modules—from identity and access management through logging, detection, and incident response—map closely to the capabilities of a modern IAM and security information and event management (SIEM) portfolio. ManageEngine AD360 and Log360 together operationalize those modules: AD360 governs identities, authentication, and access, while Log360 delivers the logging, monitoring, detection, and response the framework demands. Adopted together, they help organizations move IT-Grundschutz from a catalogue of requirements to a working, auditable security capability.

This guide reflects the IT-Grundschutz Compendium, final draft dated 1 February 2021, published by the German Federal Office for Information Security (BSI).

Our Products

ADManager Plus | ADAudit Plus | ADSelfService Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | RecoveryManager Plus | M365 Manager Plus

ManageEngine
AD360

ManageEngine AD360 is a unified identity and access management solution that seamlessly connects people, technology, and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance, and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, life sciences, finance, education, and government, AD360 simplifies identity management, fortifies security, and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download