SmartSuite

Framework / Cybersecurity / Other

# BSI Standard 200-1

BSI Standard 200-1 is a German ISMS framework guiding organizations to implement information security governance, risk management, and controls.

## What it is

BSI Standard 200-1 is a German information security management system (ISMS) framework that helps organizations establish, implement, and maintain effective cybersecurity and risk management practices. The standard provides a structured approach to protecting valuable information assets against evolving threats and vulnerabilities.

Issued by the German Federal Office for Information Security (BSI), BSI Standard 200-1 is primarily used by organizations operating in Germany and the EU, including public sector entities and private enterprises. The framework focuses on core areas such as information security governance, organizational security controls, risk assessments, and ongoing compliance management, and aligns with other ISMS standards like ISO/IEC 27001.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>Bundesamt für Sicherheit in der Informationstechnik (BSI) | TYPE<br>Standard | VERSION<br>2020 |
| EFFECTIVE<br>2018 | DOMAIN<br>Cybersecurity | FAMILY<br>Other |
| REGION<br>Germany | ADOPTION MODEL<br>Regulatory Compliance | IMPLEMENTATION COMPLEXITY<br>High |

Source: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=2

## Why it matters

- **Strengthen information security governance** Establish clear roles, responsibilities, and oversight, ensuring comprehensive management of information security risks at all organizational levels.
- **Enhance regulatory compliance** Support alignment with national and EU requirements, facilitating data protection obligations and easing certification or external audit processes.
- **Promote operational resilience** Enable proactive risk management and preparedness, helping organizations minimize the impact of potential cyber incidents or service disruptions.
- **Improve security risk awareness** Facilitate systematic risk analysis and regular assessments, enabling timely identification and mitigation of evolving threats and vulnerabilities.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

## How SmartSuite supports BS 200-1

### ISMS Governance and Policy Management

Centralize information security policies, governance documentation, and approval workflows.

### Risk Identification and Security Assessments

Track information security risks, mitigation actions, and ongoing risk evaluations.

### Control Implementation and Monitoring

Manage security controls mapped to IT-Grundschutz requirements and monitor their effectiveness.

### Security Roles and Responsibilities

Assign accountability for information security processes and track ownership of security tasks.

### Vendor and Third-Party Security Oversight

Monitor suppliers and service providers supporting critical systems.

### Security Program Reporting and Audit Readiness

Provide dashboards and reporting for ISMS performance, compliance status, and audit readiness.

## Common framework mappings

CIS Controls v8.1 | GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

## Official resources

### BSI Standard 200-1: Management Systems for Information Security

Defines requirements for establishing an Information Security Management System (ISMS) according to BSI standards.

bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=2

### BSI Standards Overview

Describes the structure and purpose of BSI standards for information security management systems.

bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=2

### IT-Grundschutz Guide

Provides comprehensive implementation guidance on BSI's IT-Grundschutz methodology for information security.

bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

## Frequently asked questions

### What is BSI Standard 200-1 used for?

BSI Standard 200-1 is used to help organizations establish, implement, and maintain an effective Information Security Management System (ISMS). It provides a framework for identifying and mitigating information security risks, ensuring the confidentiality, integrity, and availability of organizational assets. The standard is widely adopted in Germany and the EU by both public and private sector organizations.

### What organizations does BSI Standard 200-1 apply to?

BSI Standard 200-1 applies to any organization seeking to manage information security risks, with particular relevance for entities operating in Germany and the EU. It is suitable for organizations of all sizes, including government bodies, critical infrastructure operators, and private businesses aiming for structured security governance.

### What key documents and artifacts are required by BSI Standard 200-1?

Organizations implementing BSI Standard 200-1 are expected to produce an ISMS policy, risk assessment reports, a Statement of Applicability (SoA), and documentation of controls based on the IT-Grundschutz catalogs. Additional required artifacts include incident management procedures, audit records, and continuous improvement evidence.


Updated Sep 26, 2026 | © 2026 SmartSuite Inc. All rights reserved.

### How is BSI Standard 200-1 implemented in practice?

Implementation involves defining the ISMS scope, conducting systematic risk assessments, selecting appropriate technical and organizational controls from IT-Grundschutz modules, and instituting robust security policies. Organizations must also establish processes for monitoring, incident response, audits, and continuous improvement according to the PDCA (Plan-Do-Check-Act) cycle.

### Is BSI Standard 200-1 mandatory or certifiable?

BSI Standard 200-1 is not legally mandatory but may be required or recommended by regulatory bodies, particularly within Germany's public sector. While the standard itself is not a certifiable specification, it forms the foundation for certification under the BSI IT-Grundschutz certification scheme, which verifies effective ISMS implementation.

### How does BSI Standard 200-1 relate to other frameworks like ISO/IEC 27001?

BSI Standard 200-1 aligns closely with ISO/IEC 27001 in its approach to ISMS design and risk management but is tailored to German regulatory contexts and includes specific guidance on control selection through IT-Grundschutz catalogs. Many organizations integrate both standards to meet broader international and national compliance requirements.

### What are the ongoing compliance requirements of BSI Standard 200-1?

Ongoing compliance with BSI Standard 200-1 requires continuous risk monitoring, regular internal and external audits, periodic reviews and updates of controls, evidence collection, and incident response activities. Organizations must maintain an auditable trail of policy, risk assessments, and documented mitigations to demonstrate sustained ISMS effectiveness.

### How would SmartSuite support BSI Standard 200-1?

SmartSuite helps organizations manage BSI Standard 200-1 by enabling risk register creation, aligning selected controls with IT-Grundschutz modules, and automating evidence collection. It supports compliance tracking, audit readiness, and comprehensive reporting through dashboards, ensuring organizations can efficiently monitor, document, and improve their information security posture.

License included / downloadable: Yes BSI standards are publicly available through Germany's Federal Office for Information Security (BSI).

Full framework page and mappings: smartsuite.com/frameworks/bsi-standard-200-1-management-systems-for-information-security-isms


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.