SmartSuite

Framework / Cloud Security / BSI IT-Grundschutz

BSI C5:2020

C5:2020 is a BSI catalogue of cloud security controls to assess and demonstrate security and compliance of cloud services.

Federal Office for Information Security

What it is

Germany C5:2020 — Cloud Computing Compliance Controls Catalogue is a cybersecurity and compliance framework that helps organizations assess and demonstrate the security of cloud service offerings. The catalogue outlines control requirements designed to address risks related to data protection, information security, and regulatory compliance in cloud environments.

Published by the German Federal Office for Information Security (BSI), C5:2020 is used by cloud service providers, auditors, and organizations seeking assurance over the implementation of essential security controls. Its scope covers areas such as risk management, access control, physical security, incident response, and transparency, making it applicable to both national and international cloud operations.

At a glance

PUBLISHER Federal Office for Information Security (BSI)	TYPE Control Framework	VERSION C5:2020
EFFECTIVE 2020	DOMAIN Cloud Security	FAMILY BSI IT-Grundschutz
REGION Germany	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Security Baseline
IMPLEMENTATION COMPLEXITY High		

Source: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3

Why it matters

- **Support regulatory compliance efforts** Enable organizations to demonstrate adherence to German and international data protection and security regulations for cloud environments.
- **Increase audit readiness** Provide documented evidence and systematic controls that simplify audit preparations and third-party assurance activities for cloud services.
- **Strengthen security governance** Establish formalized risk management and security processes aligned with recognized best practices for cloud service providers and customers.
- **Enhance transparency and accountability** Enable organizations to communicate security practices and incident handling measures clearly to stakeholders and customers.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports BSI C5:2020

Cloud Scope and Boundary Definition

Define the cloud service scope, boundaries, and dependencies with clarity.

C5 Control Library and Ownership

Organize C5 control areas with owners, procedures, and implementation evidence.

Evidence Collection and Audit Trail

Centralize policies, technical artifacts, and proof linked to each control.

Assessments and Remediation Workflow

Track findings, remediation plans, retesting, and closure verification.

Continuous Monitoring Cadence

Schedule scanning, patching, monitoring, and recurring evidence updates.

Audit-Ready Reporting

Report readiness, gaps, and control status for auditors and customers.

Common framework mappings

GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27017 | ISO 27018 | ISO 27701 | NIST 800-53 Rev.5

Official resources

C5:2020 Cloud Computing Compliance Controls Catalogue

Provides control requirements for assessing and ensuring cloud security and compliance.

bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf

BSI Cloud Computing Overview

Outlines the key aspects and objectives of the C5 compliance framework.

bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

Implementing C5:2020 Controls

Official BSI guide on integrating C5 controls into cloud security programs.

bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

Frequently asked questions

What is Germany C5:2020 used for?

Germany C5:2020 is a framework designed to help organizations assess and demonstrate the security of cloud service offerings. It provides a structured set of control requirements covering data protection, information security, and regulatory compliance specifically for cloud environments.

Is Germany C5:2020 a mandatory or certifiable standard?

Germany C5:2020 is not legally mandatory but is commonly required by German and some European organizations as a minimum standard for cloud security assurance. While the framework itself does not grant formal certification, cloud service providers can obtain attestation through independent audits by qualified third parties.

What is the scope of Germany C5:2020?

The scope of C5:2020 includes organizational, technical, and physical security controls applicable to cloud service providers and customers. It addresses risk management, access control, incident response, physical security, and transparency for both national and international cloud operations.

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

What are key concepts and artifacts required by C5:2020?

C5:2020 requires implementing documented policies, risk assessments, evidence of security control effectiveness, incident response plans, and detailed audit logs. Organizations must also demonstrate ongoing compliance through documentation and regular reviews of control effectiveness.

How does an organization implement Germany C5:2020?

Implementation involves mapping the control catalogue to all relevant cloud services, integrating the specified security controls, and performing risk and compliance assessments. Continuous evidence collection, internal monitoring, remediation, and supporting third-party audits are also essential steps.

How does Germany C5:2020 relate to other frameworks like ISO 27001 or SOC 2?

C5:2020 is complementary to standards like ISO 27001 and SOC 2, often used in parallel to enhance cloud security and regulatory compliance. The framework includes mappings to BSI IT-Grundschutz and references ISMS best practices, supporting organizations in meeting multiple compliance obligations.

What are the ongoing compliance requirements for Germany C5:2020?

Maintaining compliance with C5:2020 requires ongoing risk assessments, regular control testing, continuous monitoring, updating documentation, and timely incident reporting. Organizations must also retain and make available evidence of compliance for audit purposes.

How would SmartSuite support Germany C5:2020?

SmartSuite facilitates C5:2020 compliance by allowing organizations to import control libraries, track associated risks, and manage policy governance. Evidence collection is streamlined through attachment and workflow features, while dashboards and exportable reports support audit readiness and ongoing compliance monitoring.

License included / downloadable: Yes The C5 framework is published by the German Federal Office for Information Security (BSI) and is publicly available through official government sources.

Full framework page and mappings: smartsuite.com/frameworks/germany-c5-2020-cloud-computing-compliance-controls-catalogue