GUIDE 2025/2026

IT-Grundschutz guide

The BSI methodology, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is IT-Grundschutz? 3

1.1 The methodology in plain words 3

1.2 The BSI 200 series standards 3

1.3 The three approaches 3

1.4 How it compares with ISO 27001 4

2 Who is IT-Grundschutz worth it for? 5

3 The path to the certificate — 8 phases 6

4 What does IT-Grundschutz cost? 7

5 The 10 most common mistakes 8

6 Readiness check: are you ready? 10

7 Glossary 12

8 Your next step 13

1 What is IT-Grundschutz?

1.1 The methodology in plain words

IT-Grundschutz is the methodology of the **German Federal Office for Information Security (BSI)** for building an information security management system. It consists of the BSI 200 series standards and the **IT-Grundschutz Compendium**, with around 100 modules and well over 1,000 concrete requirements.

The decisive difference from other standards: IT-Grundschutz tells you not only *what* you have to achieve but also *how*. For a Windows server, a server room or a cryptographic concept there is a module each, with requirements spelled out.

> **The core idea:** ISO 27001 hands you a blank sheet and a framework. IT-Grundschutz hands you a catalogue already filled in — in return you have to document more carefully.

At the end there is an **ISO 27001 certificate based on IT-Grundschutz**, issued by the BSI. It is recognised internationally and counts in the German public sector as the stronger proof, because the audit goes deeper.

1.2 The BSI 200 series standards

1. **BSI Standard 200-1** — management systems for information security. Describes how the ISMS is built, run and continually improved. Corresponds in content to clauses 4 to 10 of ISO 27001.
2. **BSI Standard 200-2** — the IT-Grundschutz methodology. The heart of it: structure analysis, determining protection requirements, modelling, the IT-Grundschutz Check and implementation planning.
3. **BSI Standard 200-3** — risk analysis. Required for high protection requirements, a missing module or an atypical scenario. Works with the catalogue of elementary threats.
4. **BSI Standard 200-4** — business continuity management. A standard of its own for emergency management, with a staged model from reactive through to standard.

On top of that comes the **IT-Grundschutz Compendium**, updated every year, which groups the modules into ten layers: ISMS, ORP, CON, OPS, DER, APP, SYS, IND, NET and INF.

> **A way to remember it:** 200-1 says *what an ISMS is*, 200-2 says *how to build one*, 200-3 says *what else to do when protection requirements are high*, 200-4 governs *the emergency*.

1.3 The three approaches

You do not have to protect everything at once. IT-Grundschutz knows three routes:

Basic	Core	Standard
a quick start, not certifiable	full protection for your most important assets	complete — the condition for the certificate

Basic protection implements only the basic requirements of every relevant module. It works quickly but is not enough for certification. **Core protection** guards one small, especially valuable part. **Standard protection** covers the whole information domain and is the only route to the certificate.

1.4 How it compares with ISO 27001

Aspect	ISO 27001 (classic)	ISO 27001 based on IT-Grundschutz
Requirements	93 controls, implementation free	around 100 modules with concrete requirements
Risk analysis	mandatory for everything	only for high protection requirements (200-3)
Documentation	moderate	considerably more extensive
Certificate	accredited body	the BSI, with certified auditors
Recognition	international	international + the standard in the German public sector

Worth knowing: anyone already running an ISMS to ISO 27001 brings around 70 % of the management system requirements with them. The extra work sits almost entirely in structure analysis and modelling — the two steps ISO 27001 does not have in this form.

2 Who is IT-Grundschutz worth it for?

IT-Grundschutz is the recognised methodology for information security in the German public sector — and increasingly wherever public bodies are the customer.

A. Public administration

Federal, state and local government use IT-Grundschutz as their authoritative standard. For many public bodies administrative rules make it mandatory — there the question is not whether, only how far.

B. Operators of critical infrastructure

For operators of critical infrastructure, IT-Grundschutz is an established way of demonstrating compliance to the BSI. Against ISO 27001 it has the advantage of far more concrete requirements — which makes it easier to evidence compliance in an audit under § 8a BSIG.

- energy and water supply
- healthcare and hospitals above the threshold
- transport and traffic
- finance and insurance (alongside DORA)
- information technology and telecommunications

C. Service providers to the public sector

IT service providers, data centres, software houses and consultancies working for public bodies increasingly have to show IT-Grundschutz in tenders — in part alongside ISO 27001, in part instead of it.

> **A special case:** if you work for several public bodies, cut the information domain so that it covers all of them. Too narrow a domain means recertifying for the next tender.

D. When is it not worth it?

If your customers ask only for ISO 27001 and no public body is involved, the direct ISO 27001 route is usually the more economical one. IT-Grundschutz calls for considerably more documentation — which only pays off when it is actually asked for.

> **A real example:** an IT service provider with 80 employees runs data centres for three state authorities. It was already certified to ISO 27001; extending to IT-Grundschutz took nine months, mostly for structure analysis and modelling. Since then it no longer has to provide separate evidence for each tender.

3 The path to the certificate — 8 phases

The approach set out in BSI Standard 200-2 is clearly prescribed. Do not cut this order short — each phase builds on the one before:

Phase 1 — Policy and security organisation

Write the information security policy and have management adopt it, appoint an information security officer, set responsibilities. *Three to five weeks.*

Phase 2 — Defining the information domain

Decide which business processes, sites and systems belong to the domain. This decision sets the effort and duration of the whole project. *Two to three weeks.*

Phase 3 — Structure analysis

Record every object: business processes, applications, IT systems, networks, rooms and communication links — with their dependencies. The most laborious single step. *Six to twelve weeks.*

Phase 4 — Determining protection requirements

Set normal, high or very high for each object — derived from the business processes and inherited by applications and systems. *Three to five weeks.*

Phase 5 — Modelling

Assign the matching Compendium modules to each object. The result is your individual catalogue of requirements. *Four to six weeks.*

Phase 6 — IT-Grundschutz Check

A target/actual comparison per requirement: dispensable, yes, partly or no — with reasons and an owner. *Six to ten weeks.*

Phase 7 — Risk analysis and implementation

A risk analysis under 200-3 for objects with high protection requirements, then prioritised implementation of the open requirements. *Four to nine months.*

Phase 8 — Internal audit and certification

Internal audit, management review, application to the BSI, the auditor's inspection on site. *Three to five months.*

> **Tip:** do not underestimate phase 3. Structure analysis needs knowledge from IT, the business units and facilities management at the same time — getting everyone in a room is often the real bottleneck, not the recording itself.

4 What does IT-Grundschutz cost?

Cost scales with the size of the information domain, not with headcount. A small domain inside a large organisation is cheaper than the other way round:

Information domain	Total cost*	Timeframe	Internal effort
Small (up to 30 target objects)	**€18,000–28,000**	8–12 months	30–45 person-days
Medium (30–80 target objects)	**€28,000–45,000**	10–16 months	45–70 person-days
Large (80–200 target objects)	**€45,000–75,000**	14–22 months	70–120 person-days
Very large (200+)	**from €75,000**	18–30 months	½–1 FTE
With ISO 27001 already in place	**−30 to −40 %**	−4 to −6 months	considerably less

* Covers consulting, structure analysis, protection requirements, modelling, the Grundschutz Check and preparation for certification. Excluding BSI certification fees and auditor costs.

What drives the cost?

- **Size of the information domain:** every additional target object means modelling, a check and evidence. A well-cut domain saves more than any negotiation over day rates.
- **Proportion with high protection requirements:** every object with high requirements pulls a risk analysis under 200-3 behind it.
- **An existing ISMS:** an ISO 27001 certification already in place cuts the effort by 30–40 %.
- **State of the documentation:** network plans, asset lists and room records that are kept up shorten the structure analysis considerably.

Running cost after certification

Plan for **25–35 % of the set-up cost per year**. The certificate runs for three years, with a surveillance audit each year. On top of that:

- incorporating the annual Compendium update
- keeping structure analysis and protection requirements current as things change
- maintaining implementation status and evidence
- an external information security officer (optional): from €850 a month

> **On transparency:** quotes made before the information domain has been defined are not worth much. Always ask to be shown how many target objects a provider is assuming — that is the only figure that really sets the price.

5 The 10 most common mistakes

From guiding a good many Grundschutz projects, we know the usual stumbling blocks:

1. **Cutting the information domain too large**
   “Let us just take everything.” Every additional target object costs modelling, a check and evidence. Too large a domain is the most common reason projects are abandoned.

2. **Underestimating the structure analysis**
   It needs knowledge from IT, the business units and facilities management. Treat it as an IT task and you miss the INF layer entirely and have to go back.

3. **Protection requirements without clear criteria**
   Without defined damage scenarios and thresholds the rating becomes arbitrary — and open to challenge in the audit. The criteria belong before the first rating, not after it.

4. **Modelling by feel**
   Modules get picked rather than assigned systematically along the modelling rules. Every module left out needs a documented reason.

5. **“Partly” without an explanation**
   In the Grundschutz Check, “partly implemented” without a reason and a plan is worthless. The auditor goes to exactly those entries first.

6. **Collecting evidence only just before the audit**
   In the audit what counts is not what is implemented but what can be shown. Linking requirement to evidence is the biggest time sink in the final stretch.

7. **Skipping the risk analysis under 200-3**
   For high protection requirements it is mandatory, not optional. Without it certification is impossible — however much has been implemented.

8. **Management involved only formally**
   A signed policy without a documented management review is not enough. The BSI checks whether management really lives up to its responsibility.

9. **Ignoring the Compendium update**
   The Compendium changes every year. Skip the new edition and it shows in the surveillance audit — even if nothing else has changed.

10. **Mistaking basic protection for certification**

Basic protection works quickly but cannot be certified. If you need a certificate, plan for standard protection from the start.

6 Readiness check: are you ready?

Answer the following ten questions honestly with yes or no. The result shows your Grundschutz maturity.

1. **Is there an information security policy adopted by management?**
   Module ISMS.1.A3 — in writing, current, made known.
2. **Is an information security officer appointed, with time for the job?**
   ISMS.1.A2 — appointed in writing, with access to management.
3. **Is the information domain clearly defined and documented?**
   BSI 200-2 sect. 8.1 — sensibly cut and able to function on its own.
4. **Does a complete structure analysis exist?**
   Processes, applications, systems, networks, rooms — with dependencies.
5. **Are protection requirements determined for every object?**
   Normal, high or very high — with defined damage scenarios.
6. **Has modelling been done against the Compendium?**
   Modules assigned systematically, omissions justified.
7. **Has an IT-Grundschutz Check been carried out?**
   Target/actual per requirement, with reasons and an owner.
8. **Are the basic requirements of every module met?**
   Requirements marked (B) are mandatory — without exception.
9. **Is there a risk analysis under 200-3 for high protection requirements?**
   Elementary threats assessed, measures derived.
10. **Does the security organisation report to management on the record?**
    At least once a year, with minutes and decisions.

Your yes answers	Where you stand	What to do
0–3 × yes	**At the beginning**	Start with the policy, the security officer and defining the domain. Expect 14–22 months to the certificate.
4–6 × yes	**Halfway there**	Usually what is missing is modelling, the Grundschutz Check or the risk analysis. 8–14 months.
7–10 × yes	**Close to certification**	Complete the evidence and prepare the internal audit. 4–8 months.

IT-Grundschutz is methodically demanding but very easy to plan — precisely because its requirements are so concrete. If you have questions about defining the domain, a free first conversation helps.

7 Glossary

The key terms around IT-Grundschutz, explained plainly:

IT-Grundschutz

The BSI methodology for information security, consisting of the BSI 200 series standards and the IT-Grundschutz Compendium.

BSI

The German Federal Office for Information Security — publisher of the methodology and the certification body.

Information domain

The defined area the ISMS applies to: business processes, applications, systems, networks and rooms.

Target object

A single element of the information domain to which modules are assigned — a server, an application or a room, for instance.

Structure analysis

The complete record of every target object with its dependencies (BSI 200-2, section 8.1).

Protection requirements

The rating of a target object as normal, high or very high — derived from the business processes and inherited by dependent objects.

Modelling

Assigning the matching Compendium modules to every target object. The result is the individual catalogue of requirements.

IT-Grundschutz Check

A target/actual comparison per requirement with the outcomes dispensable, yes, partly or no.

Module

A chapter of the Compendium on one topic — SYS.1.1 General Server, for instance. Contains basic, standard and elevated requirements.

Basic requirement (B)

A requirement that MUST be met. Standard requirements (S) SHOULD be met and need a reason where they are not.

Elementary threat

A standardised threat from the Compendium, the basis of the risk analysis under BSI Standard 200-3.

Basic protection

The approach that implements only the basic requirements. Quick to take effect, but not certifiable.

Standard protection

The complete approach across the whole domain — the condition for certification.

ISO 27001 based on IT-Grundschutz

The BSI certificate. It is recognised internationally and is the stronger proof in the public sector.

Critical infrastructure

Critical infrastructure under the BSI Act — operators carry particular duties of proof towards the BSI.

8 Your next step

You have read this guide — that is the first step already. Implementing IT-Grundschutz in a structured way secures tenders in the public sector, meets the duties of proof for critical infrastructure and builds a security organisation that holds up.

A free first conversation

In a 30-minute call, with no obligation, we work out together:

- ✓ How should your information domain be cut?
- ✓ Basic, core or standard protection — which fits your goal?
- ✓ What does an existing ISO 27001 bring you as groundwork?
- ✓ What timeframe and what budget are realistic?

No sales pitch, no pressure — just an honest assessment.

The IT-Grundschutz quick check

On **iso-easy.de** you can test your maturity in 3 minutes and get a first assessment — without leaving any contact details.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.