

— TEMPLATE · TOMORIS TOOLBOX

IT Operations Manual: Template for IT Documentation in Your Company

Outline with tables to fill in for systems, access, procedures, changes, contracts and emergencies, backed by BSI IT-Grundschutz and BSI Standard 200-2

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/it-betriebshandbuch-vorlage

AT A GLANCE

7

Parts, from general information to emergencies

6

Tables to fill in

0

Passwords in the manual, only references to the vault

1+

named deputy per administrative task (BSI)

WHO IT IS FOR

- IT managers and administrators of small and medium-sized companies
- IT service providers who manage and document their customers' IT
- Management that wants to reduce dependence on individual people
- Information security officers who need evidence for audits

WHAT THIS COVERS

If only one person knows how the IT runs, every vacation, every resignation and every outage is a risk. An IT operations manual records which systems exist, who looks after them and who deputizes, which procedures recur, what has been changed and whom to contact. This template provides an outline with tables to fill in. It is based on the BSI modules on proper IT administration, patch and change management, and data backup, the structure analysis according to BSI Standard 200-2 and the business continuity management module.

Adapt this template to your company: systems, roles, procedures and intervals depend on your IT and your protection needs. It is a TOMORIS recommendation based on the BSI sources cited.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	What an IT operations manual is for	2
02	Part 1: General information and responsible persons	3
03	Part 2: System overview	4
04	Part 3: Roles and access	4
05	Part 4: Recurring procedures	5
06	Part 5: Change and administration log	5
07	Part 6: Contracts, suppliers and support channels	6
08	Part 7: Emergency and recovery	6
09	Maintaining the manual	7
10	Sources	8

01

What an IT operations manual is for

What documentation the BSI requires in IT operations and how the manual differs from the emergency manual.

The BSI requires that administrative activities be traceable, meaning it is recorded what was changed, who did it and when (OPS.1.1.2.A5), that a deputy with the necessary knowledge and rights be named for each administrative task (OPS.1.1.2.A2), and that patches and changes be planned, approved and documented (OPS.1.1.3.A1). For data backup, plans must be created for each system covering scope, restoration order, retention and protection (CON.3.A4). The operations manual brings this information together for day-to-day work; the emergency manual under DER.4.A1 contains roles, immediate measures, alerting and recovery plans for emergencies.

Outline of this template and its basis

PART	CONTENT	BASIS
1 General	Scope, responsible persons, deputies, version and storage	OPS.1.1.2.A2, A7
2 System overview	Systems, purpose, location, responsible persons, dependencies, network diagram	BSI Standard 200-2, ch. 8.1
3 Roles and access	Administrative roles, persons, location of credentials	OPS.1.1.2.A21, A23; ORP.4.A8
4 Recurring procedures	Patches, data backup, restore test, users, monitoring	OPS.1.1.3.A15; CON.3.A5, A15
5 Change log	Who changed what, when and for what reason	OPS.1.1.2.A11; OPS.1.1.3.A11
6 Contracts and support	Suppliers, services, support channels, terms	TOMORIS recommendation
7 Emergency	Reference to the emergency manual, recovery, alternative access	DER.4.A1; CON.3.A4; OPS.1.1.2.A27

The modules come from the IT-Grundschrift-Kompodium, Edition 2023. The BSI is replacing the Kompodium with Grundschrift++; according to the milestone plan, the methodology is to be published on October 27, 2026. The documentation and evidence requirements used here remain useful in substance.

02

Part 1: General information and responsible persons

Scope, responsibilities with deputies and information on maintaining the manual.

Master data of the operations manual

FIELD	ENTRY
Company, sites, scope (which IT is included)	_____
Responsible for IT operations (name, role, availability)	_____
Deputy with the necessary knowledge and rights (OPS.1.1.2.A2)	_____
External IT service provider, contact person	_____
Version, approved by [Name, role] on [MM/DD/YYYY]	_____
Next review on [MM/DD/YYYY]	_____
Storage digital [system, path] and offline [location], access for [persons]	_____

03

Part 2: System overview

Which systems, applications and services exist, what they are used for and what they depend on.

Record the components according to the structure analysis in BSI Standard 200-2: business processes and applications, IT systems, rooms and communication networks (ch. 8.1). A network diagram shows at least IT systems such as clients, servers, switches, routers, Wi-Fi access points and network printers, the network connections between them and the external connections, such as internet connections (ch. 8.1.4). Keep it in electronic form and compare it with the actual IT. A detailed inventory can be kept separately; here, what operations needs is sufficient.

Systems, applications and cloud services

SYSTEM AND PURPOSE	LOCATION	RESPONSIBLE, DEPUTY	DEPENDS ON
[e.g. file server: department storage]	[server room]	_____	_____
[e.g. Microsoft 365: email, Teams]	[cloud]	_____	_____
[e.g. firewall and internet connection]	[technical room]	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

04

Part 3: Roles and access

Who administers what, with which role, and where the credentials are stored, without stating them here.

Administrative roles and access

ROLE	SYSTEMS	PERSONS	CREDENTIALS STORED IN
[e.g. server administration]	_____	_____	[vault, entry]
[e.g. Microsoft 365 administration]	_____	_____	[vault, entry]
[e.g. network and firewall]	_____	_____	[vault, entry]
Emergency access	_____	_____	[sealed, location]

- Do not write passwords in this manual. According to the BSI, a password may only be written down for emergency deposit and must then be stored securely; the use of a password manager should be considered (ORP.4.A8).
- Assign roles exclusively for administration, according to actual need and with the least privileges necessary (OPS.1.1.2.A21).

- Each person administers with their own ID; logins with administrative IDs are logged (OPS.1.1.2.A5).
- When a person's administrative task ends, their rights are revoked, personal administrative accounts are disabled and passwords known to them are changed (OPS.1.1.2.A4).

05

Part 4: Recurring procedures

What needs to be done on a recurring basis, how often, by whom and how it is documented.

Recurring tasks in IT operations; frequencies as placeholders

PROCEDURE	FREQUENCY	RESPONSIBLE	EVIDENCE
Assess, prioritize and install patches; justify a decision against a patch (OPS.1.1.3.A15)	[promptly after release]	_____	_____
Data backup according to the backup plan (CON.3.A5)	[daily]	_____	_____
Test restores: data can be restored flawlessly and within a reasonable time (CON.3.A15)	[interval]	_____	_____
Back up configurations, also before far-reaching changes (OPS.1.1.2.A26)	[interval]	_____	_____
Create, change and remove user accounts; review permissions	[on joining, leaving, interval]	_____	_____
Evaluate monitoring and logs	[interval]	_____	_____

06

Part 5: Change and administration log

Every change with date, person, content and reason, as OPS.1.1.2.A11 specifies as the minimum content.

Change log; for tickets, a reference to the ticket number is sufficient

DATE	WHO	WHAT WAS CHANGED	REASON, DEVIATION FROM STANDARD
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

As the minimum content of the documentation, the BSI specifies which changes were made when, by whom and for what reason, and whether and why there was any deviation from specified standards or configurations (OPS.1.1.2.A11). Major changes are planned and approved in advance, with a fallback solution (OPS.1.1.3.A1).

07

Part 6: Contracts, suppliers and support channels

Whom to contact, what has been contractually agreed and when contracts end.

Suppliers and contracts in IT operations

SERVICE	SUPPLIER, CONTRACT	SUPPORT CHANNEL, AVAILABILITY	TERM, TERMINATION
[e.g. internet connection]	_____	_____	_____
[e.g. Microsoft 365 licenses]	_____	_____	_____
[e.g. IT support]	_____	_____	_____
[e.g. firewall, server maintenance]	_____	_____	_____

TOMORIS recommendation: for each contract, record whether a data processing agreement (DPA) under Art. 28 GDPR is in place, and enter notice periods in a calendar. Prices belong in the contract files, not in the manual.

08

Part 7: Emergency and recovery

What the operations manual provides for emergencies and what it refers to.

- ☐ Reference to the emergency manual with roles, immediate measures, alerting and recovery plans (DER.4.A1)
- ☐ Order in which systems and applications are restored, aligned with the backup plans (CON.3.A4)
- ☐ Alternative for central administration tools, such as a jump host or direct access to the systems (OPS.1.1.2.A27)
- ☐ Ensured for each administrative activity that it can also be carried out in an emergency if needed (OPS.1.1.2.A7)
- ☐ Emergency access deposited and stored securely, location noted in Part 3 (ORP.4.A8)

- ☐ Manual accessible even in an emergency, for example as a current printout or on separate storage (cf. DER.4.A1 for the emergency manual)

09 —

Maintaining the manual

So that the manual helps when it is needed; TOMORIS recommendation.

- 1 Update with every change**
 New systems, service providers, roles or procedures are recorded in the manual in the same work step, not later.
- 2 Review regularly**
 Go through it completely at least once a year and after major restructuring; rules for administrative activities should be updated regularly and whenever there is cause (OPS.1.1.2.A7).
- 3 Version and approve**
 Version number, date and approval in Part 1; keep older versions so that changes can be traced.
- 4 Control access**
 The manual contains sensitive information about your IT. Read access only for the people who need it; store the offline copy securely.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

10 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- | | |
|--|--|
| <p>1 BSI IT-Grundschutz-Kompodium, module OPS.1.1.2 Proper IT Administration, Edition 2023
A2, A4, A5, A7, A11, A21, A23, A26, A27
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...</p> | <p>2 BSI IT-Grundschutz-Kompodium, module OPS.1.1.3 Patch and Change Management, Edition 2023
A1, A11, A15
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...</p> |
| <p>3 BSI IT-Grundschutz-Kompodium, module CON.3 Backup Concept, Edition 2023
A4, A5, A15
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...</p> | <p>4 BSI IT-Grundschutz-Kompodium, module ORP.4 Identity and Access Management, Edition 2023
A8 rules for password use
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...</p> |
| <p>5 BSI IT-Grundschutz-Kompodium, module DER.4 Business Continuity Management, Edition 2023
A1 creating an emergency manual
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...</p> | <p>6 BSI Standard 200-2: IT-Grundschutz Methodology
Ch. 8.1 structure analysis, 8.1.4 network diagram survey
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...</p> |
| <p>7 BSI: Grundschutz++, milestone plan (as of October 2026)
Replacement of the Kompodium
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standar...</p> | |