WolfISMS

Wolf's Information Security Management System



User Documentation

Version 4.01

As of: November 2026

© 2012–2026 WolfInfoSec GmbH

Table of contents

1. Introduction....7
1.1 System Requirements....7
1.2 Signing In....7
1.3 Navigating the Menu....8
1.4 Detail Views and Sidebar....9
1.5 Explanations (Tooltips)....9
1.6 The Interface since v4.00....10
2. Module Overview....11
3. User Roles and Permissions....13
3.1 Permissions Overview....13
3.2 Notes on Permissions....14
3.3 Multiple Owners....14
4. Home / Dashboard....15
Description....15
Features....15
Notes....15
5. Controls....16
Description....16
Features....16
6. Legal Register....18
Description....18
Features....18
7. Data Protection....20
Description....20
Record of Processing Activities....20
Threshold Analysis....20
Data Protection Impact Assessment....20
Features....21
Notes....21
8. Risks....22
Description....22
Features....22
AI Assistant for Risks....23

© 2012–2026 WolfInfoSec GmbH

9. Assets....24
Description....24
Features....24
AI Assistant for Assets....25
10. Access Matrix....27
Description....27
Permission Levels....27
Access Methods....27
Features....28
Notes....29
11. Change Management....30
Description....30
Life of a change....30
Features....30
12. Measures....32
Description....32
Features....32
13. Projects....34
Description....34
Features....34
14. Incidents....35
Description....35
Features....35
Reporting Obligations and Deadlines....36
15. Vulnerabilities....38
Description....38
Features....38
16. Audit....40
Description....40
Structure....40
Checklist and Gap Assessment....41
Features....42
Notes....43
17. Management Review....44
Description....44

© 2012–2026 WolfInfoSec GmbH

Structure of a Review 44
Features 44
Notes 45
18. Tasks 46
Description 46
Features 46
Notes 47
Absence and deputy 47
19. Operational Plan (Recurring Tasks) 48
Description 48
Features 48
20. Documents 50
Description 50
Versions and version history 50
Import from Word 51
Features 51
21. BPMN Process Modelling 54
Description 54
Features 54
22. Playbooks 55
Description 55
Features 55
23. Suppliers 57
Description 57
Features 57
Security Questionnaire 58
24. Personnel 60
Description 60
Features 60
Notes 61
Onboarding / Offboarding 61
Training 62
25. Policy Portal 63
Description 63
Features 63

© 2012–2026 WolfInfoSec GmbH

26. Contacts....65
Description....65
Features....65
27. BCM – Business Continuity Management....67
Description....67
Features....67
28. REST API and API Key Management....69
Description....69
API Key Management (/admin/api_keys)....69
Areas and Endpoints....69
29. Objectives....71
Description....71
Features....71
30. External Links....73
Description....73
Features....73
31. Reports....74
Description....74
Overview of the Reports....74
Features....74
Notes....75
32. Administration....76
Description....76
Users and Organisation....76
Catalogues and Master Data....77
System and Operations....77
33. Frequently Asked Questions (FAQ)....79
I cannot see a module – what should I do?....79
I suddenly cannot save anything – why?....79
Can an entry have several owners?....79
Why can I not create another asset, risk, document or supplier?....79
How do I change my password?....79
What does "read only" mean?....79
How do I export data to Excel?....80
How does the document workflow work?....80

© 2012–2026 WolfInfoSec GmbH

How do I get to an earlier version of a document?....80
How do I import a Word document?....80
What is a read confirmation and where do I confirm?....80
What is the access matrix for and how often must I review it?....80
Why is my access matrix empty?....80
Can I import BPMN diagrams from other tools?....81
How are supplier risks calculated?....81
How do I set up two-factor authentication (2FA)?....81
How do I work with the AI assistant for documents?....81
Why can I not upload an attachment?....81
Which AI assistants are there?....81
Which data leaves the system in the process?....81
What does the AI do for assets and gap assessments?....81
Why do the interface colours look different than before?....82
Who receives my tasks while I am away?....82
Where do I enter RTO, RPO and MTPD?....82
Where do I find the reports for the audit?....82
Why does nothing happen when I open an action in a new tab?....82
Why does the sidebar show only five entries?....82
Why does a link also show on the other entry?....82
How do I have a document translated into English?....82
Where have the buttons for linking gone?....83
Why doesn't every field have an ⓘ?....83
My account is locked – what now?....83
How do I switch on dark mode?....83
Where have the tiles above the lists gone?....83
Why can I no longer page through the lists?....83
How do I write a playbook?....83
Why do I not see the module Data Protection?....83
Who maintains the DPA of a supplier?....83
34. Glossary....84

© 2012–2026 WolfInfoSec GmbH

1. Introduction

WolfISMS is a web-based information security management system (ISMS) developed specifically for the needs of small and medium-sized enterprises in regulated environments. It supports the implementation of ISO/IEC 27001:2022, NIS 2, GDPR and industry-specific requirements (aviation, CRA).

The system has a modular design: each module covers a specific ISMS area and is reachable from the side navigation menu, where the modules are grouped by topic (see “Navigating the Menu”). All areas are role-based – users see and edit only what they are authorised for.

1.1 System Requirements

WolfISMS runs entirely in the web browser. No local installation is required.

Requirement	Specification
Browser	Chrome 90+, Firefox 88+, Edge 90+, Safari 14+
Connection	Internal network or VPN (HTTPS)
Sign-in	User name (email) + password, optionally Microsoft or Google SSO
Screen	Recommended: at least 1280 × 800 pixels

1.2 Signing In

Open the system URL in your browser and enter your email address and password. After a successful sign-in you are taken to the dashboard (Home) automatically. For questions about signing in, contact your system administrator.



Changing your password: click your name in the top right corner → "Change password". The new password must meet the minimum requirements (at least 10 characters, upper and lower case letters, a digit).

© 2012–2026 WolfInfoSec GmbH

Forgotten password: The login page carries a “Forgot password” link. You enter your email address and receive a message with a link that lets you set a new password yourself – it is valid for two hours. The page always confirms the dispatch in the same way, whether or not the address is known; that is deliberate, so that accounts cannot be discovered here. If you sign in through Microsoft or Google, your company manages the password – this route will not help then.

Single sign-on: if your organisation has enabled sign-in through Microsoft or Google, an additional button appears on the login page. You then sign in with your company account; a separate WolfISMS password is not required. Only the email domains released by your administrator are accepted.

Signing in through Microsoft directly: if Microsoft sign-in has been set up, WolfISMS forwards you there as soon as you open the page – you no longer see the password form at all. If you do need it once, for example because Microsoft is unreachable or your account does not use single sign-on yet, click "Sign in with email and password (emergency access)" on the login page. After signing out and after a failed sign-in the page stays put so that you can read the message and switch accounts.

Two-factor authentication (2FA): if enabled by the administrator, you are asked for a TOTP code after the password login. The first time, scan the displayed QR code with an authenticator app (e.g. Google Authenticator or Microsoft Authenticator). From your user area (top right → your name) you can set up or disable 2FA at any time.

Blocked accounts:
An account can be disabled by the administrator without deleting it. Signing in is then not possible, neither by password nor via SSO. Contact your administrator in that case.

1.3 Navigating the Menu

Since v3.91 the sidebar arranges the modules in groups that follow the course of an ISMS: from the requirements through the inventory and the risks to day-to-day operations and review. At the very top are the two entries almost everybody needs.

Group	Modules
My Workspace	Policy Portal, Tasks
Governance & Compliance	Controls, SoA, Legal Register, Data Protection, Documents, Objectives
Organisation & Inventory	Assets, Access Matrix, Supplier, Personnel, Process Map, Network Zones
Risk & Treatment	Risks, Measures, Vulnerabilities
Operations & Resilience	Change Management, Contacts, Incidents, Playbooks, BCM
Planning & Review	Projects, Operational Plan, Audit, Management Review, Reports
(no heading)	Links – set apart by a line

- **Collapse and expand**: clicking the heading of a group collapses it or opens it again. Your browser remembers which groups you have collapsed – on another device or in another browser the menu is fully open again
- **Current page**: the menu entry of the page you are on is highlighted. Its group is always open, even if you collapsed it before

© 2012–2026 WolfInfoSec GmbH

- **Only what you can use**: you only see modules you hold a permission for and that your licence includes. A group without such a module is left out together with its heading; users of the policy portal alone see no headings at all
- **Order**: the groups are fixed. Within a group your administrator sets the order of the entries
- **Symbols**: Since v4.00 every module has a small coloured tile with a symbol in front of it; the colour shows the group. The page you are on is highlighted in colour
- **Compact view**: The list button at the top of the sidebar, left of «, moves the entries closer together and shrinks the symbols – handy on small screens. When it is on, the button is blue. Your browser remembers the choice, just like collapsing the sidebar with «

1.4 Detail Views and Sidebar

When you open a single entry – a risk, an asset, a document – the content is on the left and a sidebar on the right. Since v3.94 it has the same structure in every module.

- **At the top:** properties such as status, owner and department, and the metadata – who created and last changed the entry, when, and where applicable reviewer and review date
- **Below:** the links, per area with their number and, if you may change them, the link “Manage”. A line closes every section below its last entry
- **Five entries at most:** if a section has more, “more … (+N)” follows and leads to the same page as “Manage”. Anyone who may not manage sees the complete list
- **Both directions:** a link also shows on the other entry. A change that names an asset therefore also appears on the asset. Such sections have no “Manage” link – the link is changed where it was created – and only appear if there are entries and you may read the other module
- **Action bar:** since v3.95 the bar above the content only holds actions such as edit, review, export and the AI assistants. The buttons for linking – such as controls, processes and documents on the document, risks, incidents and controls on the asset or measures, assets and suppliers on the risk – are gone; you link via “Manage” in the matching section of the sidebar. What the heading already shows is no longer repeated in the table below; owner, responsible persons and department are listed with the metadata. For measures the priority sits in the header next to the status

Detail view	Additionally shown since v3.94
Assets	parent assets, changes, suppliers, vulnerabilities
Risks	changes, vulnerabilities
Incidents	changes, vulnerabilities
Measures	projects, vulnerabilities, BCM exercises
Documents	risks, changes and documents that refer to this one
BPMN processes	list “Linked documents” below the diagram

1.5 Explanations (Tooltips)

Since v3.97 many form fields and column headings carry a small ⓘ. It briefly explains what a field means or does – for example the difference between likelihood before and after measures, what RTO, RPO and MTPD stand for, or which reporting deadlines a tick at GDPR or NIS-2 triggers. Buttons too – such as Review, Propagate O→I, the AI assistants or the symbol buttons – show their explanation directly on the button, without an ⓘ. The entries of the left sidebar also briefly explain what each module is for; in the collapsed sidebar the module name comes first.

© 2012–2026 WolfInfoSec GmbH

- **Mouse:** hover over the ⓘ, or briefly over the button.
- **Keyboard:** tab to the ⓘ; Esc closes the text.
- **Tablet and smartphone:** tap the ⓘ, or press a button and hold – it is not triggered; a tap elsewhere closes the text.

Clicking the ⓘ does not change the form and does not sort a table. The texts appear in the selected language. The administrators can switch tooltips off for everyone.

1.6 The Interface since v4.00

With v4.00 WolfISMS has been given a new, calmer look. The functions are the same; what looks different above all are the module lists, the buttons and the sidebar.

- **Lists:** Every entry is one row – on the left a coloured dot for status or level, next to it number and name, below them the key details, on the right the owner and, where relevant, a coloured marker. A click on the row opens the detail view. Long names are no longer cut off but wrap
- **Search:** The search field above the list filters as you type. Several words narrow it down – each must occur in the entry. The cross in the field clears the search. There is no paging any more: the list shows all entries
- **Filter:** Tiles with numbers above the list – per risk level or phase, for example – filter with one click, a second click removes the filter. Pills such as “Status” or “Category” open a selection menu. Every active filter appears as a chip with ✕; a click on it removes it, “Remove all” resets everything
- **Switch:** Where a module keeps several kinds of entries – BIA, emergency plans and exercises in BCM, or the contact types, for example – you switch via the segments above the list
- **Sort:** on the right of the filter row; a second click on the same sort order reverses the direction
- **Buttons:** The most important button of a page – such as “New” or “Save” – is filled blue, the others are plain grey, delete is red. Less frequent actions such as export or import sit in the three-dot menu next to the main button
- **Heading:** Main and detail views show their title in a white tile
- **Info tiles:** Statistics and category tiles above the lists are hidden at first; your administrator can switch them on for everyone under Design & colours
- **Light and dark:** The button with the moon or sun at the top right next to the language flag switches between light and dark mode. The choice applies to your account on every device; without your own choice your administrator’s default applies. The risk matrix, traffic-light tiles and gauges keep their colours in dark mode too
- **Version:** The footer shows on the right which WolfISMS version is running – helpful for questions to support

© 2012–2026 WolfInfoSec GmbH

2. Module Overview

The system consists of the following modules. Which areas are open to you depends on the permissions assigned to you and on which modules your administrator has enabled under Administration → Modules; their order within the menu groups is set there as well. Some areas depend on the edition of your licence as well: objectives, personnel, contacts, reports, projects, the operational plan, audits, the management review, vulnerabilities, the legal register, playbooks, BCM and the access matrix are part of the Advanced edition and of Enterprise, single sign-on and the REST API are part of the add-on “+”. The AI features are included in every paid edition, Essentials already. Your administrator can tell you which edition your installation uses.

Module	URL / permission	Main functions
Home / Dashboard	/home · all signed-in users	Risk matrix, supplier risk, open incidents, framework compliance, my tasks
Controls	/normen · norm	ISO 27001, NIS 2, BSI IT-Grundschutz: chapter overview, implementation status, linking
SoA	/berichte?berdetail=2 · norm	Statement of Applicability for ISO/IEC 27001 Annex A; only shown when ISO/IEC 27001 is installed
Reports	/berichtsuebersicht · all (cards depending on permission)	All reports and exports in one place, grouped by ISO/IEC 27001
Legal Register	/rechtsregister · norm	Legal requirements, compliance status, topic filters, Excel export
Data Protection	/datenschutz · datenschutz	Record of processing activities (Art. 30 GDPR), threshold analysis, data protection impact assessment, DPA details of the suppliers
Risks	/risiko · risk	Risk register, 5×5 matrix, treatment options, linking to assets/measures
Assets	/assets · assets	IT and information assets, CIA rating, criticality, classification, hierarchy
Access Matrix	/zugriffsmatrix · assets	Target permissions per asset and role, approval, recertification, role catalogue
Change Management	/change · assets	Change requests with implementation, test and rollback plan, approval board, post-implementation review, change calendar
Measures	/massnahmen · mass	Measure tracking, status, progress bars, linking to risks/controls/assets
Projects	/projekte · mass	ISMS frame according to ISO/IEC 27001 A.5.8: profile, sections, roles, security gates, traffic light, progress from measures
Incidents	/incidents · incidents	Incident management, reporting duty GDPR/NIS 2/CRA with deadlines and report templates, root cause analysis, escalation
Vulnerabilities	/schwachstellen · schwachstellen	Vulnerability register with CVSS score and severity, sources, links to assets, incidents, risks and measures
Audit	/audit · audit	Audit planning (internal/external), findings with type, due date and responsible, measures, attachments and links
Management Review	/managementreview · audit	Top management review per ISO 27001 clause 9.3 with live KPIs and risk situation, PDF and PowerPoint export

© 2012–2026 WolfInfoSec GmbH

Module	URL / permission	Main functions
Tasks	/aufgaben · all	My open tasks from all modules, period filter, overdue items
Operational Plan	/op_plan · master (menu) / all (own tasks)	Recurring tasks (deadline calendar) with an automatic evidence chain
Documents	/dokumente · dok	Document management, review/approval workflow, versioning, BPMN, AI assistant
BPMN	/bpmn · dok	Process modelling, editor, import/export of .bpmn files
Playbooks	/playbooks · play	Playbooks according to ISO/IEC 27035: profile, sections, procedure steps, roles, exercises, traffic light, files and links
Suppliers	/vendor · vendor	Supplier register, automatic risk scoring, tier classification, score history
Personnel	/personal · pers	Personnel directory, training document read status, department overview, onboarding/offboarding
Policy Portal	/portal · all signed-in users	Employee portal for policies with read confirmation
Contacts	/kontakte · kontakte	Address book: employees, service providers, authorities, interest groups
Process Map	/prozesslandkarte · prozesslandkarte	Processes as a map: management, core and support processes with owners and process document
Network Zones	/netzwerkzonen · netzwerkzonen	Network segmentation as a map: zones by trust level, VLAN, address range, protection needs
BCM	/bcm · bcm	Business impact analysis per asset, contingency plans, BCM exercises
Objectives	/ziele · ziele	Corporate objectives, information security objectives, KPI tracking with target value and history
External Links	/custom · custom	Central collection of links to external systems (ticketing, KPI system, SharePoint)
Administration	/admin · admin	User management, permissions, activity log, master data, departments
REST API	/api/v1 · admin	Create and query records in six areas via API, API key management (/admin/api_keys)

© 2012–2026 WolfInfoSec GmbH

3. User Roles and Permissions

Every user receives an individual combination of permissions. They are assigned by the administrator at /admin/change_user.

3.1 Permissions Overview

Permission	Code	Description
Administrator	admin	Full access to all areas including user management, master data and the activity log
Read only	readonly	Read access through the policy portal, no editing
Master	master	Extended rights: see all users' tasks, approval workflows, portal reset, create and delete roles
AI usage	ki	Use the AI assistants (yes/no); administrators always may
Assets	assets	Create, edit and export assets – includes the access matrix and change management
Documents	dok	Edit documents and BPMN, take part in the workflow (review/approval)
Measures & projects	mass	Create and edit measures and projects; manage playbook links
Risks	risk	Create, edit and link risks
Suppliers	vendor	Create, edit and export suppliers
Audit	audit	Assess and export audit questions – includes the management review
Controls & legal reg.	norm	Edit, link and export controls and the legal register
Data protection	datenschutz	Read (1) and edit (2) the record of processing activities and DPIAs; also maintains the DPA details of the suppliers
Personnel	pers	View the personnel directory and read status
Playbooks	play	Write playbooks, upload and delete playbook files
Incidents	incidents	Create, edit, link and export incidents
Vulnerabilities	schwachstellen	Read vulnerabilities (1) and create, edit and delete them (2)
Contacts	kontakte	Read contacts (1) and create/edit/delete them (2)
Process Map	prozesslandkarte	Read (1) and edit (2) the process map
Network Zones	netzwerkzonen	Read (1) and edit (2) the network zones
BCM	bcm	Read (1) and edit (2) BIAs, contingency plans and BCM exercises
Objectives	ziele	Read (1) and edit (2) corporate objectives, security objectives and KPIs
External links	custom	Access to the External Links module

© 2012–2026 WolfInfoSec GmbH

3.2 Notes on Permissions

- Most permissions have three levels: 0 = no access, 1 = read, 2 = edit.
- Users without specific permissions can use Home, Tasks and the Policy Portal.
- readonly overrides all other editing permissions – the user cannot change anything.
- master is required for review approvals, the all-tasks view, role maintenance and the reading obligation matrix of the policy portal.
- admin alone is sufficient for all areas – no further permissions are needed.
- **Permissions and roles are two different things**: the permissions above decide what you may see and change. A role – information security officer, data protection officer, head of IT – describes your function instead. It drives the columns of the access matrix and the reading obligation in the policy portal, but grants no permission of its own
- Three modules have no permission of their own: the access matrix and change management use the assets permission, the management review uses the audit permission.
- ki is a yes/no permission and off by default: without it all AI buttons are missing, even if you may edit the module. Administrators do not need it.

If the licence has expired:
All modules remain visible and readable, but saving and editing are disabled – the system then behaves like a read-only account. Administrators and master users keep write access so that a new licence can be installed.

3.3 Multiple Owners

Risks, assets, documents, measures, projects, controls, suppliers, incidents, vulnerabilities and changes can have several owners (called responsible persons for measures and projects). In the form you pick them from a list of check boxes; the search field above filters by name, people already selected are listed first, and the footer counts the selection.

- **Equal rights:** Every owner may change and delete the entry – just as the single owner could before. Master users may always.
- **Main owner:** The owner entered first stays main owner as long as he or she is selected and comes first in sorting and exports; lists and the detail view show all owners, separated by semicolons.
- **No selection:** If you select nobody, you become the owner yourself.
- **Tasks:** Due measures and change dates appear under “My Tasks” and in the reminder email for every owner.

© 2012–2026 WolfInfoSec GmbH

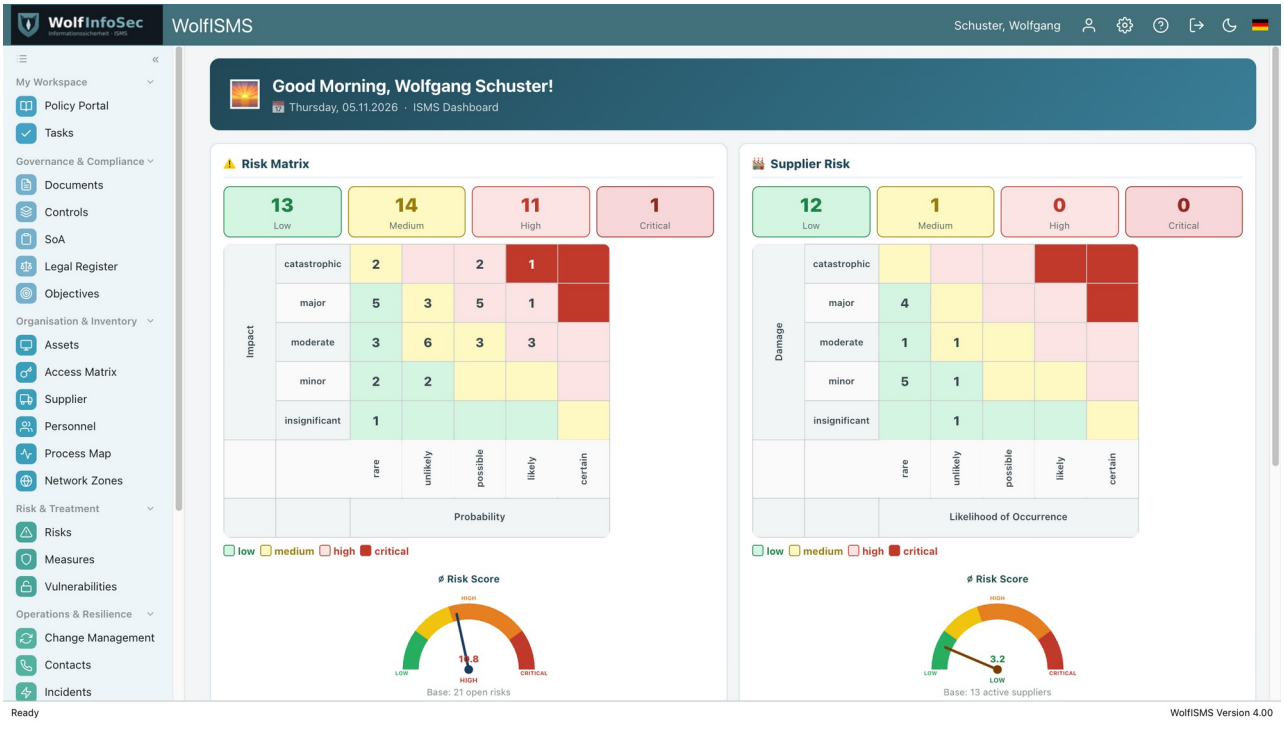
4. Home / Dashboard

Description

The dashboard is the home page after signing in and provides a compact overview of the current state of the ISMS. It shows risk matrices, open incidents, the degree of framework compliance and your own open tasks.

Features

- **Welcome banner**: Personalised greeting by time of day with the current date
- **Risk matrix (ISMS)**: 5×5 matrix of the recorded risks – colour coded (green/yellow/red/dark red). Clicking a cell opens the filtered risk list
- **Risk matrix (suppliers)**: Separate 5×5 matrix of the automatically calculated supplier risk. Clicking opens the filtered supplier list
- **Legend**: Colour key for the risk levels: low / medium / high / critical
- **Open incidents**: List of up to 15 currently open incidents with priority colour marking (critical = red)
- **Framework compliance**: Progress bar per framework (ISO 27001, NIS 2 etc.) with traffic-light colour (≥ 80 % green, ≥ 50 % orange, < 50 % red)
- **My tasks**: All open tasks of the next 7 days from measures and reviews – overdue entries highlighted in red



Notes

The dashboard is read-only – it serves purely as an overview. Clicking an entry takes you to the relevant module.

5. Controls

Description

The Controls module is the heart of the compliance documentation. It records all requirements from ISO/IEC 27001, NIS 2 and BSI IT-Grundschutz, shows their implementation status and allows them to be linked with documents and measures.

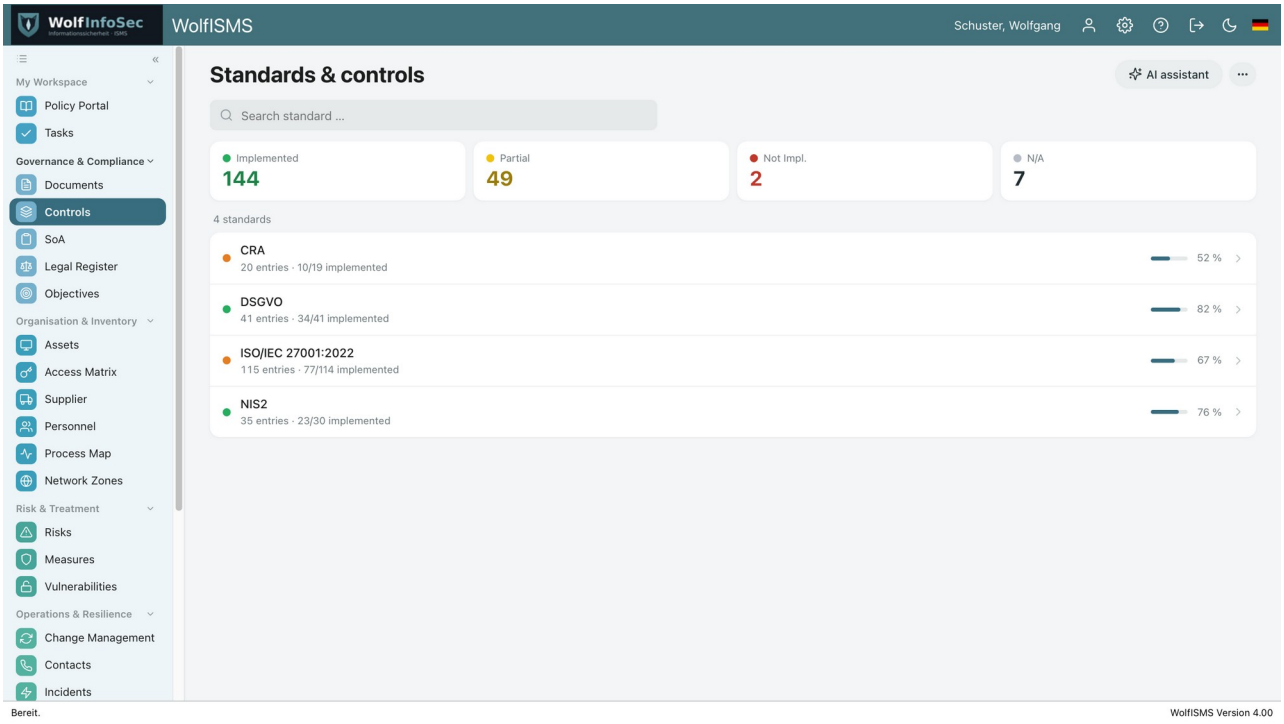
Features

- **Framework tiles**: Overview tiles per framework with a status summary
- **Chapter overview**: Tabular presentation of all chapters with the number of requirements and the degree of implementation
- **Requirement list**: Complete list of all requirements with filters by framework, chapter and status; search filters as you type, there is no paging any more
- **Detail view**: Full requirement details with description, implementation notes, reviewer and change history
- **Implementation status**: Applicability, justification and implementation notes can be maintained per requirement; the compliance level of the framework is derived from them
- **Edit (norm)**: Form editor with rich text for description and implementation notes
- **Delete:** since v3.95 only administrators may delete individual controls – only they see the button, in the chapter list as well as in the detail view. Anyone with write access to controls can still edit them; deleting a whole framework was already reserved for administrators
- **Linking (norm)**: Link individual requirements to documents, measures, risks and assets. Risks and assets are recorded on the other side: the requirement then also appears on the risk respectively the asset
- **Sidebar:** since v3.94 all links of a control – documents, measures, risks and assets – appear with their number and “Manage” in the right-hand sidebar. The tables below the description are gone; you see the status, progress or score of a linked entry after clicking it
- **Statement of Applicability**: since v3.93 a menu entry of its own, “SoA”, in the group Governance & Compliance, right below Controls. It appears as soon as a version of ISO/IEC 27001 is installed and you have read access to Controls. The number in each row leads to the detail view of the control; “File SoA as document” sits to the right of the heading (with the permission to create documents). Controls itself no longer has the button
- **Several versions of ISO/IEC 27001:** If two versions are installed, for example 2022 and 2024, SoA and report show the newest by default; a switch in the heading of the page changes to the other. “Save SoA as document” also takes the version currently shown
- **Conformity report**: Evaluation of the compliance level across all chapters of a framework
- **NIS 2 questionnaire**: Guided self-assessment of NIS 2 applicability
- **Excel export**: Complete export of all requirements including status as Controls.xlsx
- **Charts**: Pie charts: ISO 27001 status, NIS 2 status, overall status
- **Comments**: Discussion thread per requirement; editing and deleting only by the author or an administrator
- **Additional links**: in the detail view you can add your own links to the requirement – an intranet page, a ticket or the document in the DMS. Ordinary web addresses are allowed; unusual link schemes are rejected
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It answers questions (“What do I have to do about patching?”), reviews a control, describes the implementation, checks evidence, checks exclusions for indications, shows gaps, maps controls between frameworks and

© 2012–2026 WolfInfoSec GmbH

transfers the status of related controls. It never suggests an exclusion. Only what you confirm is saved.

- **Related controls:** controls of different frameworks that govern the same topic – for example ISO 27001 A.8.8, BSI OPS.1.1.3 and NIS 2 Art. 21(2)(e) – can be linked with each other. The link applies in both directions and appears in the detail view, in the link view and in the coverage per framework



6. Legal Register

Description

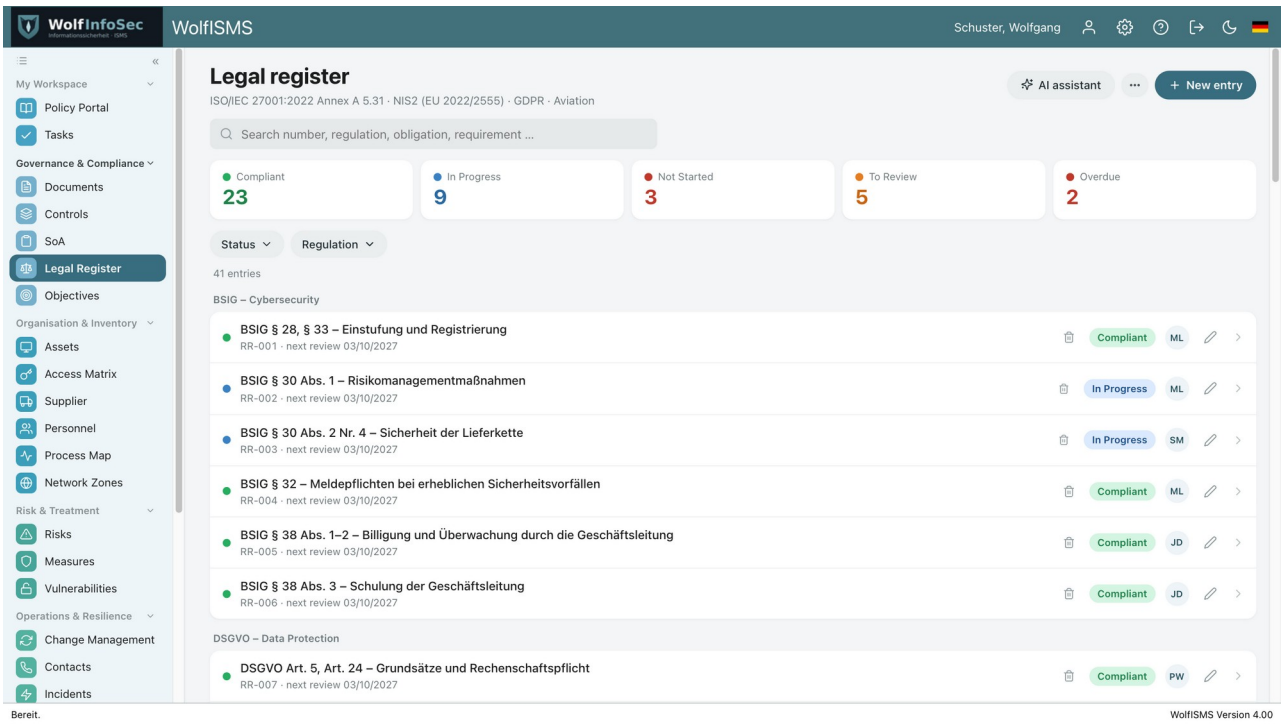
The legal register records all legal and regulatory requirements relevant to the organisation (ISO/IEC 27001 A.5.31, NIS 2, GDPR). It is pre-populated with 48 entries from EU and German law.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

Features

- **Overview**: Filtered list of all legal bases with search by topic, short code and status
- **Detail view**: since v4.00 a fixed set of ten fields – number, legal basis (short code, reference, title), category, requirement, applicability, implementation with linked measures, documents and controls, responsible, status, open items with deadline, and last and next review. Older entries were taken over into these fields once at the first start
- **New / Edit (norm)**: recording and maintenance with the status To review, Open, In progress, Compliant or Not applicable
- **Topic tiles**: Quick filter by topic (e.g. data protection, information security, aviation)
- **Status chart**: Pie chart of the compliance status distribution
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It answers questions, creates entries, finds missing legal bases, reviews entries, describes the implementation, checks evidence, goes through due reviews, looks for legal changes and writes a status report. Expressly no legal advice: new entries are always set to “To review”, and the AI never suggests “Not applicable” or “Compliant”. It only searches the internet if your administrator has set a model with web search. Only what you confirm is saved.
- **Excel export**: Export of all entries as .xlsx

© 2012–2026 WolfInfoSec GmbH



© 2012–2026 WolfInfoSec GmbH

7. Data Protection

Description

Since v4.01 the module Data Protection keeps the record of processing activities under Art. 30 GDPR, checks per processing activity whether a data protection impact assessment (DPIA) is needed, and holds the DPIA itself. You find it in the menu under Governance & Compliance. Processing activities are linked to assets, controls, measures and suppliers – so you can see which systems process which personal data and which measures protect them.

Availability: in every edition, including the free one. User permission: datenschutz (0 = no access, 1 = read, 2 = edit), off by default – also for users who existed before the update. Your administrator grants it; administrators themselves do not need it. URL: /datenschutz

Record of Processing Activities

- **As controller (Art. 30(1)):** title, description, purpose, legal bases (Art. 6 and Art. 9 to choose from, with a justification for legitimate interests), data subjects and data categories (suggestion lists, own values possible), retention period with trigger, joint controllership and responsible department
- **As processor (Art. 30(2)):** per client from the customer contacts, with the categories of processing, date and document of the DPA – without purpose, legal basis and retention period, which the client sets
- **Recipients:** internal (department), supplier, authority or other, each with a country. If the country lies outside the EU and the EEA, it is a third country; then you choose the safeguard – adequacy decision, Data Privacy Framework, standard contractual clauses, BCR or a derogation under Art. 49. A third country without a safeguard is flagged
- **Links:** assets, controls, measures and sub-processors
- **Status:** draft → under review → approved. A processing activity as controller can only be approved with purpose, legal basis and a threshold analysis with result and justification, as processor only with a client. Without a review date, approval sets it to today + 12 months
- **Art. 9 hint:** if you choose health, biometric or other special data without stating a legal basis from Art. 9, the page points that out

Threshold Analysis

For each processing activity as controller you answer two questions: does it fall under the list of the supervisory authorities under Art. 35(4) (preset with the list of the German DSK, extendable by your administrator)? And which of the nine criteria of the WP 248 guidelines apply – for example sensitive data, vulnerable data subjects, large scale, systematic monitoring or scoring? WolfISMS suggests a result: if an entry of the list applies or two or more criteria are met, a DPIA is usually required. You set the result and justify it; if it differs from the suggestion, the page says so.

Data Protection Impact Assessment

If a DPIA is needed, you create it from the detail view of the processing activity. Section 1 is preset from the processing activity. The DPIA is listed in the module under the tab “DPIA”.

- **Fixed sections under Art. 35(7):** systematic description, necessity and proportionality, risks to rights and freedoms, measures to address the risks, opinion of the data protection officer, views of the data subjects and result – residual risk acceptable or prior consultation of the supervisory authority under Art. 36

© 2012–2026 WolfInfoSec GmbH

- **Risk table:** per risk the source, the possible damage to the data subjects, likelihood and severity (1 negligible to 4 maximum each) before and after the measures. The value is the product and is always calculated. The residual risk only counts measures that are implemented – otherwise the page points that out
- **Status:** draft → in progress → DPO opinion → completed. It can only be completed with the opinion, a result and residual values for every risk
- **Review:** if the processing activity changes after completion, the DPIA shows that it has to be reviewed (Art. 35(11))
- **To the risk register:** you transfer a DPIA risk with one click via the AI assistant for risks; afterwards it points to the entry in the risk register. The AI assistant for measures creates and links mitigating measures

Features

- **List:** three tabs – as controller, as processor, DPIA – with search and status; “Create” to fold out
- **New / edit (datenschutz):** create and maintain processing activities and DPIAs; owners and master users may change and delete
- **Excel export:** per record as .xlsx, for example for the supervisory authority
- **DPA details of the suppliers:** see chapter Suppliers
- **AI assistant (Essentials and above):** If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It creates a processing activity from your description (also as processor), finds assets with personal data that have no processing activity yet, reviews an entry for gaps and contradictions, suggests the threshold analysis, drafts a DPIA and creates the annex on technical and organisational measures (Art. 32) as a Word file for DPAs. Only what you confirm is saved.

Notes

WolfISMS and its AI assistant give no legal advice. Legal basis, retention period and the result of the threshold analysis are suggestions; approving, completing a DPIA and writing the opinion of the data protection officer are done by people.

© 2012–2026 WolfInfoSec GmbH

8. Risks

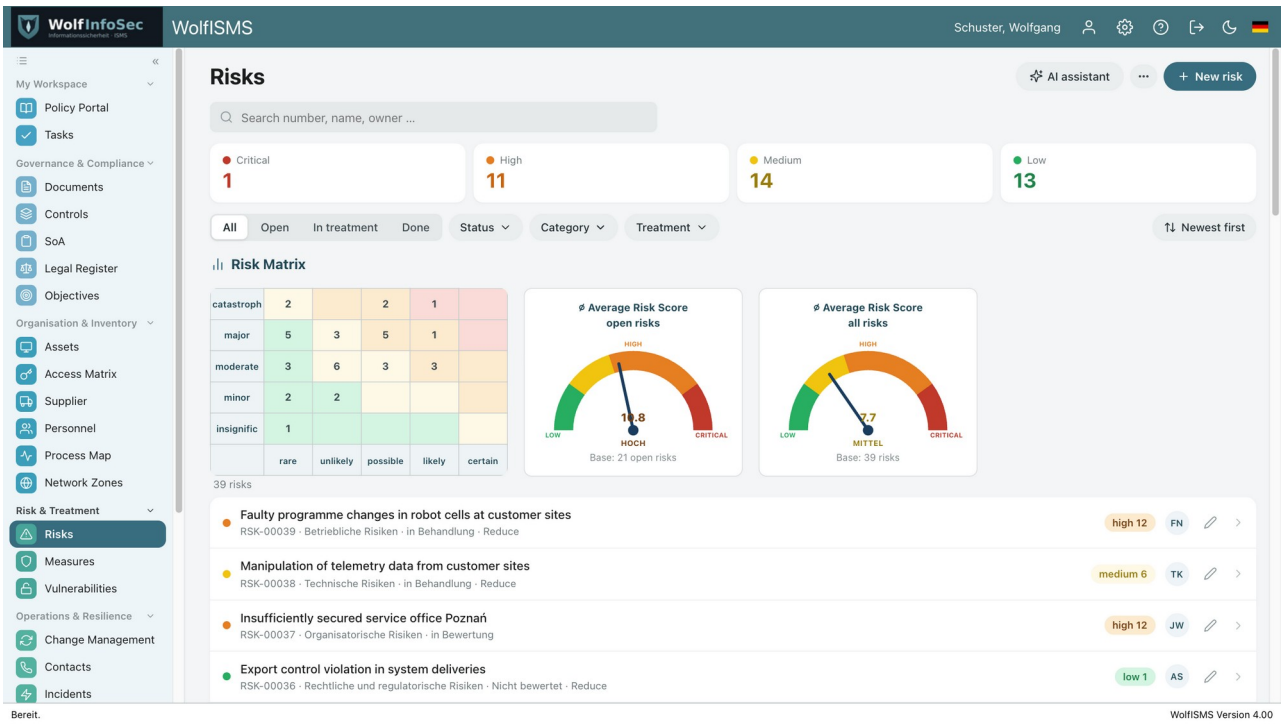
Description

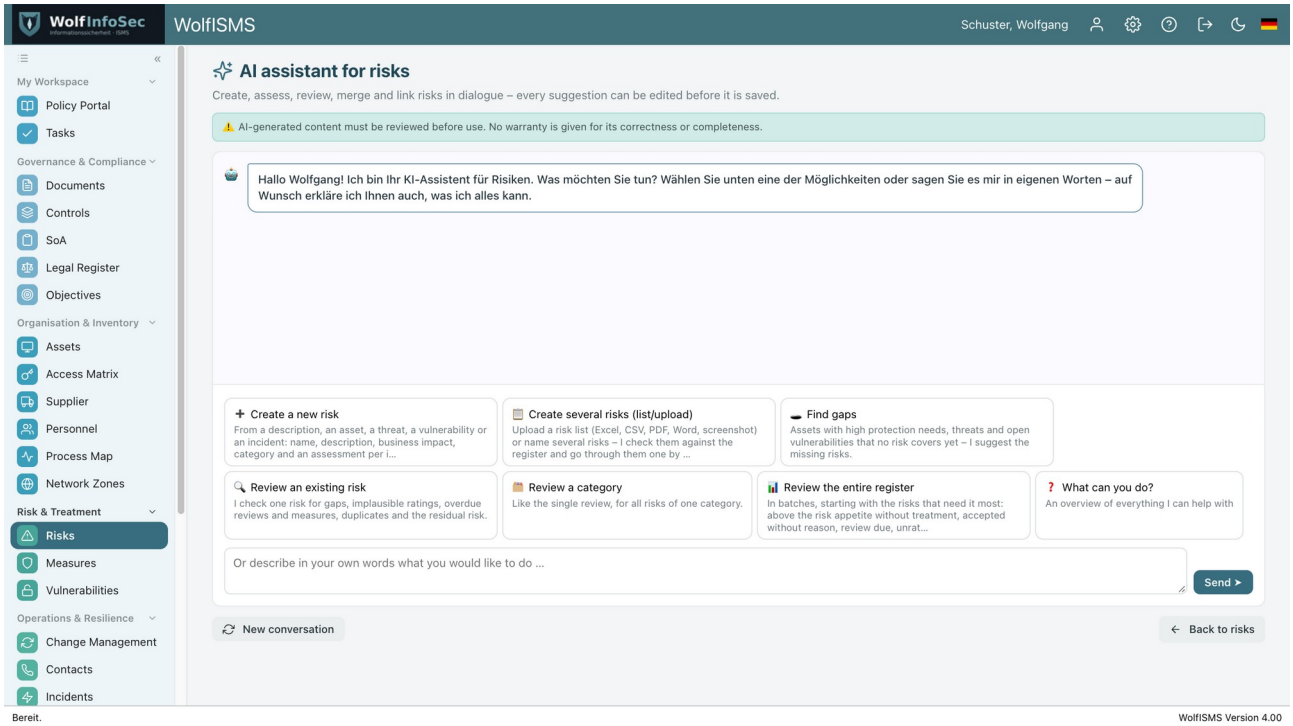
The risk module supports the complete risk management process per ISO 27001 clause 6.1. Risks are assessed, treatment options are defined, and links to assets, measures, threats and vulnerabilities are maintained.

Features

- **Risk overview**: List with search, tiles per risk level (one click filters) and filters by phase, status, category and treatment; the risk matrix can be shown or hidden via the three-dot menu
- **Risk assessment**: Likelihood and impact both before and after measures (5-point scale)
- **Risk levels**: Automatic calculation: low / medium / high / critical
- **Risk treatment**: Options: accept, reduce, avoid, transfer, share
- **Links (risk)**: Linking to assets, measures, threats and vulnerabilities
- **Business impact**: Free-text field describing the business consequences (rich text)
- **Opportunities**: the positive counterpart of the risk – what there is to gain from tackling it (ISO 27001 clause 6.1.1). The field sits below the business impact in the form, appears in the detail view and in the PDF of the risk management review, and is passed to the AI assistant whenever it is filled in
- **Risk management review**: Compilation of the open critical and high risks as input for the top management review – the same evaluation appears in the Management Review module. “PDF export” turns it into a finished document for the meeting; if PDF letterhead is stored, it is used as header and footer. Detail texts and measures can be shown or hidden beforehand
- **Risk score trend**: At /risiko/historie a line chart shows the development of three average scores over time: ⌀ open risks, ⌀ all risks and ⌀ active suppliers. Period selectable (30 days, 90 days, 6 months, 1 year, all). A snapshot is created automatically every day and can also be triggered manually
- **Excel export**: Export of the entire risk register as .xlsx
- **Category chart**: Pie chart of the risk distribution by category
- **Comments**: Discussion thread in the sidebar of every risk; every signed-in user (except readonly) can comment and reply
- **Detail view:** number and name are in the heading. Since v3.94 the sidebar shows from top to bottom the properties (category, owner, department, status, risk treatment), the metadata, the assessment before and after measures and the links. The main area starts with description, business impact and opportunities
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation in which the AI creates, reviews and links risks with you – see the section AI Assistant for Risks

© 2012–2026 WolfInfoSec GmbH





AI Assistant for Risks

The AI assistant is a conversation on a page of its own: the chat on the left, the answer options below it, on the right the draft, which you can change yourself at any time. The AI greets you, asks what you have in mind and explains on request what it can do. You need edit access to risks for it.

- **Create a new risk:** from a short description or starting from an asset, a threat, a vulnerability or an incident. The AI drafts name, description, business impact, opportunities, category and rating; then

it suggests links to threats, vulnerabilities, measures, suppliers, controls, documents and incidents. Missing measures and suppliers are created along the way if you wish
- **Create several risks:** upload a risk list (Excel, CSV, PDF, Word, screenshot) or name them in the chat; the assistant checks them against the register and goes through them one by one
- **Find gaps:** assets with high protection needs, threats and open vulnerabilities that no risk covers yet – the assistant suggests the missing risks
- **Review:** a single risk, all risks of a category or the entire register – for gaps, implausible ratings, overdue reviews and measures, duplicates and the residual risk. For the entire register it starts with the risks that need it most
- **Nothing without your yes:** every suggestion comes with a reason; you tick, give a hint in free text or skip. Only “Apply” writes. If you left the page, you can carry on at the next visit

9. Assets

Description

The asset module manages all information-processing assets of the organisation. It supports classification by confidentiality, integrity and availability (CIA) as well as criticality assessment. Categories follow the OBASHI scheme (Ownership, Business Process, Application, System, Hardware, Infrastructure) and are displayed in that order; information assets come last.

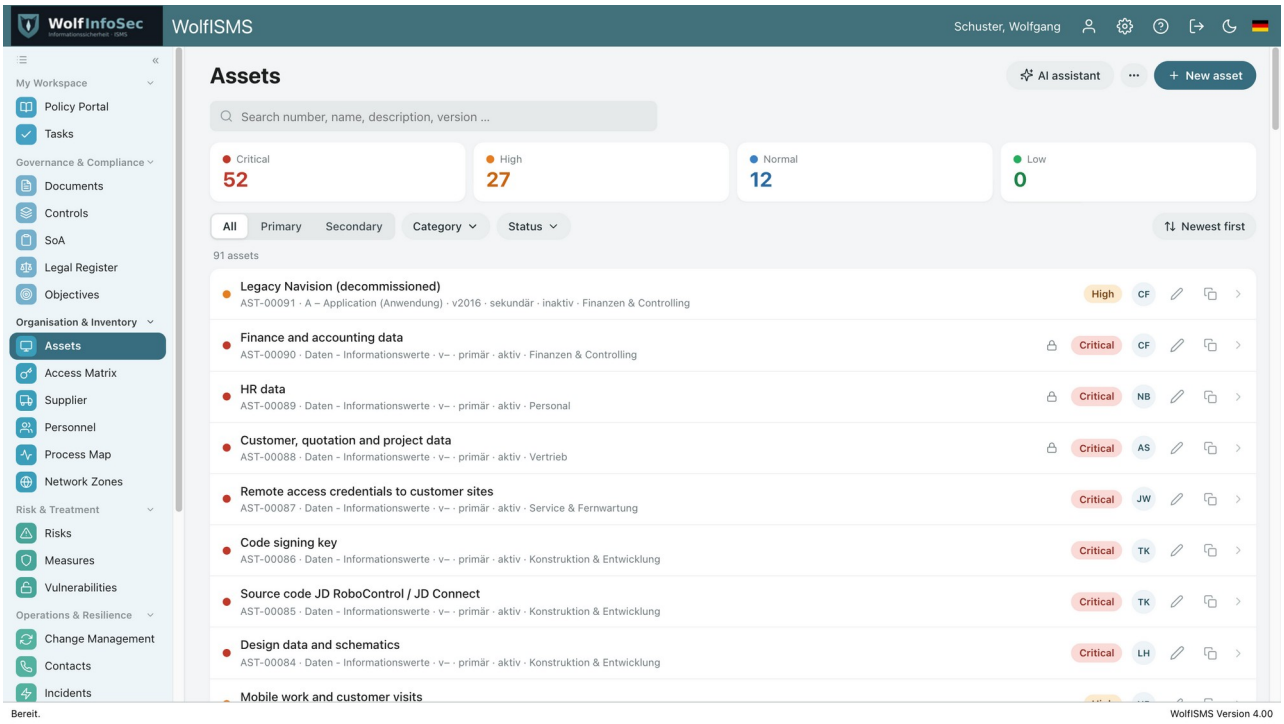
Features

- **Asset overview**: List with search and filters by type, category, department and status; the category tiles appear when your administrator has switched on the info tiles
- **Version**: Free-text field for the release or patch level of an asset (for example "2024 R2" or "15.0.4355"). It sits between name and description, forms its own column in the asset list and the Excel export and can be found through the search and sorted through the column heading. The linking lists show the version as well: the child assets in the asset module and "Link assets" in risks, suppliers, incidents and vulnerabilities.
- **CIA rating**: Classification by confidentiality, integrity, availability and authenticity (CIAA, each 1–5)
- **Remarks on the protection needs:** since v3.95 each of the four protection goals has a field of its own “Remark – why this level?”. The detail view shows the remark in small print below the level in the matching CIA card. If the AI assistant suggests the protection needs, it writes its justification there when applied, and when a protection goal is inherited, the remark notes from which parent asset and when (e.g. “Inherited from parent asset AST00012 (high) on 2026-10-17.”). Copying an asset takes the remarks along
- **Classification**: Public / Internal / Confidential / Strictly confidential
- **Criticality**: Assessment of the business criticality of the asset
- **Personal data**: Marking whether the asset processes personal data (GDPR-relevant)
- **Sub-assets and hierarchy**: Hierarchical linking of sub-assets (e.g. server → applications); the overview shows the parent/child structure indented
- **Add child asset:** since v3.95 the button in the detail view and in the tree view creates a new asset that is linked as a child asset after saving. The form is prefilled: type “secondary”, as category the next OBASHI level below the parent asset, and the protection needs of the parent asset with the inheritance note in the remarks. Coming from the tree view you return there after saving
- **CIA inheritance**: CIA values can be taken over from freely selectable source assets (button "Adopt CIA from sources") – the higher value always wins. Values can also be propagated to sub-assets (button "Inherit", OBASHI top-down principle); existing higher classifications are preserved
- **Criticality formula**: Automatic calculation by the maximum principle (BSI Standard 200-2): the criticality is the highest level of confidentiality, integrity, availability, authenticity and value. A single

© 2012–2026 WolfInfoSec GmbH

high protection goal is thus not diluted by low other values – the same rule by which inheritance passes on the protection needs. The criticality cannot be set by hand

- **Department assignment**: The department is selected from the centrally maintained department and team list instead of being typed freely
- **Review date**: Planned review date with automatic task creation
- **Recovery objectives**: RTO, RPO and MTPD for business continuity, chosen from fixed steps from 1 hour to 30 days (RPO also 0 – no data loss). The RTO must not exceed the MTPD. The values appear in the detail view, in the Excel export and import and in the BIA of the BCM module
- **Excel export**: Complete asset export as .xlsx
- **Excel import**: An exported workbook can be read back in unchanged (/assets/import). The key is the asset number in column A: a known number updates the asset, an unknown or empty one creates a new asset on request. Empty cells change nothing, a value outside the corresponding selection list is reported and the row is skipped – nothing is guessed. Without the "Apply" checkbox it stays a preview. The criticality is calculated from CIAA and value (maximum principle) and is therefore not read in, and only what you would be allowed to change in the form is changed
- **Comments**: Discussion thread in the sidebar of every asset for questions and coordination
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation in which the AI creates and reviews assets with you, suggests the protection needs and finds links right through to the risks – see the section AI Assistant for Assets. The former buttons “AI risk analysis” and “AI protection needs” have been merged into it



AI Assistant for Assets

Built like the AI assistant for risks: a conversation on a page of its own, the chat on the left, the editable draft on the right. You need edit access to assets; anything created in other modules along the way, such as a supplier or a risk, requires the permission there too.

- **Create a new asset:** from a short description the AI suggests name, description, OBASHI category, type, version, classification, protection needs and recovery targets, each with a reason. Links

follow – subordinate assets, suppliers, risks, vulnerabilities, controls and incidents. Missing suppliers are created along the way if you wish

- **Create several assets:** upload an asset list (Excel, CSV, PDF, Word, screenshot) or name them in the chat; the assistant asks for owner and department once for all of them
- **Review:** a single asset, all assets of an OBASHI level or the entire inventory – for gaps and implausible values, with suggestions for additions and links. For the entire inventory it starts with the assets without links, protection needs, owner or recovery targets
- **Protection needs:** the suggested level per protection goal appears with a reason in the draft; when applied, the reason becomes the remark of the protection goal
- **Nothing without your yes:** only “Apply” writes; you can also skip any area of the links

© 2012–2026 WolfInfoSec GmbH

10. Access Matrix

Description

The access matrix documents which role may access which asset. It is the target specification for granting permissions and the evidence for ISO/IEC 27001 A.5.15 (access control) and A.5.18 (access rights including recertification). Category and protection requirement of the assets are read live from asset management – the matrix therefore cannot diverge from the asset inventory.

Availability: The access matrix belongs to the Advanced (ADV) and Enterprise (ENT) editions. In the others the menu entry is missing; roles can still be maintained there under Administration → Roles. If the module is missing from the menu, the administrator has switched it off under Administration → Modules – the recorded data is preserved and is there unchanged once the module is switched on again.

Permission Levels

The underlying principle is deny by default: without an explicit decision, “no access” applies. Any deviation must be justified and approved.

Code	Level	Meaning
n	No access (none)	Default. Every deviation must be justified and approved
r	Read	Read access to data and configuration, no modification possible
rw	Read/write	Create and change own or functionally assigned records (incl. r)
f	Full functional access	Additionally delete, release, master data maintenance, bulk export (incl. rw)
a	Administrative / privileged (admin)	Technical system administration, rights assignment, bypassing of functional controls. Only via a separate admin account with MFA
e	Emergency access (break-glass)	Inactive, sealed account. Activation only under a documented emergency procedure, review within 24 h

The codes changed after version 3.51.
Up to and including 3.51 the levels were –, L, S, V, A and N. The new codes are the English abbreviations and are identical in both language versions, so that an export can be read regardless of the exporter’s language. WolfISMS converts the existing data once by itself, and an older Excel workbook can still be imported unchanged – the old abbreviations are recognised on import. Mind the case: “N” was emergency access, “n” today means “no access”.

Access Methods

For each asset it is also recorded how access is authenticated. This is the evidence for ISO/IEC 27001 A.5.17 (authentication information) and A.8.5 (secure authentication).

Method	Meaning
Login	Sign-in with user name and password in the system itself

© 2012–2026 WolfInfoSec GmbH

Method	Meaning
SSO	Sign-in through the central identity provider
MFA	Additional second factor
Certificate	Client certificate

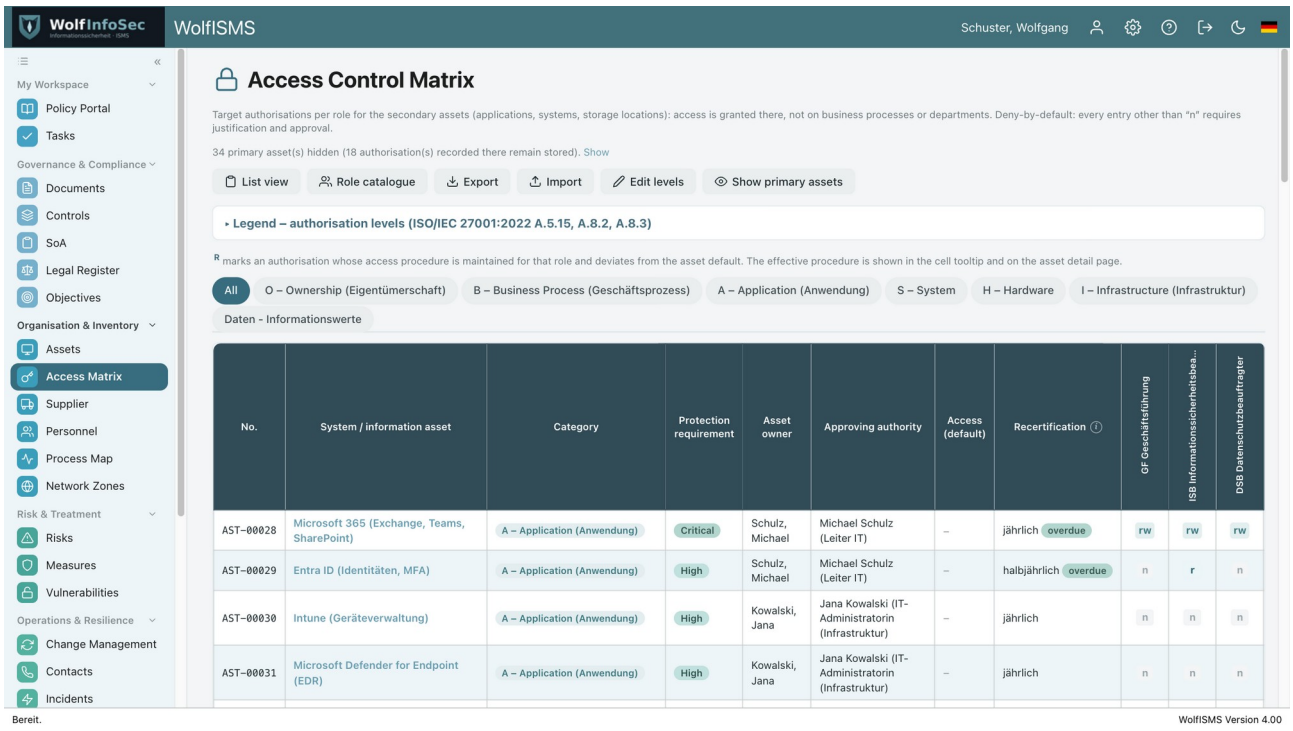
Selecting several is explicitly intended: in practice MFA and certificates come in addition to login or SSO, not instead of them. The asset carries the default that applies to all roles; individual roles may deviate – for example when MFA is required for administrative access but not for read access.

Features

- **Cross table**: Matrix asset × role with category tabs. Levels can be changed directly in the table and saved together. Since v3.99 it only shows secondary assets – applications, systems, storage locations – on which permissions are granted technically; the switch “Show primary assets” adds business processes and information assets. Existing entries for primary assets are kept
- **Per-asset detail**: For each permission the level, approver, approval date, last and next review as well as a functional justification (need-to-know) are recorded
- **Defaults per asset**: the asset carries the approving authority, the intended access method, the recertification frequency and the conditions or compensating controls. They apply to all roles as long as a role has nothing of its own recorded
- **Recertification**: Selectable frequency: quarterly, semi-annually or annually. Due and overdue reviews are highlighted in colour
- **Privileged rights**: Levels a and e count as privileged and are reported separately in lists and key figures
- **List view**: Filterable list of all permissions by role, level, privileged and recertification status – the fastest view for a review
- **Role catalogue**: Maintenance of roles with short code, organisational unit, "privileged" flag, active status, sort order and description; plus the number of privileged permissions a role holds
- **Excel export**: Export in five sheets: instructions & legend, role catalogue, access matrix, permissions and ISO 27001 mapping
- **Excel import**: Import of a completed workbook with a preview: before saving you see what will be applied and what will be skipped

Permission: assets (0 = no access, 1 = read, 2 = edit) – URL: /zugriffsmatrix

© 2012–2026 WolfInfoSec GmbH



Notes

Creating and deleting roles:
The catalogue fields of a role may be maintained by any user with editing rights on assets. The role name itself, as well as creating and deleting roles, is reserved for master and admin users, because roles are used company-wide in user management and the personnel module as well. A role that is still assigned somewhere cannot be deleted – it can be set to "not active" instead. The same role list is available under Administration → Roles; that is also where roles are assigned to user accounts.

Importing from a foreign workbook:
Mapping on import uses the role name, not the short code. In a foreign file "R01" may stand for a completely different role than in your own catalogue. Rows and columns that cannot be mapped are reported and skipped rather than mapped incorrectly.

© 2012–2026 WolfInfoSec GmbH

11. Change Management

Description

Change management controls changes to systems, applications and configurations before they happen: whoever wants to change something files a change request with a justification, a time window and the plans for implementation, testing and rollback. A board approves it, then it is implemented and finally reviewed. This produces the evidence ISO/IEC 27001 A.8.32 (change management) requires.

The module uses the assets permission: whoever may read assets sees the changes, whoever may edit assets creates and runs them. Whoever is named as an approver votes even with read permission only.

Life of a change

- **1. Draft**: title, description and justification, type, category, priority, risk and impact of the change, planned window with expected downtime, implementer and the implementation, test and rollback plan. Every change receives a number in the format CHG-00001.
- **2. Name the board**: under “Approval board” you enter the approvers, each with a role and a stage (1 to 3). A higher stage only votes once everybody on the stage below has approved.
- **3. Submit**: from now on the approvers vote. As soon as all have approved, the change is approved; a single rejection rejects it. A rejected or withdrawn change can be revised – voting then starts again.
- **4. Implement**: “Start implementation”, then “Implementation done”. If something goes wrong, “Roll back” carries out the rollback plan.
- **5. Post-implementation review**: after implementation or rollback, record within 14 days how it went – date, result and a remark. Only then can the change be closed.

Type	Meaning
Standard	Pre-approved routine change – needs no board and is approved on submission
Normal	Ordinary change approved by the board
Major	Larger change approved by the board
Emergency	May be implemented immediately; the board votes retroactively

Features

- **List**: all changes with key figures, filters by status, type, category and risk, and full-text search.
- **Detail view**: master data, the three plans, the approval board with the state of every vote, the buttons for the next possible step and the history of all status changes.
- **Links**: assets, risks, measures, incidents and documents can be linked to a change.
- **Change calendar**: all changes with a planned start in a monthly overview – overlaps become visible.
- **Tasks**: the planned window, a pending vote on the board and a due post-implementation review appear under “My Tasks” and in the reminder email.
- **Edit and delete**: by one of the owners or a master user. The status only changes through the steps, not through the form.

© 2012–2026 WolfInfoSec GmbH

- **Excel export**: button “Excel” in the filter bar, takes over the filters. The sheet “Key figures” shows per type the open, closed, rejected and rolled-back changes as well as the completed, overdue and successful post-implementation reviews; the sheet “Changes” all dates, the approval board with stage, role and vote, and the review. Overdue reviews are marked red
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It drafts and reviews changes (free or starting from a measure, vulnerability, incident or risk), accompanies a status step, suggests the board, prepares the post-implementation review, goes through your open changes, finds collisions in the change calendar and writes a status report. The assistant never votes. Only what you confirm is saved.

Permission: assets (0 = no access, 1 = read, 2 = edit) – URL: /change

© 2012–2026 WolfInfoSec GmbH

12. Measures

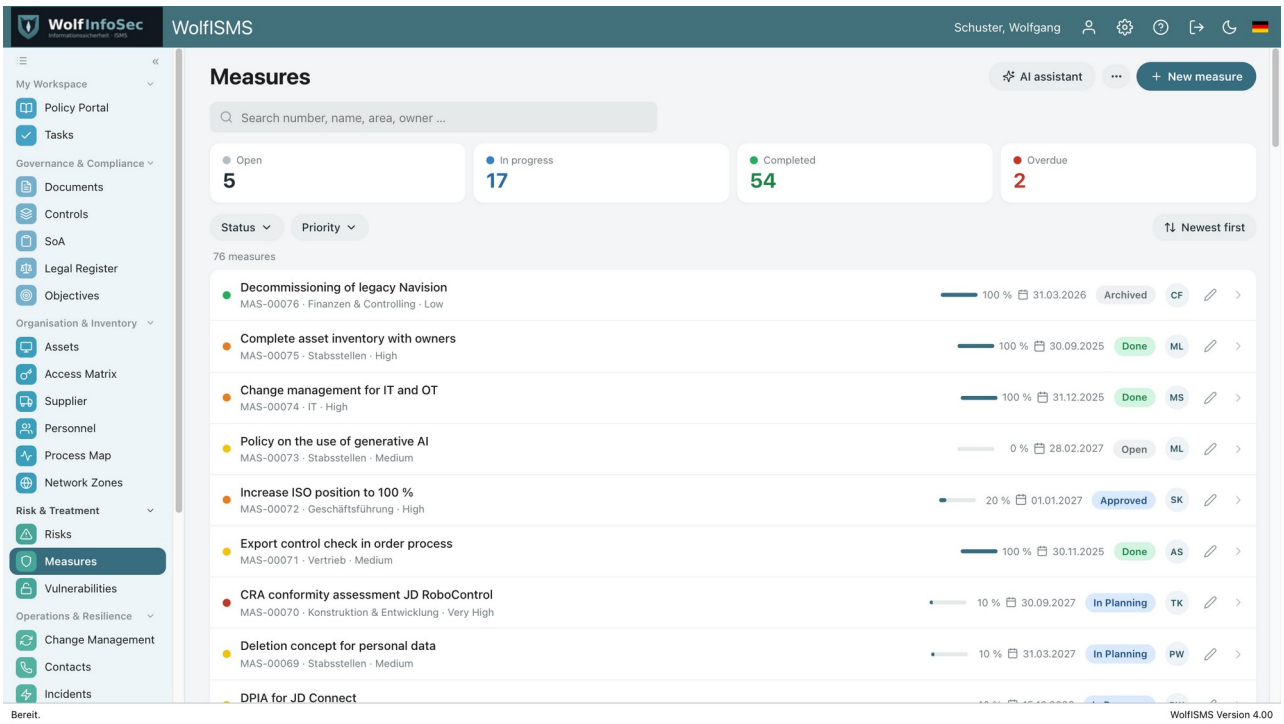
Description

The measures module tracks all security and compliance measures. It connects controls, risks, suppliers and incidents with concrete implementation tasks.

Features

- **Status tabs**: Quick filter: all / open / in progress / done / cancelled
- **Progress bars**: Percentage of implementation with a traffic-light colour per measure
- **Detail view**: Full measure description, owner, department, end date, rich-text content
- **Attachments**: Upload and management of attachments (documents, evidence) in PDF format
- **Links (mass)**: Linking to risks, controls, suppliers, incidents and assets – an asset shows its measures directly and via risks, vulnerabilities, changes and incidents
- **Management reviews**: A measure that results from a management review shows in its detail view which reviews it belongs to. This is visible to users with the audit permission – that is where the management review lives. Since v3.71 "Manage links" also sets and removes the assignment from the measure side; that requires the audit editing permission
- **Review**: Planned review date with automatic task creation
- **Excel export**: Full export or filtered by status as .xlsx
- **Status chart**: Pie chart of the measures by status
- **Ticket number**: if a measure carries a ticket number – usually set by the connected ticket system through the REST API – it appears in the list and in the detail view as a link and opens the ticket in a new tab. Only the link target and the label are taken over; foreign markup is not passed through
- **Comments**: Discussion thread per measure
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It creates measures – free or from a risk, control, finding, incident, vulnerability, supplier or the legal register, several from a report or measure plan, too –, finds what has no measure yet, reviews, merges, asks for the status of your due measures in the status round, proves implementation with evidence and suggests an order of implementation. Only what you confirm is saved.

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
My Workspace
Policy Portal
Tasks
Governance & Compliance
Documents
Controls
SoA
Legal Register
Objectives
Organisation & Inventory
Assets
Access Matrix
Supplier
Personnel
Process Map
Network Zones
Risk & Treatment
Risks
Measures
Vulnerabilities
Operations & Resilience
Change Management
Contacts
Incidents
Measures
AI assistant
New measure
Search number, name, area, owner ...
Open 5
In progress 17
Completed 54
Overdue 2
Status
Priority
Newest first
76 measures
Decommissioning of legacy Navision
MAS-00076 · Finanzen & Controlling · Low
100 % 31.03.2026 Archived CF
Complete asset inventory with owners
MAS-00075 · Stabsstellen · High
100 % 30.09.2025 Done ML
Change management for IT and OT
MAS-00074 · IT · High
100 % 31.12.2025 Done MS
Policy on the use of generative AI
MAS-00073 · Stabsstellen · Medium
0 % 28.02.2027 Open ML
Increase ISO position to 100 %
MAS-00072 · Geschäftsführung · High
20 % 01.01.2027 Approved SK
Export control check in order process
MAS-00071 · Vertrieb · Medium
100 % 30.11.2025 Done AS
CRA conformity assessment JD RoboControl
MAS-00070 · Konstruktion & Entwicklung · Very High
10 % 30.09.2027 In Planning TK
Deletion concept for personal data
MAS-00069 · Stabsstellen · Medium
10 % 31.03.2027 In Planning PW
DPIA for JD Connect
Bereit.
WolfISMS Version 4.00

13. Projects

Description

The project module runs projects under the ISMS frame of ISO/IEC 27001 A.5.8 “Information security in project management”: every project names classification and security responsibility, describes security requirements and risks, passes security gates and ends with an orderly hand-over including lessons learned. Progress is calculated from the linked measures.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

Features

- **Project overview:** list of all projects with progress, ISMS traffic light, owner and status; tiles per phase filter with one click, search as you type
- **Profile:** client, security responsibility and the highest classification of the information in the project, plus owner, status and period
- **Fixed sections:** goal and benefit, scope and boundaries, classification and storage, security requirements for the result, risk assessment at project start, result and status, hand-over to operations, lessons learned, residual risk after the project – each with a hint on what belongs there according to ISO/IEC 27001 A.5.8
- **Project roles:** role and person – a user or, for externals, a name. Client, project lead and security responsibility are suggested
- **Phases and security gates:** gates set freely per project with date, criterion, status (open, passed, passed with condition, failed), condition and evidence. G0 initiation, G1 requirements & risk, G2 test & approval and G3 hand-over & closure are ready as a suggestion
- **ISMS traffic light:** the sidebar shows what is still missing in the current phase – green, amber or red. It is a hint, not a lock
- **Links (mass):** measures – the progress is their average (0–100 %) –, plus risks, assets, documents (requirements) and suppliers
- **Excel export:** project list with progress figures as .xlsx
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It creates a project from an idea or an uploaded project order, runs the ISMS check, derives security requirements, assesses the risks, accompanies a gate review and the closure and goes through your projects that need action. Only what you confirm is saved.

© 2012–2026 WolfInfoSec GmbH

14. Incidents

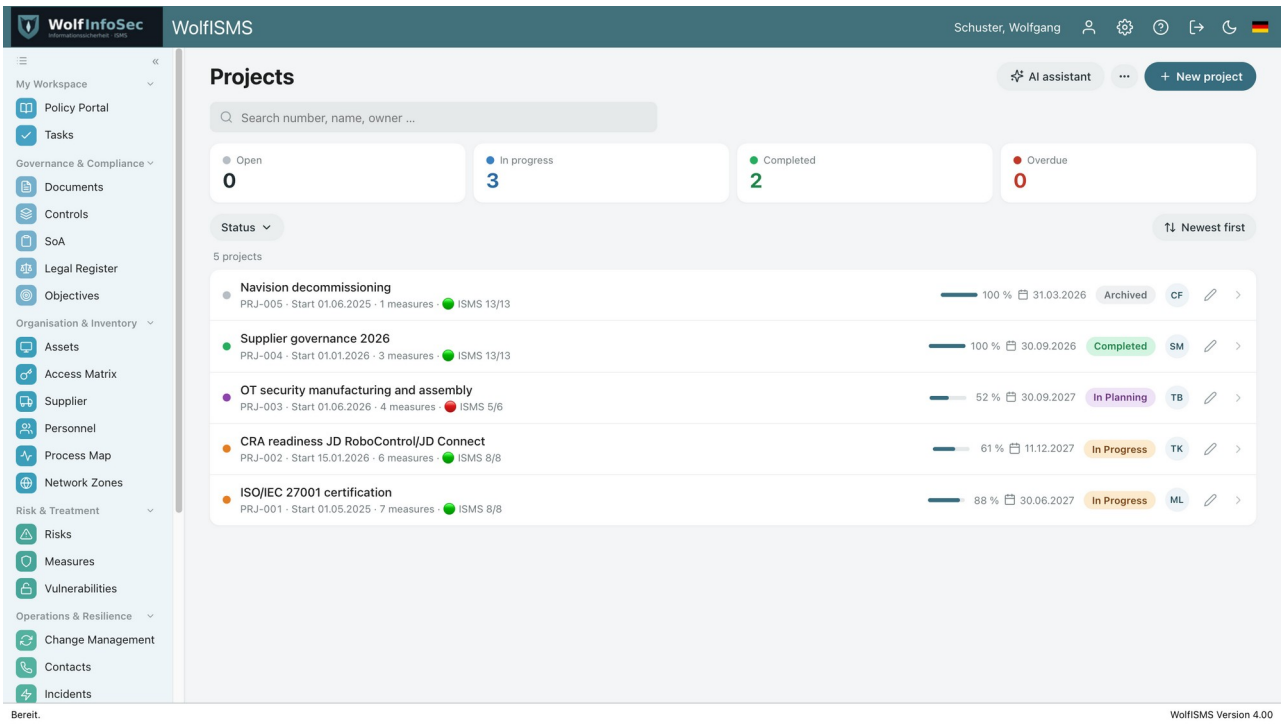
Description

The incident module supports the entire incident management process. Besides recording and tracking, reporting duties under GDPR, NIS 2 and the CRA are flagged automatically.

Features

- **Category tiles**: Overview of incidents by category (e.g. malware, phishing, data leakage); your administrator maintains the categories under Administration → Categories
- **Reporting duty badges**: Automatic marking of reportable incidents under GDPR / NIS 2 / CRA
- **Incident number**: Automatic suggestion in the format INC-YYYY-NNN
- **Escalation**: Escalation contact and escalation date can be recorded
- **Root cause analysis**: Fields for root cause, vulnerabilities and improvement measures
- **Links (incidents)**: Linking to measures, risks, assets and suppliers
- **Critical incidents**: Open incidents with priority "critical" are highlighted in red
- **Excel export**: Complete incident export as .xlsx
- **Ticket system link**: if your administrator has configured a ticket system, the number in the incident list leads straight to the corresponding ticket
- **Charts**: Pie charts: status, category, type
- **REST API**: External systems can create and query incidents automatically – see chapter 28
- **Comments**: Discussion thread per incident for coordination during handling
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It records an incident with you, reviews and merges, assesses the reporting obligation under NIS 2, GDPR and CRA, prepares the report of a stage and records it, works out cause and lessons, suggests links and goes through your open incidents – due reporting deadlines first. The assistant never reports; you do that in the authority’s portal. It replaces the former AI analysis in the detail view. Only what you confirm is saved.

© 2012–2026 WolfInfoSec GmbH



Reporting Obligations and Deadlines

If GDPR, NIS-2 or CRA is ticked on an incident, the detail view shows the section “Reporting obligations” since v3.90: per framework the reporting stages with deadline and status, templates for the report text and the reports already submitted.

Framework	Reporting stage	Deadline
NIS-2 (Sec. 32 BSIG)	Early warning	24 hours after awareness
NIS-2 (Sec. 32 BSIG)	Incident notification	72 hours after awareness
NIS-2 (Sec. 32 BSIG)	Intermediate report	on request of the BSI
NIS-2 (Sec. 32 BSIG)	Final report	one month after the 72-hour notification
GDPR	Notification to the supervisory authority (Art. 33)	72 hours after awareness
GDPR	Communication to data subjects (Art. 34)	without undue delay if a high risk is likely
CRA (Art. 14)	Early warning / notification / final report	24 hours / 72 hours / one month after the notification

- **Assessment**: per framework you record the time of awareness – including the time of day, as the deadlines run in hours –, the decision “to be assessed”, “reportable” or “not reportable” and a reasoning. For “not reportable” it is mandatory; Art. 33(5) GDPR requires breaches that were not

© 2012–2026 WolfInfoSec GmbH

notified to be documented as well. Without an assessment, midnight of the detection day counts as the time of awareness

- **Status per stage**: time remaining until the deadline, “overdue by …”, “reported” – if necessary with “late by …” –, “optional” for stages without a fixed deadline and “not required” once the incident has been assessed as not reportable
- **Report template**: contains the prescribed content of the stage, pre-filled from the incident – organisation, contact, description, affected assets, measures, the reference of an earlier report. Open points are marked […]. You copy the text into the authority’s reporting portal
- **Record a report**: keep the time, recipient, reference and the text submitted. The incident fields “Report Date” and “Reporting Authority” are updated along with it
- **Overview**: the incidents start page shows a bar with the open and overdue reporting deadlines; “Show all” leads to the list of all open mandatory reports, sorted by deadline. Archived incidents do not count
- **Tasks and reminder email:** since v3.94 open and overdue reporting deadlines also appear under “My Tasks” and in the task reminder email – for every owner of the incident, during an absence for the deputy. Once a report is recorded or the incident is assessed as not reportable, the deadline disappears there
- **Permission**: everybody with read access to incidents sees the section. The owners of the incident and master users may assess and record reports

A working aid, not legal advice
Whether an incident is significant within the meaning of NIS-2 or poses a risk to data subjects is decided by you in the assessment. WolfISMS calculates the deadlines from your entries.

© 2012–2026 WolfInfoSec GmbH

15. Vulnerabilities

Description

The vulnerability module brings the technical weaknesses of the organisation together in one place – whether they come from a vulnerability scan, a penetration test, a vendor advisory or an internal report. Every entry carries a sequential number in the format WEA-NNNNN, a title, a description, a score, a source and a status. The severity is not entered; it is derived from the score.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules. The same applies to the AI comparison against known vulnerabilities.

The usual path runs from the report through the assessment to the remediation: you record the finding, link it to the affected assets and create a measure straight from the vulnerability, which connects both in one step.

Features

- **Key figures**: six tiles above the list show the total, the open vulnerabilities and the open findings per severity (critical, high, medium, low)
- **Score and severity**: the CVSS value ranges from 0.0 to 10.0. Critical from 9.0, high from 7.0, medium from 4.0, below that low; 0.0 is purely informational. Without a score the entry stays marked as "no score"
- **Status**: new, under assessment, confirmed, being remediated, risk accepted, remediated and rejected/false positive. The last three count as finished, all others as open
- **Remediation deadline**: per severity your administrator sets how many days a vulnerability may stay open (default: critical 7, high 30, medium 90, low 180 days, no score 30). List and detail view show the due date from the date recorded, the tile “Overdue” counts the exceeded ones. If the score changes, the deadline of the new severity applies at once
- **Source**: vulnerability scan, penetration test, vendor advisory, CERT/BSI advisory, internal report, audit, bug bounty or other – so that it stays visible where a finding came from
- **Filters and search**: selection by status, source and severity, plus a full-text search across number, title and description. Every column heading sorts the list
- **Owner**: every vulnerability has one or more people responsible. Changing and deleting remain reserved for them and for master users – as in the other modules
- **Links**: assets, incidents, risks and measures are assigned in the detail view through "Manage". The sidebar links every connected entry; for assets the version is shown as well, so that systems with the same name stay distinguishable
- **Create a measure**: from the list and from the detail view a measure can be created that is linked to the vulnerability right away. This additionally requires the measures permission
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It records vulnerabilities – free, from a CVE number or an advisory –, takes over scan and pentest reports, checks the versions of your assets against known CVEs (formerly a button of its own), rates new findings one after another (triage), goes through due ones, proves remediation and writes a status report. Only what you confirm is saved.
- **Number suggestion**: the form proposes the next free number; it can be overwritten, for example to adopt the identifier of the reporting system

© 2012–2026 WolfInfoSec GmbH

- **Two languages**: title and description are stored in the language you are working in – the English version sits in its own fields next to the German one
- **REST API**: a vulnerability scanner creates its findings automatically and fetches the remediation state back later – see chapter 28
- **Excel export**: button “Excel” in the filter bar, takes over the filters set. The first sheet “Patch status” counts the open vulnerabilities per severity, how many have been open for more than 30 or 90 days, the oldest and the average age – counted from when they were recorded. The second sheet holds the list with the affected assets and the status of the linked measures

© 2012–2026 WolfInfoSec GmbH

16. Audit

Description

The audit module plans internal and external audits and tracks their findings through to the completed measure. An audit is an appointment with a period, an auditor, a framework and a status; below it hang the findings – the non-conformities – with a type, a person responsible and a due date.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

The module was rebuilt in v3.72. Up to v3.71 it was a self-check with question catalogues for ISO 27001, NIS 2, VdS, Cyber Essentials, GDPR and TISAX. Those catalogues are gone: how far a framework is implemented is kept in the Controls module – per requirement, with implementation status, chapter overview and conformity report. The answers of the former question catalogues remain in the database but are no longer shown in the interface.

Structure

The module has two tabs. "Audits" holds the appointments, "All findings" lists the findings of every audit together.

Field of an audit	Meaning
Number	AUD-00001, AUD-00002 … the next free number is assigned on saving; it can be overwritten
Designation	Mandatory, e.g. "Internal ISMS audit 2026" or "Surveillance audit ISO 27001"
Period	From (mandatory) and To. An end date before the start is rejected
Status	planned, confirmed or completed
Type	internal, external or gap assessment
Auditor	Auditor or certification body (free text)
Framework	The framework the audit refers to, e.g. ISO/IEC 27001 (free text)
Description	Scope, objective and course of the audit

Field of a finding	Meaning
Number	ABW-00001, ABW-00002 … assigned and overwritable like the audit number
Finding	Designation and description of what the auditor found
Type	Recommendation, minor non-conformity or major non-conformity
Status	open, in progress, implemented or not implemented
Responsible	The user who works the finding off
Due	Due date. Once it has passed and the finding is not implemented, the

© 2012–2026 WolfInfoSec GmbH

Field of a finding	Meaning
	date turns red
Framework / clause	The framework and the requirement concerned, e.g. ISO/IEC 27001 and A.8.16
Measures	The linked measures from the measures module

Every finding belongs to exactly one audit and is created from that audit's detail view.

Checklist and Gap Assessment

An audit can be conducted against a framework. To do so you take the requirements of a framework – ISO/IEC 27001, NIS2 or any other one kept in the Controls module – into the audit as a checklist and assess them there point by point. If all you want to know is where your organisation stands against a framework, create an audit of the type gap assessment: the checklist is the same, only the occasion differs.

The Checklist button in the audit detail view takes you there. The first time you choose the framework and, if you like, individual chapters; without a selection the complete framework is taken. By default only those requirements are taken over that are marked as applicable in the Controls module. Further chapters can be added at any time later – ratings already given are kept.

Every check point is given a rating:

Rating	Meaning
fulfilled	The requirement is implemented and evidenced
largely fulfilled	Implemented, with minor gaps
partly fulfilled	Started, essential parts are missing
not fulfilled	Not implemented – this is a gap
not applicable	Not relevant for your organisation; the point is left out of the calculation
not assessed	Not looked at yet

Each point carries two text fields: the finding – what you came across – and the evidence your judgement rests on (a document, a record, an interview). The whole list on display is saved in one go.

From the ratings WolfISMS calculates the conformity level: fulfilled counts in full, largely fulfilled three quarters, partly fulfilled one half, not fulfilled nothing at all. Points still open and those marked as not applicable are left out so that a half-completed list does not paint a false picture. You find the figure at the top of the checklist, per chapter in the audit detail view and as a column in the audit overview.

Checklist and Controls module stay separate.
A rating in the audit does not change the implementation status in the Controls module. That is deliberate: the Controls module says how far your ISMS has come, the checklist says what one particular audit found on one particular day. The wording of the requirement is copied as well when the checklist is built – an audit report has to show what was assessed, even if the requirement is changed later on.

© 2012–2026 WolfInfoSec GmbH

Wherever you have found a gap, the Create button in the Finding column turns it into a non-conformity. Clause, requirement, your finding and the evidence are already in it, and the type is proposed from the rating – not fulfilled gives a major non-conformity, partly fulfilled a minor one. Add the person responsible and the due date, and the finding runs on like any other, through to the measure. From then on the checklist shows the number of the finding next to the check point.

Perform GAP analysis: for a gap assessment with a checklist, the checklist and the detail view offer the button “Perform GAP analysis”. It guides you through the checklist step by step: every chapter is a step, every requirement a page with rating, finding and evidence. “Save & continue” moves on to the next requirement; single requirements or whole chapters can be skipped, and “Save & continue later” remembers the position. The overview shows the state and the conformity level per chapter; “Reset progress” starts again without deleting ratings and findings. Everything is stored in the same fields as in the checklist.

AI assistant (Essentials and above): If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It plans an audit with checklist and assessment questions – now for every type of audit –, suggests ratings for checklist items, prepares findings, drafts the audit report, plans the audit programme, follows up open findings and checks audit readiness. Ratings remain suggestions, the auditor decides; corrective measures are created in the measures assistant. Only what you confirm is saved.

Features

- **Key figures**: tiles above the list – audits in total and per status, open findings, open major non-conformities and overdue findings. The last two tiles are highlighted as soon as they are no longer zero
- **Filter and search**: filter by status and type, full text search across number, designation and auditor. Every column of the table can be sorted up and down
- **Audit detail**: shows the header data, the findings of the audit, all measures derived from them and, below that, the attachments and links
- **Checklist**: the requirements of a framework as check points inside the audit, rated on five levels, with a finding and the evidence for each point. The conformity level is calculated from them – see the section Checklist and Gap Assessment
- **Finding from a check point**: a check point that is not or only partly fulfilled turns into a finding at the push of a button, complete with the reference to the framework, the finding text and a proposed type
- **All findings**: the second tab lists the findings of every audit with its own key figures and filters by type, status – including "open only" – and free text
- **Link measures**: a finding is linked to existing measures. Nothing is copied: the measure stays in the measures module and is tracked there like any other
- **Create a measure**: a new measure can be created straight from the finding and is linked immediately. This additionally requires the editing permission for measures
- **Create a risk:** since v3.95 a finding can also become a risk – via “ Create risk” in its detail view or the quick button ⚠ in the list of findings. The form is prefilled: name from the finding, the owner is the person responsible, the description names finding, audit and framework, the treatment is “Reduce”, and likelihood and impact are suggested by type (major non-conformity 4 × 4, minor 3 × 3, recommendation 2 × 2). The risk is linked to the finding at once and takes over its measures; a measure created on the finding later is also attached to its risks, as far as you may change them. Existing risks are linked via “Manage” in the section Risks of the sidebar; the risk shows the finding as the back reference “Audit findings”. This requires the editing permission for audit and for risks

© 2012–2026 WolfInfoSec GmbH

- **Attachments**: PDF files on the audit – audit plan, audit report, evidence. The usual rules apply: genuine PDF files up to 16 MB
- **Links**: references out of the audit, e.g. to the certificate, a ticket or the report in the DMS
- **Excel export**: three sheets – audits, findings and checklists – with numbers, periods, due dates, responsibles, the linked measures and risks and the ratings. The checklist of a single audit can additionally be exported from the checklist itself
- **Audit report (PDF)**: in the detail view of an audit, since v3.90. Contains the header data, a summary with the conformity level and the number of findings, scope and objectives, the result per chapter with all check points, the findings with root cause analysis, transferability and effectiveness review, the corrective actions, the attachments as related documents and an approval block. “Short report” leaves out the individual check points. If the audit has not been completed yet, the report marks itself as an interim status

Notes

The module requires the audit permission: level 1 to read, level 2 to edit. The same permission governs the management review.

Deleting an audit also removes its findings, its checklist, attachments and links; the linked measures remain. The confirmation prompt says so, and the message afterwards names the number of findings deleted along with it.

© 2012–2026 WolfInfoSec GmbH

17. Management Review

Description

The management review is the review of the ISMS by top management per ISO/IEC 27001 clause 9.3. The module brings the required inputs together in one place: what you describe yourself you record as text; what the system already knows – objective achievement, risk situation and incidents – is compiled automatically from the other modules when the review is opened.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page. If the module is missing from the menu, the administrator has switched it off under Administration → Modules – the recorded data is preserved and is there unchanged once the module is switched on again.

Structure of a Review

Every review has a review period (from/to). When it is created, the end date is pre-filled with one year after the start date. The review contains the following sections:

- Status of actions from previous management reviews
- Changes in external and internal issues relevant to the ISMS
- Changes in the needs and expectations of interested parties
- Changes to business areas and the organisation affecting the ISMS
- Nonconformities and corrective actions – since v3.90 with the live list of major and minor non-conformities from the audit module: all open ones plus those implemented from audits in the period, with due date, status and effectiveness review
- Monitoring and measurement results
- Internal audit results – since v3.90 with the live list of the audits in the review period, their conformity level and number of findings
- Achievement of the information security objectives – shown as a live list of the KPIs from the Objectives module, with the values of the review period
- Results of the risk assessment and status of the treatment plan – live list of the open risks rated "critical" and "high"
- Evaluation of the incidents within the review period
- Feedback from interested parties
- Opportunities for continual improvement
- **Actions decided** – the entries from the measures module linked to the review (outputs of the review per clause 9.3.3)

Features

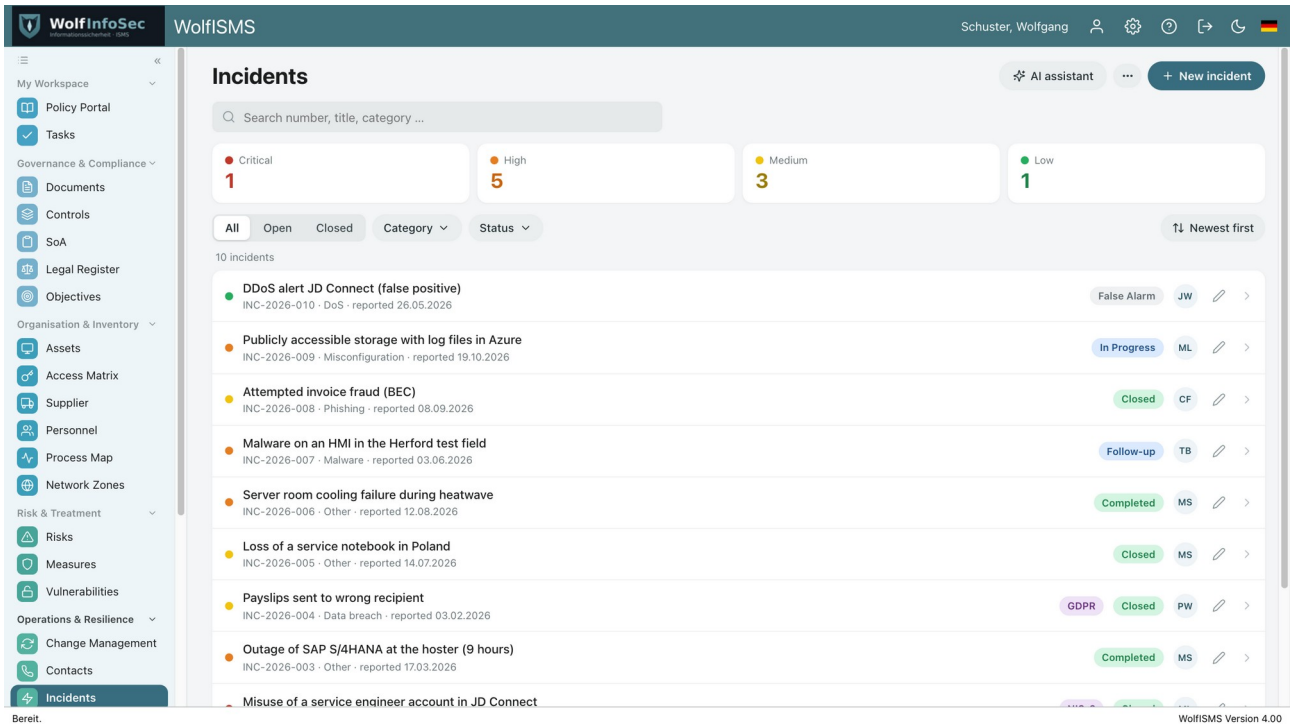
- **Overview**: List of all reviews with title, period, creator and modification date
- **Editing**: All text sections are maintained in the rich-text editor
- **Live sections**: The KPI, risk, incident and audit sections are deliberately not stored with the review but recalculated every time it is opened – the review therefore always shows the current state
- **PDF export**: Produces the complete review document. If a PDF letterhead is configured in the system, it is used as header and footer
- **PowerPoint export**: Produces a presentation of the review for the management meeting
- **Actions decided**: The section shows the linked measures with number, name, status, priority, end date, progress and person responsible, plus the total effort and cost. "Manage links" assigns existing measures or removes them; "New measure" creates a measure that is linked right away. It

© 2012–2026 WolfInfoSec GmbH

is then maintained in the measures module, which also holds effort, costs, attachments and the remaining links. The section appears in the PDF and PowerPoint export as well

- **Bilingual**: Display in German or English depending on the user setting

Permission: audit (0 = no access, 1 = read, 2 = edit) – URL: /managementreview



Notes

For the sections "Achievement of the information security objectives" and "Results of the risk assessment" to be populated, KPIs with values in the review period must be maintained in the Objectives module, and open risks rated critical or high must exist in the risk module. Otherwise the sections remain empty – this is not an error but reflects the current data.

© 2012–2026 WolfInfoSec GmbH

18. Tasks

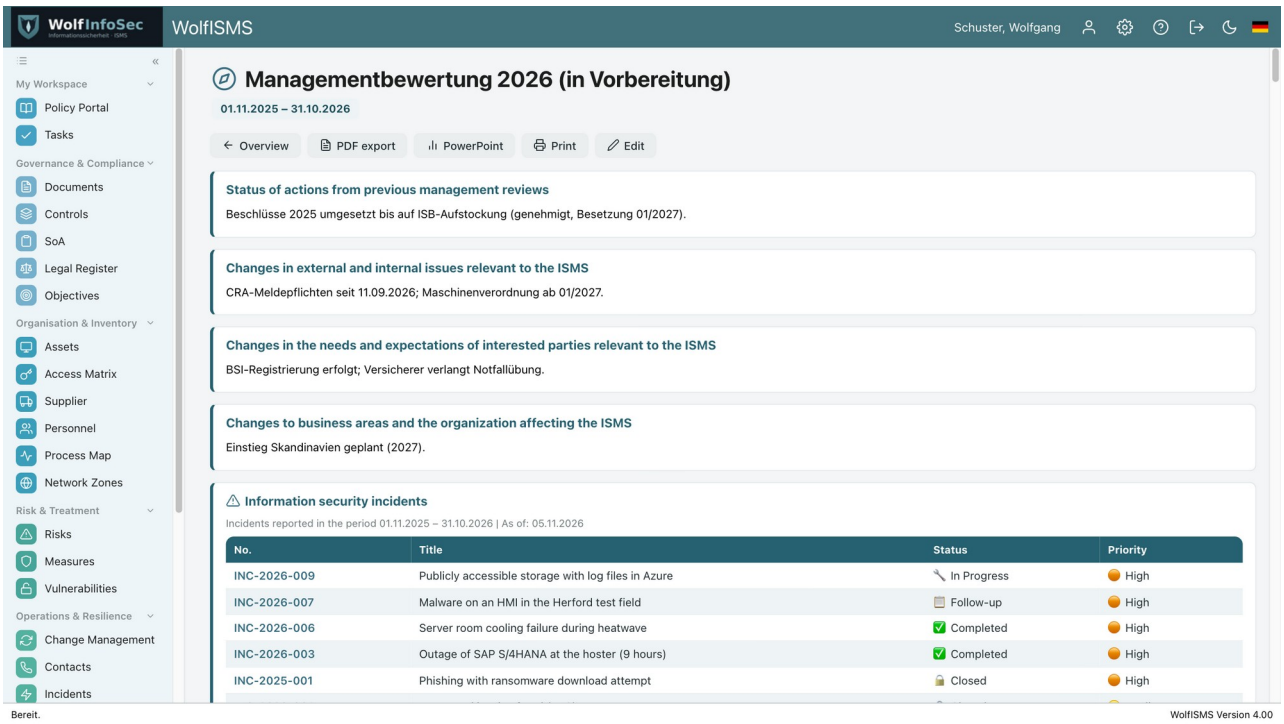
Description

The tasks module brings together all open tasks of the signed-in user from every other module in one central place. Users with the master permission also see the tasks of all other users.

Features

- **Period filter**: Today / 7 days / 30 days / 90 days / all
- **Mine / All (master)**: Switch between your own tasks and the system-wide view
- **Open measures**: Measures with an end date inside the selected period
- **Reviews**: Due reviews from all modules: measures, assets, documents, risks, suppliers
- **Document workflows**: Documents with a pending review or outstanding approval
- **Changes**: planned windows, pending votes on the approval board and due post-implementation reviews from change management
- **Reporting deadlines:** open and overdue mandatory reports on security incidents (NIS 2, GDPR, CRA) in a red section of their own at the very top, with the time of the deadline, the time left (“44 h left” or “overdue for 3 h”) and a link to the report template; plus a tile of their own. Visible with read access to incidents. The reminder email goes out once a day and is no substitute for the page with 24-hour deadlines
- **Outstanding read confirmations**: Policies that are mandatory reading for your role and that you have not yet confirmed as read in the policy portal. Documents without a reading obligation do not appear here – and somebody who holds no role receives no reminder mail about them either
- **Urgency badges**: Marking by due level (today / this week / overdue)
- **Overdue entries**: Past due dates are highlighted in red
- **Area tags**: Coloured tags show which module the task comes from

© 2012–2026 WolfInfoSec GmbH



Notes

The tasks module is read-only. Tasks are edited in their respective modules. In addition the system sends a reminder email for due tasks; the time and interval are set by your administrator.

Absence and deputy

Before your holiday, enter the period and a deputy on your account page under “Manage absence”. During that time the deputy additionally sees your tasks under “My Tasks” – with a note on whose they are – and receives your reminder emails. Who is responsible for the records does not change, and once the absence is over everything falls back automatically.

- **Only with a deputy**: a period without a deputy cannot be saved – otherwise nobody would receive the tasks. For no absence, leave all three fields empty.
- **Read confirmations**: stay with you. Nobody can confirm a policy as read on someone else’s behalf.
- **Deputy absent as well**: then the tasks move on to their deputy.
- **For others**: administrators can record a colleague’s absence from the user management, for example in the case of sick leave.

© 2012–2026 WolfInfoSec GmbH

19. Operational Plan (Recurring Tasks)

Description

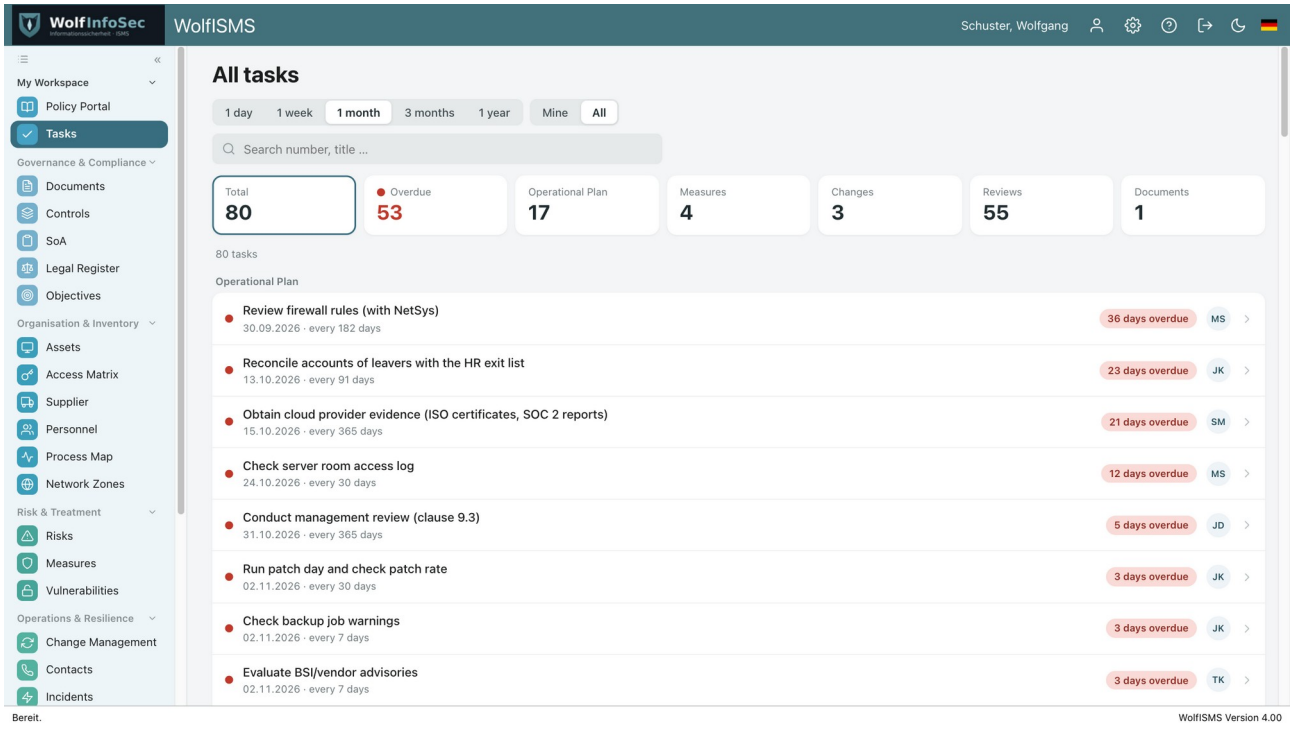
The Operational Plan module manages recurring mandatory tasks (e.g. the annual management review, a regular backup test, quarterly access reviews) as a deadline calendar with an unbroken evidence chain.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page. If the module is missing from the menu, the administrator has switched it off under Administration → Modules – the recorded data is preserved and is there unchanged once the module is switched on again. The reminder emails then no longer list operational plan dates either.

Features

- **Task list**: Overview of all open recurring tasks with the next due date, the person responsible and the frequency
- **Urgency badges**: Colour marking by due date (overdue / due today / in 7 days / in 30 days / on schedule)
- **Status and completion**: since v4.00 every open instance has a status – open, in progress, done. Only “done” archives the instance unchangeably as evidence and creates the next one with the new due date (date + frequency in days; for badly overdue tasks counted from today)
- **History / evidence chain**: All instances of a recurring task share a chain ID through which the complete completion history can be viewed as evidence
- **Mine / All (master)**: Master users can switch between their own tasks and the system-wide view
- **Delete (master)**: Only master users can delete an open instance; already completed evidence is not affected
- **Linked URL**: Optional field for a link to external instructions or a form

Permission: accessible to all signed-in users (own tasks); the menu entry, the system-wide view and deletion require the master permission – URL: /op_plan



© 2012–2026 WolfInfoSec GmbH

20. Documents

Description

The document module manages all ISMS documents with a complete approval workflow. Every change is kept as a version of its own, so that all versions stay available and an earlier one can be brought back; on top of that come bilingualism (DE/EN), write protection and linking to BPMN process diagrams. An existing Word document can be imported instead of being typed in again. The document type for process documents is called “Prozesse”; it used to be “Verfahren” and was renamed automatically during the changeover.

Versions and version history

Every change to a document is kept as a version of its own. Saving does not overwrite what was there before, it puts the new state next to it – the earlier version stays complete and can be opened again at any time. The version number has two parts: the first one counts up with every approval, the second one with every save in between. An approved v2.0 therefore becomes v2.1, v2.2 … while it is being edited, and v3.0 with the next approval.

Two versions are valid side by side:

- **The approved version** is the one that counts. The links from all other areas point to it – controls, risks, the process map, network zones and linked documents –, it is the one shown in the policy portal and the one that triggers the read confirmation.
- **The working copy** is the newest version. That is where editing, review and approval happen. As long as it has not been approved, nothing changes for the other areas – nobody works against a draft by accident.

The document list shows both in one row: the number of the valid version on top and the working copy underneath as a link. In the detail view a bar above the document tells you which of the two you are looking at and takes you to the other one in a single click.

The Versions panel in the right-hand column holds the complete history: every version with its number, status, editor and date, each of them one click away. The valid version is marked as approved – or as current, as long as the document has never been through approval – and the working copy as latest. The change log below it shows the entries of all versions, not only those of the one currently open.

An earlier version is brought back with Restore. Its content is not written over the current state; it is taken over as a new version that goes through review and approval as usual. The chain therefore stays complete: it remains traceable later on that on a particular day an older version was reverted to.

What a new version takes along.
Attachments, the reading obligation and links belong to the individual version and are carried over every time a new one is created – an old version is therefore complete when you open it again. The links to controls, risks, processes and other documents, by contrast, belong to the document as a whole: they stay on the approved version and only move on with the next approval. No area loses its reference in the process.

A superseded version is write-protected. Editing, linking, changing attachments and the AI assistant are blocked there; viewing and the Word and PDF export remain available so that a past state can be produced as evidence at any time.

© 2012–2026 WolfInfoSec GmbH

Import from Word

A document that already exists does not have to be typed in again. Above the editing form sits the box “Import from Word”: drag the Word file into it or select it and click Import. The content is then in the editor. Nothing has been saved at that point – only Save stores it as a document or as a new version. The box appears both when a new document is created and when an existing one is edited.

Headings, bullet and numbered lists, tables including merged cells, links, bold, italic and underlined text as well as images are taken over. The images go into the document text and leave it again as images in the Word export.

- **What stays out**: headers and footers of the Word file – page numbers and letterhead come from the template configured in the ISMS –, the table of contents of the Word file, text held in text boxes and in graphics as well as images in formats a browser cannot display (EMF/WMF from embedded drawings, for instance).
- **What is missing is said**: above the form you see which file the content came from and what could not be taken over. If a larger part of the text is missing, WolfISMS says so explicitly – please compare the result with the Word file in that case.
- **Limits**: .docx files up to 16 MB are read; please save older .doc files as .docx in Word first. A single image may be up to 2 MB, all images together up to 8 MB.

When a new document is created, WolfISMS suggests the name from the file – from the title in the file properties, or from the first heading instead. The text goes into the language field you are working in: anyone using the English interface fills the English document text with it.

If AI is switched on, the box offers the checkbox “Have the AI process the text right away” – ticked by default, but free to be cleared. The AI then tidies up the conversion and aligns the text with ISO 27001 and NIS2; a bar shows how far it has got. The result is afterwards in the editor, and “Back to the imported text” brings the unprocessed version back. Here, too: nothing is in the database until you save.

The import replaces the text in the form.
Whatever is in the editor is replaced by the imported document; WolfISMS asks before it does so. On a superseded version and on a write-protected document the import is blocked – editing is not intended there anyway.

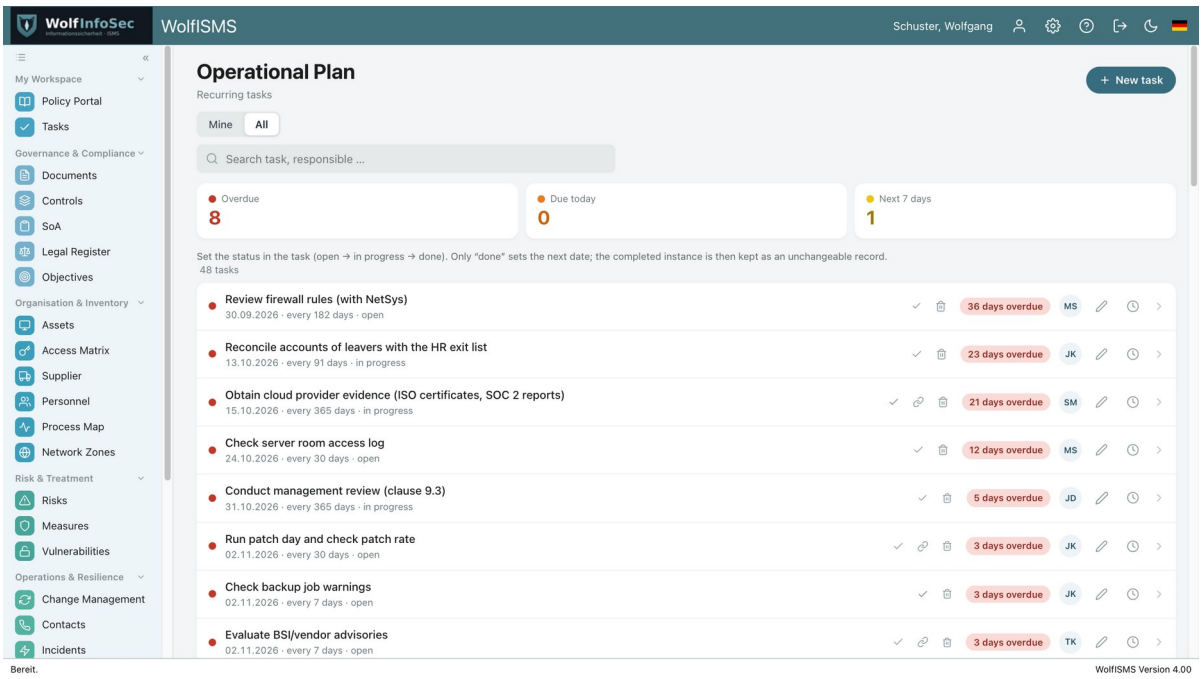
Features

- **Document list**: Filters by type, status and category; search as you type (no paging)
- **Archive**: documents that no longer apply but must be kept are archived. They disappear from the list and remain reachable through the “Archive” button – nothing is deleted
- **Detail view**: Full document content with metadata, attachments and linked BPMN diagrams
- **Collapse the form**: in the editing form the "Basic data" respectively "Metadata" block can be collapsed through its heading. The editor then grows down to the bottom of the window – convenient for long documents. The state is remembered in the browser
- **Workflow: review**: The assigned reviewer confirms the content (creates a review date)
- **Workflow: approve**: The approving user (or a master user) grants formal approval
- **Workflow: new version**: Creates the next working copy from the approved version – as a complete copy including attachments, reading obligation and links. The approved version stays untouched and remains linked everywhere until the new one is approved

© 2012–2026 WolfInfoSec GmbH

- **Version history**: the right-hand column lists every version with its number, status and date; the valid one and the working copy are marked – see the section Versions and version history
- **Restore a version**: an earlier version is taken over as a new working copy and goes through review and approval as usual – nothing is overwritten
- **Read confirmation**: A read confirmation can be requested for policies – since v4.00 for this document type only. Anyone who has not confirmed the document yet sees it as an open task; the personnel module shows the state per employee. Who has to read a document is defined by the master user in the reading obligation matrix of the policy portal – without a role assignment a released document stays visible but is mandatory for nobody. WolfISMS points this out when the document is released
- **Write protection**: Approved documents can optionally be write-protected
- **Bilingualism**: Separate fields for German and English document content
- **Attachments**: File upload per document (evidence, templates); PDF files up to 16 MB are accepted
- **Review date**: The regular review is planned and displayed as a task
- **Export**: Document list as .xlsx; individual documents as Word or PDF – bullet lists inside table cells are rendered correctly as lists. If a PDF letterhead is configured, it appears as header and footer
- **Word import**: a .docx file can be imported above the editing form – headings, lists, tables, links and images come with it. On request the AI processes the imported text right away; as always, it is only stored once you press Save – see the section Import from Word
- **Charts**: Status and type pie charts
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It creates documents, takes them over from uploaded material, revises, reviews and merges, suggests links to controls, processes, documents, measures and risks, creates the English version, hands a document over for review and finds gaps – mandatory documents and controls without a document. It replaces the former buttons “AI editing” and “AI links”; it never approves. Only what you confirm is saved.
- **AI translation (dok):** with the interface set to English, since v3.95 the detail view shows the button “AI translation”. It translates the German document text into English and proposes the result for the English text. Headings, tables, images and layout are taken over unchanged from the German version – only the text sections go to the AI. The dialog shows German and English side by side and reports when a section stayed German or the inline formatting (bold, italic, link) of a section could not be carried over. You can add an instruction of your own – such as “American English” – and apply the translated document name as well. “Apply” replaces an existing English text and, like every adoption from the AI assistant, creates a new version. Requirements: AI enabled, German text present, the document is neither approved nor in review or approval, and you may change it
- **Comments**: Discussion thread per document
- **Linked documents:** if DOK0001 refers to DOK0002, since v3.94 DOK0001 also appears on DOK0002 under “Documents” and in its linking view. The link can be removed from either side; a reference from a superseded version does not count
- **Notification on approval**: when a policy is approved, everyone who has to read it receives an email straight away with the number, name, version and a direct link into the policy portal – there is no need to wait for the next task reminder. The mail arrives in each recipient’s own language

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
My Workspace
Policy Portal
Tasks
Governance & Compliance
Documents
Controls
SoA
Legal Register
Objectives
Organisation & Inventory
Assets
Access Matrix
Supplier
Personnel
Process Map
Network Zones
Risk & Treatment
Risks
Measures
Vulnerabilities
Operations & Resilience
Change Management
Contacts
Incidents
Operational Plan
Recurring tasks
+ New task
Mine
All
Search task, responsible ...
Overdue
8
Due today
0
Next 7 days
1
Set the status in the task (open → in progress → done). Only "done" sets the next date; the completed instance is then kept as an unchangeable record.
48 tasks
Review firewall rules (with NetSys)
30.09.2026 · every 182 days · open
36 days overdue
MS
Reconcile accounts of leavers with the HR exit list
13.10.2026 · every 91 days · in progress
23 days overdue
JK
Obtain cloud provider evidence (ISO certificates, SOC 2 reports)
15.10.2026 · every 365 days · in progress
21 days overdue
SM
Check server room access log
24.10.2026 · every 30 days · open
12 days overdue
MS
Conduct management review (clause 9.3)
31.10.2026 · every 365 days · in progress
5 days overdue
JD
Run patch day and check patch rate
02.11.2026 · every 30 days · open
3 days overdue
JK
Check backup job warnings
02.11.2026 · every 7 days · open
3 days overdue
JK
Evaluate BSI/vendor advisories
02.11.2026 · every 7 days · open
3 days overdue
TK
Bereit.
WolfISMS Version 4.00

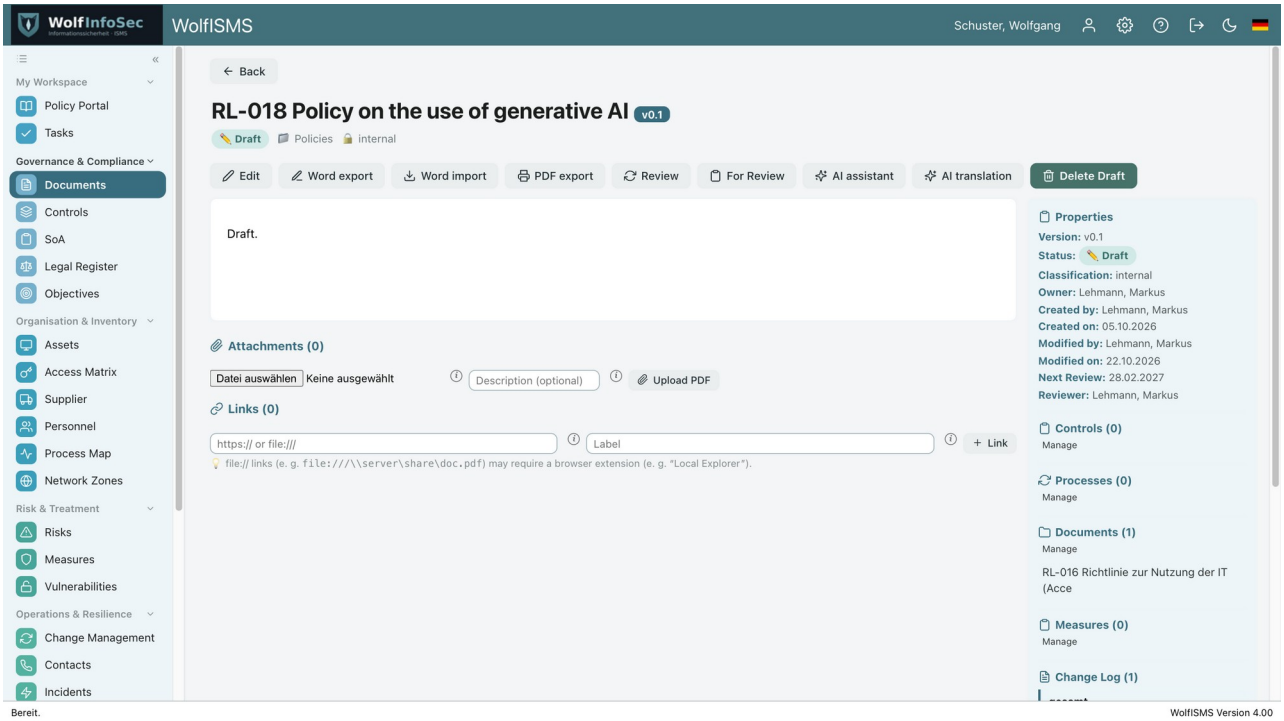
21. BPMN Process Modelling

Description

The BPMN module allows process diagrams to be created and managed directly in the browser, without external software. Diagrams can be linked to documents.

Features

- **Viewer**: Interactive, zoomable view of a BPMN diagram (read-only)
- **Editor**: Full BPMN modeller based on bpmn-js (drag & drop, insert elements)
- **Import (dok)**: Upload of a .bpmn or .xml file from an external BPMN application (e.g. Camunda, draw.io)
- **Export**: Download of the current diagram as a .bpmn file for external editing
- **Save (dok)**: Store the diagram with number, title and status in the database
- **Title suggestion**: On import the file name is adopted automatically as a title suggestion
- **Linking**: BPMN diagrams can be linked in the document detail view
- **Linked documents:** since v3.94 the viewer lists the documents linked to the process below the diagram – one row per document, preferably the valid version



22. Playbooks

Description

The playbook module describes how to respond to a scenario – ransomware, phishing, failure of a service provider, reportable incident. Since v4.00 every playbook follows a fixed frame according to ISO/IEC 27035 and NIST SP 800-61 (ISO/IEC 27001 A.5.24–A.5.28): profile with approval, fixed sections, procedure steps, roles, exercises and tests. Uploaded PDF files and external links remain and can be assigned to a playbook.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules. Texts, files and links stay stored but cannot be retrieved.

Features

- **List:** all playbooks with traffic light, type and approval status. The tiles Approved, In progress, Review due and Action needed filter with one click, plus a filter by type and the search over number, title, scenario and file names. Below are the files and links not yet assigned to a playbook
- **Profile:** number (suggested PB-001 onwards), type (incident response, emergency and recovery, reporting, operations), scenario, from which severity it applies, responsible person and deputy, approval status (draft, in review, approved, under revision), version, approval and next review
- **Approval:** if you set the approval status to “approved”, WolfISMS records date and approver, plans the next review in twelve months and sets the version to 1.0 if none is entered yet
- **Fixed sections:** purpose and scope, triggers and detection, triage and escalation, containment, eradication, recovery, communication and reporting, post-incident review – each with a hint on what belongs there, including the reporting deadlines under NIS 2, GDPR and CRA. A text written freely before appears below as “Further content”
- **Procedure steps:** phase (detection, triage, containment, eradication, recovery, communication, post-incident), step, role, deadline and evidence
- **Roles:** role and person – a user or, for externals, a name – with their task
- **Exercises and tests:** date, type (tabletop, walkthrough, simulation, live test), result (planned, successful, partly successful, not successful), participants and findings
- **Traffic light:** the sidebar checks whether a playbook is ready for use – responsible person and deputy, type and scenario, all eight sections, at least three procedure steps with a role, staffed roles, approval, next review and a test within the last twelve months. It turns red for an overdue review or a failed last test. It is a hint, not a lock
- **Links (play):** assets, risks, incidents in which the playbook was applied, documents and requirements, suppliers, authorities and service providers from the contacts, and measures
- **Files and links (play):** upload PDF files and set external links (CERT, BSI, vendor documentation) as before; both can be assigned to a playbook and then appear in its detail view
- **Edit and delete (play):** by the responsible person, the deputy, the creator – as long as nobody is responsible – or a master user. Deleting keeps assigned files and links; they appear in the list again
- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It creates a playbook – you describe the scenario or upload an existing document –, reviews it, prepares an exercise (tabletop), records a test result, sharpens it after an incident, finds gaps in the register and goes through your playbooks that need action. Only what you confirm is saved.

© 2012–2026 WolfInfoSec GmbH

© 2012–2026 WolfInfoSec GmbH

23. Suppliers

Description

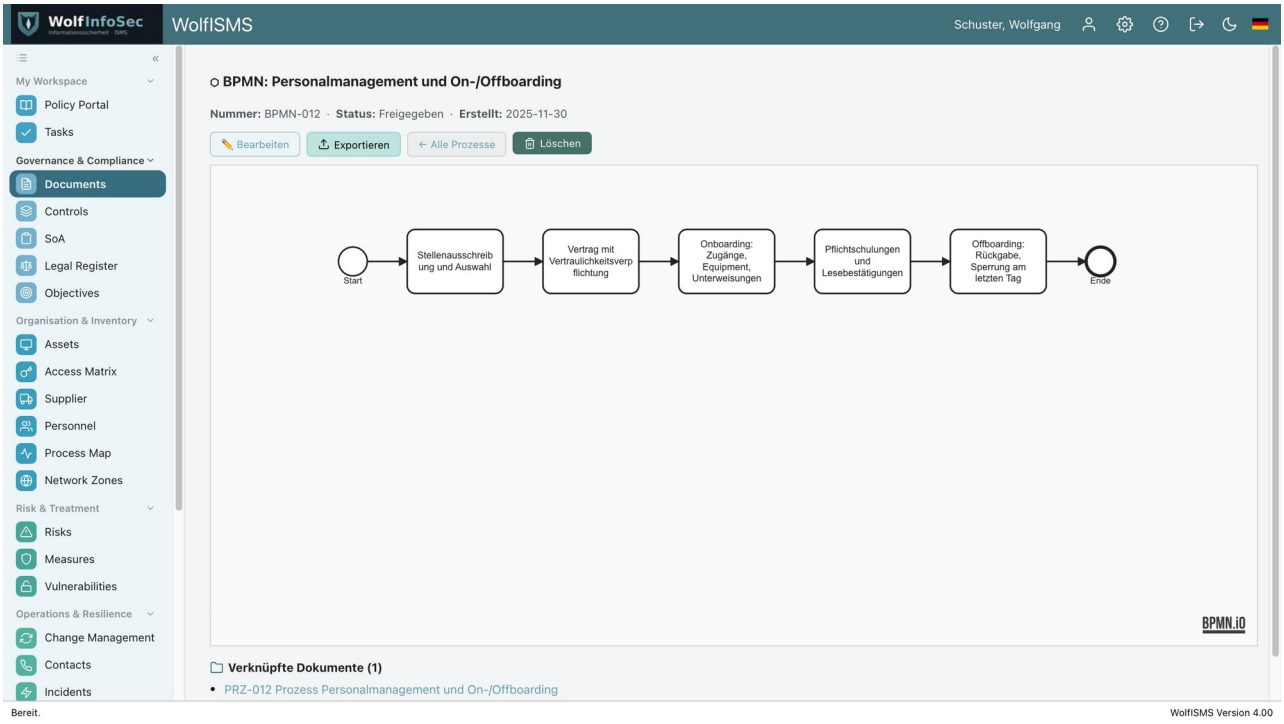
The supplier module manages all external service providers and vendors. It automatically calculates a risk score based on contract status, certifications, data protection and early warning indicators.

Features

- **Supplier register**: List with search and filters by type, tier and risk level; the type tiles appear when your administrator has switched on the info tiles
- **Description**: Since v4.00 a free-text field with an editor in the edit form and the detail view – for the scope of services, locations or particulars, for example. It is also part of the Excel export and can be read and written via the REST API
- **Risk assessment**: Since v4.00 the block with the assessment criteria only appears in the edit form; the detail view stays clearer as a result
- **Risk score**: Automatic calculation from: personal data, contract, certifications, security level, impact, likelihood
- **Tier classification:** Tier 1 (critical) to Tier 3 (uncritical) or immaterial to mission-critical. Since v4.01 the tier counts double in the impact and sets a floor: a mission-critical supplier or tier 1 has at least impact 4, a business-critical one at least 3
- **Score history**: Every recalculation is recorded so that the development of a supplier risk can be traced over time
- **Questionnaire status**: Tracking of the supplier security questionnaire
- **Links (vendor)**: Linking to measures and incidents
- **Review date**: Regular supplier assessment with task creation
- **Excel export**: Complete supplier list as .xlsx – with email, the seven assessment criteria and the cloud exit strategy as plain text; the workbook doubles as the import template
- **Import:** the button “Import” next to “Export” reads an .xlsx or .csv file (comma or semicolon, at most 8 MB); only the column “Name” is mandatory. A preview first shows what would be created, changed (“old value → new value”) or skipped – nothing is written until you upload the same file again with the tick “Apply”. A known supplier number updates that supplier, without a number the supplier with exactly that name; everything else is created if “Create new” is ticked. Empty cells change nothing. Rows with values outside the selection lists, unknown or ambiguous owners, an invalid email address, duplicate rows and other people’s suppliers you may not change are skipped with a reason. Enter owners as email address or “Last name, First name”, several separated by “;”. WolfISMS recalculates risk and score; the column cloud exit strategy is not read so that its formatting survives. Write access to suppliers is required
- **Cloud exit strategy:** suppliers of a type the administrator has marked as cloud/SaaS have a section of their own in the edit form, with an editor and guidance – data export, deletion after the contract ends, alternative providers, notice periods, migration effort, last test. It appears or disappears as soon as the type changes; text already entered is kept. The detail view shows the strategy, or a warning with “Record now”. Above the list WolfISMS states how many cloud/SaaS suppliers still lack a strategy; “Show” filters for exactly those, and the table marks them with ☁⚠
- **DPA details (datenschutz):** Since v4.01 the detail view of a supplier that processes personal data (“personal data” Yes or Partly) shows the block processing on behalf under Art. 28 GDPR: DPA in place, date, document, third country with safeguard and transfer impact assessment, and the sub-processors. Anyone with the permission “Data protection” set to edit may maintain it – the supplier permission is not enough
- **Charts**: Risk level and type pie charts
- **Comments**: Discussion thread per supplier

© 2012–2026 WolfInfoSec GmbH

- **AI assistant (Essentials and above)**: If your administrator has enabled AI and given you the permission “AI usage”, the button “AI assistant” sits at the top of the list and in the detail view. It opens a conversation on a page of its own, built like the AI assistant for risks. It creates suppliers (free, from an asset or a document, several from a list, too), reviews single ones, a type, a tier or the entire register, evaluates evidence, finds gaps, merges and sends the security questionnaire with suitable questions; it evaluates returned answers – also third-party formats such as CAIQ or VDA ISA/TISAX. Only what you confirm is saved.



Security Questionnaire

The questionnaire asks the supplier, in writing, how they implement information security. The template follows ISO/IEC 27001:2022 and NIS2 and comprises 49 questions in 12 categories – from company details through access control, encryption and continuity management to reporting duties and subcontractors. Which questions are asked is defined by your administrator in the question catalogue.

- **Sending:** In the supplier’s detail view the drop-down menu “Questionnaire” has bundled all questionnaire actions since v3.95; its first entry opens the dispatch dialogue. The supplier receives an email with a link to a form they fill in without signing in. An email address and a contact person must be stored on the supplier; if either is missing, WolfISMS says so before sending.
- **Validity:** The link is valid for 30 days. After that the questionnaire shows as “expired” and accepts no more answers – sending again issues a new link.
- **Address in the link**: if your ISMS is reachable for suppliers under a different address than for your own staff, the administrator stores that domain with the question catalogue. The link in the email then points there
- **Without mail dispatch:** Alternatively the questionnaire can be sent as a PDF or generated as an email file and sent from your own mail client. You then enter the answers yourself.

© 2012–2026 WolfInfoSec GmbH

- **Entering manually:** If the answer comes back on paper or as a completed PDF, you record it by hand. The original can be attached, together with the date of receipt and a remark.
- **Status:** sent, being entered, answered or expired – visible at a glance in the supplier overview.
- **Evaluation:** The answers are shown per supplier under “Questionnaire” – grouped by category, with the framework reference of each question. A short summary shows how many questions were answered Yes, Partly or No.
- **Effect on the assessment:** When the answers arrive, the supplier’s “questionnaire” field is set to “Yes” and the risk score is recalculated.

A questionnaire you record yourself does not expire.
The deadline applies only to the link that was sent – that is where a token becomes invalid. A questionnaire sent as a PDF or entered by hand stays open until you complete it.

© 2012–2026 WolfInfoSec GmbH

24. Personnel

Description

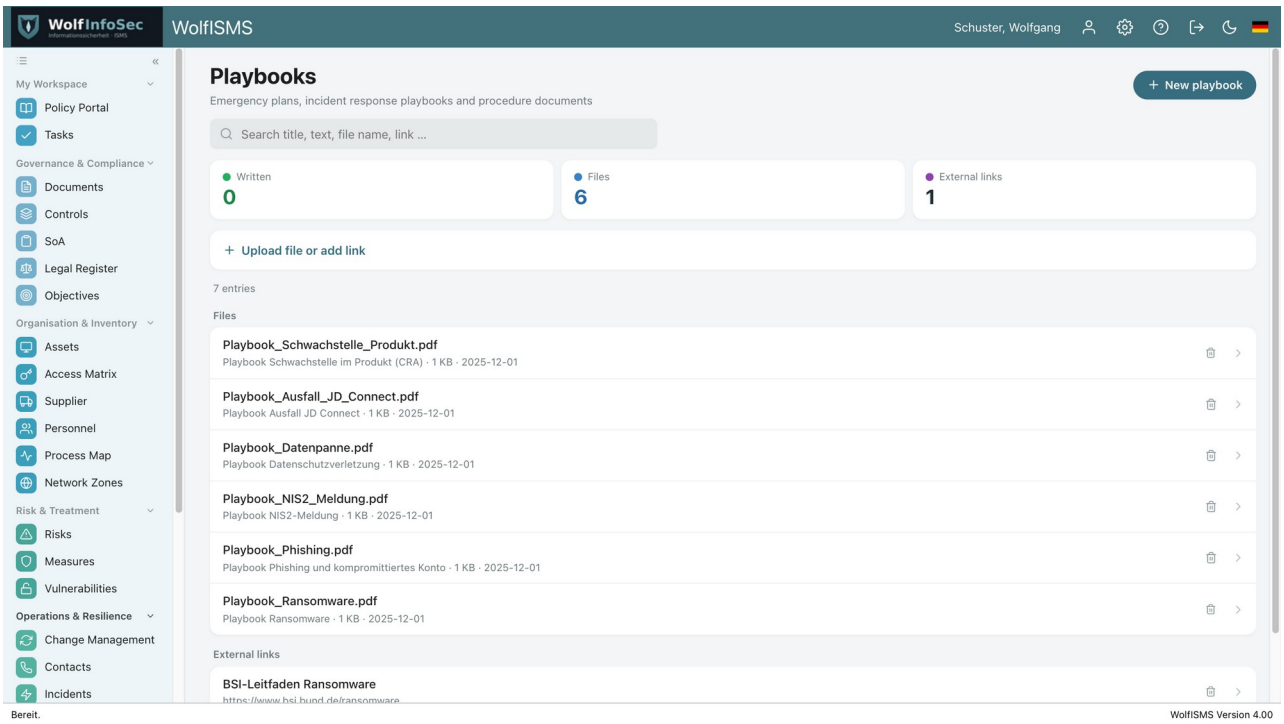
The personnel module provides an overview of all employees and their read status for training documents. It supports the evidence trail for security training per ISO 27001 A 6.3.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

Features

- **Avatar tiles**: Employee tiles with initials, department, position and a read status bar
- **Department filter**: A tab per department – departments and teams come from the centrally maintained master data list – plus an alphabet navigation bar
- **Document status**: Per employee: which training documents have been read, which are still outstanding and which trigger no reading obligation at all for the roles of that employee
- **Read status bar**: Percentage of the mandatory documents read. Only what the employee has to read according to the reading obligation matrix is counted – somebody with nothing to read stands at 100 %
- **Excel export (pers)**: Two sheets: employee overview and the complete read status matrix. The matrix knows three states: read, outstanding and – for documents without a reading obligation – a dash
- **Awareness report**: button next to “Export”, visible with read access to personnel. PDF with the overall reading rate, the rate per mandatory document (with version, release and last confirmation) and per department, and the open reading obligations per person. Only active accounts count – the rate can therefore differ from the tiles above, which include former employees

© 2012–2026 WolfInfoSec GmbH



Notes

The personnel module only shows documents that require a read confirmation. Whether an employee actually has to read such a document is decided by the reading obligation matrix of the policy portal; it is maintained by the master user. Creating users is done at /admin.

Onboarding / Offboarding

Since v3.72 there are two tabs above the staff directory: "Directory" and "On-/Offboarding". The second one tracks people joining and leaving – from the employment contract through the system accounts to the return of the equipment.

A process describes one person with a joining or leaving date, a department and a function. Three items are fixed, two lists you fill in yourself:

- **Employment contract / NDA**: for joiners only. Once the contract and the confidentiality agreement are signed, the item is ticked off
- **Company email**: the mailbox is set up – for a leaver: blocked or forwarded
- **ISMS user**: derived from the link to a user account. For a joiner the item counts as done as soon as an account is linked; for a leaver only once the account is blocked. Blocking is possible straight from the process
- **Accounts**: the system accounts with a designation, the account name and a note. When the process is created the list can be pre-filled line by line
- **Equipment**: the equipment with its inventory or serial number – laptop, phone, keys, token

Besides "open" and "done" the three fixed items also know "not required"; marked that way they do not count towards the progress. The bar on the process shows the completed items against all counting ones – including both lists.

- **Overview**: tabs for joiners, leavers and completed processes, plus a search across name, department and email address
- **Complete**: a completed process is locked against changes. To work on it again it is reopened

© 2012–2026 WolfInfoSec GmbH

- **Leaver from joiner**: the matching offboarding is created from an onboarding at the press of a button. Master data, accounts and equipment are carried over as open items – what has to come back is exactly what was handed out
- **Block user**: sets the linked ISMS account to inactive. Your own account and the last remaining active administrator respectively master user cannot be blocked
- **Log**: creating, changing, completing and deleting a process is recorded in the activities

The personnel permission applies: level 1 to read, level 2 to edit. User accounts themselves are still created under Administration; the process only refers to them.

Training

Since v3.93 there is a third tab above the staff directory, “Training”. There you plan security training sessions and record who attended them – in addition to the read confirmations the personnel module shows anyway (ISO/IEC 27001 A.6.3).

- **Training list:** date, title, location, trainer, participants (attended/assigned) and the share that has completed the session as a percentage with a bar. Above it key figures, the filters “All”, “Upcoming”, “Not completed” and “Completed”, and a search
- **Create and edit:** title and date are mandatory, location, trainer and description optional
- **Assign all users:** a button in the detail view assigns every active user who is not yet assigned
- **Assign individually:** a list with check boxes and a filter field; “select all shown” picks, for example, a whole department at once
- **Record attendance:** “attended” or “reset” per person, or “Mark all as attended”. The date of the session is used as the attendance date. Once it has passed, the open ones are shown as “missed”
- **For the employees:** the staff list has the column “Open training” (missed sessions in red), the tiles show for example “2 training sessions open”, and the detail page of a person lists open and attended sessions with their date

Read access to personnel is enough to view the sessions; creating them, assigning people and recording attendance needs write access. Every change appears in the activity log.

© 2012–2026 WolfInfoSec GmbH

25. Policy Portal

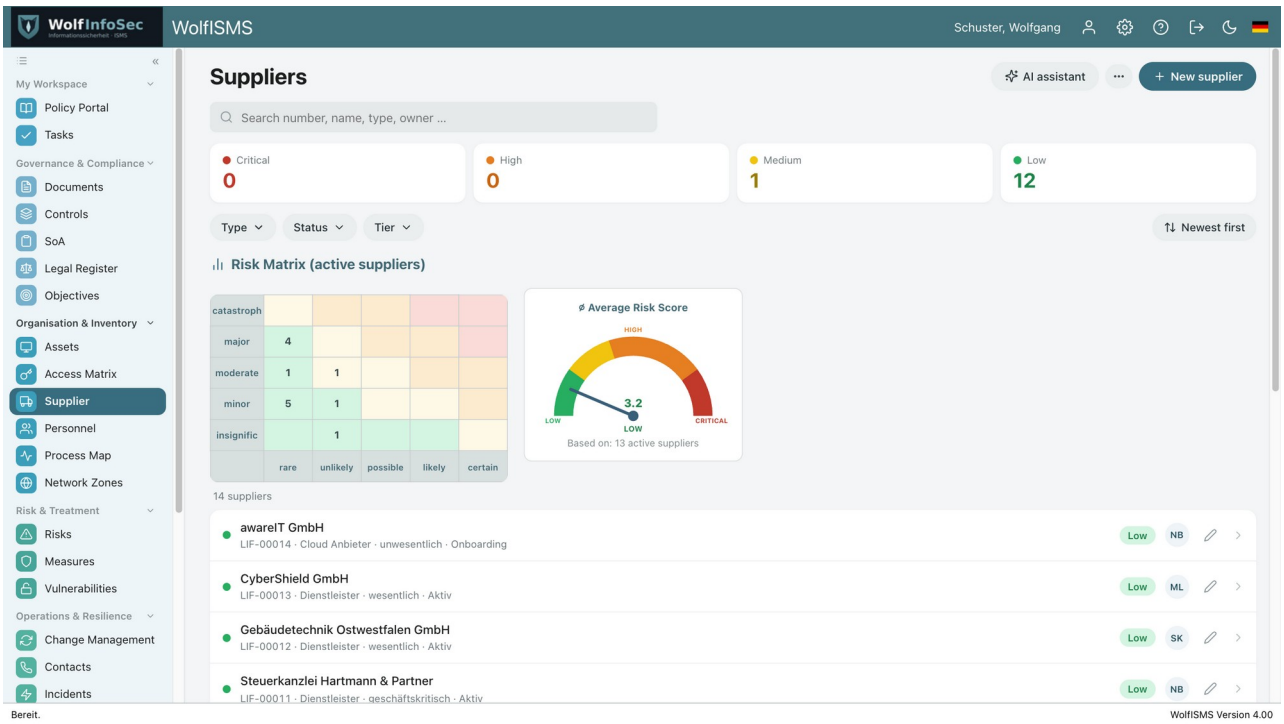
Description

The policy portal is the employee portal for the company's policies. Employees without ISMS editing rights can read the documents assigned to them here and confirm that they have read them.

Features

- **Policy display**: Since v4.00 the portal shows policies only; the selection of document types has been dropped. Read status and Excel export are likewise limited to policies
- **Mandatory and optional documents**: which documents you have to read depends on your role since v3.71. The mandatory reading appears at the top and is labelled "Not read" until you have acknowledged it; all other documents carry the label "Optional" – you may read and acknowledge them, but you do not have to. If there is no reading obligation for your role at all, the text below the heading says so
- **Read confirmation**: Clicking "Read" marks the document as confirmed. Since v3.90 the time is recorded as well; the awareness report shows it as the last confirmation. Earlier confirmations still count, just without a date. Only then does the entry disappear from your open tasks
- **Read status**: Overview of which documents have already been confirmed. Administrators and master users reach the evaluation across all employees directly through the "Reading status" button in the portal
- **Attachments**: if files are attached to a policy, you open them straight from the portal – without access to the documents module. Documents not yet read appear at the top of the list
- **Read status reset (master)**: Master users can reset the read status of individual documents – for example after a substantive revision, when all employees should confirm again
- **Reading obligation matrix (master)**: the button "Reading obligation matrix" opens a cross table of released documents and roles. A tick means: whoever holds this role must read and acknowledge the document. A row without any tick – the state of every newly released document – means nobody has to read it; the document stays visible and can still be acknowledged voluntarily. The roles themselves and their assignment to users are maintained by the administrator under Administration → Roles
- **Export**: Export of the read status as .xlsx
- **Bilingual**: Display in German or English depending on the user setting
- **Notification**: as soon as a policy that is mandatory reading for your role is approved, an email arrives with a direct link to the document in the portal. If the document is not assigned to any role, no mail goes out. If you would rather not receive mail from WolfISMS, contact your administrator

© 2012–2026 WolfInfoSec GmbH


WolfInfoSec
WolfISMS
Schuster, Wolfgang
My Workspace
Policy Portal
Tasks
Governance & Compliance
Documents
Controls
SoA
Legal Register
Objectives
Organisation & Inventory
Assets
Access Matrix
Supplier
Personnel
Process Map
Network Zones
Risk & Treatment
Risks
Measures
Vulnerabilities
Operations & Resilience
Change Management
Contacts
Incidents
Suppliers
AI assistant
New supplier
Search number, name, type, owner ...
Critical 0
High 0
Medium 1
Low 12
Type
Status
Tier
Newest first
Risk Matrix (active suppliers)
catastroph
major 4
moderate 1 1
minor 5 1
insignific 1
rare unlikely possible likely certain
Ø Average Risk Score
HIGH
LOW
3.2
LOW
CRITICAL
Based on: 13 active suppliers
14 suppliers
awarelT GmbH
LIF-00014 · Cloud Anbieter · unwesentlich · Onboarding
Low NB
CyberShield GmbH
LIF-00013 · Dienstleister · wesentlich · Aktiv
Low ML
Gebäudetechnik Ostwestfalen GmbH
LIF-00012 · Dienstleister · wesentlich · Aktiv
Low SK
Steuerkanzlei Hartmann & Partner
LIF-00011 · Dienstleister · geschäftskritisch · Aktiv
Low NB
Bereit.
WolfISMS Version 4.00

26. Contacts

Description

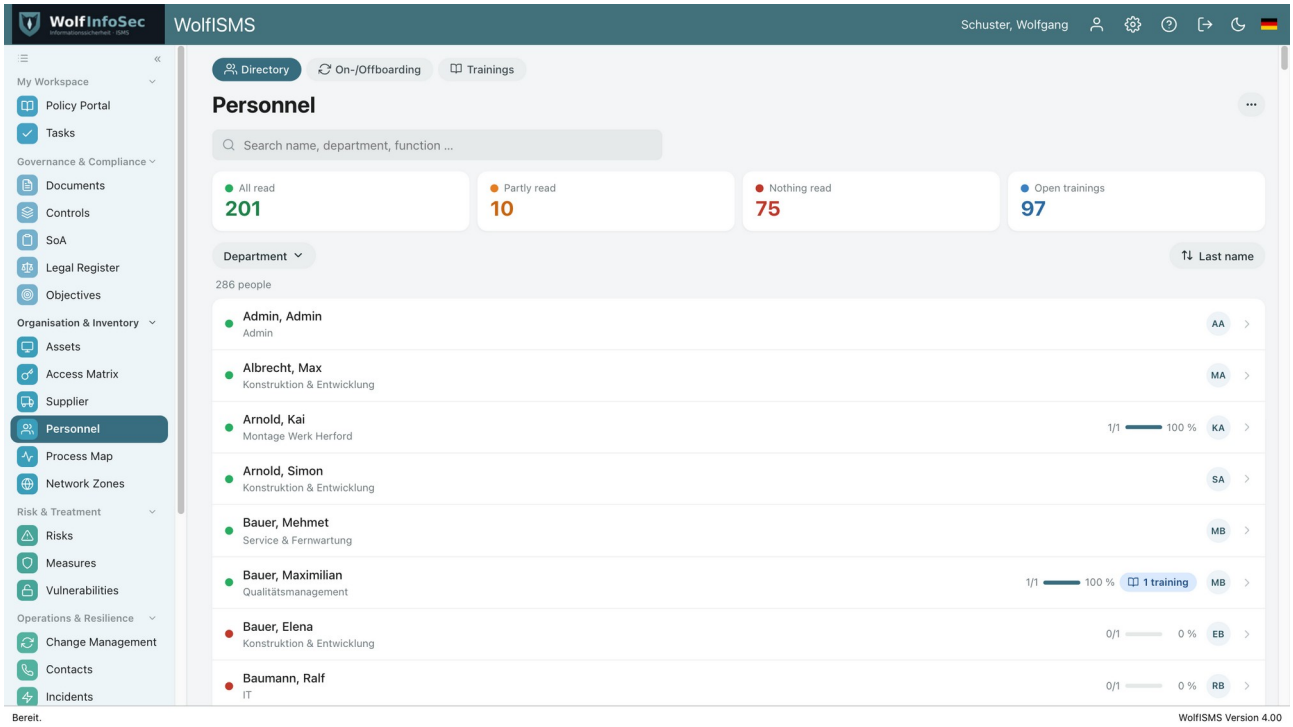
The contacts module is the central address book of the ISMS. It manages four categories of contacts in separate tabs: internal employees, external service providers, authorities and interest groups (e.g. associations, NGOs, partner organisations). The module supports the documentation of relevant points of contact per ISO 27001 and NIS 2.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

Features

- **Four tabs**: Employees, service providers, authorities and interest groups – each category in its own overview table with search and filtering
- **Contact data**: Phone, mobile, email (clickable as a mailto link), website, department, position, location and remarks
- **Statistics tiles**: Number of entries per category at a glance
- **Detail view**: Complete contact information on a dedicated page
- **Create / Edit / Delete**: Full functionality for users with editing rights (kontakte ≥ 2)
- **Interest groups**: Additional fields for type (e.g. association, NGO) and relevance (high/medium/low)

Permission: kontakte (0 = no access, 1 = read, 2 = edit) – URL: /kontakte



© 2012–2026 WolfInfoSec GmbH

27. BCM – Business Continuity Management

Description

The BCM module supports the planning and monitoring of business continuity per ISO 22301 and ISO/IEC 27001 (A.5.29, A.5.30). The starting point is the assets: for an asset – usually a business process or an information asset – the business impact analysis assesses how severe an outage becomes over time. Contingency plans and BCM exercises are assigned to an asset as well.

Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

The recovery objectives RTO, RPO and MTPD are held on the asset itself and maintained in the asset module; the BIA displays them.

Changed with v3.84: no separate critical processes any more.
Up to v3.83 BCM kept a process list of its own. It has been dropped – processes are kept as primary assets. An older BIA that still refers to a former process shows “formerly process: …”; assign an asset to it via ✏ and enter RTO, RPO and MTPD on the asset.

Features

- **Business impact analysis (BIA)**: the start page of the module. For each asset the consequences of an outage are rated in four dimensions – financial, operational, regulatory, reputation – across the time steps 1 h, 4 h, 24 h, 72 h and 1 week (1 = insignificant to 4 = critical). This yields an overall score rated low, medium, high or critical. Every BIA carries a number in the format BIA-00001.
- **Overview**: list of all BIAs with asset, asset owner, overall score, the highest value per dimension and RTO/RPO/MTPD. The tiles count the BIAs recorded, the critical ones and the primary assets without a BIA.
- **Recovery objectives**: RTO (recovery time), RPO (tolerated data loss) and MTPD (maximum tolerable period of disruption) are highlighted in colour – the shorter, the more critical. They are maintained on the asset.
- **Contingency plans**: contingency plan, recovery plan, communication plan, crisis team plan, IT contingency plan and other – with version, validity, status workflow (draft → in review → approved, withdrawn) and the asset the plan applies to.
- **BCM exercises**: tabletop, functional exercise, full-scale exercise and technical test with date, participants, result (passed, partial, failed) and findings, assigned to the asset exercised.
- **Measures from exercises:** since v3.95 measures can be assigned to an exercise – existing ones via “Manage” in the section Measures of the sidebar, new ones with “New measure & link”, which are linked at once. The measure shows the exercise as the back reference “BCM exercises”. This requires the editing permission for BCM, for creating additionally the one for measures.
- **Bilingual content**: titles and texts can additionally be maintained in English.
- **Excel export**: “Excel export” on the right of the tab bar. The sheet “Coverage” shows per asset the BIA score, approved plans and the last exercise and names the gaps – no BIA, no approved plan, never exercised, exercise older than twelve months, last exercise failed. Plus one sheet each for the BIA (highest value per dimension and from which time step the impact becomes significant), the contingency plans (expired ones red) and the exercises

© 2012–2026 WolfInfoSec GmbH

- **Exercise report (PDF)**: in the detail view of an exercise. Header data and result, the recovery objectives of the asset exercised, the related contingency plans – a plan expired on the day of the exercise is shown red –, participants, findings, earlier exercises of the same asset and an approval block

Permission: bcm (0 = no access, 1 = read, 2 = edit) – URL: /bcm

© 2012–2026 WolfInfoSec GmbH

28. REST API and API Key Management

Description

WolfISMS offers a REST API that lets external systems create and query records automatically – a SIEM reports incidents, a ticket system fetches open measures, a CMDB reconciles the asset inventory, a purchasing system reports suppliers, a vulnerability scanner delivers its findings, a reporting tool reads risks. Access is secured by API keys, which only administrators manage. Every key is stored as a SHA-256 hash and is visible in plain text only once, when it is created.

Availability: The REST API is part of the add-on “+” – Essentials Plus and Advanced Plus, recognisable by the “+” in the licence code – and of Enterprise (ENT). In the other editions the API key administration is missing and every API call ends with status 403. Keys already issued remain stored and become valid again as soon as a matching licence is installed.

This chapter gives the overview. Anyone building an integration will find the full description with all fields, filters and examples in the separate document “WolfISMS REST API”.

API Key Management (/admin/api_keys)

- **Creating a key:** The administrator enters a description; the system generates a cryptographically secure 64-character hex key. It is shown in plain text only once and must be copied immediately
- **Enable / disable:** Keys can be blocked and re-enabled at any time without deleting them
- **Delete:** Removes a key for good; afterwards every request using it is rejected
- **Overview:** All keys are listed with description, creation date and status

Areas and Endpoints

Every request must send the X-API-Key header with a valid, active API key. The six areas are cut the same way; <area> stands for incidents, massnahmen, assets, risiken, lieferanten or schwachstellen.

Endpoint	Function
POST /api/v1/<area>	Create a record. The number is assigned by the calling system and must be unique – only for vulnerabilities does WolfISMS assign it on request
GET /api/v1/<area>	Query a list: filters, full-text search, a freely chosen date field, sorting and pagination via limit and offset. The response contains total, count and items
GET /api/v1/<area>/<number>	Retrieve a single record as JSON
PATCH /api/v1/<area>/<number>	Acknowledge the synchronisation state. Business content deliberately cannot be changed through the API – that is what the interface is for. Exceptions are the additional owners, which can be maintained everywhere except for incidents, and vulnerabilities, where status, score and owner may also be written back
GET /api/v1/<area>/werte	Permitted values from the master data – for assets, risks, suppliers and vulnerabilities. A client should query them rather than hard-coding them

© 2012–2026 WolfInfoSec GmbH

The API is not throttled: a sync client may read and acknowledge every few seconds. It is protected by the API key alone – so create a separate key for every connecting system and delete the ones no longer needed.

What the synchronisation fields mean.
Every record carries the fields sync and synctime. sync = 0 means “not yet transferred”, sync = 1 “transferred”, and empty means “not intended for transfer”. This way WolfISMS remembers the state, not the connected system – a client that is rebuilt therefore does not resend old records.

© 2012–2026 WolfInfoSec GmbH

29. Objectives

Description

The Objectives module documents the corporate objectives and the information security objectives derived from them (ISO 27001 clauses 5.2 / 6.2) and tracks their achievement using freely definable key figures (KPIs) with a complete history.

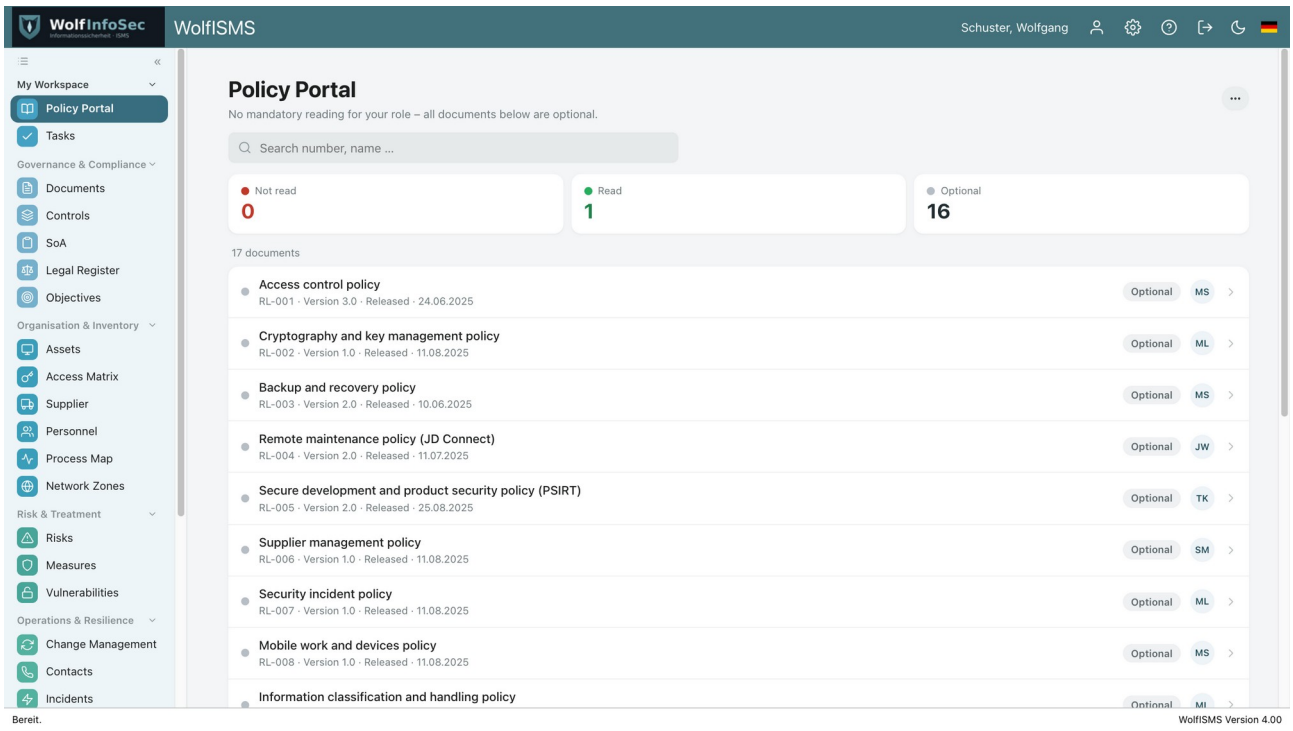
Availability: The module is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing and a direct call ends on a notice page; the recorded data is preserved and is there unchanged once a matching licence has been installed. If the module is missing despite a matching licence, the administrator has switched it off under Administration → Modules.

Features

- **Corporate objectives**: Expandable free-text field for the overarching corporate objectives (e.g. growth, customer satisfaction, market position)
- **Information security objectives**: Expandable free-text field for the security objectives derived from them (e.g. availability, confidentiality, integrity of critical systems)
- **Create KPIs**: Freely definable key figures with name, description, unit, target value and direction (higher is better / lower is better)
- **Record a value**: Every measured value is stored as a new history entry and never overwritten – the current value is always the most recent entry (complete audit trail)
- **History**: Line chart per KPI with the target value marked, plus a tabular value history including comment, author and timestamp
- **Trend indicator**: Arrows show the development compared to the previous measurement (increased / decreased / unchanged)
- **Colour coding**: The current value is highlighted green (target met) or red (target missed), depending on the chosen direction
- **Bilingual**: Separate fields for the German and English display of objective texts as well as KPI name, description and unit
- **Use in the management review**: The KPIs maintained here appear automatically in the section "Achievement of the information security objectives" of the management review
- **KPI report**: choose the period – the last twelve months are preset –, then “KPI report (PDF)” or “Excel”. The PDF contains the information security objectives, an overview with target, latest value, share of values on target and trend, and per KPI the history chart and the values with comments; the Excel workbook holds all values of the period. Track phishing click rates or training rates as KPIs and they appear in the report

Permission: ziele (0 = no access, 1 = read, 2 = edit), which administrators and master users need as well – menu: Governance & Compliance, URL: /ziele

© 2012–2026 WolfInfoSec GmbH



© 2012–2026 WolfInfoSec GmbH

30. External Links

Description

The External Links module offers a central collection of references to external systems that are frequently needed in day-to-day work, e.g. a ticketing system, a KPI system or SharePoint.

Features

- **Link list**: Overview of all stored external links with label and target URL, clickable in a new tab
- **Add**: Record new links with a label and a URL
- **Delete**: Remove links that are no longer needed

Permission: custom (0 = no access, 1 = access) – URL: /custom

© 2012–2026 WolfInfoSec GmbH

31. Reports

Description

Since v3.90 the menu entry “Reports” brings all reports and exports of the ISMS together in one place. The cards are grouped by their role in ISO/IEC 27001 – management system, risks and measures, operations and controls, people and awareness – and each names its clause. The page itself produces nothing: every button leads to the report in the module concerned, where it can still be found as well.

Availability: The reports overview is part of the Advanced (ADV) and Enterprise (ENT) editions. In Free and Essentials the menu entry is missing; the individual reports remain available in their modules.

Overview of the Reports

Report	Format	In module	Clause
Management review	PDF, PowerPoint	Management Review → open a review	9.3
Audit report	PDF	Audit → open an audit	9.2
KPI report	PDF, Excel	Governance & Compliance → Objectives	6.2, 9.1
ISO/IEC 27001 status, SoA, NIS-2	Page	Controls	4–10, 6.1.3 d
Risk report	PDF, Excel	Risks	8.2, 8.3
Measures, projects	Excel	Measures or Projects	6.1.3, 8.3
Reporting deadlines	Page	Incidents	A.5.24–5.26, NIS-2
Security incidents	Excel	Incidents	A.5.24–5.28
Vulnerabilities and patch status	Excel	Vulnerabilities	A.8.8
Change management	Excel	Change Management	A.8.32
BCM, exercise report	Excel, PDF	BCM	A.5.29–5.30
Assets, access matrix, suppliers, legal register, documents	Excel	the module concerned	A.5.9, A.5.15–5.22, A.5.31, 7.5
Awareness report	PDF	Personnel	7.3, A.6.3
Personnel and reading status	Excel	Personnel	7.2

Features

- **Only what you may see**: a card appears only if the module is switched on, your licence includes it and you hold the module permission – the same rules as in the main menu. Groups without a visible card are left out

© 2012–2026 WolfInfoSec GmbH

- **Individual objects**: the audit report, management review and BCM cards offer the most recent audits (PDF and short report), reviews (PDF and PowerPoint) and exercises (exercise report) directly
- **Period**: you choose the period of the KPI report right on the card; the last twelve months are preset
- **Reporting deadlines**: the card shows how many reporting deadlines are open and how many are overdue
- **Filters**: called from the reports page, the Excel exports are unfiltered. Called from a module list, they take over the filters set there

Notes

A report shows the data at the moment it is generated; the date of generation is in its header. If your administrator has set up a PDF letterhead, it lies under every page of the PDF reports.

© 2012–2026 WolfInfoSec GmbH

32. Administration

Description

The administration area provides complete user management, permission assignment and system monitoring. It is accessible only to users with the admin permission. A detailed description of all functions is contained in the administration documentation.

Users and Organisation

- **Admin overview**: Statistics tiles (users, activities) and quick links to all sub-areas
- **Company**: At /admin/unternehmen the master data of your own organisation is held – name, address, legal form, number of employees, revenue class, sites, industry and NACE code. It describes the context of the organisation (ISO/IEC 27001, clause 4); number of employees and revenue class additionally determine the size category under NIS2. It is the only system setting master users may maintain as well
- **All users**: Complete user list with search, role tabs, alphabet filter and permission badges
- **Create / edit user**: Define user permissions, master data, language and roles. The roles are a multiple selection – a user can be the information security officer and the data protection officer at the same time
- **Enable / disable account**: An account can be blocked without deleting it – blocked users cannot sign in, neither by password nor via SSO
- **Absence**: the absence with deputy can also be recorded for another user – via the user list
- **Import users**: Import user master data from a file
- **Password reset**: Reset a user's password as an administrator
- **Departments and teams**: At /admin/abteilungen departments and teams are maintained centrally – with a head and a parent/child structure. All modules then select the department from this list instead of typing it freely
- **Org chart**: The button "Graphical view" in the department administration opens the org chart – the same data as a tree. Boxes can be re-assigned by dragging, a click opens name, head, parent department, description and colour. The root is the company name from the company data. The graphic can be exported as PNG or SVG or printed directly
- **Departments as Excel**: The department list can be downloaded as a workbook and read back in – with the parent department and the head in plain text, so that the workbook can also be extended by hand. The import never deletes, never guesses and only writes after the preview with the checkbox ticked
- **Process map and network zones**: Two further graphical views, since v4.00 menu entries in the group Organisation & Inventory. Access is governed by the permissions prozesslandkarte and netzwerkzonen (1 = read, 2 = edit), which administrators and master users need as well. The process map arranges the processes into management, core and support processes; the network zones show the network segmentation from the external networks through DMZ, internal networks and OT to the high-security zone; the administrator adjusts the bands of both maps under Administration → Categories. Both work like the org chart: drag, click, export as PNG or SVG. Owner, department and a linked document (process description or network concept) are shown in the side panel
- **Plans & Registers**: repository for network and process diagrams (PNG, PDF, draw.io) and the asset register as a spreadsheet – for administrators and master users, reached via the tile in the admin area
- **Activity log**: Complete log of all system activities; filters by area and user
- **Excel exports**: User list with permissions and the activity log as .xlsx

© 2012–2026 WolfInfoSec GmbH

Catalogues and Master Data

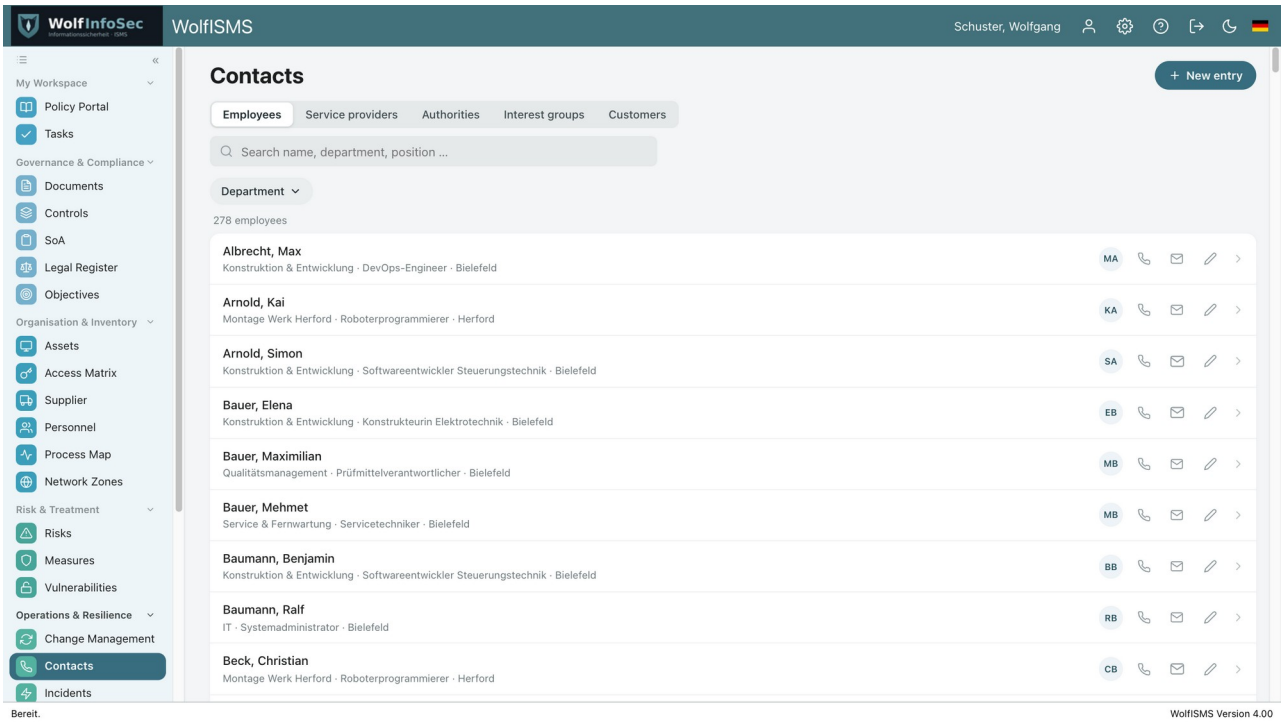
- **Master data**: Management of drop-down values (status, types, categories)
- **Categories:** under Administration → Categories the administrator maintains on one page the categories of incidents, change management, the legal register and contacts (service providers) as well as the bands of the process map and the network zones: create, rename (German and English, for the bands and the legal register also the colour), sort and delete. A category still in use cannot be deleted; renaming a category changes all entries that use it. Asset, risk, threat and vulnerability categories are reached through tabs on the same page and are still maintained in their own forms
- **Threats & vulnerabilities**: Maintenance of the catalogues used when linking a risk in the risk module
- **Impact / risk scale**: Configuration of the names and descriptions of the 5-point impact scale
- **Asset categories**: Maintenance of the OBASHI categories of asset management
- **Risk categories**: Maintenance of the category list of the risk module
- **Supplier types**: Maintenance of the type list of the supplier module; a tick marks cloud/SaaS types whose suppliers need a cloud exit strategy
- **Risk parameters**: Configuration of the scoring weights and thresholds for the automatic supplier risk assessment
- **Roles**: At /admin/rollen the company-wide roles are created, renamed and assigned to users; the list also shows who holds each role. It is the same role list as in the role catalogue of the access matrix (/zugriffsmatrix/rollen) – which additionally carries the short code, the active flag and the remaining catalogue fields. A role that is still in use cannot be deleted. The tile is open to master users as well
- **Reading obligation matrix**: which role has to read which released document is defined by the master user in the policy portal under "Reading obligation matrix". A newly released document carries no reading obligation at first – it is set once, deliberately. Without an assignment the document stays visible in the portal but triggers neither tasks nor reminder mails

System and Operations

- **Email / SMTP**: Configuration of the outgoing mail server for task emails and notifications; test mail function
- **Single sign-on**: At /admin/sso the sign-in via Microsoft Entra ID and via Google can be set up – credentials, permitted email domains and the question whether unknown users are created automatically as read-only accounts. A switch at the top of the form decides whether these values apply or those from the server configuration. "Save & check discovery" tests the connection to the provider; no restart is required
- **Cron times**: Setting the time and interval of the background jobs (task reminder, risk score snapshot). Each job can also be triggered manually at once
- **Backup & restore**: Download of a combined backup (.tar.gz) of the database dump and the uploaded files; restore by upload. Before files are restored, the previous uploads folder is automatically preserved as a timestamped copy
- **Updates**: Checks the bundled JavaScript libraries – editor and BPMN modeller – and updates them. Since v4.00 new WolfISMS versions are installed by the operator of the installation, no longer by the application itself. Not available in containerised installations
- **Framework import**: Import of framework chapters from CSV/JSON as well as direct installation from an online framework catalogue; frameworks that already exist are detected automatically
- **Data SQL export/import**: Export and import of the master data of documents, risks and measures between WolfISMS instances – individually or as a combined package. Imported records are reset to a fresh editing state; attachments, histories and links are not transferred

© 2012–2026 WolfInfoSec GmbH

- **Modules**: At /admin/module every module can be switched on and off individually and its position within its menu group set by dragging or with the arrow buttons; each row shows its group. A deactivated module disappears from the menu, its pages and its REST area are blocked; recorded data is kept and is there unchanged once the module is switched on again. The policy portal cannot be switched off, because read-only users would otherwise have no destination left
- **2FA / TOTP**: Enable or disable system-wide two-factor authentication
- **AI settings**: Configuration of the AI support for the AI assistants of all modules, the AI translation and the Word import: provider (Anthropic, OpenAI, Mistral, Google Gemini, nele.ai, Azure OpenAI, Microsoft Copilot or an OpenAI-compatible service), model, API key – for Azure OpenAI and Copilot optionally sign-in via Microsoft Entra ID –, base URL and an optional prompt addendum. AI functions are available in every paid edition; in the free edition the area is locked
- **Design & colours**: colour scheme of the interface at /admin/design – teal (default), classic with the original colours or, since v4.00, black / grey / white. In addition there are dark mode as default (every user can switch for themselves), the header bar colour and the switch for the info tiles above the module lists, hidden by default. The setting applies to all users; Excel, Word and PDF exports are unaffected, as are the risk matrix, the risk level tiles and the score gauges, which always show green to red
- **Branding**: Upload of your own company logo (PNG), a Word template for exports and a PDF letterhead for document exports
- **Ticket system**: URL template through which the number of an incident links to the ticket system
- **Licence**: Upload of a licence file (*.lic)
- **Administrator manual**: Download the administration documentation as a PDF directly from the application
- **About**: Version, licence and licence terms of the installation – since v4.00 a tile under System and Operations instead of the logo at the top right
- **Back to the overview**: On every administration page “‹ Administration” leads back to the overview



33. Frequently Asked Questions (FAQ)

I cannot see a module – what should I do?

If a module is missing from the navigation menu or you receive a "no permission" message, you lack the corresponding right. Contact your system administrator, who can assign it at /admin/change_user. An administrator can also switch a module off entirely under Administration → Modules; it then disappears from the menu for every user, while the recorded data is preserved. It is also possible that the edition of the licence does not include the module: objectives, personnel, contacts, reports, projects, the operational plan, audits, the management review, vulnerabilities, the legal register, playbooks, BCM and the access matrix are part of the Advanced edition, the REST API is part of the add-on “+”, and the AI features require a paid edition. In that case calling the page directly shows a notice naming the edition required.

Collapsed group: before you ask your administrator, check whether the module’s group is collapsed in the menu – then only its heading is shown. Clicking it opens the group again.

I suddenly cannot save anything – why?

There are usually two causes: either your account has been given the readonly permission, or the system licence has expired. In the second case all modules remain readable, but every save button is disabled until the administrator installs a valid licence. If, on the other hand, only creating new assets, risks, documents or suppliers is blocked, the volume limit of the free edition has been reached – see the following question.

Can an entry have several owners?

Yes. In risks, assets, documents, measures, projects, controls, suppliers, incidents, vulnerabilities and changes you tick several people in the field “Owner” (or “Responsible”). Each of them may edit the entry and is reminded of due tasks.

Why can I not create another asset, risk, document or supplier?

If WolfISMS runs without a licence file, that is in the free edition, these four areas are limited to ten entries each. Once the limit is reached the form for a new entry no longer opens and the application reports: The free edition is limited to 10 assets. Everything already recorded stays visible, editable and exportable – only creating is blocked.

You have two options: delete an entry you no longer need, which releases the slot immediately, or ask your administrator for a paid licence, which removes the limit. For documents, by the way, the document numbers are what counts: a new version of an existing document can still be created once the ten are reached.

How do I change my password?

Click your name in the top right corner and select "Change password". The new password must be at least 10 characters long and contain upper and lower case letters as well as a digit. If you sign in via Microsoft or Google, manage your password there rather than in WolfISMS.

What does "read only" mean?

Users with the readonly permission can read the content visible to them through the policy portal but cannot create, edit or delete data. All save and edit buttons are hidden.

© 2012–2026 WolfInfoSec GmbH

How do I export data to Excel?

Every module list has a three-dot menu at the top right with the entry Export. The export contains the currently filtered view as an .xlsx file that opens directly in Microsoft Excel.

How does the document workflow work?

Documents pass through three stages: (1) in progress – edited by the owner. (2) to be reviewed – a reviewer confirms the content. (3) approved – the approver grants formal approval. A new version resets the process to "in progress". Every save keeps a version of its own; the approved version stays alongside it until the new one is approved.

How do I get to an earlier version of a document?

Open the document and look at the Versions panel on the right: every version is listed there with its number, status and date, and one click opens it. If you want to carry on from an old version, choose Restore – its content is then taken over as a new working copy and goes through review and approval as usual. Nothing is deleted or overwritten in the process.

How do I import a Word document?

Create a new document or open an existing one for editing. Above the form sits the box “Import from Word”: drag the file into it or select it and click Import – the content is then in the editor, headings, lists, tables and images included. Check it and then save; before that nothing is in the database. If AI is switched on, it processes the text right away on request. .docx files up to 16 MB are read – please convert older .doc files in Word first.

What is a read confirmation and where do I confirm?

A read confirmation can be required for policies. The documents concerned appear in your open tasks and in the policy portal. Open the document in the portal and click "Read" – the date and confirmation are stored and tracked as evidence in the personnel module. If a document is substantively revised, a master user can reset the read status; a fresh confirmation is then required. Since v3.71 the reading obligation depends on your role: only the documents assigned to your role are mandatory – all others carry the label "Optional" in the portal and count neither towards your progress nor towards your tasks or the reminder mails. Which roles you hold is maintained by the administrator; which role has to read what by the master user in the reading obligation matrix.

What is the access matrix for and how often must I review it?

The access matrix records which role may access which asset, who approved it and when the permission was last reviewed. You set the review frequency per permission (quarterly, semi-annually or annually). Due and overdue reviews are highlighted in colour; the list view with the "privileged" filter shows the critical cases first.

Why is my access matrix empty?

The matrix is built from two sources: the non-archived secondary assets (primary ones only via “Show primary assets”) and the active roles. If either side is missing, the view stays empty. Check whether assets of the selected category exist in asset management and whether roles are marked "active" in the role catalogue.

© 2012–2026 WolfInfoSec GmbH

Can I import BPMN diagrams from other tools?

Yes. In the BPMN editor you will find the "Import" button. .bpmn and .xml files from common BPMN tools such as Camunda Modeler, draw.io or Signavio are supported. The import happens directly in the browser.

How are supplier risks calculated?

The risk score is calculated automatically from several factors: processing of personal data, contract status, certifications, security level, potential impact, likelihood and tier criticality. Since v4.01 the tier counts double in the impact and sets a floor – a mission-critical supplier no longer ends up “low” just because it processes no personal data. The score feeds into the supplier risk matrix on the dashboard; every recalculation is recorded in the score history.

How do I set up two-factor authentication (2FA)?

If the administrator has enabled 2FA system-wide, you are prompted to set it up at your next login. You can also start it manually: click your name in the top right corner and select "Set up 2FA". Scan the displayed QR code with a TOTP app and confirm with the generated 6-digit code. To disable 2FA, select "Disable 2FA" in the same menu.

How do I work with the AI assistant for documents?

Your administrator has to enable AI and give you the permission “AI usage”; it requires a paid edition, Essentials or above. Then the button “AI assistant” sits in the document list and in the detail view. Say in the conversation what you have in mind – create a new document, upload and take over a template, revise or review a document. You can change the draft on the right yourself at any time; it is only saved with “Apply”, as a new draft version. Approved documents stay untouched until you create a new version.

Why can I not upload an attachment?

Attachments must be genuine PDF files and must not exceed 16 MB. A file that merely carries the .pdf extension but is internally a different format is rejected. In that case save the document as a PDF again.

Which AI assistants are there?

Since v4.00 every module has one: risks, assets, suppliers, documents, measures, vulnerabilities, changes, incidents, projects, controls, legal register, data protection, audits and playbooks. All are built the same way – a conversation on a page of its own, the chat on the left, the draft on the right – and reached via the button “AI assistant” in the list and in the detail view. What each assistant can do is described in the chapter of its module. It needs the same permission as editing in the module plus the permission “AI usage”, and nothing is saved without your confirmation.

Which data leaves the system in the process?

The details at hand – for example the risk, the document or the incident –, extracts from the catalogues needed for the step concerned and the conversation so far. Catalogues are truncated and pre-sorted by topic. Whether and with which provider the AI works at all is decided by your administrator.

What does the AI do for assets and gap assessments?

The AI assistant for assets creates new assets with you, suggests protection needs and recovery targets with a reason and finds links right through to the risks; it also reviews single assets, an OBASHI level or the entire inventory. In the audit the AI assistant formulates assessment questions

© 2012–2026 WolfInfoSec GmbH

for every requirement. Every AI dialog points out that AI-generated information must be checked before use – no liability is accepted for its correctness or completeness.

Why do the interface colours look different than before?

Since v4.00 WolfISMS has a new look – calmer lists, plain grey buttons and symbols instead of colourful pictures (see “The Interface since v4.00”). In addition, your administrator can set a colour scheme for the whole installation under “Design & colours”: teal, classic or black / grey / white. You choose light or dark yourself with the button next to the language flag. The risk matrix, the risk level tiles and the score gauges always keep their green-to-red colours, and so do Excel, Word and PDF exports.

Who receives my tasks while I am away?

The deputy you enter for the period under “Manage absence” on your account page. They see your tasks under “My Tasks” and receive your reminder emails; once the period is over everything falls back automatically. Without a recorded absence the tasks stay with you.

Where do I enter RTO, RPO and MTPD?

On the asset: in the edit form under “Recovery objectives”. The values are chosen from fixed steps, and the RTO must not exceed the MTPD. The BIA in the BCM module shows them for the asset assessed. Since v3.84 there is no separate process list in BCM any more.

Where do I find the reports for the audit?

In the menu entry “Reports”. It shows all reports and exports you have access to, with their reference to ISO/IEC 27001 – from the audit report and the management review to the awareness report.

Why does nothing happen when I open an action in a new tab?

Since v3.93 WolfISMS only carries out links that change data – linking and unlinking, deleting contacts, the read confirmation in the policy portal, supplier actions, the treatment plan – as a protected form request. That way no link on another website can trigger a change in your name. An ordinary click works as before. If you open such an action in a new tab with the middle mouse button or Ctrl-click, you only get a notice – click the link in the original tab instead.

Why does the sidebar show only five entries?

So that long lists do not push the other sections down. Since v3.94 every section with “Manage” shows five entries at most, followed by “more … (+N)”. The link opens the linking view with all entries. If you may not change the links, you see the complete list.

Why does a link also show on the other entry?

A link is stored on the entry where it was created. Since v3.94 the other side shows it as well – the change on the asset, for example, or DOK0001 on DOK0002 when DOK0001 refers to DOK0002. It is changed on the entry that created it; only between two documents can you remove it from either side.

How do I have a document translated into English?

Switch the interface to English and open the document. The detail view then shows the button “AI translation”. The AI translates the German text section by section; headings, tables and images stay as they are. You see German and English side by side and apply the result with one click –

© 2012–2026 WolfInfoSec GmbH

this creates a new version. The button is missing as long as the document has no German text, is approved or in review.

Where have the buttons for linking gone?

Since v3.95 you link via the sidebar: every section there – controls, risks, measures and so on – has the link “Manage” if you may change the links. The buttons of the same name in the bar above the content led to the same pages and have therefore been removed.

Why doesn't every field have an ⓘ?

Fields are explained when their meaning is not already clear from the label. Search and filter fields never have one.

My account is locked – what now?

After ten wrong passwords WolfISMS locks sign-in for this account for 15 minutes; the message states the remaining time. After that it simply works again. If you no longer know your password, use “Forgot password” on the login page in the meantime. Signing in via Microsoft or Google is not affected by the lockout.

How do I switch on dark mode?

With the button at the top right next to the language flag: the moon switches to dark, the sun back to light. The choice is stored with your account and applies on every device. If you have never switched, your administrator’s default applies.

Where have the tiles above the lists gone?

Since v4.00 the statistics and category tiles above the module lists are hidden at first so that the list itself takes centre stage. Your administrator can switch them on again for everyone under Design & colours. Filtering still works via the tiles with numbers and the filters directly above the list.

Why can I no longer page through the lists?

Since v4.00 every list shows all entries on one page. Type into the search field: the list filters immediately, and every word you enter must occur in the entry.

How do I write a playbook?

Open Playbooks and click “New playbook” at the top right. You enter title, description and text in the same editor as for documents; after “Save” the playbook appears in the list under “Written playbooks”. You need the Playbooks permission for this. Uploading PDF files and setting links work as before.

Why do I not see the module Data Protection?

The permission “Data protection” is off for every user at first, also after the update. Your administrator gives you read or edit; afterwards “Data Protection” appears in the menu under Governance & Compliance.

Who maintains the DPA of a supplier?

Whoever has the permission “Data protection” with edit – the supplier permission is not enough and not needed either. So the data protection officer can maintain the DPA details without changing the other supplier data. The block appears as soon as “personal data” is set to Yes or Partly for the supplier.

© 2012–2026 WolfInfoSec GmbH

34. Glossary

Term	Meaning
API key	Cryptographic access key for the REST API; stored as a SHA-256 hash and shown in clear text only once
Asset	Information-processing system, application or information of value to the organisation
Audit	Systematic review of the implementation of ISMS requirements
Backup	Combined backup archive (.tar.gz) of the database dump and the uploaded files
BCM	Business continuity management – systematic management to maintain business-critical processes during a crisis (ISO 22301 / ISO 27001)
BIA	Business impact analysis – assessment of the consequences of an outage of an asset for finance, operations, reputation and compliance across different time steps
BPMN	Business Process Model and Notation – standardised process modelling language
Break-glass	Emergency access through a sealed account that is activated only after a documented emergency procedure (level N of the access matrix)
Change	Change request (RfC) for a change to systems or configurations; approved by a board and reviewed after implementation (ISO 27001 A.8.32)
CIA	Confidentiality, integrity, availability – the core values of information security
CRA	Cyber Resilience Act – EU regulation on the cybersecurity of connected products
Deny by default	Core principle of the access matrix: without an explicit decision there is no access; every deviation must be justified and approved
DPA	Data processing agreement under Art. 28 GDPR between controller and processor (supplier)
DPIA	Data protection impact assessment under Art. 35 GDPR – assessment of the risks of a processing activity for the data subjects when the threshold analysis requires it
GDPR	General Data Protection Regulation – EU regulation on the protection of personal data
Incident	Security incident – an actual or potential breach of information security
ISMS	Information security management system – a systematic framework for managing information security
ISO 27001	International standard for ISMS (2022 edition)
AI editing	former button in the document module; since v4.00 the AI assistant for documents does this. The AI assistants of the modules need an AI provider enabled by the administrator
Comments	Discussion function per entry in assets, suppliers, risks, documents, measures, incidents and controls; editing and deleting only by the author or an admin
KPI	Key performance indicator – freely definable metric with a target value and a history for measuring objective achievement (Objectives module)
Read confirmation	An employee’s confirmation of having read a policy or training document; serves as evidence for security training
Management review	Review of the ISMS by top management per ISO 27001 clause 9.3
Measure	Concrete activity for risk treatment or compliance with a framework
master	User permission for extended system functions (approvals, all-tasks view, role maintenance)
MTPD	Maximum tolerable period of disruption – the longest acceptable period a process may be interrupted before unacceptable business damage occurs

© 2012–2026 WolfInfoSec GmbH

Term	Meaning
NIS 2	Network and Information Systems Directive 2 – EU directive on the cybersecurity of critical infrastructure
norm	User permission for editing controls and the legal register
OBASHI	Classification scheme for assets: Ownership, Business Process, Application, System,
	Hardware, Infrastructure – determines the order of the asset categories
Operational Plan	Module for recurring mandatory tasks (deadline calendar); on completion a new instance is created automatically and the previous one is preserved unchangeably as evidence
PIR	Post-implementation review of an implemented change; required before it can be closed
Playbook	Predefined response plan for security incidents
privileged	Marking of particularly far-reaching permissions (levels A and N of the access matrix) that receive separate attention during recertification
readonly	User permission for read-only access through the policy portal
Recertification	Recurring review of whether a granted permission is still required (ISO 27001 A.5.18)
Record of processing	Record of processing activities under Art. 30 GDPR (RoPA)
Review	Planned periodic review of an entry (asset, document, risk etc.)
Risk score	Numeric value derived from likelihood × impact
RPO	Recovery point objective – the maximum tolerable data loss in an outage
RTO	Recovery time objective – the maximum tolerable recovery time after an outage
SoA	Statement of Applicability – declaration of the applicability of the controls
SSO	Single sign-on – signing in with an existing company account via Microsoft or Google
Threshold analysis	Check whether a processing activity needs a DPIA – based on the list of the supervisory authority and the nine criteria of WP 248
Tier	Criticality level of a supplier (Tier 1 = critical, Tier 3 = uncritical)
TOTP	Time-based one-time password (RFC 6238) – a time-based one-time code used as a second authentication factor; generated by authenticator apps and valid for 30 seconds
Access matrix	Target overview of which role may access which asset and to what extent (ISO 27001 A.5.15 / A.5.18)

WolfISMS – Wolf's Information Security Management System

© 2012–2026 WolfInfoSec GmbH

Version: 4.01 | As of: November 2026