COMPLIANCE ASPEKTE

Release Notes

Version
9.0

Contents

Release 9.0 Summary

The new version contains several major updates such as re-branding of the tool (new name and UI improvements), Protection needs features, like distribution and cumulative principles, granular permission model (per asset or/and process), login with Azure AD, and many more.

Major Features

1. New product name and UI improvements

Infopulse Standards Compliance Manager (Infopulse SCM) compliance management tool changes its name to Compliance Aspekte as well as releases a new logo and several UI modernizations that will all support the product growth and strategy.

The new name represents what the product has evolved into after all these years: from managing standards compliance to covering all the aspects of compliance management. New Logo and UI redesigns underline the simplicity and modern touch we envision in the product.

2. Protection Needs

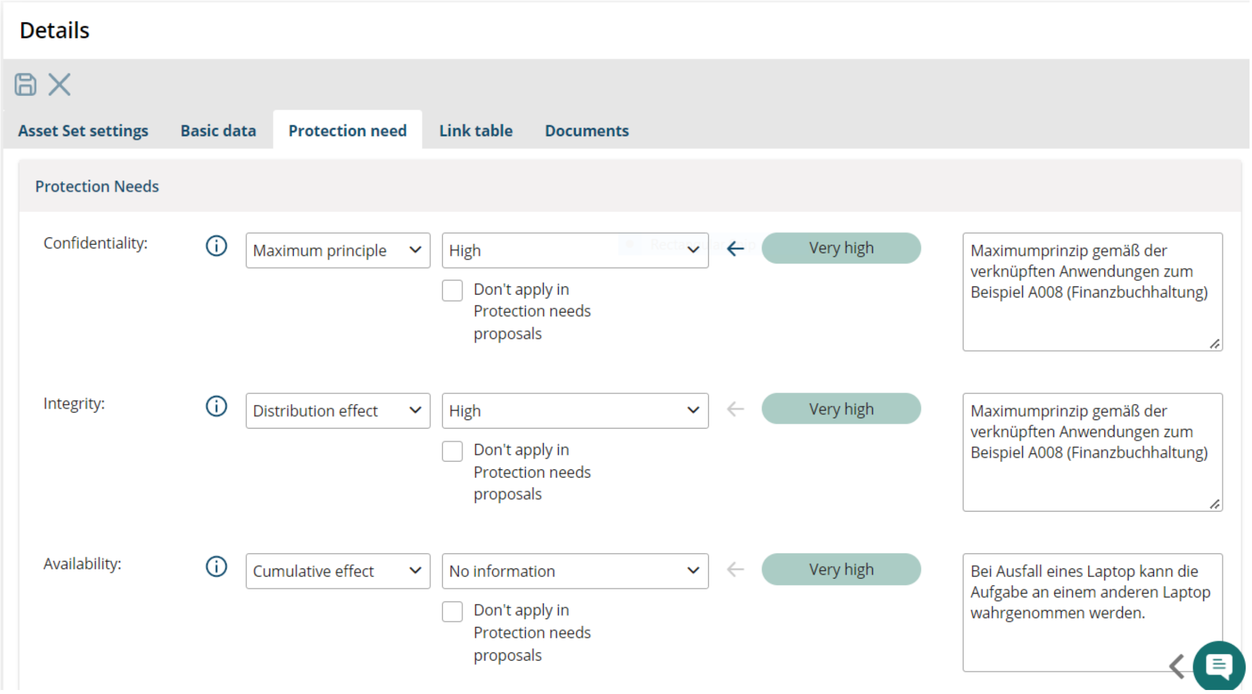
2.1 Support of Distributive and Cumulative principles

There are three principles when determining the protection needs – maximum principle, distribution, and cumulative.

Previously, only the maximum principle was supported. From this version, the other two principles were added: cumulative and distributio.

The Cumulative principle is used when damage is accumulated based on several minor damages. If the cumulative principle is selected for some protection goal of an Asset, the system does not allow applying protection need proposal for this Asset.

The Distribution principle is applicable when serious damage is distributed on several damages. If the Distribution principle is selected for some protection goal of an Asset, the system does not allow applying a proposal for this Asset.



Details

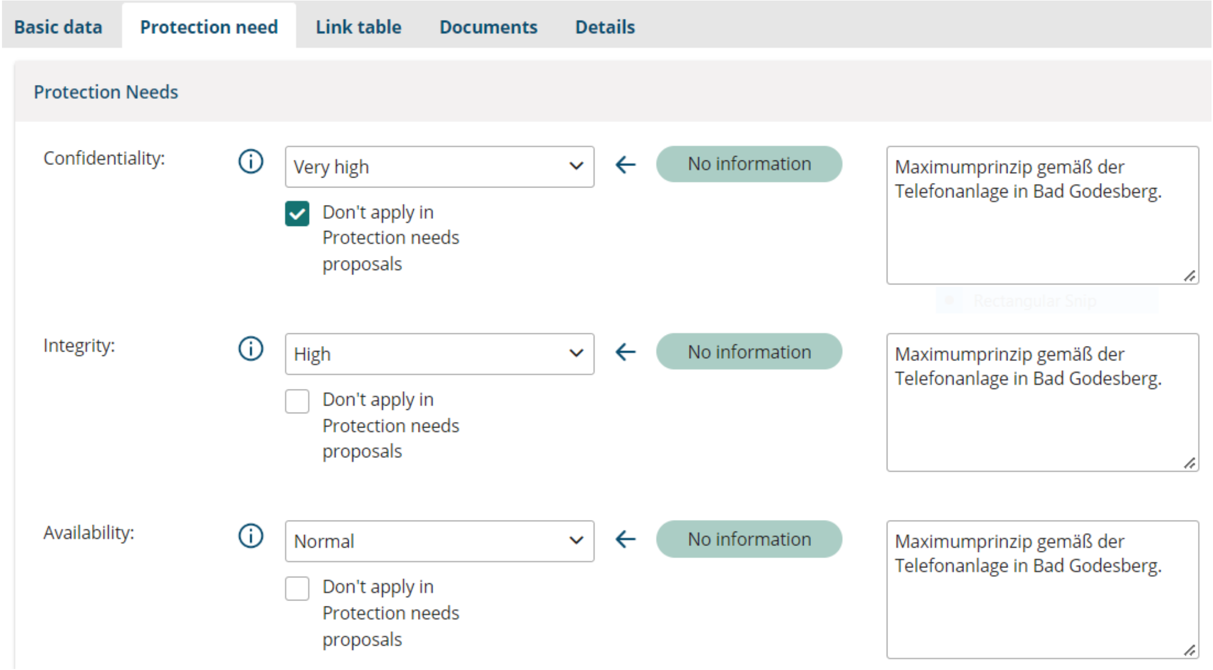
Asset Set settings | Basic data | Protection need | Link table | Documents

Protection Needs

Confidentiality:	Maximum principle	High □ Don't apply in Protection needs proposals	Very high	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
Integrity:	Distribution effect	High □ Don't apply in Protection needs proposals	Very high	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
Availability:	Cumulative effect	No information □ Don't apply in Protection needs proposals	Very high	Bei Ausfall eines Laptop kann die Aufgabe an einem anderen Laptop wahrgenommen werden.

2.1 Exclude protection need value from further Protection goals suggestions

The new checkmark *‘Don’t apply in Protection needs proposals’* was added for each protection goal (Confidentiality, Availability, Integrity, custom protection goals). When activated, the value of the protection need (e.g. ‘Very high’ for Confidentiality) will be excluded from the further suggestions of protection needs for all linked superordinate Assets.



Protection Needs

Confidentiality: Very high ← No information
☑ Don't apply in Protection needs proposals
Maximumprinzip gemäß der Telefonanlage in Bad Godesberg.

Integrity: High ← No information
□ Don't apply in Protection needs proposals
Maximumprinzip gemäß der Telefonanlage in Bad Godesberg.

Availability: Normal ← No information
□ Don't apply in Protection needs proposals
Maximumprinzip gemäß der Telefonanlage in Bad Godesberg.

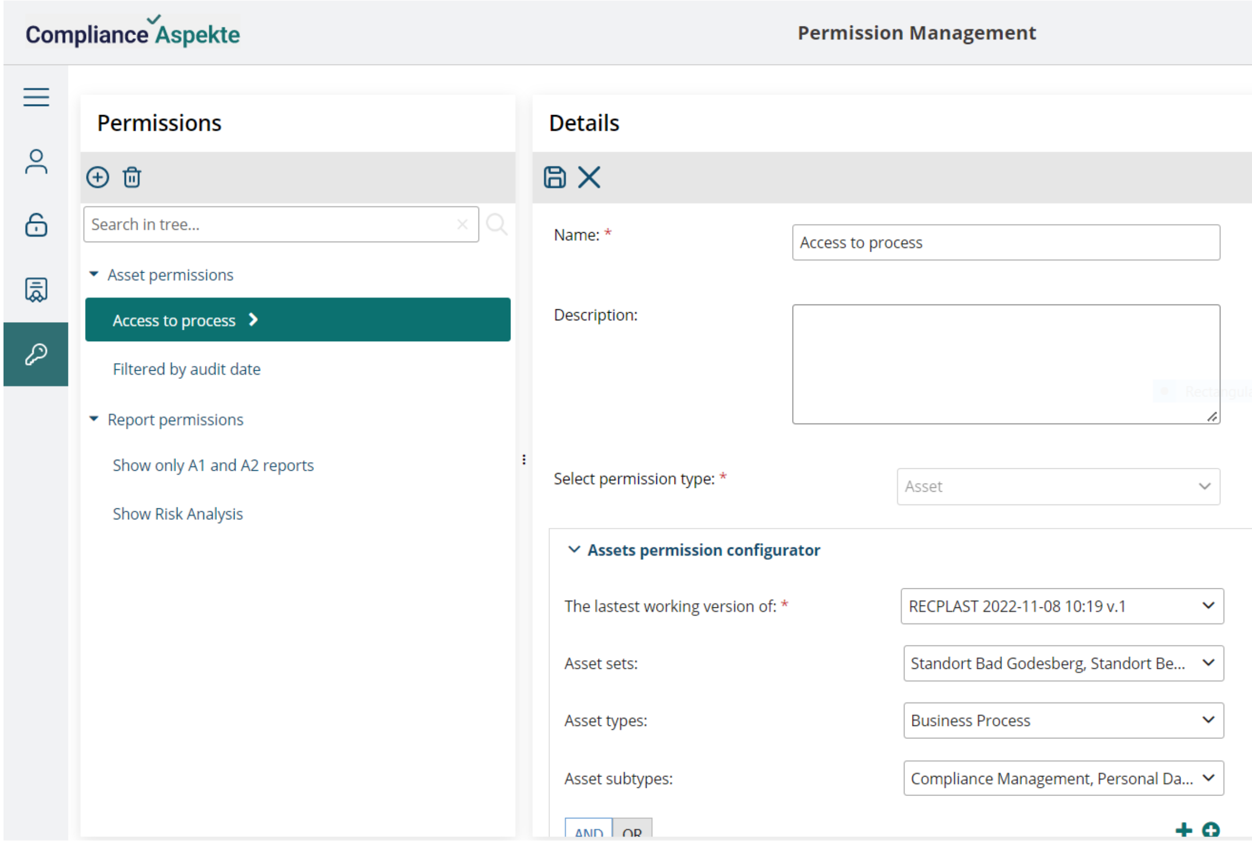
2.2 If Protection needs <High>/ <Very high>, then Requirements for Increased protection are applied automatically

If maximum of the Protection needs is <High>/ <Very high>, Requirements for Increased protection appear in Compliance Check for the Asset automatically.

3. Permission Management

3.1 Permissions per Asset

Granular permissions per Asset/Asset Group or Process can be set with the help of additional configurations.



- Asset permissions
  - Access to process
  - Filtered by audit date
- Report permissions
  - Show only A1 and A2 reports
  - Show Risk Analysis

Name: * Access to process

Description:

Select permission type: * Asset

Assets permission configurator

The lastest working version of: * RECPLAST 2022-11-08 10:19 v.1

Asset sets: Standort Bad Godesberg, Standort Be...

Asset types: Business Process

Asset subtypes: Compliance Management, Personal Da...

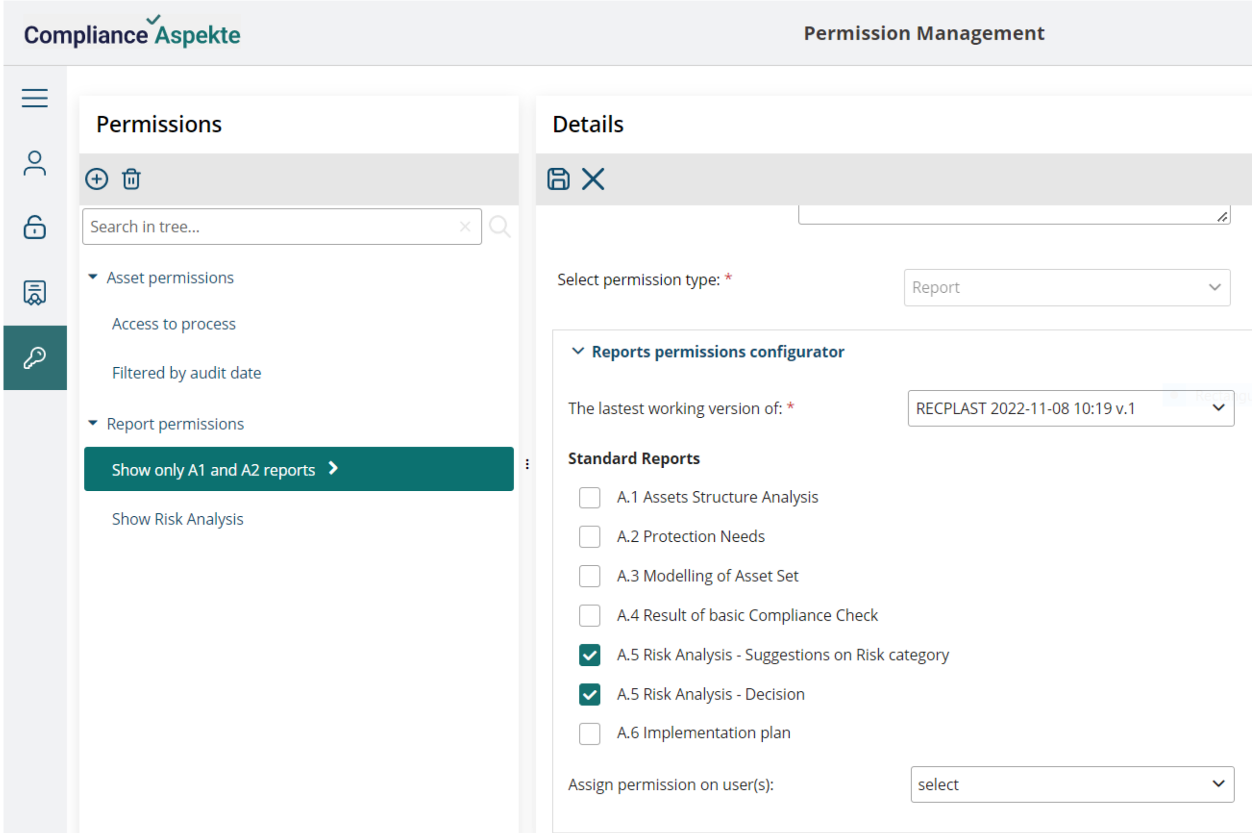
The selected user will see Assets in Inventory Analysis/Compliance Check/Risk Analysis and/or Reports according to the configured selection, based on access to some views (via a role).

3.2 Permissions for Reports

More detailed permission configurations for Reports allow giving access to some reports in a selected Concept.

Admin or user with the privilege “Manage Users’ in User Management can create shared filters in the Permission Management view.

After permissions are created, the selected user will see the defined reports list.



Compliance Aspekte

Permission Management

Permissions

Search in tree...

- Asset permissions
  - Access to process
  - Filtered by audit date
- Report permissions
  - Show only A1 and A2 reports
  - Show Risk Analysis

Details

Select permission type: * Report

Reports permissions configurator

The lastest working version of: * RECPLAST 2022-11-08 10:19 v.1

Standard Reports

☐ A.1 Assets Structure Analysis
☐ A.2 Protection Needs
☐ A.3 Modelling of Asset Set
☐ A.4 Result of basic Compliance Check
☑ A.5 Risk Analysis - Suggestions on Risk category
☑ A.5 Risk Analysis - Decision
☐ A.6 Implementation plan

Assign permission on user(s): select

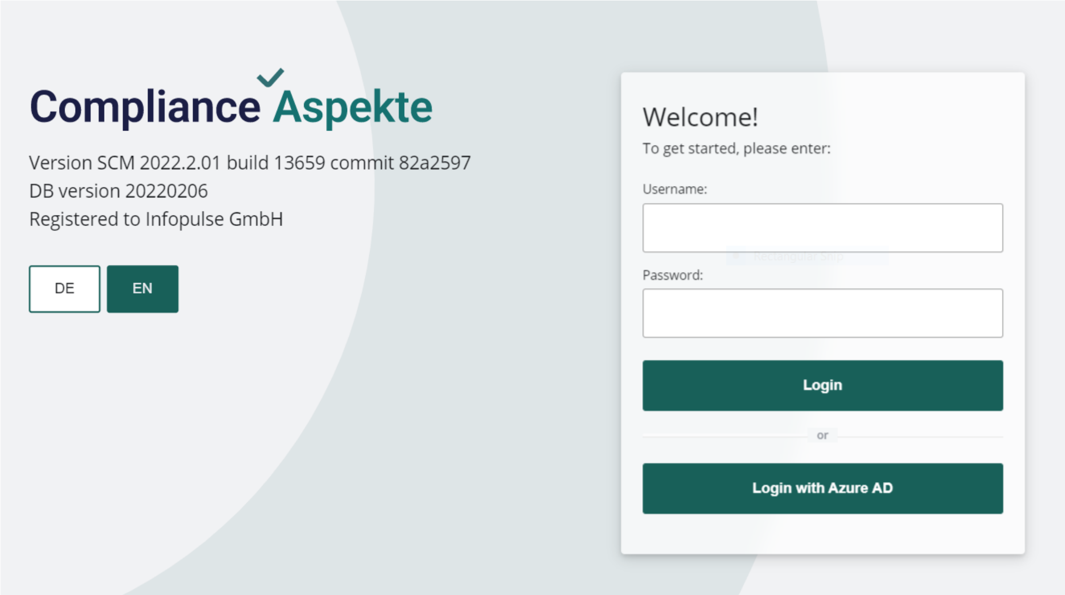
4. Azure AD login

Azure Active Directory (Azure AD) is an enterprise identity service that provides single sign-on, multi-factor authentication, and conditional access to protect against 99.9 percent of cybersecurity attacks.

From now on, the users of Compliance Aspekte can benefit from:

- Single Sign-On (SSO) and multi-factor authentication (MFA): user accesses all the applications with one set of credentials and has second-factor authentication, such as a phone call or text message.
- Increased security and compliance with possibilities to enforce strong authentication policies, restrict access to sensitive data, monitor user activity, generate reports on user activity

- Possibility to manage user accounts, assign permissions, and control access centrally, assign individual or user groups rights, without entering the application itself
- Reduce manual work as all user data is pulled automatically, the password (or other types of authentication) is also changed centrally



Compliance Aspekte

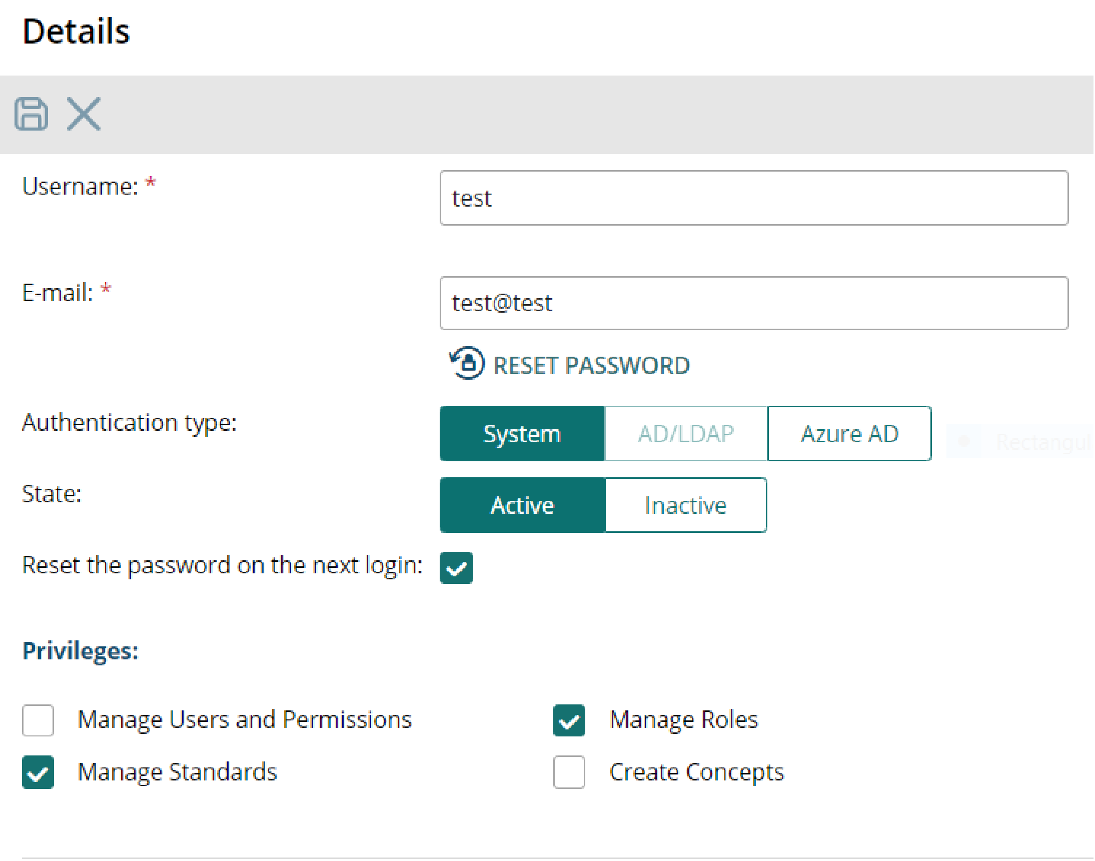
Version SCM 2022.2.01 build 13659 commit 82a2597
DB version 20220206
Registered to Infopulse GmbH

Welcome!

To get started, please enter:

5. User Management/Reset the password on the new login

The option to force the user to change their password when logging in the system was added. It’s often applicable when the new user is granted access and logging in for the first time.



Details

Username: * test

E-mail: * test@test

Authentication type: [✓ System] AD/LDAP Azure AD

State: [✓ Active] Inactive

Reset the password on the next login: ☑

Privileges:

☐ Manage Users and Permissions

☑ Manage Roles

☑ Manage Standards

☐ Create Concepts

6. Automatic Migration to ISO 27001/27002:2022

New version of ISO 27002 standard was published in 2022. Users can migrate to the new version of the standard automatically without losing their previous compliance evaluations.

7. New and updated Standards

The new standard:

ISO_SAE 21434_2021 Road vehicles — Cybersecurity engineering. This automotive standard specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

Updated to the newest versions standards:

ISO 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

TISAX 5.1.0 Trusted Information Security Assessment Exchange, an information security standard (ISA) for the automotive sector that was established by the VDA, Association of the Automotive Industry.

Other improvements

1. Renaming of Inventory Analysis

The Inventory Analysis tab was renamed to Asset Structure Analysis. The renaming was done only for the English version of the product.

2. Changelog

Changes that are logged by the system were extended by the following list of user actions:

- grant access to Concept (User ID/ Concept ID/ Role ID/name/description via which the user got access to the Concept);
- create/delete/update of Users (User ID/User name/E-mail/Active/inactive/ Authentication type/Privileges/Details – first name/second name/position/department/organization;
- create/delete/update of Roles (Role ID/Role name/Role description/Permissions)
- import/delete/update of Standards (Standard ID/Standard name/filters in Permission Management)

- create/delete/update of Filters (Filter ID/Filter name/Filter description/Filter type/Concept version to filter in, Filter options: Asset set IDs, Asset type IDs, Subtype IDs, Custom field IDs, Reports IDs)
- generate reports (report name/who generated report)
- Login/Logout (User ID, time)
- navigation (view/User ID)

3. Shortcuts

Number of shortcut keys were added:

Shortcut	Description
F1	Open Help
Ctrl/Command+D	Open the selected Profile Object (Module/Requirement/Control/Threat) description in Compliance Check and Risk Analysis
Ctrl/Command+S	Save changes
Esc	Cancel changes

4. Archive Reports function

After the report is generated, it is archived in the Tomcat folder. The user can configure t how often the folder with reports needs to be cleaned up.

5. Accessibility of information for People with Disabilities

Compliance Aspekte was tested and improved in accordance with *Federal Ordinance on Barrier-Free Information Technology (Barrierefreie-Informationstechnik-Verordnung (BITV 2.0)*

With the Ordinance, people with disabilities can have access to and use information and communication technology in a comprehensive and unrestricted manner.

Compliance Aspekte follows the recommendations to information and services that are made available electronically are accessible and usable by people with disabilities are based on World Wide Web Consortium’s stated (W3C) and further Web Content Accessibility Guidelines (WCAG) 2.1.

Examples of features that comply with the Ordinance are: ensuring sufficient color contrast for text, and icons that are interactive or convey information, using informative descriptive link text, avoid non-informative link phrases such as- click here/here/more/info, enabling keyboard navigation and so on.

6. Customer-requested features

There are a number of features that have been developed by customer request such as Custom Reports, and integration between FNT Command and Compliance Aspekte.

7. Technical: Upgrade to the latest Angular version

Angular 9 is the latest version of Angular, the framework that is used in Compliance Aspekte for the front-end of the application.

The newest version contains lots of technical features that enable the development team to deliver faster and with even better quality. Among new features are augmented performance, faster testing, better debugging.

8. Bug Fixing

Title	Description
Specially proposed for the Threat does not filter Controls according to mapping Threat-Requirements	Now the system shows only Controls that correspond to the Requirements with Protection level ‘For increased Protection Needs’ and that have the same Security Aspects as a selected Threat

Save/Cancel buttons were not clickable after the selection of switcher/dropdown/multi-choice	Previously if a User selected some data type (not switcher/dropdown/multi-choice) while custom fields creation, Save/Cancel buttons were not clickable because the system wanted values to be defined. It was fixed.
Not possible to share Organization by its owner	Now the owner of the organization can share Organization level data to other users
Save/Cancel buttons were not clickable after entering existing Concept name	Now system shows validation that this Concept name is used
<Null> if no Catalog description for Module in Compliance Check	This bug is fixed and Catalog description is optional and not visible if it is not defined