Compliance Aspekte

Release Notes 9.3

Contents

Release 9.3 Summary

The new version 9.3 of Compliance Aspekte includes significant updates, such as the ability to apply changes from Master Concept, reminders, the NIST report, mandatory custom fields, and more.

Major Features

1. Master-Child Concepts Relations

Compliance Aspekte provides the possibility of updating Child Concepts with changes made in the Master Concept. This allows for the creation of reusable Assets and applying their evaluations.

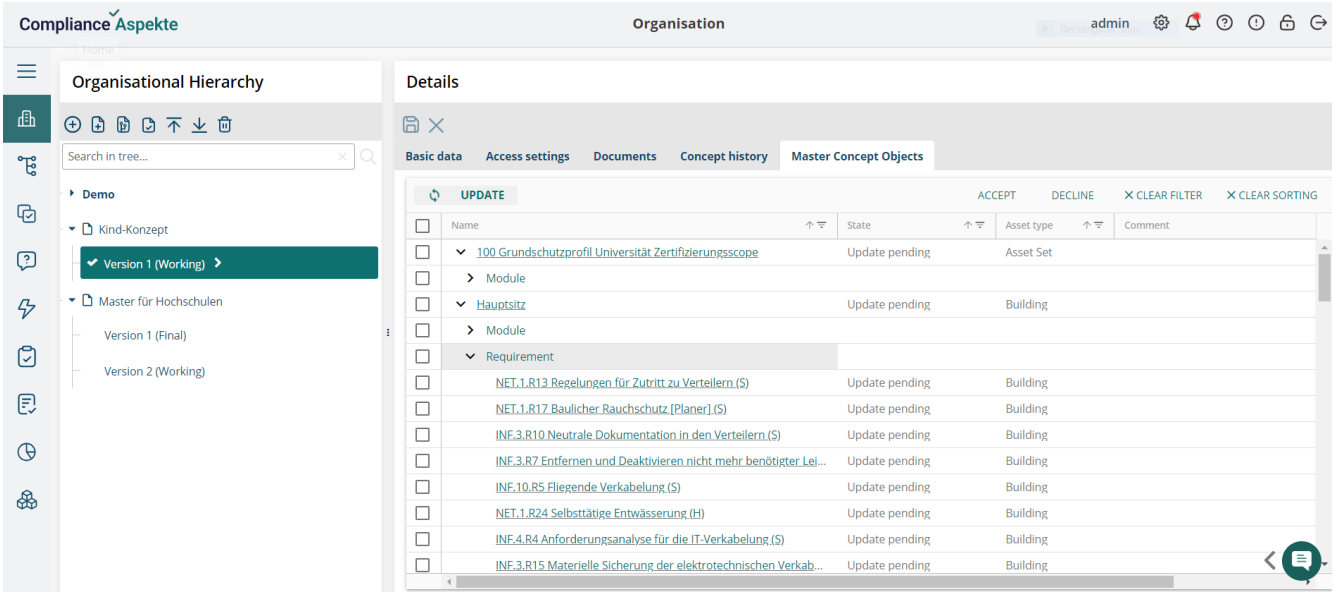
Definition of a Master Concept - some Concepts can have just one Master Concept, while others can serve as the Master for multiple Concepts.

In a Master Concept, define which Assets can be suggested in Child Concepts - It is possible to select all or a few Assets.

Accept/decline changes in Child Concepts - Child Concepts can view the main changes from their Master Concept and either accept or decline those changes.

Changes made in the Master Concept include:

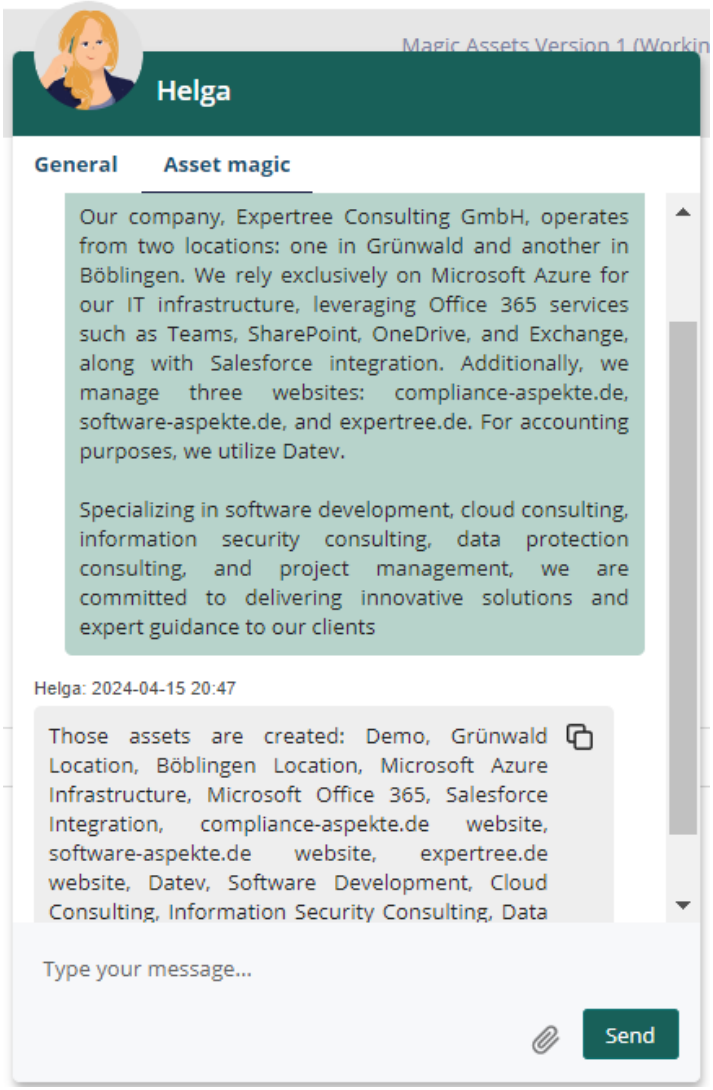
- New Assets
- Basic data and protection need of Assets
- Changes in requirement evaluations (realization, explanation)
- Control evaluations (realization, explanation, start/end dates)
- Threat evaluations (state, explanation, probability, potential damage, relevance, risk category, sufficient protection)
- Documents for Assets/Requirements/Controls/Threats



2. AI Magic: Automated Infrastructure Creation via AI Chat

Compliance Aspekte introduces a feature that streamlines the creation of company infrastructure through intuitive Helga AI Chat interaction or a file uploading.

Based on the information provided by the user, our platform dynamically generates assets such as buildings, networks, servers, databases, and more to reduce the time and efforts required to design and deploy complex company infrastructure.



3. Password policies

Compliance Aspekte provides password policies dictate the requirements for creating and managing passwords, aiming to prevent unauthorized access and protect sensitive information.

Password length - [8-30] symbols

Password complexity* requires passwords to include a combination of different types of characters, such as uppercase letters, lowercase letters, numbers, and special characters @ # $ % ^ & * ( ) _ + !

Password expiration* mandates that passwords expire after a certain period to prompt users to change them regularly.

Password history: prevents users from reusing old passwords by storing a history of 10 previously used passwords.

Password Storage: ensures that passwords are stored securely using cryptographic hashing algorithms to protect them from unauthorized access.

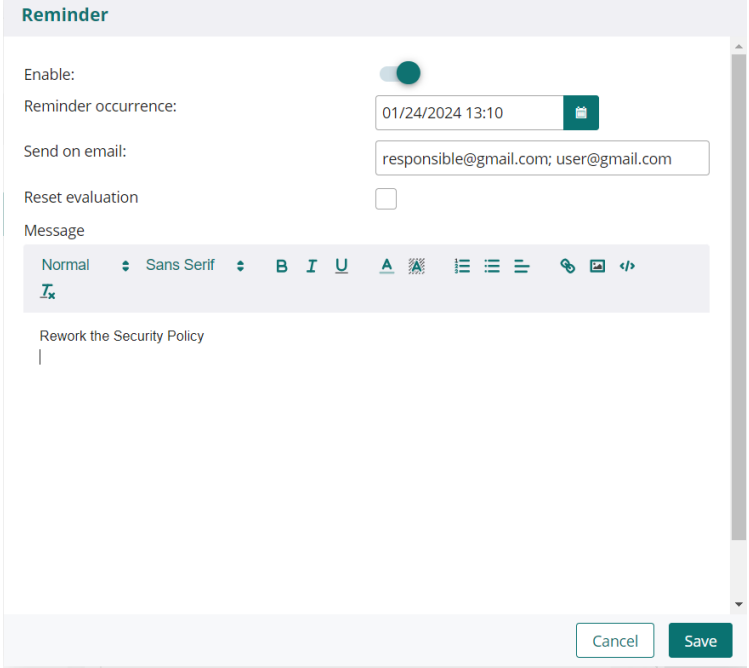
**Those policies can be configured by clients.*

4. Reminders for Requirements/Controls/Threats/Assets

Reminder emails are automatically sent to users defined by a reminder owner for Assets in Compliance Check/Risk Analysis, Requirements, Controls, and Threats.

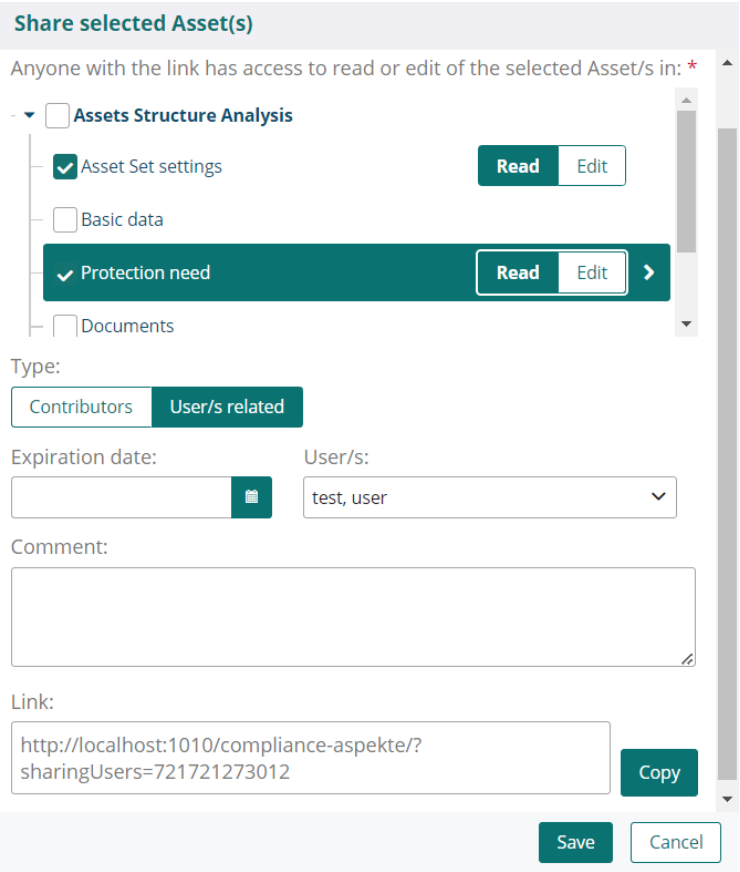
The reminder shows:

- Date: When the reminder occurs.
- Email(s): User email(s) to send the reminder.
- Message: Text to send to users.



5. Share Assets with system users

The implemented feature "Contributor/Shared links" allows users to share Assets with external users. In comparison, the new feature "Share Asset with system users" provides the possibility to share Assets with system users to review and track changes made by them on the shared Assets in the "History" tab.



6. Dashboard improvements

6.1. Custom data source in Grids (table views)

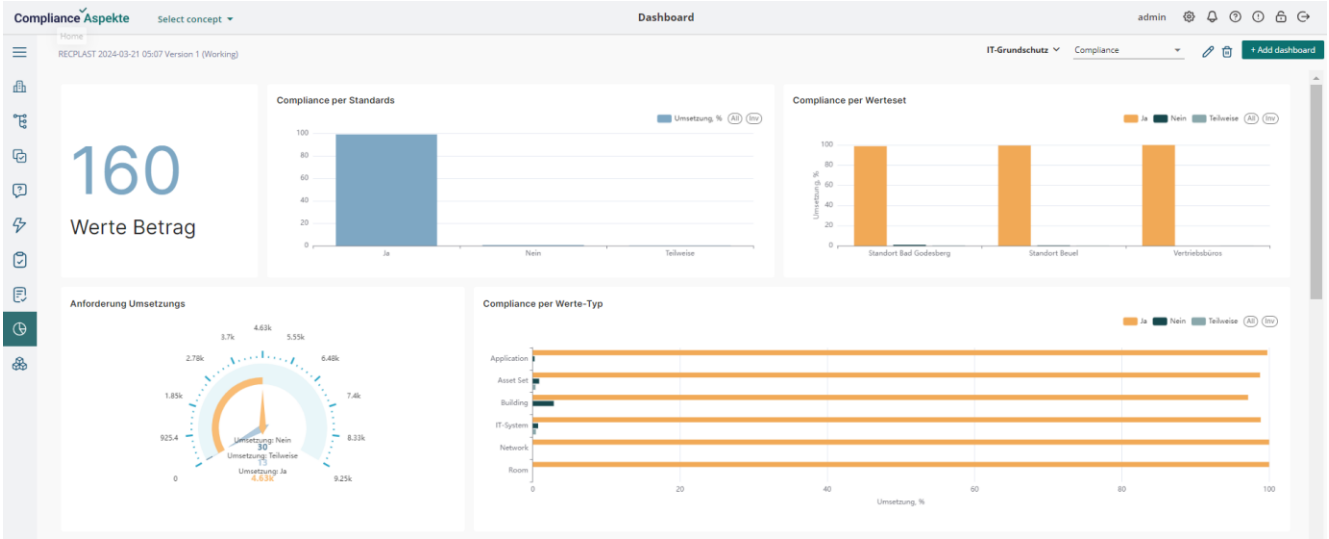
As part of the customization, Custom Grids provide users with flexible and tailored views of custom data or content. Typically, custom grids allow you to:

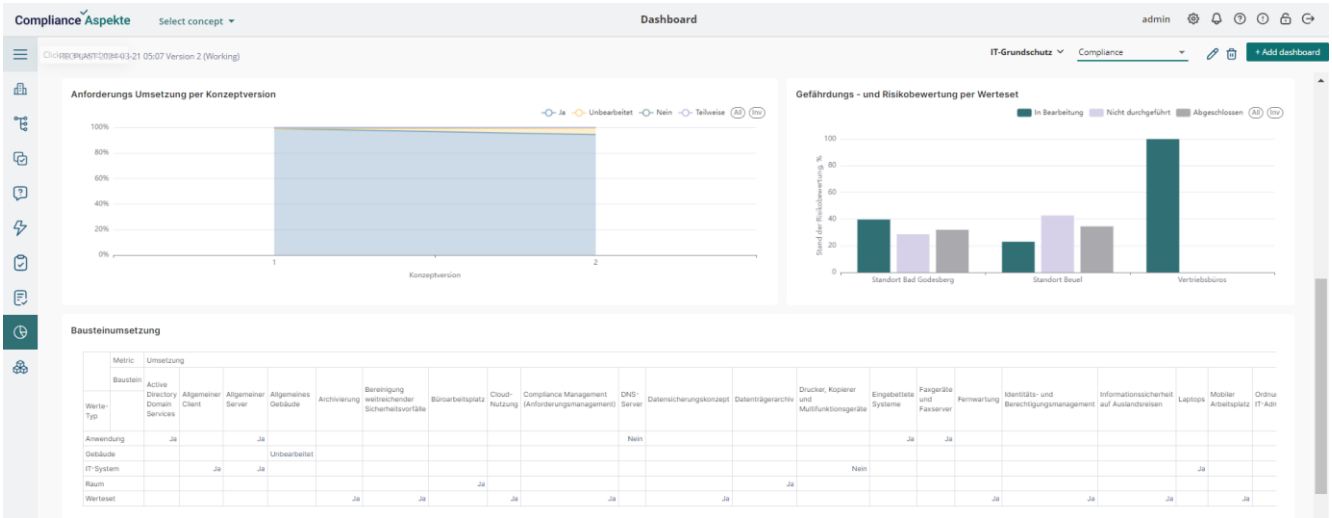
- Display data in a table view.
- Apply filtering, including advanced filters, and sorting options.
- Group data.
- Perform searches.
- Export data to various formats, such as CSV and Excel.

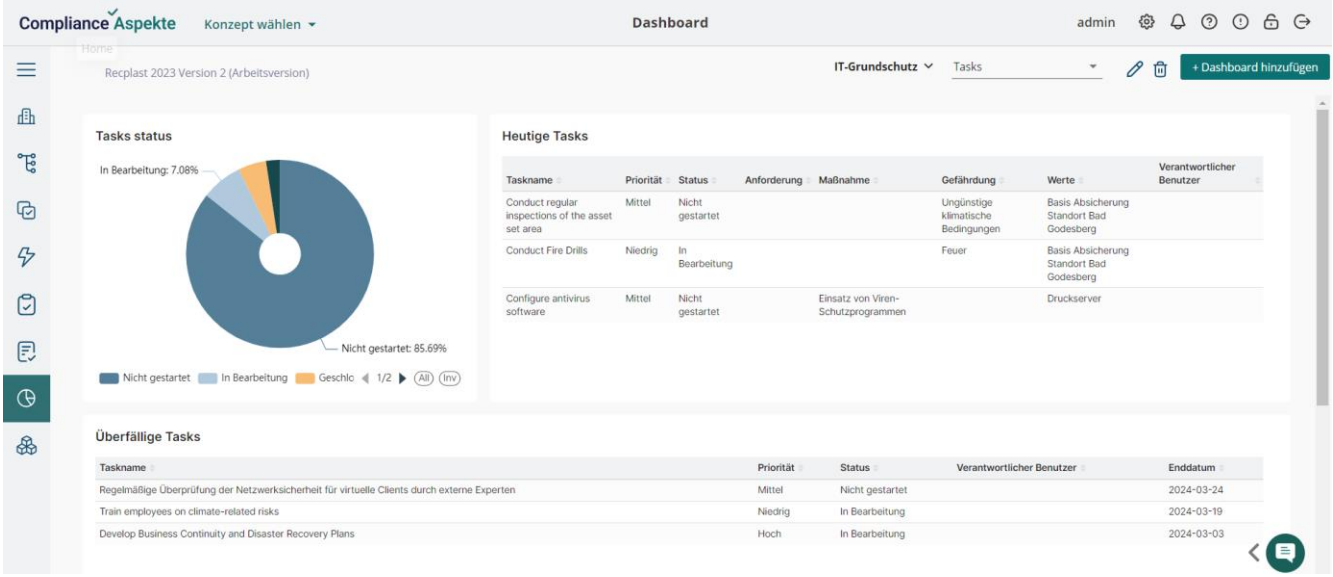
6.2. Dashboards based on Superset

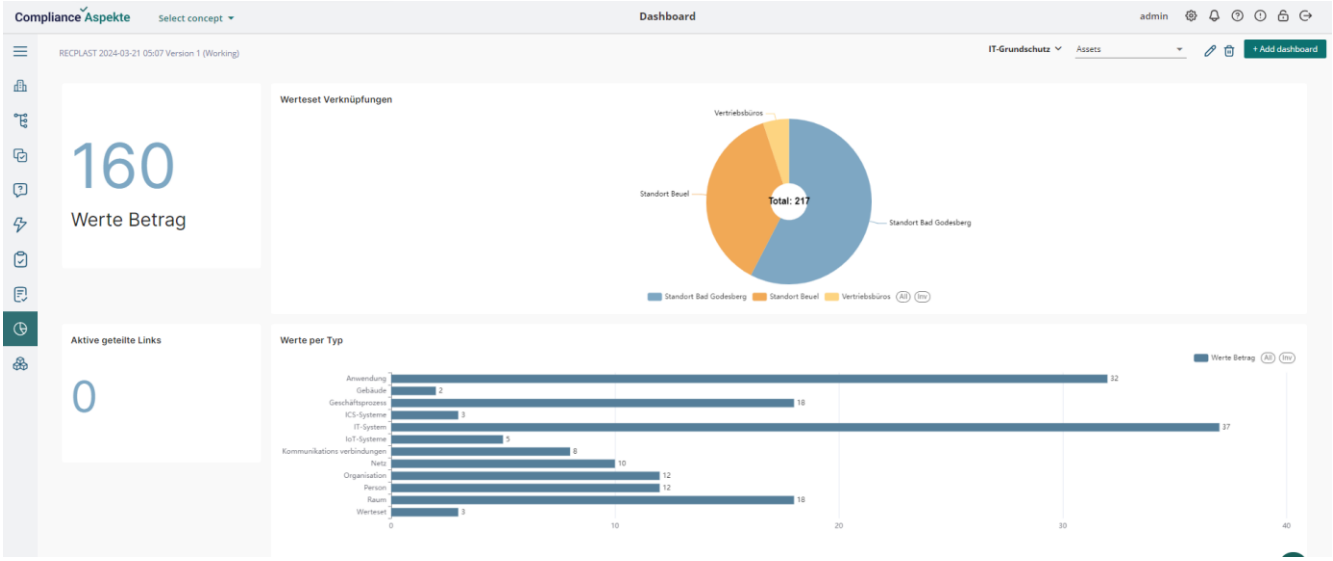
Superset is fast, lightweight, intuitive, and loaded with options that make it easy for users of all skill sets to explore and visualize their data, from simple line charts to highly detailed geospatial charts (read more about the Superset *here*)

Compliance Aspekte provides new dashboards based on Superset.









7. NIST report for NIST 800.171

A NIST 800-171 DoD assessment evaluates compliance with the NIST 800-171 requirements (Basic and Derived Security Requirements) and helps improve an organization's security implementations, as needed.

NIST 800-171 compliance is scored via the 110 security requirements. Each implemented requirement represents a single point score, with the highest score possible on a NIST 800-171 DoD assessment being 110 and the lowest possible being -203.

Compliance Aspekte

NIST 800-171 Self Assessment

27.11.2023 15:58

DEMO NIST.SP.800.171 + NIST report, version 1 (working)

Asset Set: NIST scope, scope

Description:

NIST 800-171 Requirements		Basic/Derived	Realization	Value	Family score	Total score
Access Control	3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Basic	No	5	3	66
Access Control	3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Basic	Yes	5		
Access Control	3.1.3 Control the flow of CUI in accordance with approved authorizations.	Derived	Partial	1		
Access Control	3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Derived	Yes	1		
Access Control	3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Derived	Yes	3		
Access Control	3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	Derived	Untreated	1		
Access Control	3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Derived	Yes	1		
Access Control	3.1.8 Limit unsuccessful logon attempts.	Derived	Yes	1		
Access Control	3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	Derived	Untreated	1		
Access Control	3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Derived	Yes	1		
Access Control	3.1.11 Terminate (automatically) a user session after a defined condition.	Derived	Yes	1		
Access Control	3.1.12 Monitor and control remote access sessions.	Derived	No	5		
Access Control	3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Derived	Yes	5		
Access Control	3.1.14 Route remote access via managed access control points.	Derived	Yes	1		
Access Control	3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Derived	Yes	1		
Access Control	3.1.16 Authorize wireless access prior to allowing such connections.	Derived	No	5		

8. New and updated Standards

The new standards:

DORA - The Digital Operational Resilience Act (Regulation (EU) 2022/2554) solves an important problem in the EU financial regulation. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardize the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

ISA TISAX 6.0 - defines the baseline and state of the art for information and cyber security of organizations from an automotive industry perspective.

ISO/IEC 27017 - code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018 - code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

NIST CSF 2.0 Core - includes a set of cybersecurity activities, outcomes, and references that are common across critical infrastructure sectors. It provides a high-level view of the cybersecurity functions that organizations should consider.

ISO/IEC DIS 27019: 2023 - information security controls for the energy utility industry.

BSI TR-03138 RESISCAN - contains information on the name of this Technical Guideline (TR), the responsibles, version management, the change service and the update of the TR.

ISO 26262: 2018 - intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

It addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

- **ISO 26262:** Road vehicles — Functional safety — Part 2: Management of functional safety
- **ISO 26262:** Road vehicles — Functional safety — Part 3: Concept phase
- **ISO 26262:** Road vehicles — Functional safety — Part 6: Product development at the software level

Updated to the newest versions standards:

NIST 800.171 - is the authoritative source of the assessment procedures for the CUI security requirements.

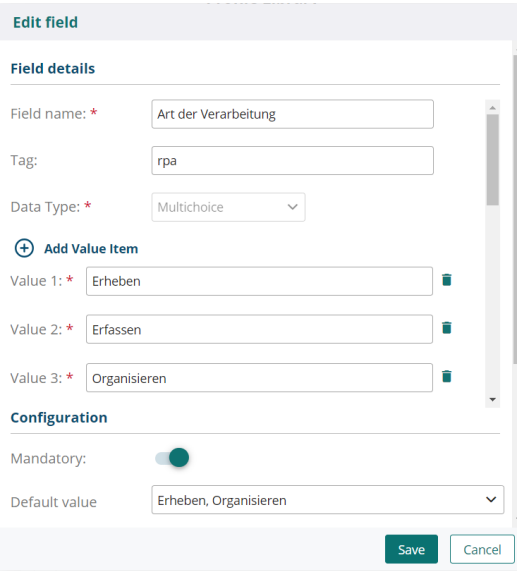
Other improvements

1. Mandatory custom fields with default value

Depending on your organization's needs, you may want to make certain fields required to ensure that you're gathering the right information.

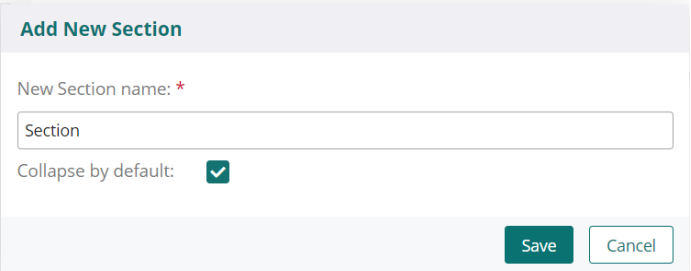
Required fields should have default value.

You can set a default value for a custom field to automatically fill each custom field. All types of custom fields may allow for default values.



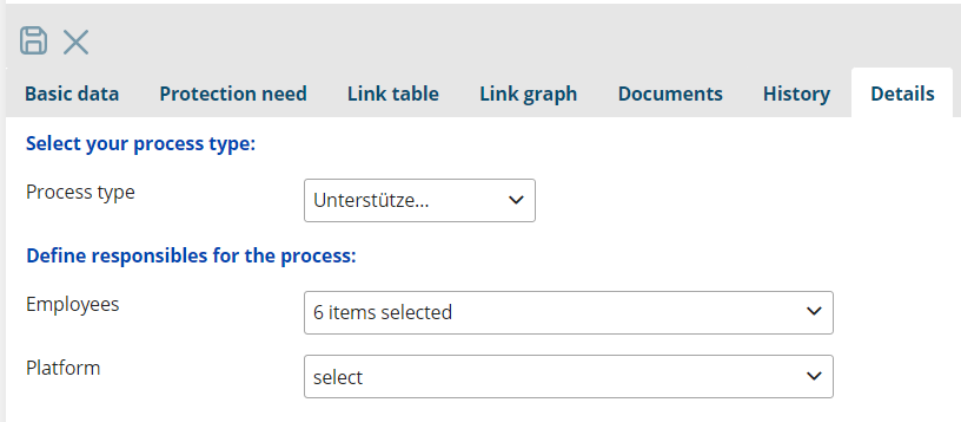
2. Expanded/collapsed sections with custom fields setup

Sections can be configured in Profile Library to collapsed/expanded them in the system.



3. Label as custom field data type

The Compliance Aspekte suggests an additional data type – Label to created read-only custom fields.



4. Jira Server synchronization

The Compliance Aspekte 9.3 provides possibility to synchronize with Jira Server.

The previous version allows Jira Cloud synchronization.

Bug Fixing

Title	Description
The damage and probability show a technical level in the Risk Analysis Grid	Now Critical level for damage and probability is hidden in the Risk Analysis Grid
'Show objects prefixes' for standards was activated by default	Not 'Show objects prefixes' for standards (except IT-Grundschutz) is deactivated by default to have more readable Object names (Requirements, Controls, etc.)
Usual user (not admin) couldn't create a new Concept on trial instance	Now restriction on user ID column is changed and user can work as admin on trial instance
Enrta ID (Azure) did not have license	Entra ID user has the 'lowest' license package after the 1st login automatically