COMPLIANCE ASPEKTE

Release Notes 9.2

Compliance Aspekte

Contents

Compliance Aspekte

Release 9.2 Summary

The new version includes significant updates, including the Helga AI bot powered by GPT, integrations with SAP and Azure, an ASPICE dashboard, reports, and more.

Major Features

### 1. Helga AI bot: integrating GPT into the ISMS software using Azure AI

The Information Security Copilot based on a GPT technology allows the collection of crucial information and generating concrete tasks to fulfill IT security requirements or mitigate risks.

- Task definition: based on the collected information, the copilot offers actionable tasks for IT managers to fulfill the requirements of the C5 standard and other relevant guidelines.

- The AI-enabled chatbot answers questions about information security and data protection standards and regulations. It also peovides guidance on how to implement them with the help of the Compliance Aspekte software.

- Answering questions related attached documents: The software uses existing information in all documents attached to different items in the Compliance Aspekte to generate context-specific answers and tips from those documents.

2. Azure integration

Compliance Aspekte allows organizations operating IT infrastructure in Azure to build an Information Security Management System (ISMS) and Data Security Management System (DSMS) around their Azure infrastructure.

- The Compliance Aspekte application connects to Azure and extracts essential information about IT assets (e.g., virtual machines, applications, services, users, etc.).

- Compliance Aspekte automatically assigns requirements and controls from BSI C5, BSI IT Grundschutz, ISO/IEC 27001, SAP® ERP 6.0 (DSAG), and other regulations and standards to the IT assets from Microsoft Azure.
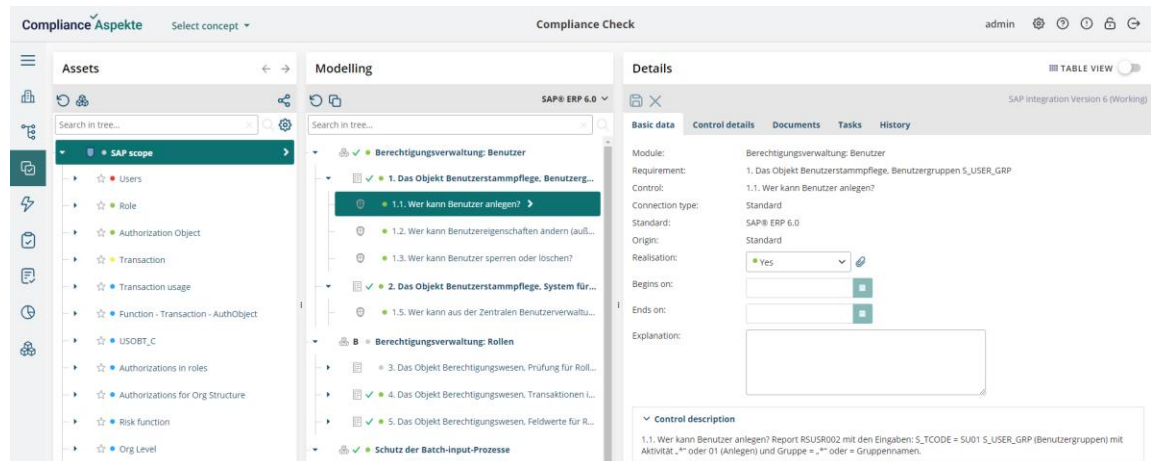
- The software tracks changes in Azure IT infrastructure, creates comprehensive summaries, and notifies responsible persons e.g. regarding all the changes in the Azure Infrastructure made within some time.

- Compliance Aspekte allows to logically connect assets to understand their dependencies from a business continuity management standpoint, create a dependency graph, and identify issues, such as the impact of a single virtual machine becoming unavailable.

- The software automatically assigns relevant threats for the IT infrastructure elements and allows assessment and mitigation of corresponding risks.

3. SAP integration

Compliance Aspekte integrates with SAP to extract data such as Users, Roles, Transactions, Authorization objects, and other items used for SAP security configuration.

Once the information about security-related assets is integrated into Compliance Aspekte, the platform assigns best practices, monitors changes in real-time, and provides visibility into the best and worst practices, crucial for identifying deviations.

Compliance Aspekte provides integration of the following SAP objects:

Users:

- <u>SAP User:</u> An SAP user is an individual who accesses and interacts with the SAP system. Users can have different roles and authorizations based on their job responsibilities. Each user typically has a unique user ID and associated parameters.

- <u>User Authorizations:</u> Authorizations define which actions and data a user can access within the SAP system. Authorizations are assigned through roles and profiles to ensure users have the necessary permissions to perform their tasks.

Roles:

- <u>SAP Role:</u> An SAP role is a collection of authorizations and permissions bundled together for a specific job function or responsibility. Roles simplify the assignment of authorizations to users. Common SAP roles include financial accountant, sales representative, and purchasing manager.

- <u>Composite Roles</u>: Composite roles are roles that combine multiple individual roles. This is useful when a user needs to perform tasks that span multiple job functions.

- <u>Single Roles:</u> Single roles are created by copying and modifying existing roles. This allows for efficient role management by reusing existing authorizations.

SAP Transactions: Transaction codes are shortcuts or codes that allow users to access specific transactions or functionality within the SAP system.

www.compliance-aspekte.de   5

SAP Reports: Reports are used to generate and analyze data from the SAP system (Users/Role/Risk views).

4. Links graph and table

In Compliance Aspekte the **Links Graph** is a visual representation of links between Assets. It shows how different Assets are connected, with arrows indicating the direction of the link. Link graphs are used to map the Assets Structure, and to understand how different Assets relate to each other.

New **Links table** implementation gives the possibility to see all directly and non-directly linked Assets of the selected Asset.
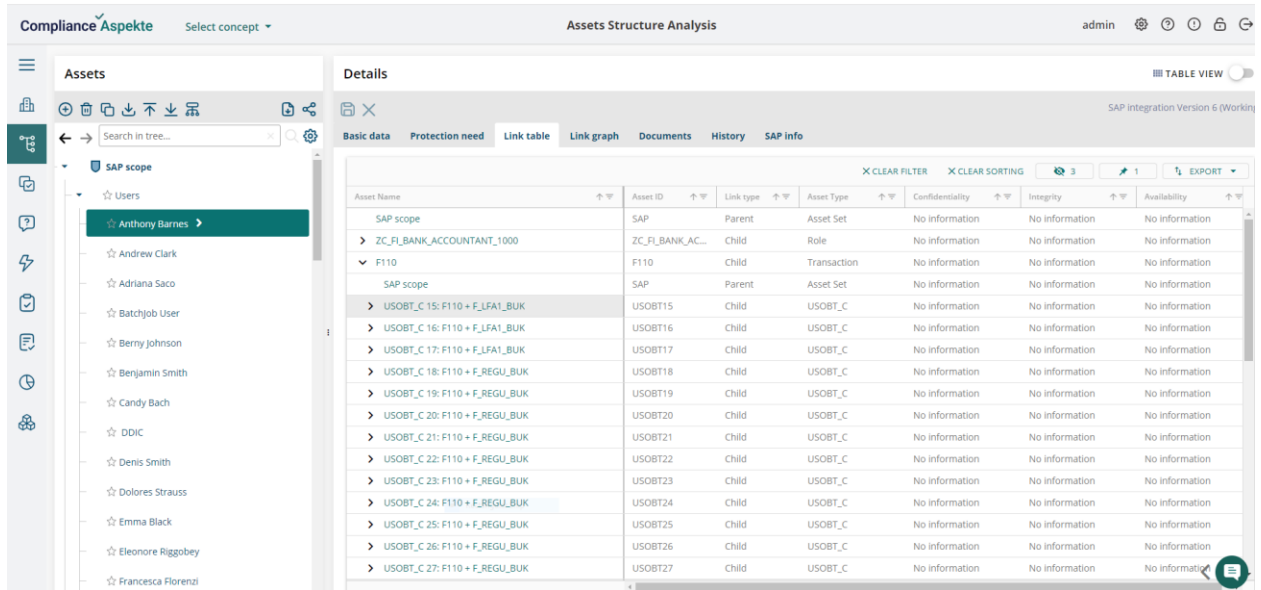
5. Asset grouping by Subtype

Each Assets tree in Compliance Aspekte can show or hide Assets subtypes via activation of the 'Show subtypes' option. It is an easy way to group Assets by their subtype(s).
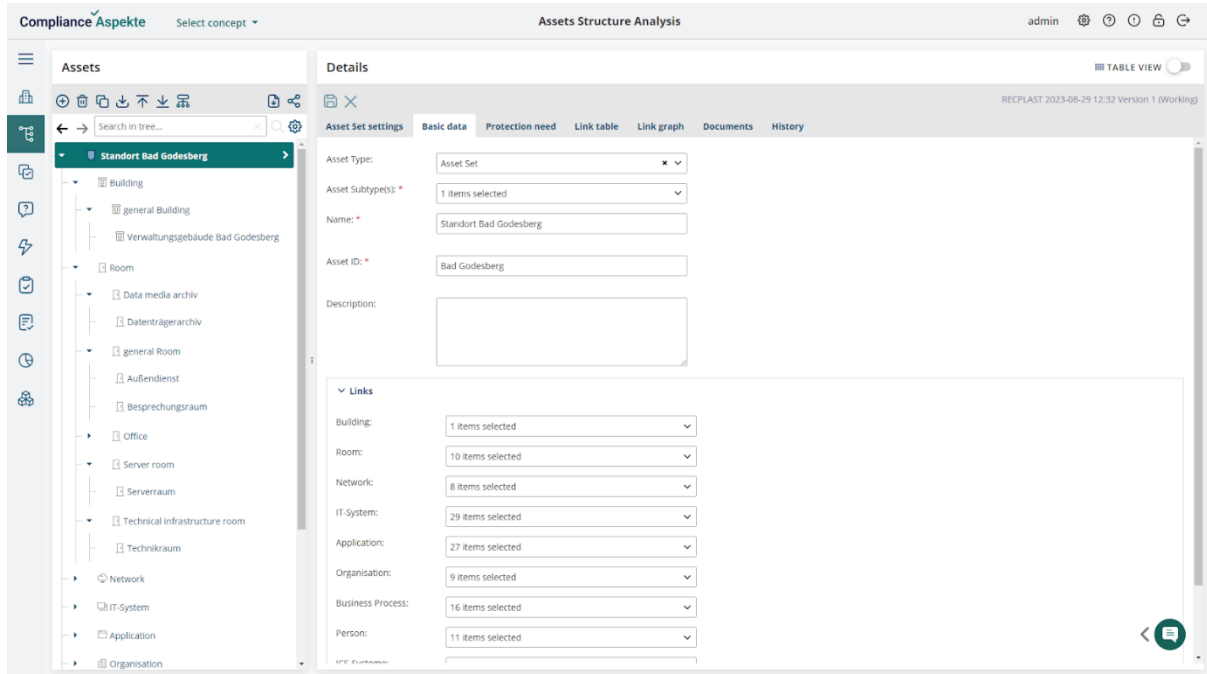
6. ASPICE report and dashboard

For Automotive SPICE standard Compliance Aspekte provides a custom report and dashboard.

ASPICE report shows the implementation of all practices in the context of Asset set:

ASPICE dashboard shows expected and actual capability level mode for each process outcome:
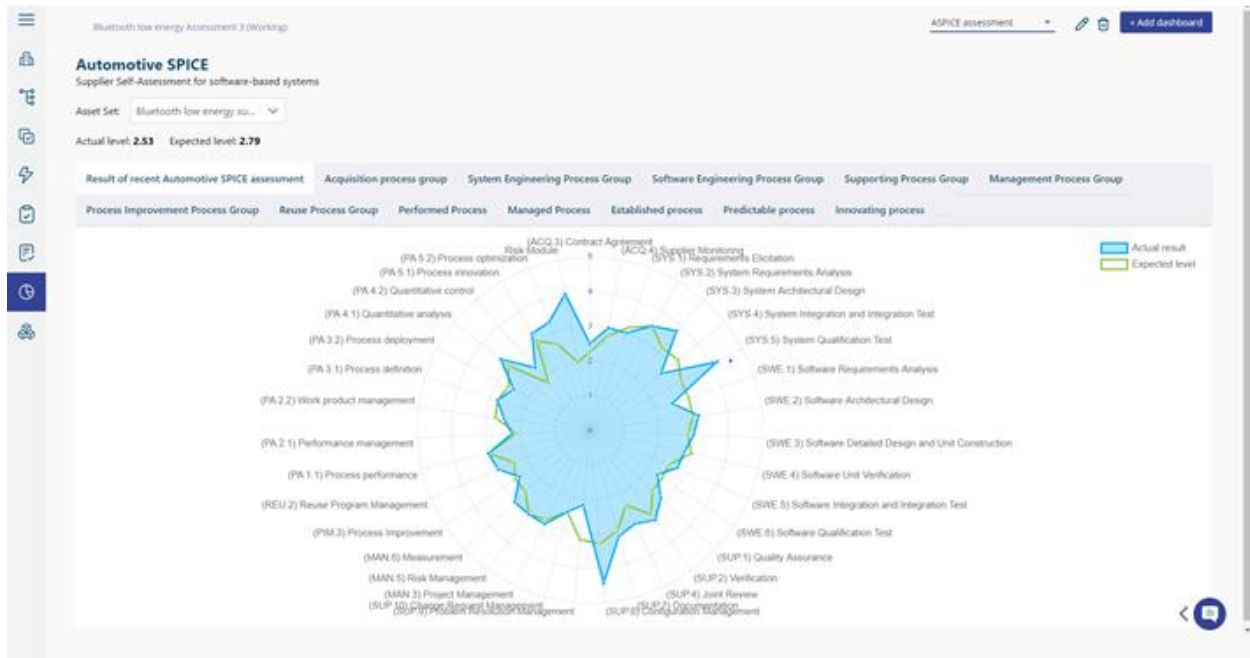
7. New and updated Standards

The new standards:

- **IT-Grundschutz 2023**

- **BSI C5:2020** Cloud Computing Compliance Criteria Catalogue – C5:2020: This criteria catalogue contains 17 objectives regarding the information security of cloud services. Each objective is broken down into the criteria required to achieve the objective.
  The criteria are divided into basic criteria and additional criteria (C5 criteria).

- **Anforderungen der BnetzA** - Catalog of security requirements for the operation of telecommunications and data processing systems as well as for the processing of personal data in accordance with Section 109 of the Telecommunications Act (TKG). These requirements affect various areas, including telecommunications, energy and postal services. They serve to ensure that companies in these industries meet certain quality and performance standards to protect consumers' interests and ensure fair competition.

- **B3S-WA** - The "Industry Specific Safety Standard Water/Wastewater Version 3" is a specific safety document used in the water and wastewater industry. This standard specifies the safety requirements and practices that must be followed in this specific industry. This standard is critical to ensuring the integrity, availability and confidentiality of water supply and wastewater systems while minimizing potential risks.

- **DSAG: Prüfleitfaden SAP® ERP 6.0** Best-Practice-Empfehlungen des DSAG-Arbeitskreises Revision u. Risikomanagement

- **Guideline for good clinical practice E6(R2)** - Good Clinical Practice (GCP) is an international ethical and scientific quality standard for designing, conducting, recording and reporting trials that involve the participation of human subjects. Compliance with this standard provides public assurance that the rights, safety and

well-being of trial subjects are protected, consistent with the principles that have their origin in the Declaration of Helsinki, and that the clinical trial data are credible.

- **APP.4.2: SAP-ERP-System -** Enterprise resource planning systems from SAP (SAP ERP systems for short) are used to automate and provide technical support for internal and external business processes. SAP ERP systems, therefore, typically process confidential information, so all components and data must be appropriately protected

- **Group Basic Software Requirements (KGAS)** - Basic requirements that the Volkswagen Group demands on vehicle-based and vehicle-related software.

- **OPDV Programmfreigabe nach BAIT/KAIT -** to a process or method in the context of banking supervision. The OPDV program release ensures that IT systems used in banks meet regulatory standards and thus ensure data security, integrity and compliance. This process is crucial to minimize risks in the banking sector and ensure the reliability of IT applications in financial institutions**.**

- **IT-Grundschutz: KOMMUNALVERWALTUNG** - refers to a special area of IT-Grundschutz that focuses on information security in local administrations.
  In this context, specific security measures and practices are developed and implemented to ensure the confidentiality, integrity and availability of information in local administrations. This is critical because these administrations manage a variety of sensitive data, including citizen information and public records.

- **Landesbanken Standard** – ensures that these banks adhere to guidelines set forth by regulatory authorities, maintain financial stability, and fulfill their roles in supporting regional economic development and financial services.

Updated to the newest versions standards:

ASPICE 3.1 Automotive SPICE

Other improvements

1. Import/export Protection needs to/from excel file

The import/export excel mechanism allows updating the Protection needs of exported Assets:

- **Integrity/Availability and Confidentiality values** (incl. Custom protection goals values)

- **Protection principles:** Maximum principle, Distribution and Cumulative effects

- **Ignoring Protection needs proposals**

2. Storing secret keys in Azure Key Vault

Azure Key Vault allows Compliance Aspekte to securely store and access items such as passwords, usernames and database connections in the Azure portal. Instead of supplying the items in plaintext, we have the template reference the secret in the Key Vault.

Bug Fixing

Title	Description
Bulk edit selects all items in Grids ignoring the filter	Now possible to bulk edit only selected items in the filtered list
The new Concept version is not selected in case of failed Asset import via Excel	After fixing, the new Concept version is nor created automatically in case of failed Asset import via Excel
No values for custom fields in custom views in the new Concept version	Values for custom fields in custom views in the new Concept version are saved now
Not possible to edit custom fields if some system tab is hidden by license	Indexes of all tabs were fixed and currently hidden tabs don't impact custom tabs with fields

www.compliance-aspekte.de   12