

verinice

VDA Information Security Assessment



verinice 1.27, 06/13/2024

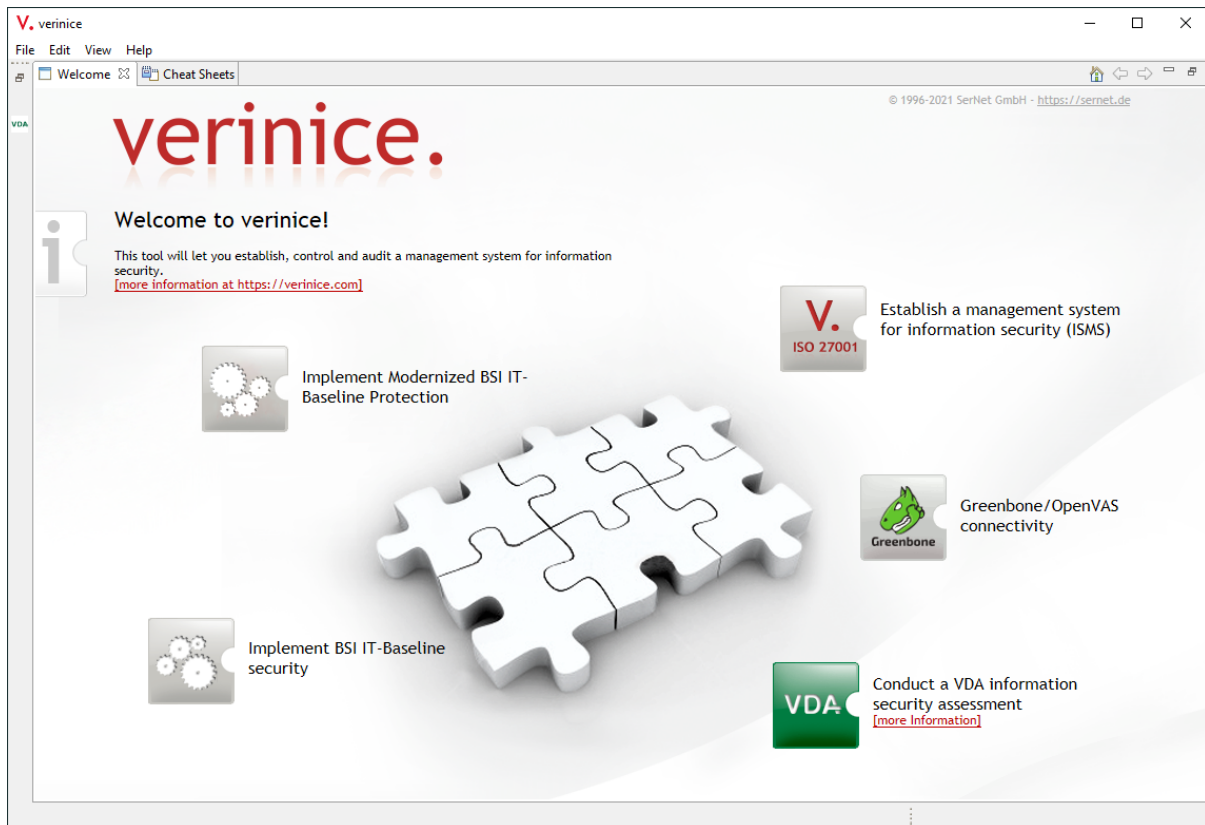
verinice.

Table of content

1. Introduction	1
2. VDA ISA version 6 [new]	2
2.1. Integration of the VDA ISA catalog 6	2
2.2. Inserting report templates	2
2.2.1. verinice.PRO	2
2.2.2. verinice.client	3
3. The VDA ISA perspective	4
4. The VDA ISA catalog	5
5. The VDA Information Security Assessment	6
5.1. Creating a new security assessment	6
5.2. Performing a security assessment	6
5.3. Create report	7
5.4. Export of the results	7



1. Introduction



This manual describes the use of the VDA Information Security Assessment (VDA ISA) in verinice.

Please always refer to the reference manual for basic functions in verinice!



Version 6.0.1 of the VDA ISA catalog is now available for use in verinice. Please note the following chapter for use in verinice from version 1.27!



2. VDA ISA version 6 [new]

2.1. Integration of the VDA ISA catalog 6

verinice creates Information Security Assessments based on the latest version of the VDA ISA catalog by default. In order to be able to carry out information security assessments on other versions, at least the respective previous version is available in verinice.

The following two versions are supplied as standard with verinice 1.27:

- samt-catalog-5.0.3_en.csv or samt-catalog-5.0.3.csv
- samt-catalog-4.1.1_en.csv or samt-catalog-4.1.1.csv

To use version 6, copy the file **samt-catalog-6.0.1_en.csv** from the directory **Catalog (CSV)** to the directory **<user><installation directory>/workspace/conf/**.

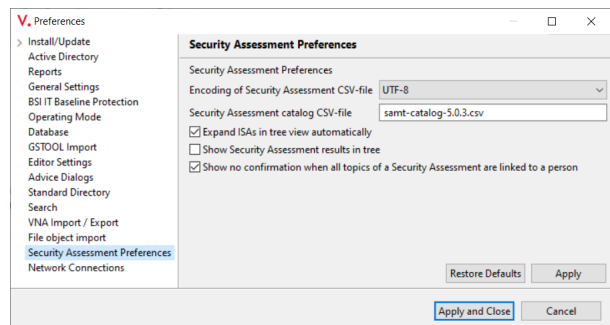


Figure 1. VDA ISA versions

You can then specify the corresponding CSV file in the *Security Assessment CSV file* field via the **Edit >Settings >Security Assessment Settings** menu.

Please note that the file with the extension **_de** is the German-language catalog, while the English version does not specify the language as a fallback.

2.2. Inserting report templates

Please note that the report templates must always match the version used! The report templates for VDA ISA 6 can be found in the **Reporttemplates (RPTDESIGN)** directory. The integration is different for users of verinice.PRO or the single-user version:

2.2.1. verinice.PRO

verinice.PRO users can conveniently import the report templates via the **Report filing** view and thus make them available centrally on your verinice.PRO server for all users. You can access the view via **View >Show view... >Report filing**.

A detailed description of the view can be found in the verinice user manual.

2.2.2. verinice.client

For the verinice client in the single-user version, you can store the report templates in a specially configurable directory. You configure the directory via the menu **Edit >Settings >Reports >Report Templates**. The default setting is the directory `<HOME>/verinice/report_templates_local` of the home directory. If a report template in the `.rptdesign` file format is stored in this directory, it is listed in the report dialog.

The output formats offered there for selection and the suggested name can be configured via a file (`.properties`) that exists specifically for this template. If not available, this file is created when the report dialog is opened for the first time and can then be adapted to your own requirements in any text editor.

3. The VDA ISA perspective

The **VDA ISA perspective** contains the following views as standard:

- The **Security Assessment** model view.
- The **Security Assessment ISA Progress** view.
- The **Object browser** view for displaying the contents of the respective VDA ISA catalog.
- The view **Cheat sheet** with the instructions for carrying out an Information Security Assessment in verinice.

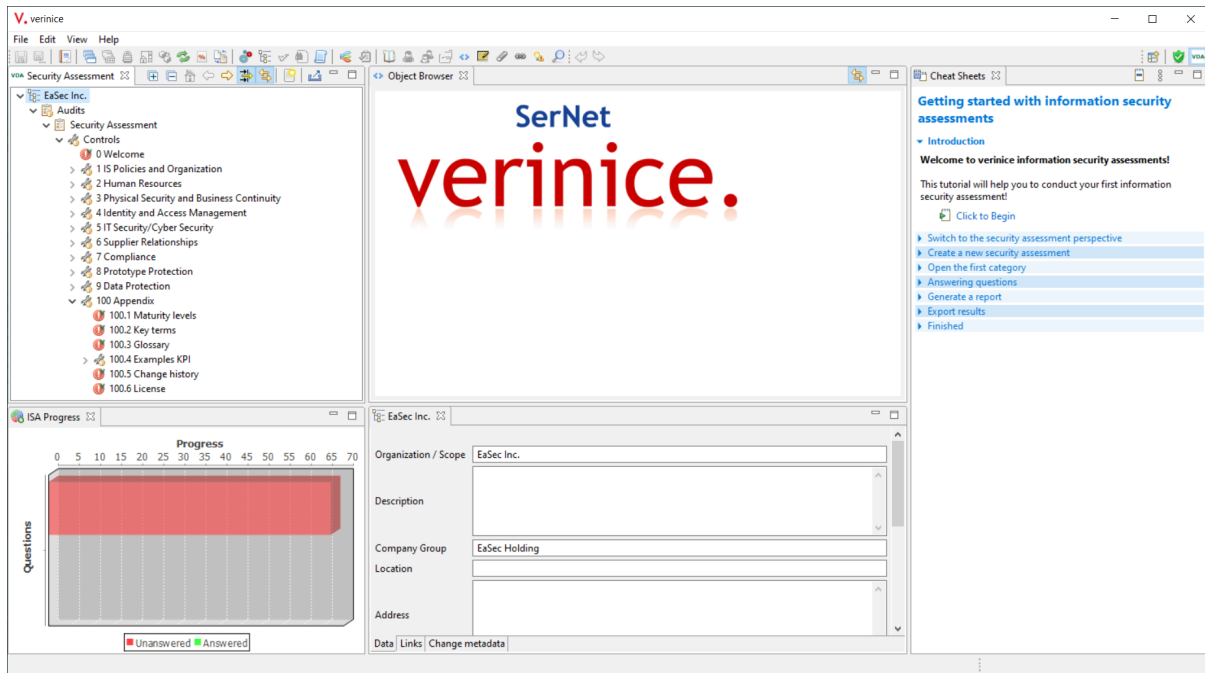


Figure 2. VDA ISA perspective



4. The VDA ISA catalog

The VDA ISA catalog is published and updated by the **German Association of the Automotive Industry (VDA)**. It serves as a basis for:

- A self-assessment to determine the state of information security in the organization.
- audits by internal specialist departments (e.g. auditing, information security).
- the assessment according to **TISAX (Trusted Information Security Assessment Exchange)**.




Please check the VDA website to ensure that you are using the current version of the VDA ISA.



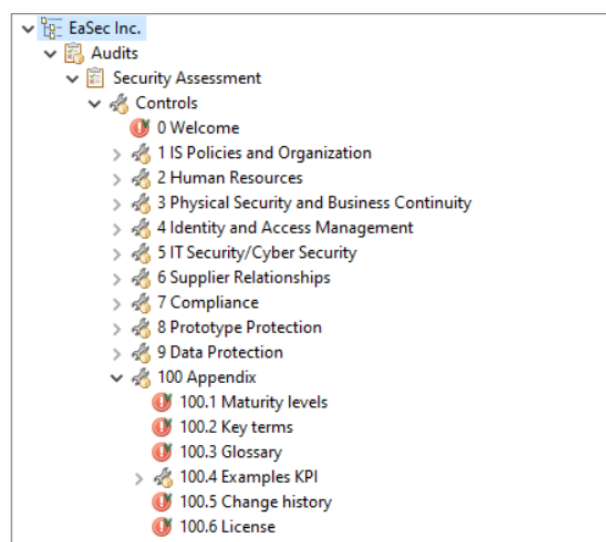
5. The VDA Information Security Assessment

5.1. Creating a new security assessment

First you must create a new security assessment. This is done by clicking on: **File >New Security Assessment**. Double-click on the root element **My company** to open the editor, in which the default name can and should be changed by entering a name for the new security assessment. You can save your entries at any time: with the button , via the **File >Save** menu or with the key combination **Ctrl + S**.

5.2. Performing a security assessment

Information Security Assessment



Once the root objects have been expanded, they can be recognized:

- The VDA ISA Controls in chapters 1 to 7
- The VDA ISA controls for *prototype protection* in chapter 8
- The VDA ISA controls for data protection
- The appendix with explanations of *Maturity Model*, *Key Terms*, *Glossary*, *KPIs*, *Change History* and *License*

Double-click on a control to open a form window in the editor that allows you to enter data for this control:

- In the *Public comment* field, you document *Findings* or *Test results* that are output in the report, analogous to the original VDA Excel table.
- In the *Private comment* field, you can optionally enter additional information that is not to be output in the report.
- In the *Maturity level* field, select the maturity level achieved on the basis of the maturity model.
- In the *Measures* field, document the *measures* implemented to fulfill the control, analogous to the original VDA Excel table.



- The *Data protection fulfilled* field only needs to be filled in for the ISA controls in chapter 9 *Data protection*, but is not evaluated in the report.
- To store accompanying documentation, open the *Files* view via the menu **View > Show View... > Files** and save any files in verinice. The stored files are listed in the report and can be added to the verification in digital form. A direct output of attached files in the report is not possible due to the different file formats!

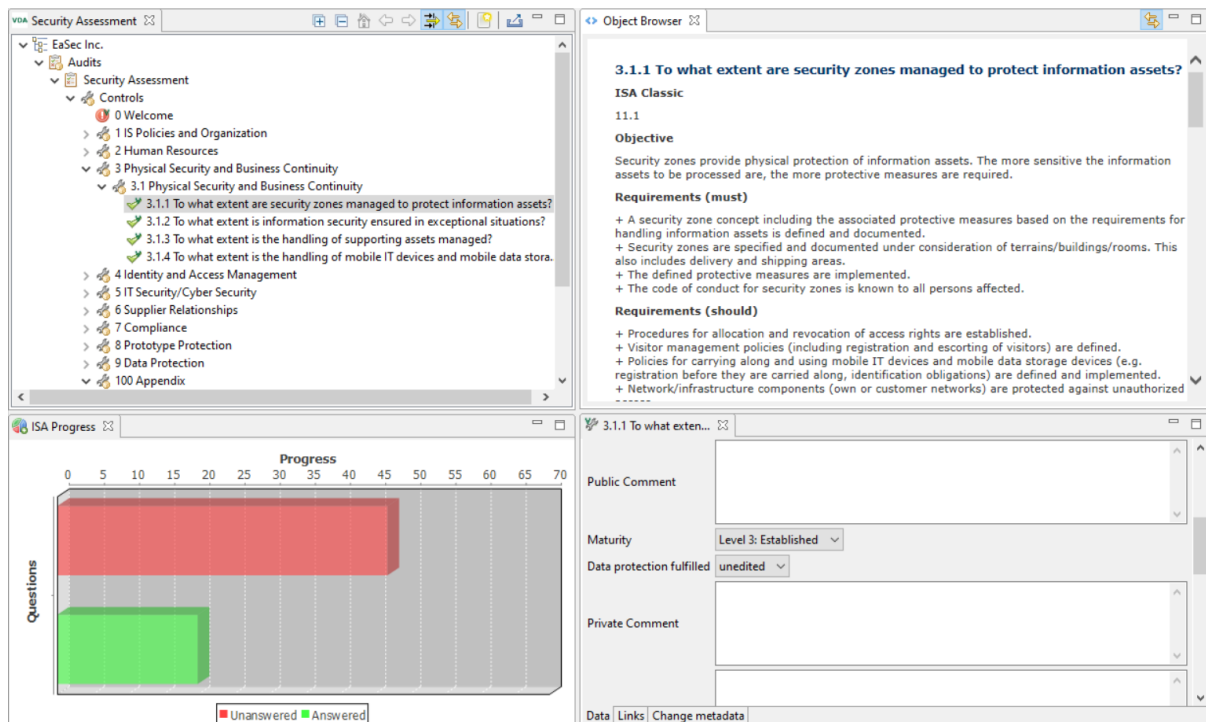


Figure 3. VDA ISA Control

When processing the controls, you can see the progress (bottom left) in the window/view with the name **Security Assessment ISA Progress**. The absolute number of processed and unprocessed controls is displayed there. This overview does **not** show the maturity level quality of the ISMS. The red bar shows the number of unprocessed controls. The green bar shows the processed controls. In order for a control to be marked as answered, the maturity level status of a control must be changed.

5.3. Create report

You can create a report on the assessment results via the menu **File > Create report** or by right-clicking on an organization via the context menu **Create report....** The respective report template must match the VDA ISA catalog used, as the calculation of the target maturity level differs in different versions!

5.4. Export of the results

If an export of the results of the assessment is desired in order to obtain a backup or to use the possibility of importing this data again later, the data can be exported. To export the data, you can either click the **Export** button  in the security assessment window or export the data via the menu: **File > Security Assessment > Export to file**.

The window for the export settings now appears. By clicking on the checkboxes, the user selects one or more organizations for which the data is to be exported. A *Source-ID* can also

be entered, which can be used to identify the exported data later - for example, time stamps can be used here.

Finally, a storage location should be selected and the **OK** button pressed.