

# verinice

VDA Information Security Assessment



verinice 1.27, 13.06.2024

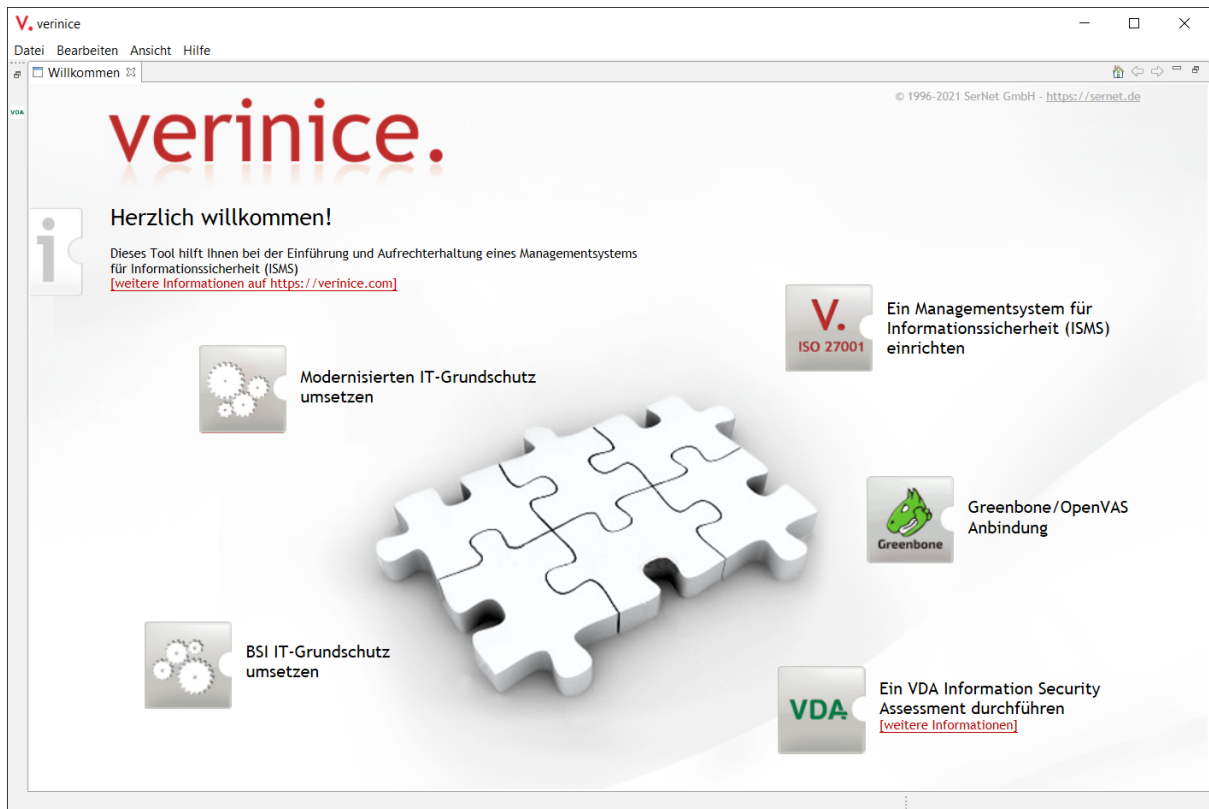
# verinice.

# Inhaltsverzeichnis

1. Einleitung .....	1
2. VDA ISA Version 6 [neu] .....	2
2.1. Einbinden des VDA ISA Katalogs 6 .....	2
2.2. Einfügen von Report-Vorlagen .....	2
2.2.1. verinice.PRO .....	2
2.2.2. verinice.Client .....	3
3. Die VDA ISA Perspektive .....	4
4. Der VDA ISA Katalog .....	5
5. Das VDA Information Security Assessment .....	6
5.1. Anlegen eines neuen Security Assessments .....	6
5.2. Durchführen eines Security Assessments .....	6
5.3. Report erstellen .....	7
5.4. Export der Ergebnisse .....	8



# 1. Einleitung



In diesem Handbuch wird der Einsatz des VDA Information Security Assessment (VDA ISA) in verinice beschrieben.

Bitte beachten Sie für grundlegende Funktionen in verinice immer auch das Referenzhandbuch!



Ab sofort ist Version 6.0.1 des VDA ISA Katalogs zum Einsatz in verinice verfügbar. Bitte beachten Sie das folgende Kapitel zur Verwendung in verinice ab Version 1.27!

## 2. VDA ISA Version 6 [neu]

### 2.1. Einbinden des VDA ISA Katalogs 6

verinice erstellt Information Security Assessments standardmäßig auf Basis der aktuellsten Version des VDA ISA Katalogs. Um Information Security Assessments auch auf anderen Versionen ausführen zu können, steht in verinice mindestens die jeweilige Vorgängerversion zur Verfügung.

Mit verinice 1.27 werden standardmäßig die beiden folgenden Versionen ausgeliefert:

- samt-catalog-5.0.3\_de.csv bzw. samt-catalog-5.0.3.csv
- samt-catalog-4.1.1\_de.csv bzw. samt-catalog-4.1.1.csv

Zum Einsatz der Version 6 kopieren Sie die Datei **samt-catalog-6.0.1\_de.csv** aus dem Verzeichnis **Katalog (CSV)** in das Verzeichnis **<Benutzer><Installationsverzeichnis>/workspace/conf/**.

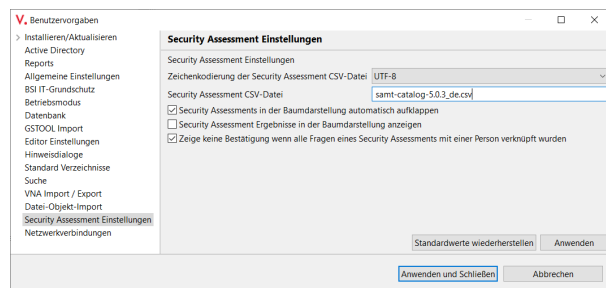


Abbildung 1. VDA ISA Versionen

Im Anschluss können Sie über das Menü **Bearbeiten > Einstellungen > Security Assessment Einstellungen** die entsprechende CSV-Datei im Feld *Security Assessment CSV-Datei* festlegen.

Zu beachten ist, dass es sich bei der Datei mit der Endung **\_de** jeweils um den deutschsprachigen Katalog handelt, während die englische Version als Fallback auf die Angabe der Sprache verzichtet.

### 2.2. Einfügen von Report-Vorlagen

Bitte beachten Sie dabei immer auch, dass die Reportvorlagen zur verwendeten Version passen müssen! Die Reportvorlagen für VDA ISA 6 finden Sie im Verzeichnis **Reporttemplates (RPTDESIGN)**. Die Einbindung erfolgt unterschiedlich für Anwender von verinice.PRO bzw. der Einzelplatzversion:

#### 2.2.1. verinice.PRO

verinice.PRO Anwender können die Report-Vorlagen komfortabel über den View **Report-Ablage** importieren und damit zentral auf Ihrem verinice.PRO Server für alle Anwender zur Verfügung stellen. Den View erreichen Sie über **Ansicht > Zeige View... > Report-Ablage**.

Eine genaue Beschreibung des Views finden Sie in der verinice-Benutzeranleitung.

### 2.2.2. verinice.Client

Für den verinice Client in der Einzelplatzversion können Sie die Reportvorlagen in einem speziell dafür konfigurierbaren Verzeichnis ablegen. Das Verzeichnis konfigurieren Sie über das Menü **Bearbeiten >Einstellungen >Reports >Report Templates**. Die Standard-Einstellung ist das Verzeichnis `<HOME>/verinice/report_templates_local` des Heimatverzeichnisses. Wird eine Reportvorlage im Dateiformat `.rptdesign` in diesem Verzeichnis abgelegt, wird sie im Reportdialog aufgelistet.

Die dort zur Auswahl angebotenen Ausgabeformate und der vorgeschlagene Name können über eine speziell für diese Vorlage vorhandene Datei (`.properties`) konfiguriert werden. Diese Datei wird, sofern nicht vorhanden, beim ersten Öffnen des Reportdialogs angelegt und kann anschließend in einem beliebigen Texteditor an die eigenen Anforderungen angepasst werden.

### 3. Die VDA ISA Perspektive

Die **VDA ISA Perspektive** beinhaltet standardmäßig die folgenden Views:

- Den Modell-View **Security Assessment**.
- Den View **Security Assessment ISA Fortschritt**.
- Den View **Objektbrowser** zur Anzeige von Inhalten des jeweiligen VDA ISA Kataloges.
- Den View **Spickzettel** mit der Anleitung zur Durchführung eines Information Security Assessment in verinice.

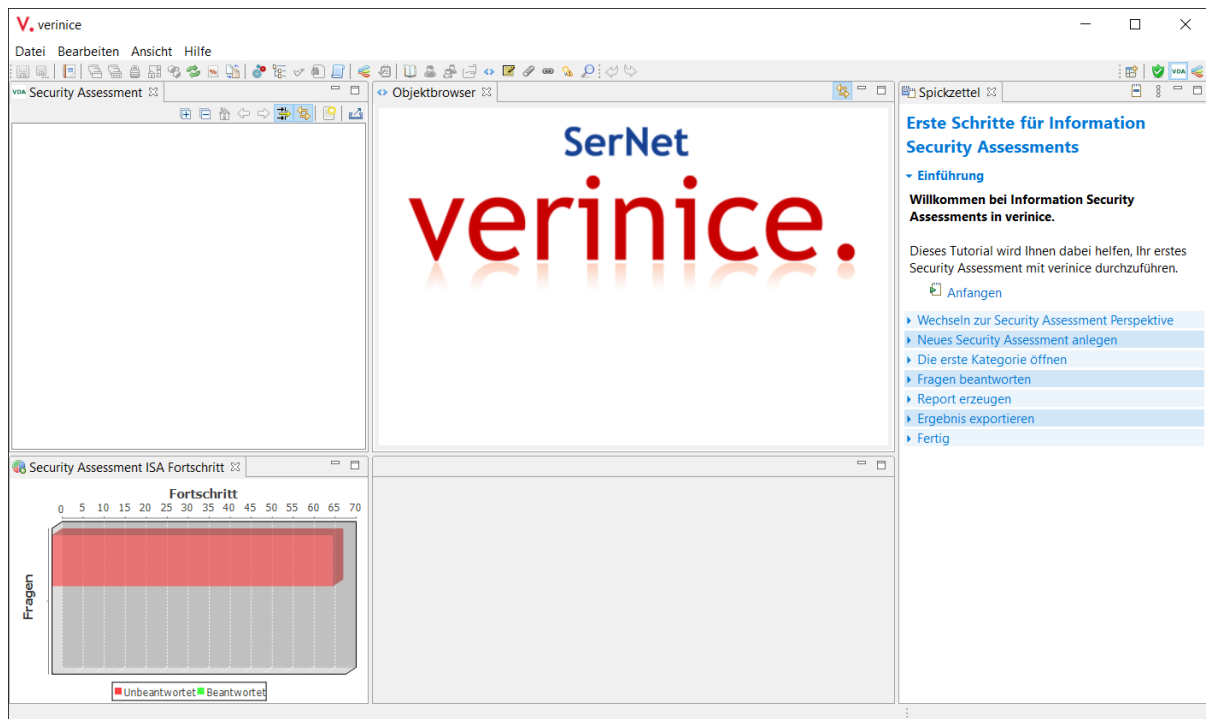


Abbildung 2. VDA ISA Perspektive

## 4. Der VDA ISA Katalog

Der VDA ISA Katalog wird vom **Verband der Automobilindustrie (VDA)** herausgegeben und aktualisiert. Er dient als Basis für:

- ein Self-Assessment zur Bestimmung des Zustandes der Informationssicherheit in der Organisation.
- Audits durch interne Fachabteilungen (z. B. Revision, Informationssicherheit).
- die Prüfung nach **TISAX (Trusted Information Security Assessment Exchange)**.




Bitte überzeugen Sie sich auf der Webseite des VDA, dass Sie die jeweils gültige Fassung des VDA ISA verwenden.



# 5. Das VDA Information Security Assessment

## 5.1. Anlegen eines neuen Security Assessments

Als Erstes müssen Sie ein neues Security Assessment anlegen. Dies erfolgt durch Klick auf: **Datei > Neues Security Assessment**. Mit einem Doppelklick auf das Wurzelement **Mein Unternehmen** öffnet sich der Editor, in welchem der Standardname durch Eingabe eines Namens für das neue Security Assessment geändert werden kann und sollte. Sie können Ihre Eingaben jederzeit speichern: mit dem Button , über das **Menü Datei > Speichern** oder mit der Tastenkombination **Strg + S**.

## 5.2. Durchführen eines Security Assessments

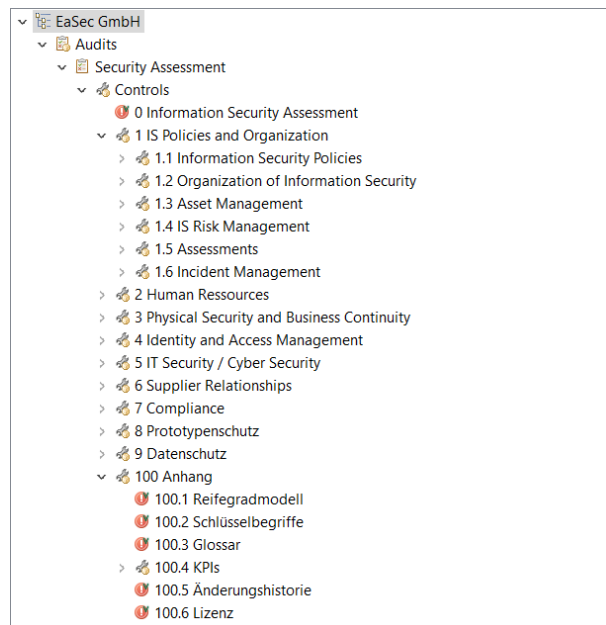


Abbildung 3. Information Security Assessment

Nach dem Aufklappen der Wurzelobjekte sind zu erkennen:

- Die VDA ISA Controls in den Kapiteln 1 bis 7
- Die VDA ISA Controls für den *Prototypenschutz* in Kapitel 8
- Die VDA ISA Controls für den *Datenschutz*
- Der Anhang mit Erläuterungen zu *Reifegradmodell*, *Schlüsselbegriffen*, *Glossar*, *KPIs*, *Änderungshistorie* und *Lizenz*

Durch doppelten Mausklick auf ein Control erscheint im Editor ein Formularfenster, das Ihnen ermöglicht, Daten zu diesem Control einzutragen:

- Im Feld *Öffentlicher Kommentar* dokumentieren Sie analog zur Original Excel-Tabelle des VDA *Feststellungen* bzw. *Prüfergebnisse*, die im Report ausgegeben werden.
- Im Feld *Privater Kommentar* können Sie optional zusätzliche Angaben hinterlegen, die im Report nicht ausgegeben werden sollen.
- Im Feld *Reifegrad* wählen Sie den erzielten Reifegrad auf Grundlage des Reifegradmodells aus.



- Im Feld *Maßnahmen* dokumentieren Sie analog zur Original Excel-Tabelle des VDA die umgesetzten *Maßnahmen* zur Erfüllung des Controls.
- Das Ausfüllen des Feldes *Datenschutz erfüllt* ist nur für die ISA Controls des Kapitels 9 *Datenschutz* erforderlich, wird allerdings im Report nicht ausgewertet.
- Um Begleitdokumentation zu hinterlegen, öffnen Sie den View *Dateien* über das Menü **Ansicht >Zeige View... >Dateien** und speichern beliebige Dateien in verinice. Die hinterlegten Dateien werden im Report aufgelistet und können zum Nachweis in digitaler Form hinzugefügt werden. Eine direkte Ausgabe angehängter Dateien im Report ist aufgrund der möglichen unterschiedlichen Dateiformate nicht möglich!

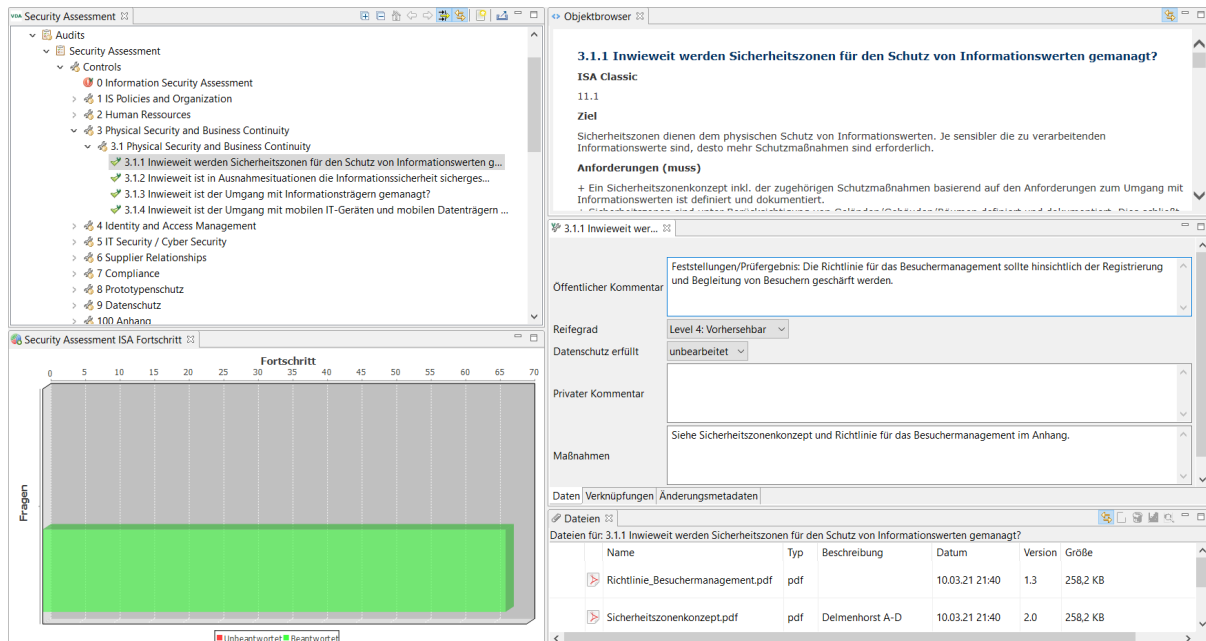


Abbildung 4. VDA ISA Control

Beim Abarbeiten der Controls, sieht man den Fortschritt (unten links) im Fenster/View mit dem Namen **Security Assessment ISA Fortschritt**. Dort wird die absolute Anzahl der bearbeiteten und unbearbeiteten Controls angezeigt. Diese Übersicht zeigt **nicht** die Reifegrad-Qualität des ISMS an. Der rote Balken zeigt die Anzahl von unbearbeiteten Controls an. Der grüne Balken zeigt die bearbeiteten Controls an. Damit ein Control als beantwortet markiert werden kann, muss der Reifegradstatus eines Controls verändert werden.

## 5.3. Report erstellen

Einen Report über die Assessment-Ergebnisse können Sie über das Menü **Datei >Report erzeugen** oder durch rechten Mausklick über das Kontextmenü **Erzeuge Report...** auf einer Organisation erstellen. Das jeweilige Report Template muss dabei zum verwendeten VDA ISA Katalog passen, da die Berechnung des Zielreifegrads sich in unterschiedlichen Versionen unterscheidet!

## 5.4. Export der Ergebnisse

Wird ein Export der Ergebnisse des Assessments gewünscht, um eine Sicherung zu erhalten oder die Möglichkeit zu nutzen, diese Daten später wieder einzuspielen, so können die Daten exportiert werden. Um die Daten zu exportieren kann entweder der **Export**-Button  im Security-Assessment-Fenster betätigt werden oder der Export erfolgt über das Menü: **Datei >Security Assessment >Export in Datei**.

Nun erscheint das Fenster für die Export-Einstellungen. Der Nutzer wählt durch Anklicken der Checkboxen eine oder mehrere Organisationen aus, für die die Daten exportiert werden sollen. Es kann weiterhin eine *Source-ID* eingetragen werden, mit der die exportierten Daten später identifiziert werden können - hier kann z.B. mit Zeitstempeln gearbeitet werden.

Zuletzt sollte noch ein Speicherort ausgewählt und der **OK**-Button gedrückt werden.