

IT-Grundschutz-Kompendium

Edition 2022



Version 10.0, 24.02.2022

verinice.

Inhaltsverzeichnis

Produktinformationen	1
Das IT-Grundschutz-Kompendium Edition 2022 des BSI	1
Lieferumfang	2
Ihr Nutzen auf einen Blick	2
Weiterführende Informationen	2
Autorenschaft und Urheberrecht	2
1. Einsatz in verinice	3
1.1. Vorbereitung	3
1.2. Aufbau	3
1.3. Verwendung	9



Produktinformationen

Abbildung des **IT-Grundschutz-Kompodium Edition 2022** in verinice.

Das IT-Grundschutz-Kompodium Edition 2022 des BSI

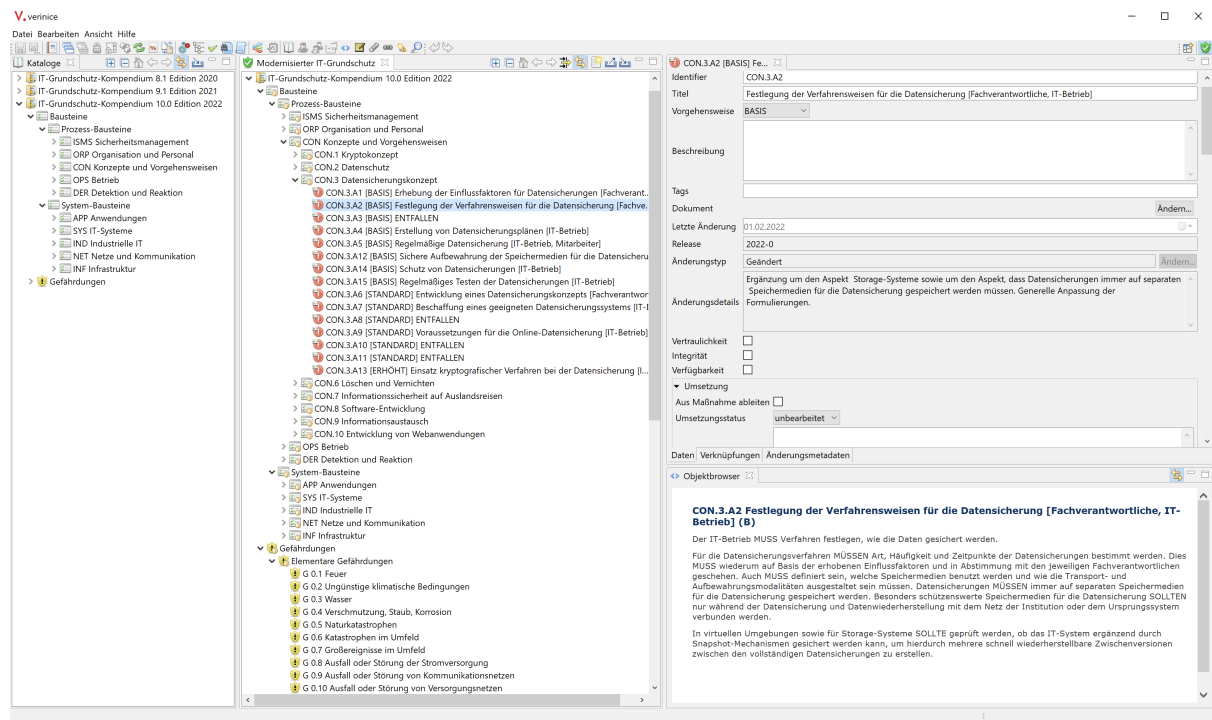


Abbildung 1. IT-Grundschutz-Kompodium 10.0 Edition 2022

Das IT-Grundschutz-Kompodium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für alle, die sich umfassend mit dem Thema Informationssicherheit befassen möchten. Im Fokus des IT-Grundschutz-Kompodiums stehen die sogenannten IT-Grundschutz-Bausteine. In diesen Texten wird jeweils ein Thema zu allen relevanten Sicherheitsaspekten beleuchtet. Im ersten Teil der IT-Grundschutz-Bausteine werden mögliche Gefährdungen erläutert, im Anschluss wichtige Sicherheitsanforderungen. Die IT-Grundschutz-Bausteine sind in zehn unterschiedliche Schichten aufgeteilt und reichen thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS).

Vertiefende Informationen dazu, wie einzelne Maßnahmen umgesetzt werden können, sind in den sogenannten Umsetzungshinweisen zu finden. Sie beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Bislang gibt es noch nicht zu jedem Baustein einen Umsetzungshinweis. Weitere Umsetzungshinweise werden sukzessive veröffentlicht, diese sind ab dem IT-Grundschutz-Kompodium 2020 losgelöst von der jeweils aktuellen Edition zu verwenden.

Bei der Erstellung der Bausteine wurde bereits eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Die Anforderungen in den Bausteinen bilden den aktuellen Stand der Technik ab.

Lieferumfang

Der Download (.ZIP-Format) enthält:

- Eine Anleitung im PDF-Format.
- Das **IT-Grundschutz-Kompendium 10.0 Edition 2022** als .VNA-Datei zum Import in verinice ab Version 1.22 und höher.

Ihr Nutzen auf einen Blick

Das **IT-Grundschutz-Kompendium 10.0 Edition 2022** für verinice:

- Stellt alle Bausteine und elementaren Gefährdungen zur Modellierung von Informationsverbünden in verinice zur Verfügung.
- Enthält alle Texte der Anforderungen und elementaren Gefährdungen zur Betrachtung im Objektbrowser.
- Ermöglicht das Update von Informationsverbünden, die mit einer vorherigen Edition des IT-Grundschutz-Kompendiums modelliert wurden.

Weiterführende Informationen

Diskussion im verinice.FORUM: <https://forum.verinice.com/>

Videos auf YouTube: <https://www.youtube.com/c/verinice/videos>

Autorenschaft und Urheberrecht

IT-Grundschutz-Kompendium Edition 2022:

© 2022
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

verinice IT-Grundschutz-Kompendium 10.0 Edition 2022:

© 2022
SerNet Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen



1. Einsatz in verinice

1.1. Vorbereitung

Das IT-Grundschutz-Kompodium wird als ZIP-komprimiertes verinice-Archiv (.VNA) bereitgestellt, das Sie an einen Ort Ihrer Wahl entpacken können (Windows-Systeme speichern u.U. als .zip ab – in diesem Fall ändern Sie bitte die Endung zu .VNA um).

Um das Grundschutz-Kompodium in verinice einzubinden, wechseln Sie in die Perspektive **Modernisierter IT-Grundschutz**. Diese finden Sie unter **Ansicht > Zeige Perspektive...> Modernisierter BSI Grundschutz**.

Hier importieren Sie das Kompodium im View **Kataloge** über das Icon **Importiere Katalog aus Datei....** Im Dialog wählen Sie die heruntergeladene Datei über die Schaltfläche **Datei auswählen...** aus.

1.2. Aufbau

Das **IT-Grundschutz-Kompodium 10.0 Edition 2022** enthält alle

- Bausteine inklusive der einzelnen Bausteinanforderungen
- Elementaren Gefährdungen

Bitte beachten Sie die folgende Hinweise:

1.2.1. Besonderheiten beim Update

Bei 9 Bausteinen des IT-Grundschutz-Kompodiums Edition 2022 wurden neben den Anforderungen auch die elementaren Gefährdungen überarbeitet. Da die verinice Update-Funktion keine Elemente oder Verknüpfungen löscht, müssen Sie anschließend folgendes manuell nachpflegen:

- Bei **neu hinzugekommenen Gefährdungen** werden durch die Update-Funktion von verinice die entsprechenden Gefährdungen neu angelegt und mit den dazugehörigen Zielobjekten und Anforderungen (laut Kreuzreferenztafel) verknüpft.
 - Sie müssen lediglich die neuen Gefährdungen bewerten.
- Die **entfallenen Gefährdungen** werden durch die Update-Funktion von verinice nicht automatisch gelöscht, da diese gegebenenfalls von Ihnen bereits bewertet wurden. Aus diesem Grund müssen Sie prüfen, ob die entfallenen Gefährdungen (eventuell aus Dokumentationsgründen) noch benötigen werden.
 - Werden die Gefährdungen gar nicht mehr benötigt, so können diese manuell (durch *Rechtsklick > löschen*) gelöscht werden.
 - Wollen Sie die Gefährdungen weiterhin zu Dokumentationszwecken in Ihrer Modellierung beibehalten, diese sollen aber in keine Bewertung einfließen, so können Sie die Verknüpfungen zu den Anforderungen und dem Zielobjekt entfernen.
 - Sollen die Gefährdungen weiterhin betrachtet und bewertet werden, so ist keine manuelle Nacharbeit nötig.
- Zudem wurden **grundsätzlich** die Kreuzreferenztabellen in diesen Bausteinen überarbeitet. Dies bedeutet, dass nicht nur Gefährdungen hinzugekommen oder entfallen sind, sondern dass auch zahlreiche **Verknüpfungen der vorhandenen**

Gefährdungen überarbeitet wurden. In diesem Fall sind Verknüpfungen (insbesondere die Entfallenen) zwischen den einzelnen Anforderungen und Gefährdungen zu prüfen und gegebenenfalls zu löschen.

Bei folgenden Bausteinen wurden die elementaren Gefährdungen überarbeitet:

- CON.3 Datensicherungskonzept
- OPS.1.1.5 Protokollierung
- APP.3.1 Webanwendungen und Webservices
- APP.4.3 Relationale Datenbanken
- SYS.1.1 Allgemeiner Server
- SYS.1.5 Virtualisierung
- SYS.2.1 Allgemeiner Client
- SYS.2.2.3 Clients unter Windows 10
- APP.1.2 Webbrowser

Geänderte Bausteine Edition 2022	Gefährdung hinzugekommen	Gefährdung entfallen
CON.3 Datensicherungskonzept	G 0.16 , G 0.39	
CON.8 Software-Entwicklung		
CON.10 Entwicklung von Webanwendungen		
OPS.1.1.5 Protokollierung		G 0.40
OPS.1.1.6 Software-Tests und -Freigaben		
OPS.1.2.5 Fernwartung		
APP.3.1 Webanwendungen und Webservices	G 0.14	G 0.21, G 0.22, G 0.32, G 0.36
APP.4.3 Relationale Datenbanken	G 0.28	G 0.19, G 0.21, G 0.39, G 0.40, G 0.43
APP.6 Allgemeine Software		
SYS.1.1 Allgemeiner Server	G 0.37	G 0.9, G 0.44
SYS.1.5 Virtualisierung	G 0.14, G 0.28, G 0.31	G 0.40
SYS.1.7 IBM Z		
SYS.2.1 Allgemeiner Client	G 0.8, G 0.18, G 0.27, G 0.29, G 0.37	G 0.20, G 0.43
SYS.2.2.3 Clients unter Windows 10	G 0.14, G 0.37	G 0.16, G 0.17, G 0.31, G 0.32, G 0.45, G 0.46
APP.1.2 Webbrowser	G 0.46	G 0.26
INF.2 Rechenzentrum sowie Serverraum		

Abbildung 2. Übersicht der neuen und entfallenen Gefährdungen

Anforderung	Verknüpfung hinzugekommen	Verknüpfung entfallen
CON.3.A.12		G 0.19
CON.3.A.9		G 0.19, G 0.29
OPS.1.1.5.A1	G 0.18	G 0.29
OPS.1.1.5.A4		G 0.29
OPS.1.1.5.A5	G 0.32, G 0.46	
OPS.1.1.5.A6		G 0.29
OPS.1.1.5.A9	G 0.18, G 0.27	
OPS.1.1.5.A10	G 0.22	
OPS.1.1.5.A11	G 0.37	
OPS.1.1.5.A13	G 0.27	G 0.40
APP.3.1.A1		G 0.36
APP.3.1.A7	G 0.31	
APP.3.1.A8		G 0.21, G 0.28, G 0.30
APP.3.1.A9		G 0.23
APP.3.1.A11	G 0.23	G 0.18
APP.3.1.A21	G 0.14, G 0.23	G 0.15, G 0.19, G 0.31
APP.3.1.A22	G 0.28	
APP.3.1.A20		G 0.19
APP.4.3.A1		G 0.30
APP.4.3.A3		G 0.19, G 0.21, G 0.39, G 0.46
APP.4.3.A4	G 0.18	G 0.14, G 0.15, G 0.19, G 0.21, G 0.22, G 0.23, G 0.30, G 0.46
APP.4.3.A9	G 0.27	G 0.21, G 0.22, G 0.46
APP.4.3.A11		G 0.25, G 0.26, G 0.40
APP.4.3.A12	G 0.18, G 0.31	G 0.14, G 0.15, G 0.19, G 0.21, G 0.22, G 0.23, G 0.30, G 0.39, G 0.46
APP.4.3.A13	G 0.31	G 0.23
APP.4.3.A16		G 0.43
APP.4.3.A17	G 0.18, G 0.45, G 0.46	G 0.21, G 0.22, G 0.26
APP.4.3.A18		G 0.40
APP.4.3.A19	G 0.28	G 0.19, G 0.21, G 0.22, G 0.23, G 0.31, G 0.39, G 0.46
APP.4.3.A20	G 0.28, G 0.31	G 0.19, G 0.22, G 0.23, G 0.26, G 0.30, G 0.46
APP.4.3.A21		G 0.19, G 0.21, G 0.46
APP.4.3.A22	G 0.27	G 0.25, G 0.40, G 0.45
APP.4.3.A23	G 0.18	G 0.21, G 0.22
APP.4.3.A24	G 0.45	G 0.15, G 0.19, G 0.22, G 0.23, G 0.39, G 0.46
APP.4.3.A25	G 0.31	G 0.15, G 0.18, G 0.19, G 0.21, G 0.22, G 0.26, G 0.30, G 0.39, G 0.46
APP.1.2.A1		G 0.39
APP.1.2.A2	G 0.15	G 0.19
APP.1.2.A3		G 0.19, G 0.22
APP.1.2.A9		G 0.26, G 0.28, G 0.39

Abbildung 3. Übersicht der geänderten Verknüpfungen zwischen Gefährdungen und Anforderungen - Teil 1

Anforderung	Verknüpfung hinzugekommen	Verknüpfung entfallen
SYS.1.1.A1	G 0.21	G 0.8, G 0.9, G 0.25, G 0.26, G 0.44
SYS.1.1.A5		G 0.14, G 0.19, G 0.22, G 0.30, G 0.32, G 0.46
SYS.1.1.A6	G 0.18	G 0.30
SYS.1.1.A9		G 0.21, G 0.22, G 0.40
SYS.1.1.A10	G 0.37	G 0.23, G 0.25, G 0.26, G 0.30
SYS.1.1.A11		G 0.8, G 0.9, G 0.16, G 0.20, G 0.25, G 0.27, G 0.28, G 0.30, G 0.44, G 0.45
SYS.1.1.A12		G 0.8, G 0.9, G 0.16, G 0.25, G 0.27, G 0.28, G 0.30, G 0.39, G 0.44
SYS.1.1.A13		G 0.23, G 0.26, G 0.28, G 0.32
SYS.1.1.A15		G 0.25, G 0.26
SYS.1.1.A16	G 0.18	G 0.20, G 0.25, G 0.26, G 0.28, G 0.30, G 0.46
SYS.1.1.A19		G 0.25, G 0.40
SYS.1.1.A21	G 0.18, G 0.22, G 0.37, G 0.45	G 0.8, G 0.9, G 0.14, G 0.16, G 0.21, G 0.25
SYS.1.1.A22	G 0.18, G 0.27	G 0.14, G 0.19
SYS.1.1.A23	G 0.18	G 0.21, G 0.22, G 0.23, G 0.32, G 0.40
SYS.1.1.A24		G 0.25, G 0.26, G 0.27
SYS.1.1.A25	G 0.19, G 0.27, G 0.31	G 0.9
SYS.1.1.A35	G 0.14, G 0.27	G 0.25, G 0.26
SYS.1.1.A37	G 0.21, G 0.31, G 0.39, G 0.45	
SYS.1.1.A27	G 0.30	G 0.25, G 0.26, G 0.27
SYS.1.1.A28	G 0.27	G 0.8, G 0.9, G 0.16
SYS.1.1.A30		G 0.23, G 0.32, G 0.40
SYS.1.1.A31		G 0.20, G 0.21, G 0.22, G 0.40
SYS.1.1.A33	G 0.18, G 0.23	G 0.19, G 0.40
SYS.1.1.A34		G 0.21
SYS.1.1.A36	G 0.21	G 0.25, G 0.28
SYS.1.1.A38	G 0.21, G 0.28, G 0.39, G 0.46	
SYS.1.5.A2	G 0.23, G 0.28, G 0.31	
SYS.1.5.A3	G 0.18, G 0.21, G 0.31	G 0.29, G 0.30
SYS.1.5.A5	G 0.21	G 0.22
SYS.1.5.A6		G 0.25, G 0.26, G 0.29
SYS.1.5.A7		G 0.25, G 0.26, G 0.27
SYS.1.5.A8	G 0.18	G 0.26
SYS.1.5.A10	G 0.18	G 0.19
SYS.1.5.A11		G 0.19
SYS.1.5.A13	G 0.27	
SYS.1.5.A14	G 0.18	G 0.19, G 0.23, G 0.29, G 0.30
SYS.1.5.A15		G 0.22, G 0.26, G 0.27, G 0.30
SYS.1.5.A16	G 0.14	
SYS.1.5.A17	G 0.18	
SYS.1.5.A19	G 0.18	G 0.29
SYS.1.5.A20	G 0.27	
SYS.1.5.A22	G 0.28	G 0.19, G 0.22
SYS.1.5.A23	G 0.14, G 0.23	G 0.15, G 0.22
SYS.1.5.A24	G 0.25, G 0.31	G 0.22, G 0.26, G 0.30
SYS.1.5.A25	G 0.30	G 0.26, G 0.40
SYS.1.5.A26		G 0.22
SYS.1.5.A28	G 0.14	G 0.15

Abbildung 4. Übersicht der geänderten Verknüpfungen zwischen Gefährdungen und Anforderungen - Teil 2

Anforderung	Verknüpfung hinzugekommen	Verknüpfung entfallen
SYS.2.1.A1	G 0.30	G 0.14, G 0.19, G 0.22, G 0.23, G 0.36
SYS.2.1.A3		G 0.20, G 0.25, G 0.26
SYS.2.1.A6		G 0.22, G 0.26, G 0.40
SYS.2.1.A8		G 0.21, G 0.31, G 0.45
SYS.2.1.A42	G 0.29	G 0.22, G 0.45, G 0.46
SYS.2.1.A9	G 0.18	G 0.19, G 0.31, G 0.43
SYS.2.1.A10	G 0.18	G 0.22, G 0.23, G 0.31, G 0.43
SYS.2.1.A11	G 0.18	G 0.25, G 0.31
SYS.2.1.A14		G 0.21, G 0.26
SYS.2.1.A15		G 0.21, G 0.22, G 0.40, G 0.45
SYS.2.1.A16		G 0.19, G 0.40, G 0.45
SYS.2.1.A18		G 0.19, G 0.45
SYS.2.1.A20	G 0.18	G 0.15
SYS.2.1.A21		G 0.19
SYS.2.1.A23	G 0.23	G 0.21, G 0.40, G 0.43
SYS.2.1.A24	G 0.21, G 0.23	
SYS.2.1.A26		G 0.21
SYS.2.1.A27	G 0.45	G 0.14
SYS.2.1.A43	G 0.18, G 0.29	G 0.23, G 0.26, G 0.30, G 0.31
SYS.2.1.A44	G 0.18	G 0.23
SYS.2.1.A28	G 0.31	G 0.15, G 0.45
SYS.2.1.A29		G 0.21, G 0.40
SYS.2.1.A30	G 0.25	G 0.21
SYS.2.1.A32		G 0.19, G 0.21, G 0.22, G 0.30, G 0.39, G 0.40, G 0.43, G 0.45
SYS.2.1.A33	G 0.23	G 0.21, G 0.45
SYS.2.1.A36		G 0.14, G 0.19, G 0.20, G 0.23, G 0.30
SYS.2.1.A37		G 0.39, G 0.43, G 0.45
SYS.2.1.A39	G 0.8	G 0.25, G 0.31
SYS.2.1.A40	G 0.18	G 0.21, G 0.25
SYS.2.1.A41	G 0.27	G 0.25, G 0.31, G 0.43
SYS.2.1.A45	G 0.37	G 0.30, G 0.31
SYS.2.2.3.A1		G 0.19, G 0.36, G 0.45, G 0.46
SYS.2.2.3.A4		G 0.15, G 0.18, G 0.29, G 0.36, G 0.46
SYS.2.2.3.A5		G 0.21, G 0.22, G 0.23, G 0.28
SYS.2.2.3.A6		G 0.15, G 0.36
SYS.2.2.3.A9		G 0.18, G 0.31
SYS.2.2.3.A11		G 0.18, G 0.28
SYS.2.2.3.A12		G 0.18, G 0.19, G 0.32, G 0.46
SYS.2.2.3.A13		G 0.18, G 0.29, G 0.46
SYS.2.2.3.A14		G 0.18, G 0.29, G 0.46
SYS.2.2.3.A15		G 0.18, G 0.29, G 0.46
SYS.2.2.3.A16		G 0.18
SYS.2.2.3.A17	G 0.19	G 0.16, G 0.17, G 0.18
SYS.2.2.3.A18		G 0.15, G 0.18, G 0.31
SYS.2.2.3.A19		G 0.15, G 0.18, G 0.19, G 0.31
SYS.2.2.3.A20		G 0.19, G 0.28, G 0.30, G 0.31, G 0.32
SYS.2.2.3.A21	G 0.14	G 0.16, G 0.17, G 0.18
SYS.2.2.3.A22	G 0.30	G 0.18
SYS.2.2.3.A23	G 0.14	G 0.18
SYS.2.2.3.A24	G 0.37	
SYS.2.2.3.A25	G 0.30, G 0.37	G 0.15, G 0.18, G 0.29

Abbildung 5. Übersicht der geänderten Verknüpfungen zwischen Gefährdungen und Anforderungen - Teil 3



Diese Hinweise betreffen **nur** die Nachmodellierung beim **Update des IT-Grundschutz-Kompends von der Edition 2021 auf die Edition 2022**. Wird eine Neumodellierung vorgenommen, so werden die Bausteine, Anforderungen, elementaren Gefährdungen und die dazugehörigen Verknüpfungen korrekt modelliert.

1.2.2. Umsetzungshinweise

Die Umsetzungshinweise sind **laut BSI** nicht Bestandteil des IT-Grundschutz-Kompends. Aus diesem Grund beinhaltet das **IT-Grundschutz-Kompendum 10.0 Edition 2022** keine Umsetzungshinweise mehr. Diese werden jedoch ab Edition 2022 separat zur Verwendung in verinice zur Verfügung gestellt.



Aufgrund der zahlreichen Veränderungen an den Bausteinen und Anforderungen über die letzten Jahre, ist die *Passgenauigkeit* bei einigen Umsetzungshinweisen der einzelnen Editionen inzwischen teilweise fragwürdig. Das verinice.TEAM stellt diese dennoch **ohne jegliche inhaltliche Redaktion** bereit. Anwenderinnen und Anwender der Umsetzungshinweise sollten die Verwendung im Detail prüfen!

Die einzelnen Umsetzungshinweise werden jeweils nach Editionen sortiert zur Verfügung gestellt. Folgende Editionen der Umsetzungshinweise sind im Shop oder Repository zu finden:

- Umsetzungshinweise aus der Edition 2019
- Umsetzungshinweise aus der Edition 2020
- Umsetzungshinweise aus der Edition 2021
- Umsetzungshinweise aus der Edition 2022

Da die Umsetzungshinweise ab sofort in einzelnen .VNA-Dateien zur Verfügung gestellt werden, sind **keine** Verknüpfungen mehr zwischen Anforderungen und Maßnahmen vorhanden. Aus diesem Grund sollten Sie folgende Einstellung für die korrekte Modellierung vornehmen: **Bearbeiten > Einstellungen > BSI IT-Grundschutz > Modelliere Umsetzungshinweise / Maßnahmen deaktivieren**. Diese Einstellung wird ab verinice 1.24 nicht mehr nötig sein. Sollte diese Einstellung in Vorfeld **nicht** vorgenommen werden, so werden die Anforderungen stets mit "Aus Maßnahme ableiten" angelegt. Dies kann natürlich nachträglich mit Mehraufwand im Editor geändert werden.



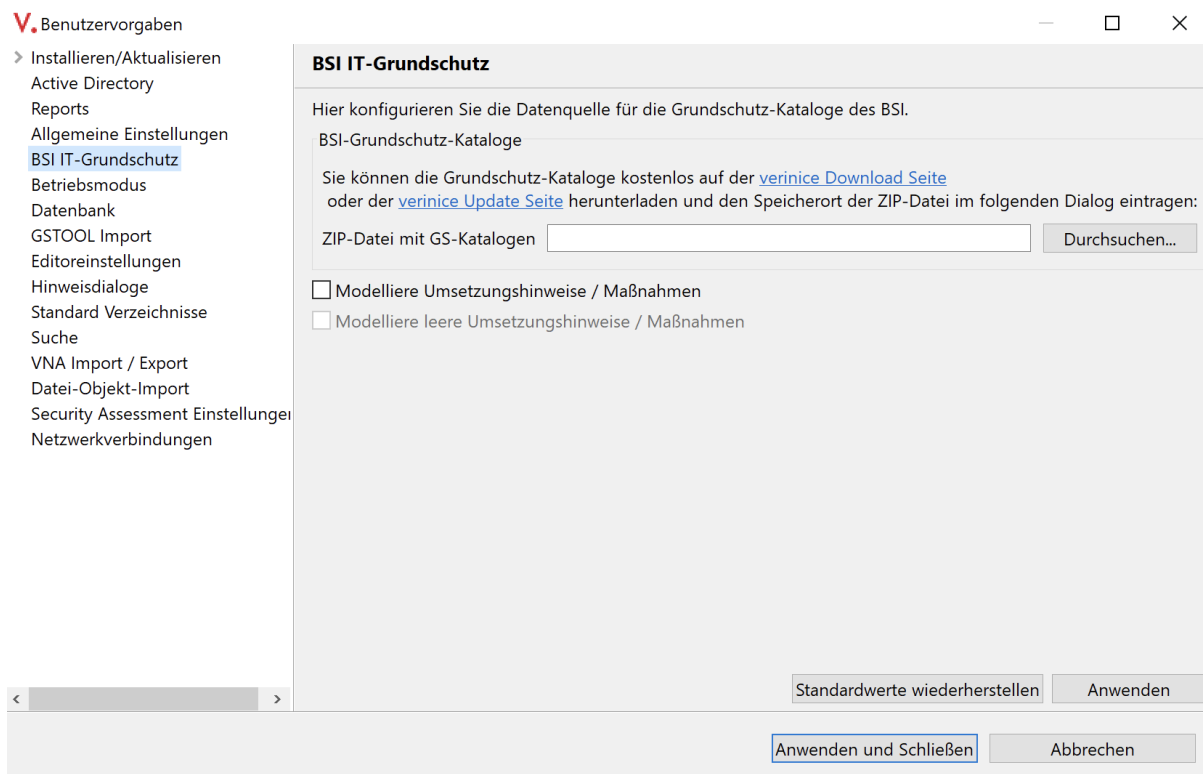


Abbildung 6. Einstellungen: Modelliere Umsetzungshinweise



Weitere **wichtige Informationen** entnehmen Sie direkt den Umsetzungshinweisen.

1.3. Verwendung

Im View **Kataloge** steht das gesamte IT-Grundschatz-Kompodium zur Modellierung zur Verfügung. Dabei sind alle Elemente im View **Kataloge** schreibgeschützt. Sie können Bausteine nun per Drag-and-Drop aus dem View **Kataloge** auf Zielobjekte in Ihrem Informationsverbund modellieren.

Bitte beachten Sie hierzu auch das verinice Referenzhandbuch und das Trainingshandbuch für den Modernisierten IT-Grundschatz. Die bereits mit verinice 1.20 eingeführte Update-Funktion aus einer vorherigen Edition des IT-Grundschatz-Kompodiums ist ausführlich im **folgenden Video** beschrieben.

