
VIVA2

Release latest

25.05.2023

1	Einführung	3
2	Systemvoraussetzungen	5
3	Installation	7
4	Einrichtung	9
5	Aktualisierung des Kompendiums	11
6	IT-Grundschutz-Profile	13
7	Migration von VIVA1 zu VIVA2	15
8	Übersicht	19
9	VIVA2-Objektypen	21
10	Strukturanalyse	25
11	Schutzbedarfsfeststellung	29
12	Modellierung des Informationsverbundes	37
13	IT-Grundschutz-Check	41
14	Reports	43
15	Changelog	45
16	License	55

Das VIVA2 Add-On unterstützt beim Aufbau und der Dokumentation eines ISMS (Information Security Management Systems) nach den neuen BSI IT-Grundsicherungsstandards 200-1 und 200-2.



Das VIVA2 Add-on ist eine technisch und inhaltlich modernisierte Version des VIVA Add-on, die sich an den BSI IT-Grundschutzstandards 200-1 und 200-2 orientiert. Wie auch das vielfach bewährte VIVA Add-On unterstützt Sie das neue VIVA2 beim Aufbau eines Managementsystems für die Informationssicherheit (ISMS) nach der modernisierten BSI IT-Grundschutz-Methodik.

- Aufbau eines ISMS nach BSI-Standards 200-1 und 200-2, nahtlos in die CMDB integriert
- Import der offiziellen Bausteine aus dem BSI IT-Grundschutz-Kompendium
- Zuordnen von Verantwortlichkeiten
- Verwaltung der Anforderungen aus den Bausteinen
- Übersichtliche Verwaltung und Darstellung des IT-Grundschutz-Check
- Erstellung von Berichten und grafischen Übersichten
- Dokumentation des Schutzbedarfs mit visueller Darstellung der Schutzbedarfsvererbung
- Assistentengestützte Datenmigration von VIVA1 nach VIVA2

Bemerkung: Wenn nicht anders erwähnt, bezieht sich diese Dokumentation immer auf die aktuellste Version des VIVA2-Add-ons.

Systemvoraussetzungen

Als Addon für die i-doit CMDB setzt das VIVA2-Addon natürlich ein funktionsfähiges i-doit voraus. Auf ein paar Besonderheiten sollte geachtet werden:

- **Für Upload und Import des Grundschriftkompodiums sollte die maximale Uploadgröße und die PHP-Execution-Time m**

- `upload_max_filesize = 10MB`
 - `post_max_size = 10MB`
 - `max_execution_time = 300`
 - `max_input_time = 300`

- Um das IT-Grundschrift-Kompodium des BSI importieren zu können, muss das Zip-Paket installiert sein, dabei muss die Bibliothek libzip Version 1.2.0 oder höher verwendet werden.
- Der variable Report `IT-Grundschrift-Check` benutzt eine Datenbankfunktion, die von MySQL 5.6 und 5.7 noch nicht unterstützt wird. Für eine vollständige Funktionalität sollte MariaDB ≥ 10.1 oder MySQL ≥ 8.0 eingesetzt werden (s. [Known issues](#)).

Die Installation des VIVA2 Add-Ons entspricht dem Standardvorgehen für die Installation von i-doit Add-Ons:

- Einloggen in des i-doit Admin-Center
- Auf den Reiter „Add-ons“ gehen
- Auf den Button „Install/update Add-on“ klicken
- Das ZIP-Paket des Addons auswählen
- Auf den Knopf „Upload und install“ klicken
- Fertig

3.1 Wichtige Hinweise für das Update auf Version 3.0

Warnung: Da sich innerhalb des VIVA2-Addons die Speicherstrukturen der Anforderungsumsetzungen geändert haben, ist eine Datenmigrationen der schon vorhandenen Daten notwendig. Wenn Sie das VIVA2-Addon in der Version 2.x schon im Einsatz und mit Daten befüllt haben, empfehlen wir daher, vor der Installation des VIVA2 3.0 ein Backup der i-doit-Datenbanken und des i-doit-Verzeichnisses zu machen.

Bemerkung: Folgende Datenänderungen werden durch die Updateskripte durchgeführt:

- Der Umsetzungsstand der Anforderungen in der Kategorie „IT-Grundschutz-Check“ wird jetzt nicht mehr am Baustein gespeichert, sondern an den Zielobjekten/-gruppen bzw. am Informationsverbund. Bei der Updateinstallation wird der am Baustein gespeicherte Umsetzungsstand einer Anforderung an alle Zielobjekten/-gruppen kopiert, denen der Baustein zugeordnet ist.
- Alle Kontaktzuweisungen an Bausteinen, die die Rolle „Ansprechpartner“ haben, werden auf die Rolle „IT-GD: Grundsätzlich zuständig“ umgestellt.

- Die Reports „Nicht vom Informationsverbund abgedeckt“ und „Nicht von Informationsverbänden abgedeckt“ werden gelöscht, alle anderen Reports in der Report-Kategorie „IT-Grundschatz“ werden aktualisiert. Wenn Sie an diesen Reports manuelle Änderungen durchgeführt und in Verwendung haben, sollten Sie diese Reports vor dem Update unter einem anderen Namen speichern.

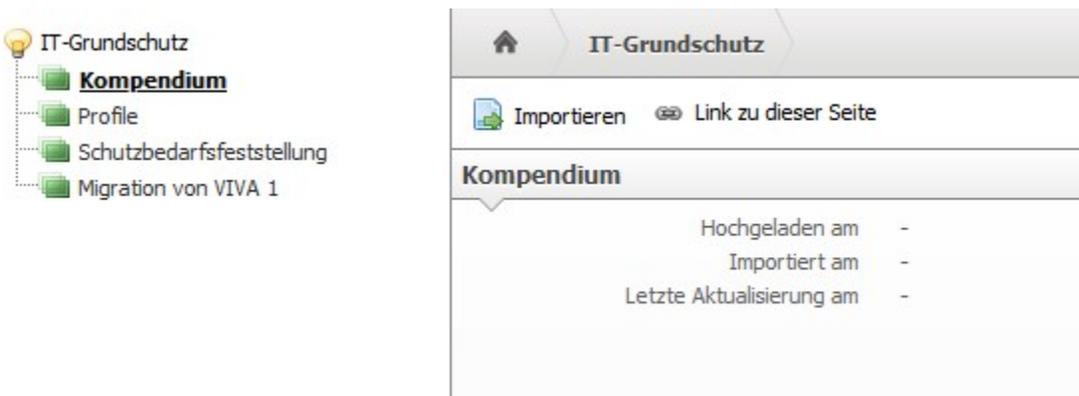
Seit der Version 2.0.3 wird der Anforderungstyp (Basisanforderung/Standardanforderung/Anforderung bei erhöhtem Schutzbedarf) beim Import des IT-Grundschatz-Kompendiums an der Anforderung gespeichert. Wenn seit der Installation der Version 2.0.3 das Kompendium nicht importiert wurde, sollte dies wiederholt werden (egal ob vor oder nach dem Update auf Version 3.0), um den vollen Funktionsumfang des VIVA2 3.0 nutzen zu können.

3.2 Known issues

- Bei Verwendung von MySQL 5.6 und 5.7 funktioniert der variable Report Report: IT-Grundschatz-Check nicht, der mit der gleichnamigen Kategorie am Informationsverbund hängt, da MySQL die Funktion REGEXP_SUBSTR erst ab Version 8.0 implementiert hat. Bei Verwendung von Maria DB gibt es keine Probleme.

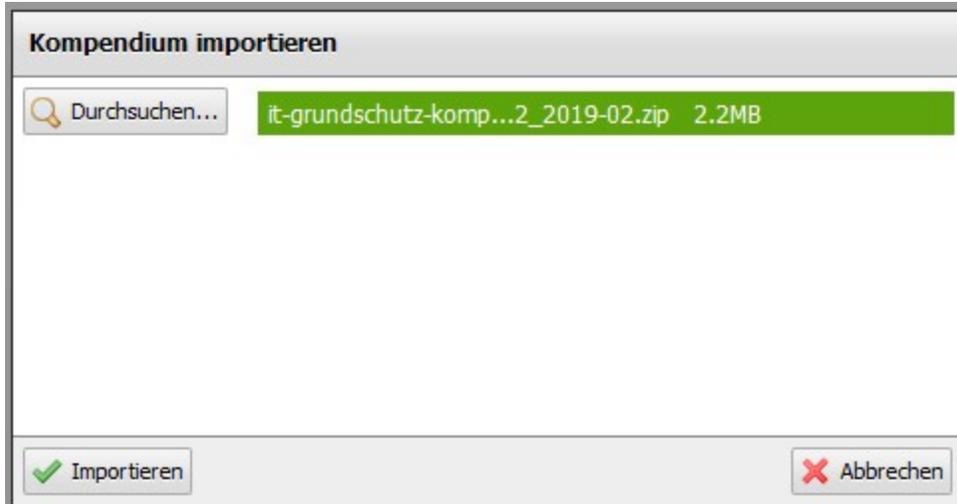
Bevor man mit dem VIVA2-Addon ein ISMS nach BSI Grundschutz-Methodik aufbauen kann, muss das aktuelle Grundschutzkompendium installiert. Dazu geht man im Menü auf Extras IT-Grundschutz und dort auf den ersten Punkt Kompendium.

Warnung: Das IT-Grundschutz-Kompendium ab Edition 2022 kann erst ab VIVA2 Version 3.2 importiert werden. Bitte auch unbedingt die *Systemvoraussetzungen* beachten.



Das Grundschutz-Kompendium zum Import in das VIVA2-Addon kann man sich im i-doit Kundenportal (<https://login.i-doit.com>) herunterladen.

Ein Klick auf den „Importieren“-Button öffnet ein Popup, in dem man über den „Durchsuchen“-Button die ZIP-Datei vom IT-Grundschutz-Kompendiums auswählen muss. Nach dem Auswählen wird die Datei automatisch hochgeladen. Ein grüner Balken signalisiert, dass der Upload erfolgreich war.



Ein Klick auf den „Importieren“-Button startet den initialen Import des IT-Grundschutz-Kompendiums. Dieser Importvorgang kann mehrere Minuten dauern. Sobald sich das Popup automatisch schließt, ist der Importvorgang abgeschlossen und auf der Übersichtsseite ist unter „Importiert am“ der Zeitstempel des Imports eingetragen.

Die technische Einrichtung des VIVA2-Addons ist jetzt abgeschlossen.

Bemerkung: Durch den initialen Import des IT-Grundschutz-Kompendiums des BSI werden mehrere lizenzpflichtige Objekte angelegt. Die genaue Anzahl ist abhängig von der Version des Kompendiums. Bei der aktuellen Edition 2023 sind das:

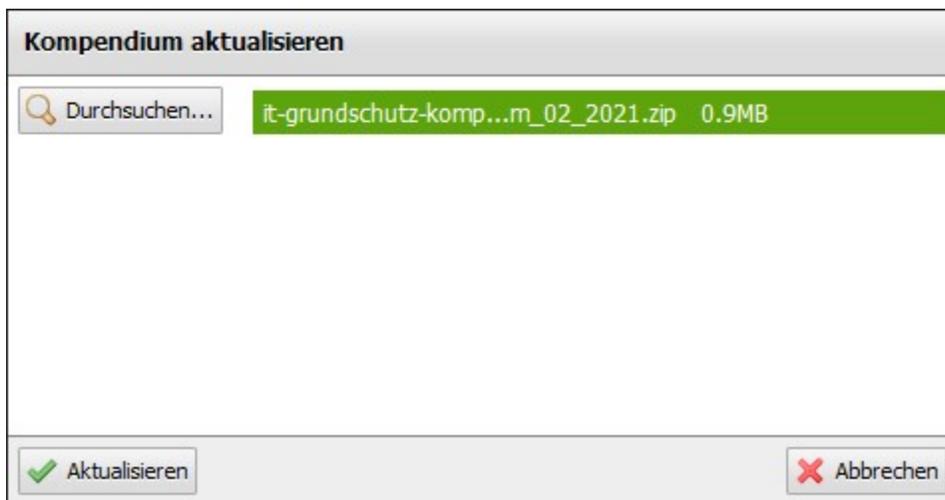
Objekttyp	Anzahl Objekte
Anforderung	2109 (davon 288 entfallen*)
Baustein	111
Gefährdung	691

** Mit dem Import des Grundschutzkompendiums werden auch inzwischen obsoletere Anforderungen mit importiert. Das BSI hat diese Anforderungen mit dem Titel „ENTFALLEN“ versehen. Aus Gründen der Abwärtskompatibilität werden diese Anforderungen alle mit importiert, können aber problemlos hinterher alle gelöscht werden.*

Aktualisierung des Kompendiums

Der Import einer neuen Version des IT-Grundschutz-Kompendiums funktioniert prinzipiell genauso wie der Import während der Ersteinrichtung. Zum Import einer neuen Version des Kompendiums geht man auf Extras IT-Grundschutz und dort auf den ersten Punkt Kompendium.

Ein Klick auf den „Aktualisieren“-Button öffnet ein Popup, in dem man über den „Durchsuchen“-Button die ZIP-Datei vom IT-Grundschutz-Kompendiums auswählen muss. Nach dem Auswählen wird die Datei automatisch hochgeladen. Ein grüner Balken signalisiert, dass der Upload erfolgreich war.



Ein Klick auf den „Aktualisieren“-Button startet den initialen Aktualisierungsassistenten. Dieser vergleicht die installierten Bausteine mit denen im hochgeladenen Grundschutzkompendiums und fragt, welche Elemente importiert werden sollen und welche nicht. Die Auflistung ist unterteilt in die Abschnitte „Neue Bausteine“, „Geänderte Bausteine“ und „Benutzerdefinierte Bausteine“. Standardmäßig werden alle Bausteine, die im hochgeladenen Kompendium enthalten, sowie alle benutzerdefinierten Bausteine zur Übernahme markiert. Der Klick auf den „Weiter“-Button führt zur gleichen Übersicht, nur mit Gefährdungen, ein weiterer Klick auf den „Weiter“-Button führt dann zu den Anforderungen. Wenn man mit den Anforderungen fertig ist, startet der Klick auf den „Übernehmen“-Button den eigentlichen Importvorgang. Dieser Importvorgang kann mehrere Minuten dauern. Sobald sich das Popup automatisch schließt,

ist der Aktualisierungsvorgang abgeschlossen und auf der Übersichtsseite ist unter „Letzte Aktualisierung am“ der Zeitstempel des Imports eingetragen.

Aktualisierung: Bausteine

Neue Bausteine

Liste neuer Bausteine, die durch die Aktualisierung hinzugefügt werden

<input type="checkbox"/> Baustein	Nummer	Im Kompendium enthalten?
<input checked="" type="checkbox"/> SYS. 4.5 Wechseldatenträger	SYS. 4.5	Ja
<input checked="" type="checkbox"/> INF. 11 Allgemeines Fahrzeug	INF. 11	Ja
<input checked="" type="checkbox"/> APP. 6 Allgemeine Software	APP. 6	Ja
<input checked="" type="checkbox"/> APP. 7 Entwicklung von Individualsoftware	APP. 7	Ja
<input checked="" type="checkbox"/> OPS. 1. 2. 5 Fernwartung	OPS. 1. 2. 5	Ja
<input checked="" type="checkbox"/> INF. 5 Raum sowie Schrank für technische Infrastruktur	INF. 5	Ja
<input checked="" type="checkbox"/> INF. 12 Verkabelung	INF. 12	Ja
<input checked="" type="checkbox"/> CON. 10 Entwicklung von Webanwendungen	CON. 10	Ja
<input checked="" type="checkbox"/> APP. 5.3 Allgemeiner E-Mail-Client und -Server	APP. 5.3	Ja
<input checked="" type="checkbox"/> CON. 9 Informationsaustausch	CON. 9	Ja
<input checked="" type="checkbox"/> CON. 8 Software-Entwicklung	CON. 8	Ja

Geänderte Bausteine

Liste bestehender Bausteine, die durch die Aktualisierung verändert werden

<input type="checkbox"/> Baustein	Nummer	Im Kompendium enthalten?
<input checked="" type="checkbox"/> OPS. 1. 1. 2 Ordnungsgemäße IT-Administration	OPS. 1. 1. 2	Ja
<input checked="" type="checkbox"/> OPS. 1. 1. 5 Protokollierung	OPS. 1. 1. 5	Ja
<input checked="" type="checkbox"/> APP. 2. 1 Allgemeiner Verzeichnisdienst	APP. 2. 1	Ja
<input checked="" type="checkbox"/> CON. 2 Datenschutz	CON. 2	Ja
<input checked="" type="checkbox"/> NET. 4.2 VoIP	NET. 4.2	Ja
<input checked="" type="checkbox"/> NET. 3.2 Firewall	NET. 3.2	Ja
<input checked="" type="checkbox"/> APP. 3.4 Samba	APP. 3.4	Ja
<input checked="" type="checkbox"/> IND. 2.2 Speicherprogrammierbare Steuerung (SPS)	IND. 2.2	Ja

Weiter
 Abbrechen

Bemerkung: Alle Bausteine, Gefährdungen und Anforderungen, die nicht mit einem Häkchen in der ersten Spalte versehen werden, werden nicht übernommen. Für bereits vor dem Import vorhandene Elemente bedeutet dies, dass die jeweiligen Objekte automatisch archiviert werden.

IT-Grundschutz-Profile

In VIVA-2 können Grundschutzprofile angelegt, exportiert, importiert und angewendet werden. Ein Profil besteht aus einem Subset von Bausteinen mit zugehörigen Anforderungen und Gefährdungen.

Zur Profilverwaltung kommt man über die Menüpunkte Extras IT-Grundschutz und dort auf den Punkt Profile. Auf der Übersichtsseite sind alle eingerichteten Profile aufgelistet.

The screenshot shows the 'IT-Grundschutz' web interface. On the left is a navigation menu with items: 'IT-Grundschutz', 'Kompendium', 'Profile', 'Schutzbedarfsfeststellung', and 'Migration von VIVA 1'. The main content area has a header 'IT-Grundschutz' with a home icon and a search bar. Below the header is a toolbar with buttons: 'Neu', 'Editieren', 'Löschen', 'Profil importieren', 'Profil exportieren', 'Profil anwenden', and 'Link zu dieser Seite'. A search bar labeled 'Profil-Bezeichnung' is present. Below this is a table with columns: 'Profil-Bezeichnung', 'Bausteine', and 'Gefährdungen'. The table contains one row with a checkbox, 'Profilname', '9', and '222'.

<input type="checkbox"/>	Profil-Bezeichnung	Bausteine	Gefährdungen
<input type="checkbox"/>	Profilname	9	222

Über den Button „Neu“ kann man ein neues Profil anlegen. Dafür muss man dem Profil nur einen Namen geben und die Bausteine auswählen, die Bestandteil des Profils sein sollen. Nach dem Klick auf „Speichern“ werden alle zugehörigen Anforderungen und Gefährdungen angezeigt.

Bausteine
Auswahl der Bausteine: Baustein >> ISHS.1 Sicherheitsmanagement, Baustein >> SYS.1.1 Allgemeiner Server, Baustein >> NET.4.3 Faxgeräte und Faxserver, Baustein >> APP.3.3 Fileserver, Baustein >> APP.3.6 DNS-Server, Baustein >> APP.3.2 Webserver, Baustein >> SYS.1.3 Server unter Unix, ...

Gefährdungslage
Gefährdung: Zeige 50 / 222 Einträge(n)

Gefährdung	Baustein
Software-Schwachstellen oder -Fehler	SYS.1.1 Allgemeiner Server
Datenverlust	SYS.1.1 Allgemeiner Server
Verhinderung von Diensten	SYS.1.1 Allgemeiner Server
Bereitstellung unbenötigter Betriebssystemkomponenten und Applikationen	SYS.1.1 Allgemeiner Server
Überlastung von Servern	SYS.1.1 Allgemeiner Server
G.0.8 Ausfall oder Störung der Stromversorgung	SYS.1.1 Allgemeiner Server
G.0.9 Ausfall oder Störung von Kommunikationsnetzen	SYS.1.1 Allgemeiner Server
G.0.14 Ausspähen von Informationen (Spionage)	SYS.1.1 Allgemeiner Server
G.0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	SYS.1.1 Allgemeiner Server
G.0.18 Fehlplanung oder fehlende Anpassung	SYS.1.1 Allgemeiner Server

Seiten: Previous **1** 2 3 4 5 ▶

Anforderungen
Anforderung: Zeige 50 / 177 Einträge(n)

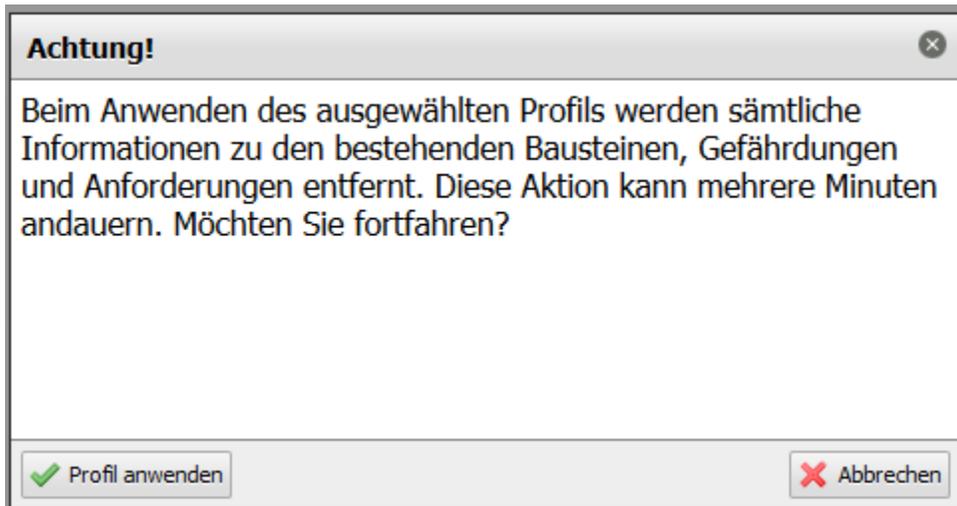
Anforderung	Baustein
Geeignete Aufstellung	SYS.1.1 Allgemeiner Server
Benutzerauthentisierung	SYS.1.1 Allgemeiner Server
Restriktive Rechtevergabe	SYS.1.1 Allgemeiner Server
Rollenrennung	SYS.1.1 Allgemeiner Server
Schutz der Administrationschnittstellen	SYS.1.1 Allgemeiner Server
Deaktivierung nicht benötigter Dienste und Kennungen	SYS.1.1 Allgemeiner Server
Updates und Patches für Firmware, Betriebssystem und Anwendungen	SYS.1.1 Allgemeiner Server
Regelmäßige Datensicherung	SYS.1.1 Allgemeiner Server
Einsatz von Viren-Schutzprogrammen	SYS.1.1 Allgemeiner Server
Protokollierung	SYS.1.1 Allgemeiner Server

Seiten: Previous **1** 2 3 4 ▶

Ein Klick auf den Knopf „Profil exportieren“ lädt das gerade erstellte als ZIP-Paket runter. Dies kann aber auch später über jederzeit die Übersichtsseite gemacht werden.

Diese Zip-Pakete können später auf anderen i-doit-System über den Knopf „Profil importieren“ importiert werden.

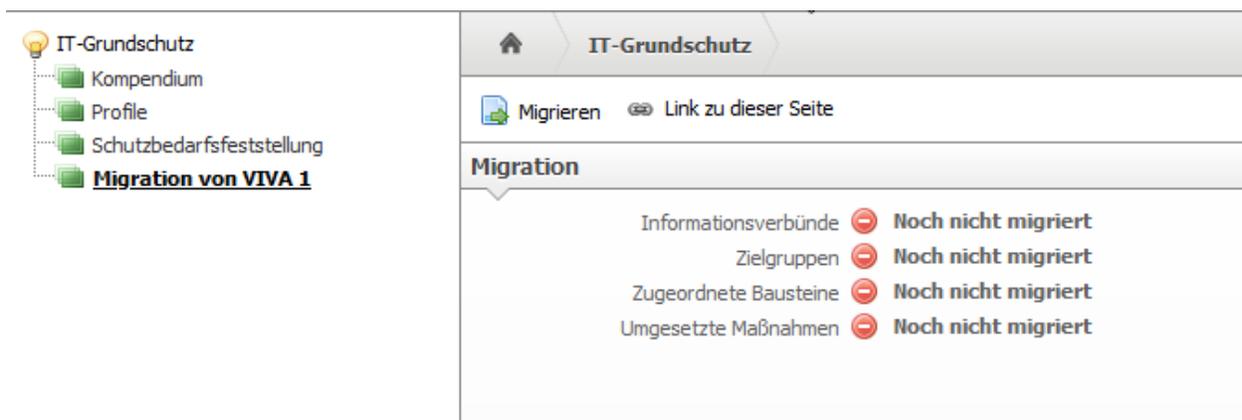
Zum Anwenden eines Profils muss das gewünschte Profil vorne markiert und dann auf den Knopf „Profil anwenden“ geklickt werden.



Diese Warnung sollte auf jedenfall beachtet werden, es werden wirklich alle Bausteine, Gefährdungen und Anforderungen gelöscht und danach die Bausteine, Gefährdungen und Anforderungen aus dem Profile importiert.

Migration von VIVA1 zu VIVA2

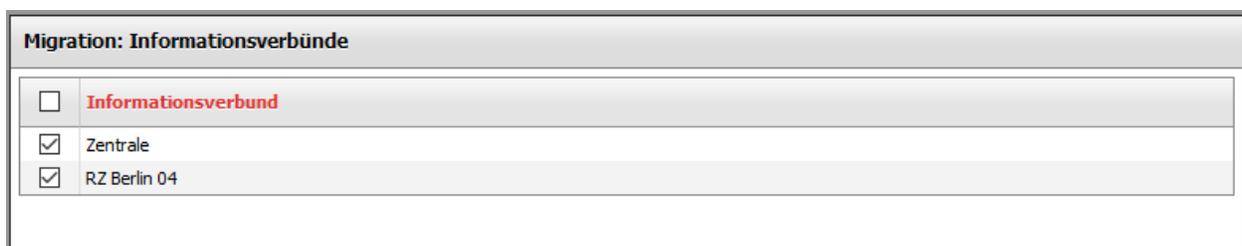
Um Daten aus dem VIVA1-Addon in das VIVA2-Addon zu migrieren, müssen beide Addons installiert und das Grundschutzkompendium im VIVA2-Addon importiert sein. Um die Migration zu starten, geht man im Menü auf Extras IT-Grundschutz und dort auf den Punkt Migration von VIVA 1.



Ein Klick auf den Knopf „Migrieren“ startet den Migrationsassistenten.

Schritt 1: Informationsverbände auswählen

Im ersten Schritt müssen die Informationsverbände ausgewählt werden, die migriert werden sollen.



Mit Klick auf den Knopf „Weiter“ führt zum Schritt 2.

Schritt 2: Zielgruppen migrieren

Im zweiten Schritt werden die Zielobjektgruppen migriert.

Migration: Zielgruppen		
Informationsverbund: Zentrale		
<input type="checkbox"/>	Schicht	Zielobjektgruppe
<input checked="" type="checkbox"/>	IT-Systeme	Administrator-Notebook
<input checked="" type="checkbox"/>	IT-Systeme	Client Switche
<input checked="" type="checkbox"/>	IT-Systeme	Interne Switche
<input checked="" type="checkbox"/>	Infrastruktur	Internes Rack
<input checked="" type="checkbox"/>	IT-Systeme	ITSM VMs
<input checked="" type="checkbox"/>	IT-Systeme	Mitarbeiter-Notebook
<input checked="" type="checkbox"/>	Übergreifende Aspekte	RZ Berlin 04
<input checked="" type="checkbox"/>	Infrastruktur	Serverraum B
<input checked="" type="checkbox"/>	Infrastruktur	Serverraum F
<input checked="" type="checkbox"/>	Netze	Verbindung

Sobald alle zu migrierenden Gruppen markiert sind, geht es mit Klick auf den Knopf „Weiter“ zum nächsten Schritt.

Schritt 3: Bausteine migrieren

Im dritten Schritt werden die Bausteine des alten Standards in Bausteine des neuen Standards migriert. Dafür muss für jeden in VIVA1 zugewiesenen Baustein aus dem Grundschatzkatalog der entsprechende Baustein aus dem Grundschatzkompendium zugewiesen werden.

Migration: Zugewiesene Bausteine			
<input type="checkbox"/>	Baustein	Ausgewählter Baustein	Zielobjektgruppe
<input checked="" type="checkbox"/>	(B 1.0) Sicherheitsmanagement	(ISMS.1) Sicherheitsmanagement	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.1) Organisation	(ORP.1) Organisation	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.2) Personal	(ORP.2) Personal	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.3) Notfallmanagement	(DER.4) Notfallmanagement	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.4) Datensicherungskonzept	(CON.3) Datensicherungskonzept	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.5) Datenschutz	(CON.2) Datenschutz	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.6) Schutz vor Schadprogrammen	-	RZ Berlin 04
<input checked="" type="checkbox"/>	(B 1.7) Kundenkontakt	-	RZ Berlin 04

Der Migrationsassistent versucht zu erkennen, welches der richtige neue Baustein ist und wählt ihn aus. Diese Auswahl sollte trotzdem bei jedem Baustein auf Richtigkeit überprüft werden. Wenn kein passender Baustein gefunden wurde, dann ist kein Baustein vorausgewählt und es muss einer ausgewählt werden. Wenn kein Zielbaustein ausgewählt wird, wird dieser Baustein nicht migriert. Wenn man die komplette Liste der Bausteine bearbeitet hat, geht es mit einem Klick auf den Knopf „Weiter“ zum vierten Schritt.

Schritt 4: Anforderungen migrieren

Im vierten Schritt werden die Maßnahmen aus den alten Bausteine auf die Anforderungen des neuen Standards migriert. Ähnlich wie im vorhergehenden Schritt muss für jede in VIVA1 vorhandene Maßnahme aus dem Grundschatz-

katalog die entsprechende Anforderung aus dem Grundschutzkompendium zugewiesen werden.

Migration: Umgesetzte Maßnahmen

Zentrale >> 3 IT-Systeme >> Mitarbeiter-Notebook

VIVA 1	(B 1.4) Datensicherungskonzept	(M 2.41) Verpflichtung der Mitarbeiter zur Datensicherung
VIVA 2	(CON.3) Datensicherungskonzept	(CON.3.A11) Sicherungskopie der eingesetzten Software

Zentrale >> 3 IT-Systeme >> Administrator-Notebook

VIVA 1	(B 1.4) Datensicherungskonzept	(M 6.33) Entwicklung eines Datensicherungskonzepts
VIVA 2	(CON.3) Datensicherungskonzept	-

Zentrale >> 3 IT-Systeme >> Administrator-Notebook

VIVA 1	(B 1.4) Datensicherungskonzept	(M 6.35) Festlegung der Verfahrensweise für die Datensicherung
VIVA 2	(CON.3) Datensicherungskonzept	-

Auch hier versucht der Migrationsassistent zu erkennen, welches die richtige neue Anforderung ist und wählt sie aus. Diese Auswahl sollte trotzdem für jede Anforderung auf Richtigkeit überprüft werden. Wenn keine passende Anforderung gefunden wurde, dann ist keine Anforderung vorausgewählt und es muss eine ausgewählt werden. Wenn keine Anforderung ausgewählt wird, wird diese Anforderung nicht migriert. Wenn man die komplette Liste der Maßnahmen/Anforderungen bearbeitet hat, geht es mit einem Klick auf den Knopf „Weiter“ zum letzten Schritt.

Schritt 5: Migration starten

Im letzten Schritt werden alle Maßnahmen zur Überprüfung angezeigt, die nicht migriert werden.

Auswertung von umgesetzten Maßnahmen nach Anforderungen

Folgende Abweichungen werden nicht migriert

Baustein	Maßnahme (VIVA 1)	Zielobjektgruppe
(B 1.4) Datensicherungskonzept	(M 2.41) Verpflichtung der Mitarbeiter zur Datensicherung	Zentrale -> 3 IT-Systeme -> Mitarbeiter-Notebook
(B 1.4) Datensicherungskonzept	(M 6.33) Entwicklung eines Datensicherungskonzepts	Zentrale -> 3 IT-Systeme -> Administrator-Notebook
(B 1.4) Datensicherungskonzept	(M 6.35) Festlegung der Verfahrensweise für die Datensicherung	Zentrale -> 3 IT-Systeme -> Administrator-Notebook
(B 1.4) Datensicherungskonzept	(M 2.137) Beschaffung eines geeigneten Datensicherungssystems	Zentrale -> 3 IT-Systeme -> Administrator-Notebook
(B 1.4) Datensicherungskonzept	(M 6.37) Dokumentation der Datensicherung	Zentrale -> 3 IT-Systeme -> Administrator-Notebook
(B 1.4) Datensicherungskonzept	(M 6.20) Geeignete Aufbewahrung der Backup-Datenträger	Zentrale -> 3 IT-Systeme -> Administrator-Notebook

Ein Klick auf den Knopf „Migration starten“ schließt den Assistenten und startet das eigentlich Migrationskript. Je nach Datenmenge kann die Migration mehrere Minuten in Anspruch nehmen.

Sobald auf der Übersichtsseite vor allen Punkten ein grüner Haken ist, ist die Migration abgeschlossen.

Migration

- Informationsverbünde  **Wird migriert**
- Zielgruppen  **Wird migriert**
- Zugeordnete Bausteine  **Wird migriert**
- Umgesetzte Maßnahmen  **Wird migriert**

Übersicht

Durch das VIVA2-Addon wird eine neue Objekttypgruppe „IT-Grundschatz“ erstellt. Dieser Objekttypgruppe werden sechs neue Objekttypen zugeordnet:

- Baustein
- Anforderung
- Gefährdung
- Informationsverbund
- Zielobjektgruppe
- Kommunikationsverbindung

Die Objekte der drei Objekttypen Baustein, Anforderung und Gefährdung werden durch den Import des Grundschatz-kompendiums angelegt und können natürlich auch problemlos durch eigene Bausteine, Anforderungen und Gefährdungen erweitert werden.

Bei der Definition des Informationsverbundes (oder auch mehrerer Informationsverbünde) und im Rahmen der *Strukturanalyse* werden die Objekte der Objekttypen Informationsverbund, Zielobjektgruppe und Kommunikationsverbindung angelegt.



In der *Schutzbedarfsfeststellung* können die Schutzbedarfe definiert und begründet werden. Außerdem kann die Vererbung des Schutzbedarfs in der grafischen Darstellung nachvollzogen und verändert werden.

Im Rahmen der *Modellierung des Informationsverbundes* müssen dem Informationsverbund und den Zielobjekten/Zielobjektgruppen die entsprechenden Bausteine zugeordnet und den Bausteinen die Hauptansprechpartner zugewiesen werden.

Der *IT-Grundsutz-Check* liefert eine Übersicht über die Anforderungen, die an den zugewiesenen Bausteinen hängen, unterteilt nach Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf. Zu den Anforderungen können u.a. Umsetzungsstand, -datum und Verantwortlicher gepflegt werden.

Das VIVA2-Addon installiert mehrere *Reports* zur erweiterten Auswertung und Dokumentation des ISMS.

VIVA2-Objekttypen

Das VIVA2-Addon führt sechs neue Objekttypen ein, die alle in der Objekttypgruppe „IT-Grundschutz“ eingeordnet werden:

9.1 Objekttyp Baustein



Der Objekttyp „Baustein“ bildet die Bausteine aus dem Grundschutzkompendium ab. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Baustein:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

Anforderungen Dies ist eine Multivalue-Kategorie, in der alle Anforderungen verknüpft sind, die zu diesem Baustein gehören.

Baustein Diese Kategorie enthält die textuellen Beschreibungen des Bausteins aus dem Grundschutzkompendium, wie z.B. Nummer, Titel, Einleitung, Zielsetzung und Abgrenzung.

Dateien (*i-doit Standardkategorie*) Hier können zusätzlich Dateien zu diesem Baustein verlinkt werden.

Gefährdungslage Dies ist eine Multivalue-Kategorie, in der alle Gefährdungen verknüpft sind, die zu diesem Baustein gehören.

Kontaktzuweisung (*i-doit Standardkategorie*) Hier müssen die entsprechenden Ansprechpartner für den Baustein eingetragen werden.

Zielobjekte/-gruppen Dies ist eine Multivalue-Kategorie, in der alle Objekte verknüpft sind, denen dieser Baustein zugewiesen (entweder über die Kategorie „Prozessbausteine“ oder über die Kategorie „Zugeordnete Bausteine“).

Zugriff (*i-doit Standardkategorie*) Über die Zugriffs-Kategorie ist der Baustein mit der Bausteinbeschreibung auf der Internetseite des IT-Grundschutzkompendiums des BSI verlinkt.

9.2 Objekttyp Anforderung



Der Objekttyp „Anforderung“ bildet die Anforderungen aus den Bausteinen des Grundsatzkompodium ab. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Anforderung:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

Anforderung Diese Kategorie enthält die textuellen Beschreibungen der Anforderung aus dem Grundsatzkompodium, wie z.B. Nummer, Titel, Anforderungstyp und Beschreibung.

Bausteine Diese Kategorie verknüpft die Anforderung mit dem zugehörigen Baustein. Obwohl dies eine Multivalue-Kategorie ist, macht eine Zuweisung zu mehreren Bausteinen in der Regel keinen Sinn.

Zugriff (*i-doit Standardkategorie*) Über die Zugriffs-Kategorie ist die Anforderung mit der zugehörigen Bausteinbeschreibung auf der Internetseite des IT-Grundsatzkompodiums des BSI verlinkt.

9.3 Objekttyp Gefährdung



Der Objekttyp „Gefährdung“ bildet die Gefährdungen aus den Bausteinen des Grundsatzkompodium ab. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Gefährdung:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

Bausteine Diese Multivalue-Kategorie verknüpft die Gefährdung mit den zugehörigen Bausteinen.

Gefährdung Diese Kategorie enthält die textuellen Beschreibungen der Gefährdung aus dem Grundsatzkompodium, wie z.B. Nummer (nur bei Elementargefährdungen), Titel und Beschreibung.

Zugriff (*i-doit Standardkategorie*) Über die Zugriffs-Kategorie ist die Gefährdung mit der zugehörigen Bausteinbeschreibung auf der Internetseite des IT-Grundsatzkompodiums des BSI verlinkt.

9.4 Objekttyp Informationsverbund



Für jeden Informationsverbund gibt es genau ein Objekt vom Typ „Informationsverbund“. In der Regel gibt es also nur ein Objekt vom Typ Informationsverbund, das VIVA2-Addon bietet aber auch die Möglichkeit, mehrere Informationsverbünde zu dokumentieren. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Informationsverbund:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

IT-Grundsatz (Informationsverbund) Dies ist eine Kategorien-Gruppe, die die folgenden vier Kategorien beinhaltet:

Informationsverbund Hier werden die grundlegenden Informationen zum Informationsverbund dokumentiert wie der bereinigte Netzplan und die Leitlinie zur Informationssicherheit

Infrastrukturanalyse Diese Multivalue-Kategorie zeigt alle mit diesem Informationsverbund über die rückwärtige Kategorie „Informationsverbünde“ direkt verknüpften Objekte an. Mehr dazu findet man unter *Strukturanalyse*.

IT-Grundschutz-Check Die Übersichtsseite zeigt alle durch die Bausteine zugewiesenen Anforderungen, sortiert nach Baustein und Anforderungsnummer. Mehr dazu findet man unter *IT-Grundschutz-Check*.

Prozessbausteine Hier können die Prozessbausteine zugewiesen werden, die für den gesamten Informationsverbund gelten. Aus technischer Sicht können auch Systembausteine zugewiesen werden, in der Regel werden diese jedoch den jeweiligen Zielobjekten bzw. Zielobjektgruppen zugewiesen. Mehr dazu findet man unter *Strukturanalyse*.

Kontaktzuweisung (*i-doit Standardkategorie*) Hier müssen die entsprechenden Rollen für den kompletten Informationsverbund eingetragen werden, allen voran natürlich der Informationssicherheitsbeauftragte (ISB).

Report: Anwendungen ohne Installation Dieser variable Report zeigt alle Anwendungen an, die auf keiner Maschine installiert sind (laut Dokumentation in i-doit). Es werden alle Anwendungen überprüft, die entweder direkt diesem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die diesem Informationsverbund zugeordnet ist.

Report: IT-Grundschutz-Check Dieser variable Report zeigt alle Anforderungen und deren Umsetzungsstatus an, die über Bausteine diesem Informationsverbund zugeordnet sind. Es werden dabei nicht nur die Anforderungen aus den direkt zugewiesenen Bausteinen berücksichtigt, sondern auch die aus den Bausteinen, die den zugewiesenen Zielobjekten/Zielobjektgruppen zugewiesen sind.

Report: Physische Hardware ohne Standort Dieser variable Report zeigt alle Objekte an, denen die Kategorie „Standort“ zugewiesen ist, diese aber nicht gepflegt ist. Es werden alle Objekte überprüft, die entweder direkt diesem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die diesem Informationsverbund zugeordnet ist.

Report: Räume ohne Gebäude Dieser variable Report zeigt alle Räume an, bei denen die Standortkategorie nicht gepflegt ist oder bei denen das Standortobjekt keine Adresse eingetragen hat. Es werden alle Räume überprüft, die entweder direkt diesem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die diesem Informationsverbund zugeordnet ist.

Report: Räume ohne Raumnummer Dieser variable Report zeigt alle Räume an, bei denen keine Raumnummer eingetragen ist. Es werden alle Räume überprüft, die entweder direkt diesem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die diesem Informationsverbund zugeordnet ist.

Report: Vom Informationsverbund abgedeckt Dieser variable Report zeigt alle Objekte an, die entweder direkt diesem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die diesem Informationsverbund zugeordnet ist.

9.5 Objekttyp Zielobjektgruppe



Im Rahmen der Strukturanalyse sollen „ähnliche“ Zielobjekte zur Komplexitätsreduzierung gruppiert werden. Der Objekttyp Zielobjektgruppe dient der Abbildung dieser Gruppierung von Zielobjekten. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Zielobjektgruppe:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

IT-Grundschutz (Zielobjekte) Dies ist eine Kategorien-Gruppe, die die folgenden sieben Kategorien beinhaltet:

Informationsverbünde Diese Multivalue-Kategorie zeigt alle Informationsverbünde an, denen diese Zielobjektgruppe zugewiesen ist (über die rückwärtige Kategorie „Infrastrukturanalyse“). Auch wenn es tech-

nisch möglich ist, die Zielobjektgruppe mehreren Informationsverbänden zuzuweisen, sollte eine Zielobjektgruppe ein der Regel nur einem Informationsverbund zugeordnet werden. Mehr dazu findet man unter *Strukturanalyse*.

IT-Grundschutz-Check Die Übersichtsseite zeigt alle durch die Bausteine zugewiesenen Anforderungen, sortiert nach Baustein und Anforderungsnummer. Mehr dazu findet man unter *IT-Grundschutz-Check*.

Klassifikation von Informationen Hier kann die Klassifikation der Informationen vorgenommen werden, die laut BSI Standard 200-2 Teil der Dokumentation des Sicherheitsprozesses ist.

Schutzbedarfsfeststellung Hier kann der Schutzbedarf für dieses Objekt oder diese Objektgruppe in den definierten Grundwerten festgelegt und begründet werden. Mehr dazu findet man unter *Schutzbedarfsfeststellung*.

Zugeordnete Bausteine Hier können die Bausteine zugeordnet werden, die für dieses Objekt oder diese Objektgruppe gelten sollen. In der Regel werden hier Systembausteine zugeordnet, es ist aber auch möglich hier Prozessbausteine zuzuweisen, wenn es für dieses Objekt oder diese Objektgruppe Abweichungen von den im Informationsverbund zugewiesenen Prozessbausteinen gibt. Mehr dazu findet man unter *Strukturanalyse*.

Zugewiesene Anforderungen Dies ist eine virtuelle Kategorie, die alle Anforderungen anzeigt, die durch die zugeordneten Bausteine zugewiesen werden.

Zugewiesene Gefährdungen Dies ist eine virtuelle Kategorie, die alle Gefährdungen anzeigt, die durch die zugeordneten Bausteine zugewiesen werden.

Kontaktzuweisung (*i-doit Standardkategorie*) Hier können die entsprechenden Ansprechpartner oder andere Rollen für diese Zielobjektgruppe eingetragen werden.

Objektgruppe (*i-doit Standardkategorie*) Hier wird definiert, welche Objekte dieser Zielobjektgruppe zugeordnet sind. Bitte beachten, dass der Typ auf „statisch“ gestellt sein muss, damit die ganzen *Reports* funktionieren.

9.6 Objekttyp Kommunikationsverbindung



Der Objekttyp „Kommunikationsverbindung“ dient der Dokumentation der für den Informationsverbund relevanten Kommunikationsverbindungen. In der Standardkonfiguration gehören folgende Kategorien zu Objekten vom Typ Kommunikationsverbindung:

Allgemein (*i-doit Standardkategorie*) Gehört zu jedem Objekt.

IT-Grundschutz (Zielobjekte) Diese Kategoriegruppierung dient der Zuordnung zum Informationsverbund, der Schutzbedarfsfeststellung, der Zuordnung von Bausteinen und dem IT-Grundschutz-Check (s. *Zielobjektgruppe* für eine ausführlichere Beschreibung).

Kommunikationsverbindung Hier kann dokumentiert werden, welche Objekte oder Objektgruppen diese Kommunikationsverbindung verwenden. Von diesen Objekten wird der Schutzbedarf dann (nach dem Maximumprinzip) auf die Kommunikationsverbindung vererbt. Außerdem kann zur Veranschaulichung der Netzplan mit der hervorgehobenen Kommunikationsverbindung verlinkt werden.

Kontaktzuweisung (*i-doit Standardkategorie*) Hier sollen die Hauptansprechpartner für die Kommunikationsverbindung dokumentiert werden.

Strukturanalyse

Im Rahmen der Strukturanalyse muss sichergestellt werden, dass alle für die Dokumentation des Informationsverbund benötigten Objekte in i-doit angelegt sind. Dies umfasst unter anderem:

- Geschäftsprozesse
- Anwendungen
- IT-System
- ICS-Systeme
- Sonstige Geräte
- Räume

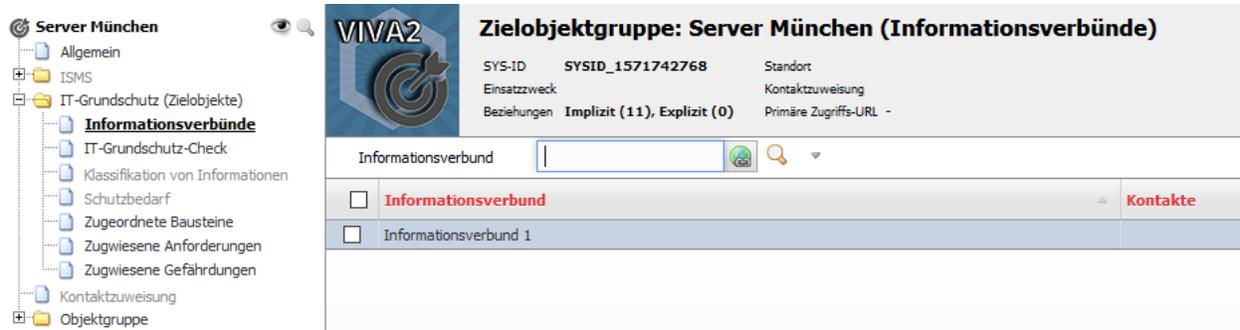
Des Weiteren müssen natürlich auch die Abhängigkeiten der Objekte untereinander vollständig in i-doit dokumentiert werden, u.a.:

- Welche Anwendungen gehören zu welchem Prozess?
- Auf welchen IT-System laufen welche Anwendungen?
- In welchen Räumen stehen welche IT-Systeme?

Unter *Schutzbedarfsfeststellung* finden sich detailliertere Informationen, über welche Objektbeziehungen der Schutzbedarf vererbt wird.

Gruppenbildung

Zur Reduzierung der Komplexität sollten gleichartige Objekte im Objekttyp Zielobjektgruppe gruppiert werden. Der Typ der Objektgruppe muss dabei auf statisch gesetzt bleiben. Die Zielobjektgruppe wird dann über die Kategorie „Informationsverbünde“ dem Informationsverbund zugeordnet werden.



Es ist technisch möglich, eine Zielobjektgruppe mehreren Informationsverbänden zuzuordnen, es wird jedoch empfohlen, eine Zielgruppe immer nur einem Informationsverbund zuzuordnen.

Zuordnung von einzelnen Objekten zum Informationsverbund

Wenn es einzelne Objekte gibt, die dem Informationsverbund zugeordnet werden müssen und denen Bausteine zugeordnet werden müssen, dann gibt es zwei Möglichkeiten, dies umzusetzen:

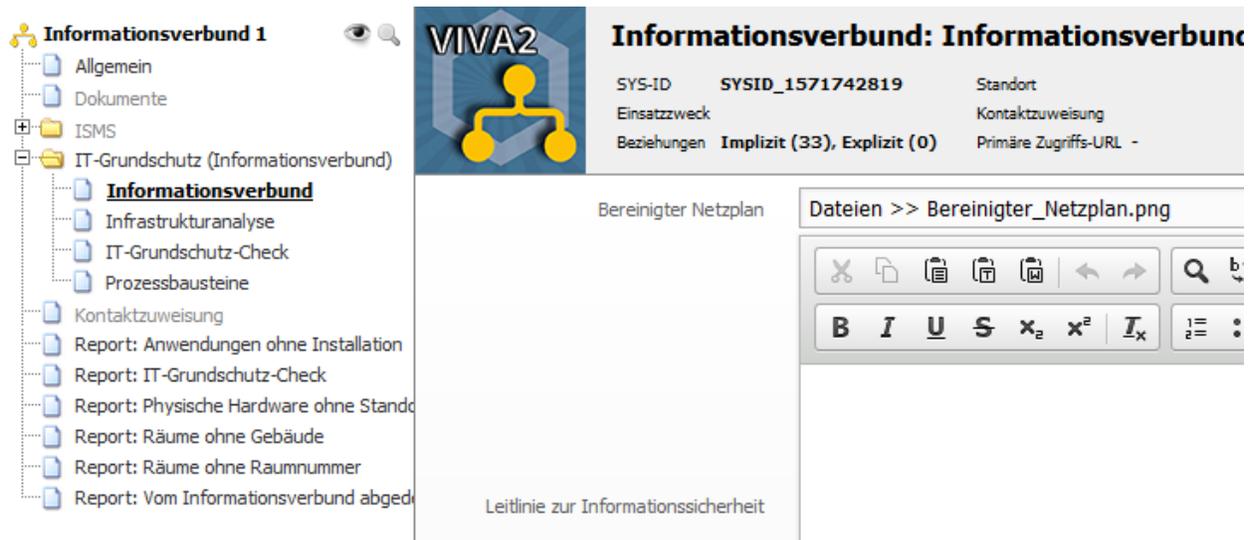
1. Für dieses Objekt wird eine Zielobjektgruppe erstellt und das Objekt wird als einziges Objekt dieser Objektgruppe zugeordnet. Die Zielobjektgruppe wird dann ganz normal dem Informationsverbund zugewiesen.
2. Dem Objekttyp dieses Objekts wird über den Quick Configuration Wizard die Kategorie „IT-Grundschatz (Zielobjekte)“ zugewiesen. In diesem Fall wird dann das Objekt direkt dem Informationsverbund zugewiesen.

Verantwortlichkeiten

Bei allen relevanten Objekten sollte die Dokumentation der Verantwortlichkeiten über die Kategorie Kontaktzuweisung vorgenommen werden.

Bereinigter Netzplan

Der bereinigte Netzplan sollte in der Kategorie „Informationsverbund“ am Informationsverbund verlinkt werden.



Kommunikationsverbindungen

Die zu dokumentierenden Kommunikationsverbindungen werden über den neuen Objekttypen Kommunikationsverbindung in i-doit eingepflegt.

Informationsverbund 1

- Allgemein
- Dokumente
- ISMS
- IT-Grundschatz (Informationsverbund)
 - Informationsverbund**
 - Infrastrukturanalyse
 - IT-Grundschatz-Check
 - Prozessbausteine
- Kontaktzuweisung
- Report: Anwendungen ohne Installation
- Report: IT-Grundschatz-Check
- Report: Physische Hardware ohne Stand
- Report: Räume ohne Gebäude
- Report: Räume ohne Raumnummer
- Report: Vom Informationsverbund abged

VIVA2

Informationsverbund: Informationsverbund

SYS-ID	SYSID_1571742819	Standort
Einsatzzweck		Kontaktzuweisung
Beziehungen	Implizit (33), Explizit (0)	Primäre Zugriffs-URL -

Bereinigter Netzplan

Dateien >> Bereinigter_Netzplan.png

Leitlinie zur Informationssicherheit

Kommunikationsverbindungen werde in der Regel direkt dem Informationsverbund zugeordnet, deswegen ist dem Objekttypen „Kommunikationsverbindung“ die Kategorie „IT-Grundschatz (Zielobjekte)“ initial zugeordnet. In der Kategorie „Informationsverbünde“ muss dann noch der entsprechende Informationsverbund zugeordnet werden.

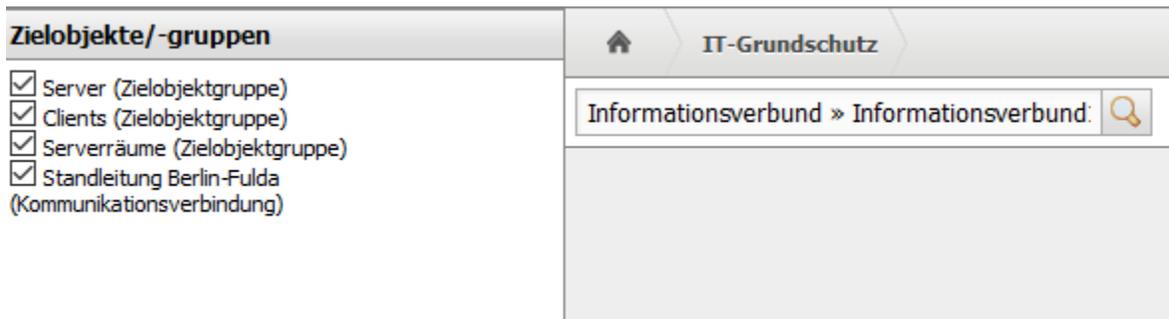
Wenn in der Kategorie „Kommunikationsverbindung“ Objekte bei „Verbindungsteilnehmer“ eingetragen sind, dann wird in der Schutzbedarfsfeststellung der Schutzbedarf von diesen Objekten auf die Kommunikationsverbindung vererbt.

Schutzbedarfsfeststellung

Über den Menüpunkt **Extras** **IT-Grundschutz** und dort auf den Punkt **Schutzbedarfsfeststellung** kommt man zur grafischen Darstellung der Schutzbedarfsfeststellung und -vererbung eines Informationsverbundes.

Um die Schutzbedarfsfeststellung zu laden, muss oben im Objektbrowser zuerst ein Informationsverbund ausgewählt werden. Bei großen Informationsverbänden kann dies durchaus mehrere Sekunden dauern.

Sobald der Informationsverbund geladen ist, werden im linken Bereich alle Zielobjekte/Zielobjektgruppen angezeigt, die über die Kategorie „Informationsverbände“ (bzw. zugehörigen der rückwärtigen Kategorie „Infrastrukturanalyse“ im Informationsverbund) dem ausgewählten Informationsverbund zugeordnet sind.



Im Hauptbereich wird der komplette Informationsverbund grafisch dargestellt.

11.1 Die Schutzbedarfsvererbung

Der Schutzbedarf wird dabei von oben nach unten vererbt, oben angefangen mit den Zielobjekten/Zielobjektgruppen, die dem Informationsverbund zugeordnet sind. Nach unten werden dann alle Objekte geladen (und der Schutzbedarf vererbt), die über einer der folgenden Beziehungen miteinander verbunden sind:

- Gruppenmitgliedschaft
- Service-Komponente
- Softwarezuweisung

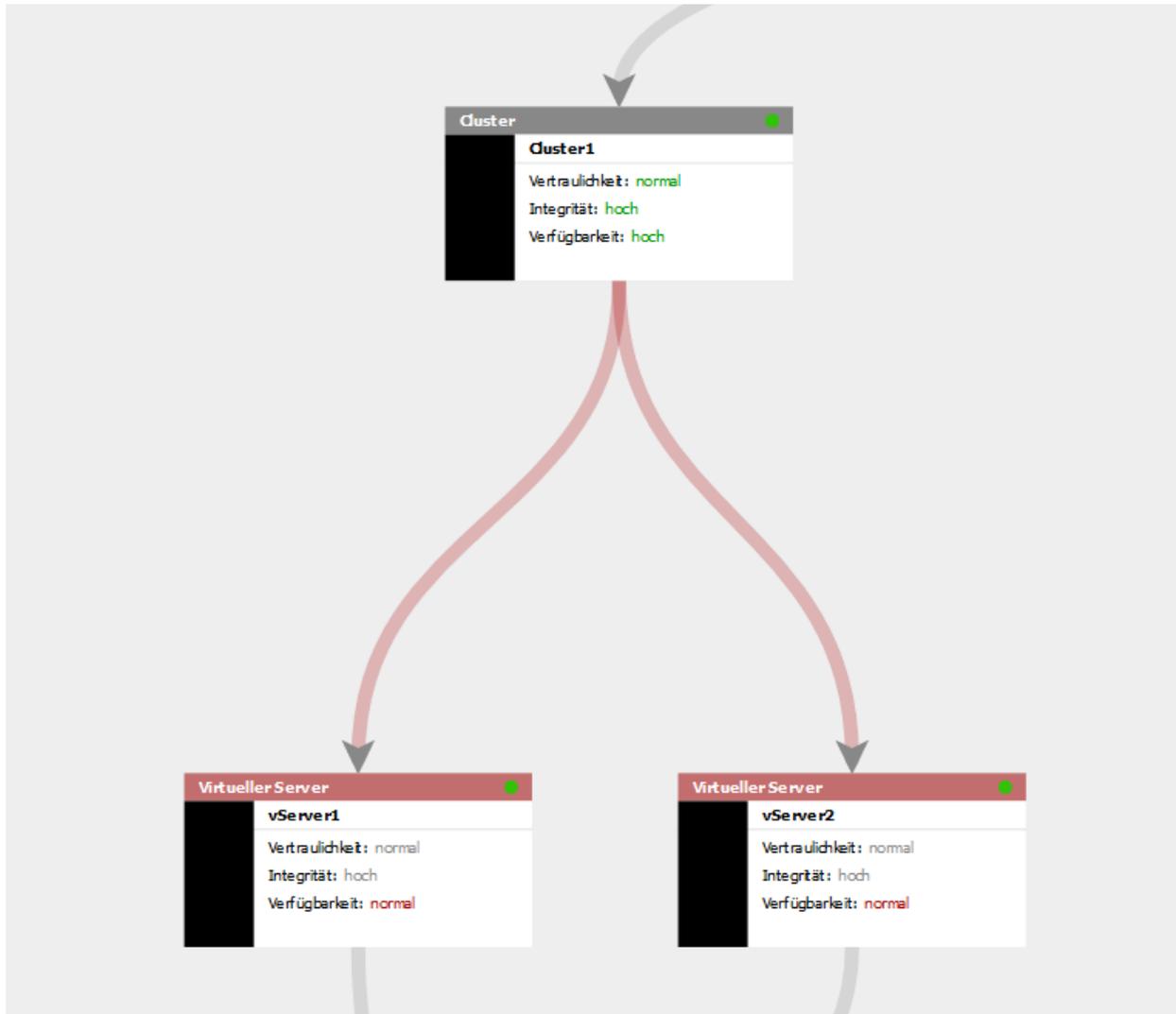
- Anschlüsse
- Clustermitgliedschaften
- Virtuelle Maschine
- Vertragszuweisung
- Kommunikationsverbindung
- Standort

Der Schutzbedarf in den verschiedenen Grundwerten wird dabei nach dem Maximumprinzip nach unten vererbt.



Wenn der Schutzbedarf direkt am Objekt eingetragen ist, dann wird der Wert in grüner Schrift dargestellt, wenn der

Wert vererbt ist, dann wird er grau dargestellt. Wenn der Wert am Objekt niedriger eingestellt wird, als es die Vererbung eigentlich ausgibt, wird der Wert in roter Schrift dargestellt (z.B. beim Verteilungseffekt).



11.2 Filtern der Ansicht

Da die grafische Darstellung von großen Informationsverbänden schnell unübersichtlich wird, besteht die Möglichkeit, die Ansicht auf bestimmte „Teilbäume“ zu beschränken. Standardmäßig sind im linken Bereich alle Zielobjekte/Zielobjektgruppen aktiviert und es wird der komplette Informationsverbund geladen. Wenn man die Ansicht einschränken möchte, kann man im linken Bereich nur die Zielobjekte/Zielobjektgruppen auswählen, die man betrachten möchte. Ein Klick auf den Knopf „Filter anwenden“ rendert die Ansicht dann neu und zeigt nur die Vererbungsbäume der ausgewählten Zielobjekte/Zielobjektgruppen an.

11.3 Schutzbedarf eintragen/ändern

Der Schutzbedarf eines Objektes kann direkt in der grafischen Darstellung bearbeitet werden. Wenn man ein Objekt in der Baumdarstellung anklickt, wird das Objekt in den linken Bereich geladen.

The screenshot displays the VIVA2 interface. On the left, the 'Objektinformationen' (Object Information) panel shows the VIVA2 logo and details for the 'Zielobjektgruppe » Serverräume' (Target Object Group » Server Rooms). It indicates the status is 'In Betrieb' (In Operation) and lists security levels: Vertraulichkeit (Confidentiality) is normal, Integrität (Integrity) is normal, and Verfügbarkeit (Availability) is normal.

Below this, the 'Funktionen' (Functions) panel contains two buttons: 'Objekt öffnen' (Open Object) and 'Schutzbedarf bearbeiten' (Edit Protection Requirement).

On the right, a 'Zielobjektgruppe' (Target Object Group) window is open, showing a tree view with 'Serverräume' (Server Rooms) selected. The details for 'Serverräume' are: Vertraulichkeit: normal, Integrität: normal, and Verfügbarkeit: normal. A blue arrow points from the 'Objekt öffnen' button to this window.

At the bottom of the interface, a timestamp and log entry are visible: '12.05.2020 - 14:27 vServer2 (Typ: "Virtueller Server"): Ein Eintrag in K'.

Wenn man den Schutzbedarf eintragen oder ändern möchte, kann man jetzt mit einem Klick auf „Schutzbedarf bearbeiten“ in die Bearbeitungsmaske gelangen, in der man den Schutzbedarf in den Grundwerten eintragen und eine Begründung für die Einstufung eintragen kann.

Objektinformationen

■ **Zielobjektgruppe »
Serverräume**

■ **In Betrieb**

Vertraulichkeit normal

Integrität normal

Verfügbarkeit normal

Vertraulichkeit

normal ▼

Begründung

Integrität

normal ▼

Begründung

Verfügbarkeit

normal ▼

Begründung

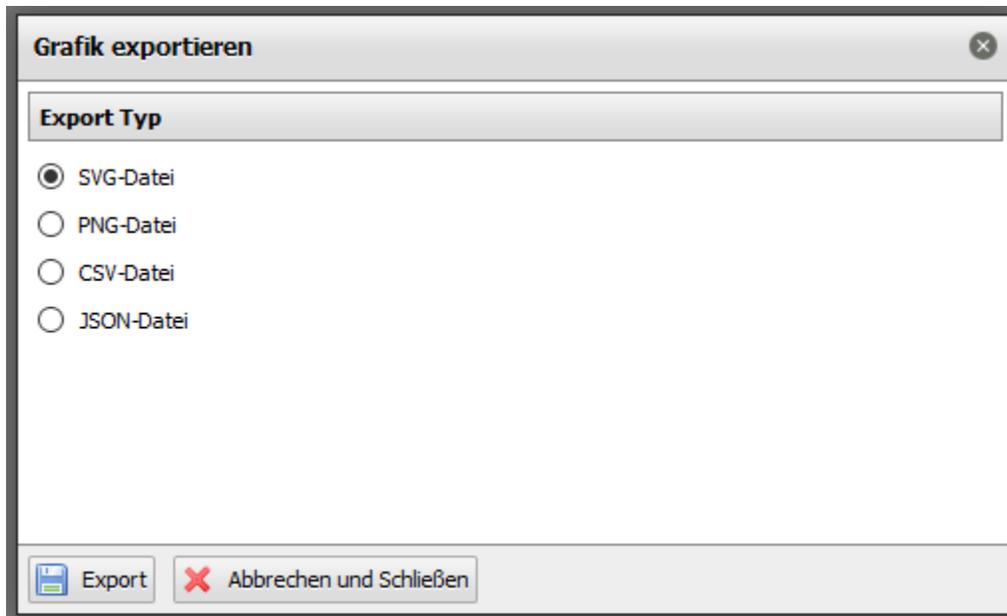
Speichern

Wenn man dann auf Speichern drückt, wird das Objekt mit den entsprechenden Werten gespeichert. Nach dem Speichern muss der Informationsverbund komplett neu geladen werden, weil die Schutzbedarfsvererbung neu berechnet werden muss.

11.4 Schutzbedarf exportieren

Über den Knopf „Export“ rechts oben kann die Schutzbedarfsfeststellung und -vererbung exportiert werden:

- SVG: Der komplette gerenderte Bereich wird im SVG-Format gespeichert.
- PNG: Es wird nur der gerade sichtbare Bereich als PNG-Datei gespeichert.
- CSV: Die Schutzbedarfsfeststellung des gesamten Informationsverbundes wird als CSV-Datei zum Export angeboten. Eine ggf. angegebene Filterung wird ignoriert.
- JSON: Die Schutzbedarfsfeststellung des gesamten Informationsverbundes wird im JSON-Format zum Export angeboten. Eine ggf. angegebene Filterung wird ignoriert.



Modellierung des Informationsverbundes

Bei der Modellierung des Informationsverbundes müssen hauptsächlich die Bausteine des Grundsatzkompendiums dem Informationsverbund und seinen Zielobjekten bzw. Zielobjektgruppen zugeordnet werden. Unterschieden wird hier zwischen der Zuweisung von Prozessbausteinen am Informationsverbund und von (hauptsächlich System-)Bausteinen an Zielobjekten bzw. Zielobjektgruppen.

Die Zuweisung von Prozessbausteinen zum Informationsverbund geschieht über die Kategorie „Prozessbausteine“ am Informationsverbund.

The screenshot shows the VIVA2 interface for an 'Informationsverbund: Information'. On the left, a tree view shows the hierarchy: 'Informationsverbund 1' > 'IT-Grundschutz (Informationsverbund)' > 'Prozessbausteine'. The main panel displays the 'Baustein' (Building Block) list for this information bundle. The list includes various components like 'CON. 1 Kryptokonzept', 'CON. 2 Datenschutz', etc., each with an unchecked checkbox. A search bar at the top right of the list contains the text 'Baustein'.

Baustein	Beziehungen
<input type="checkbox"/> Baustein	
<input type="checkbox"/> CON. 1 Kryptokonzept	Implizit (33), Explizit (0)
<input type="checkbox"/> CON. 2 Datenschutz	
<input type="checkbox"/> CON. 3 Datensicherungskonzept	
<input type="checkbox"/> CON. 4 Auswahl und Einsatz von Standardsoftware	
<input type="checkbox"/> CON. 5 Entwicklung und Einsatz von Allgemeinen Anwendungen	
<input type="checkbox"/> CON. 6 Löschen und Vernichten	
<input type="checkbox"/> CON. 7 Informationssicherheit auf Auslandsreisen	
<input type="checkbox"/> DER. 1 Detektion von sicherheitsrelevanten Ereignissen	
<input type="checkbox"/> DER. 2. 1 Behandlung von Sicherheitsvorfällen	
<input type="checkbox"/> DER. 2. 2 Vorsorge für die IT-Forensik	
<input type="checkbox"/> DER. 2. 3 Bereinigung weitreichender Sicherheitsvorfälle	

Hier müssen jetzt alle relevanten Prozessbausteine dem Informationsverbund zugewiesen werden.

Die Zuweisung von Bausteinen zu Zielobjekten/Zielobjektgruppen geschieht über die Kategorie „Zugeordnete Bausteine“ am Zielobjekt/an der Zielobjektgruppe.

The screenshot shows the VIVA2 interface for a 'Zielobjektgruppe: Server'. On the left, a tree view shows the hierarchy: 'Server' > 'IT-Grundschutz (Zielobjekte)' > 'Zugeordnete Bausteine'. The main panel displays the 'Baustein' (Building Block) list for this target object group. The list includes components like 'SYS. 1. 1 Allgemeiner Server' and 'SYS. 1. 3 Server unter Unix', each with an unchecked checkbox. A search bar at the top right of the list is empty.

Baustein	Beziehungen
<input type="checkbox"/> Baustein	
<input type="checkbox"/> SYS. 1. 1 Allgemeiner Server	Implizit (6), Explizit (0)
<input type="checkbox"/> SYS. 1. 3 Server unter Unix	

Hier müssen jetzt alle für dieses Zielobjekt/diese Zielobjektgruppe relevanten Systembausteine zugeordnet werden. Es können natürlich auch Prozessbausteine zugeordnet werden, wenn dies an dieser Stelle sinnvoll ist (z.B. abweichende

Backupkonzepte für einzelne Objekte).

Kontaktzuweisungen

Für jeden verwendeten Baustein sollten die Verantwortlichkeiten entsprechend über die Kategorie „Kontaktzuweisung“ eingetragen werden.

Reihenfolge

Über die Spalte „Reihenfolge“ kann eine Bearbeitungsreihenfolge der Bausteine eingetragen werden.

IT-Grundschutz-Check

In der Kategorie „IT-Grundschutz-Check“ werden alle Anforderungen aufgelistet, die zu den Bausteinen gehören, die diesem Objekt zugewiesen sind. Dabei werden die Anforderungen sortiert nach Schicht, Baustein und Anforderungstyp aufgelistet. Neben der Anforderungsnummer und dem Titel werden auch die für die Umsetzung der Anforderung Verantwortlichen, der Umsetzungsstatus und das Datum der Umsetzung angezeigt.



ISMS.1 Sicherheitsmanagement

Basisanforderungen

Aktion	Anforderung	Anforderungstitel	Verantwortung	Umsetzungsstatus	Datum der Umsetzung	
		ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Kai Schubert-Altman	ja	06.04.2020
		ISMS.1.A2	Festlegung der Sicherheitsziele und -strategie	Kai Schubert-Altman	nein	31.05.2020
		ISMS.1.A3	Erstellung einer Leitlinie zur Informationssicherheit		nein	
		ISMS.1.A4	Benennung eines Informationssicherheitsbeauftragten		nein	
		ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten		nein	
		ISMS.1.A6	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit		nein	
		ISMS.1.A7	Festlegung von Sicherheitsmaßnahmen		nein	

Ein Klick auf das Lupensymbol zeigt außerdem noch den Text der Anforderung und die Umsetzungsbeschreibung an.

		ISMS.1.A2	Festlegung der Sicherheitsziele und -strategie	Kai Schubert-Altman	nein	31.05.2020
Beschreibung Der Sicherheitsprozess MUSS durch die Leitungsebene initiiert und etabliert werden. Dafür MÜSSEN angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert werden. Es MÜSSEN konzeptionelle Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder der Behörde zu ermöglichen. Die Sicherheitsstrategie und -ziele MÜSSEN von der Institutionsleitung getragen und verantwortet werden. Sicherheitsziele und -strategie MÜSSEN regelmäßig daraufhin überprüft werden, ob sie noch aktuell und angemessen sind sowie wirksam umgesetzt werden können.			Umsetzung FEHLT!			

Ein Klick auf das Stift-Icon öffnet die Bearbeitungsmaske, um den Stand der Umsetzung dieser Anforderung zu dokumentieren.

Anforderungstyp **Basisanforderung**

Anforderung **ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene**

Umsetzungsstatus

Datum der Umsetzung

Verantwortung

Umsetzung

Einmalige Investitionskosten €

Wiederkehrende Kosten €

Einmaliger Personalaufwand

Wiederkehrender Personalaufwand

Bemerkung: In dem Feld „Verantwortung“ können nur Einträge hinzugefügt werden, die in der Kontaktzuweisung des zugehörigen Bausteins eingetragen sind.

Wenn alle Basisanforderungen eines Bausteins umgesetzt sind (Umsetzungstatus „Ja“), dann wird der Baustein mit „Basisabsicherung erreicht“ markiert.

SYS.1.3 Server unter Unix **Basisabsicherung erreicht!**

Basisanforderungen

Aktion	Anforderung	Anforderungstitel	Verantwortung	Umsetzungsstatus
	SYS.1.3.A1	Benutzerauthentisierung unter Unix	Ad Ministrator	ja
	SYS.1.3.A2	Sorgfältige Vergabe von IDs	Ad Ministrator	ja
	SYS.1.3.A3	Automatisches Einbinden von Wechsellaufwerken	Ad Ministrator	ja
	SYS.1.3.A4	Schutz von Anwendungen	Ad Ministrator	ja
	SYS.1.3.A5	Sichere Installation von Software-Paketen	Ad Ministrator	ja

Analog dazu wird der Baustein mit „Standardabsicherung erreicht“ markiert, wenn alle Basisanforderungen umgesetzt sind und alle Standardanforderungen als umgesetzt oder als entbehrlich dokumentiert sind.

Durch das VIVA2-Addon werden mehrere Reports installiert, die der Report-Kategorie „IT-Grundschatz“ zugeordnet werden. Dies umfasst aktuell vier „normale“ Reports:

Meine mir zugewiesenen Anforderungen Dieser Report zeigt alle noch offenen Anforderungen an, die im IT-Grundschatz-Check dem aktuell eingeloggteten User zugewiesen sind (als „zuständig für die Umsetzung“), sortiert nach geplanten Umsetzungsdatum.

Report: Fehlende Verantwortlichkeiten Dieser Report zeigt alle direkt einem Informationsverbund zugewiesene Zielobjekte/Zielobjektgruppen an, die *keine* Kontaktzuweisung mit einer der folgenden Rollen hat:

- Service-Manager
- IT-GS: Informationssicherheitsbeauftragter (ISB)
- IT-GS: Grundsätzlich zuständig
- IT-GS: Fachverantwortliche
- Administrator

Report: Verantwortlichkeiten Dieser Report zeigt alle direkt einem Informationsverbund zugewiesene Zielobjekte/Zielobjektgruppen mit deren Kontaktzuweisung an, die eine der folgenden Rollen hat:

- Service-Manager
- IT-GS: Informationssicherheitsbeauftragter (ISB)
- IT-GS: Grundsätzlich zuständig
- IT-GS: Fachverantwortliche
- Administrator

Report: Von Informationsverbänden abgedeckt Dieser Report zeigt alle Objekte -sortiert nach Informationsverbund- an, die entweder direkt einem Informationsverbund zugeordnet sind oder die Mitglieder einer Zielobjektgruppe sind, die einem Informationsverbund zugeordnet ist.

Die sechs variablen Reports sind alle über gleichnamige benutzerdefinierte Kategorien beim [Informationsverbund](#) eingebunden und dort beschrieben.

15.1 Version 3.2.3

15.1.1 Deutsch

```
[Verbesserung] Der JSON- und CSV-Export berücksichtigen jetzt auch die gesetzten ↵
↳Filter
[Verbesserung] In der Listenansicht der Infrastrukturanalyse wird jetzt auch die ↵
↳Objekt-ID angezeigt
[Verbesserung] Im CSV-Export werden in der "Verbunden mit"-Spalte Objekt-ID und ↵
↳Objekt-Titel mit angezeigt
[Verbesserung] Alphabetische Sortierung der Zielobjekte/-objektgruppen in der ↵
↳Filterung der Schutzbedarfsvererbung
[Verbesserung] Attribut "Abgrenzung" entsprechend dem Grundschutzkompendiums ↵
↳umbenannt nach "Abgrenzung und Modellierung"
[Verbesserung] "Basisabsicherung erreicht" erscheint jetzt auch, wenn Anforderungen ↵
↳als entbehrlich markiert sind
[Verbesserung] Anpassung der Optik und der Iconsets an das neue i-doit Layout
[Bug] Bei Änderung des Schutzbedarfes wurden keine Logbucheinträge erstellt
[Bug] Die Installationroutine des Add-Ons war nicht kompatibel mit i-doit ↵
↳Version >= 23
[Bug] In der Kategorie IT-Grundschutz-Check war an zwei Stellen der ↵
↳Standardname der i-doit-Datenbank hardcodiert
[Bug] In der Kategorie IT-Grundschutz-Check wurde bei "Umsetzung bis" die ↵
↳Uhrzeit mit angezeigt
[Bug] In der Kategorie Schutzbedarf kam es in idoit 25 zu einem Server error
```

15.1.2 English

```
[Improvement] The JSON and CSV export now also consider the applied filters.
[Improvement] The object ID is now displayed in the list view of the infrastructure ↵
↳analysis.
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
[Improvement] The CSV export now includes the object ID and object title in the
↳"Connected with" column.
[Improvement] Alphabetical sorting of target objects/object groups in the
↳protection inheritance filtering.
[Improvement] Renamed attribute "Differentiation" to "Differentiation and modelling
↳" according to the IT-Grundschutz Compendium.
[Improvement] "Basisabsicherung erreicht" now appears even when requirements are
↳marked as dispensable.
[Improvement] Adjustment of the appearance and icon sets to the new i-doit layout.
[Bug] No log entries were created when changing the protection requirement.
[Bug] The installation routine of the add-on was not compatible with i-doit
↳version >= 23.
[Bug] In the IT-Grundschutz-Check category, the standard name of the i-doit
↳database was hardcoded in two places.
[Bug] In the IT-Grundschutz-Check category, the time was displayed for the
↳implementation date
[Bug] In the Protection requirement category an server error occured in
↳idoit 25
```

15.2 Version 3.2.2

15.2.1 Deutsch

```
[Neue Funktion] Die Objekte/Knoten in der grafischen Schutzbedarfsfeststellungen
↳lassen sich jetzt auch vertikal verschieben
[Verbesserung] Weitere optische Anpassungen an das neue i-doit Design
[Verbesserung] Die Höhe der Objekte/Knoten passt sich jetzt der Anzahl der
↳konfigurierten (und vererbten) Grundwerte an
[Verbesserung] Das Attribut "Verantwortung" aus der Kategorie IT-Grundschutz-Check
↳kann jetzt im Report ausgewählt werden
[Verbesserung] Die Kategorie "Klassifikation von Informationen" kann jetzt im Report
↳ausgewählt werden
[Verbesserung]
[Bug] Das Anlegen, Bearbeiten und Verwenden von Grundschutzprofilen war
↳nicht PHP 8 kompatibel
```

15.2.2 English

```
[New function] The objects/nodes of the visual protection requirement assessment can
↳be dragged now in vertical direction too
[Improvement] More visual adaptations to the new i-doit layout
[Improvement] The height of the objects/nodes adapt now to the number of configured
↳(and inherited) basic values
[Improvement] The attribute "Contact person" of the category IT baseline protection
↳can be chosen in the report manager now
[Improvement] The category "Classification of information" can be chosen in the
↳report manager now
[Bug] Creating, editing and the usage of IT baseline protection templates
↳were not compatible with PHP 8
```

15.3 Version 3.2.1

15.3.1 Deutsch

[Verbesserung]	Kompatibilität zu i-doit 1.19
[Verbesserung]	Kompatibilität zu PHP 8.0
[Verbesserung]	Optische Anpassungen an neues Layout von i-doit 1.19
[Bug]	In der Kategorie "Bausteine" wurden die zugewiesenen Zielobjekte/- ↪objektgruppen nicht angezeigt
[Bug]	Die Objekttypicons von "Kommunikationsverbindung" und "Gefährdung" ↪konnten nicht geladen werden
[Bug]	Beim Editieren der Kategorie "IT-Grundschutz-Check" gingen die ↪Verantwortlichen verloren, wenn man aus der "View"-Sicht kam

15.3.2 English

[Improvement]	Compatibility to i-doit 1.19
[Improvement]	Compatibility to PHP 8.0
[Improvement]	Optical improvements to fit new layout of i-doit 1.19
[Bug]	In category "Modules" the assigned target objects/object group were ↪not shown
[Bug]	The object type icons of "Communication link" and "Threat" could'nt ↪be loaded
[Bug]	The responsible contacts were lost, if editing the category "IT ↪baseline check" and coming from "View" view

15.4 Version 3.2

15.4.1 Deutsch

[Neue Funktion]	Unterstützung des neuen Formats des IT-Grundschutzkompendiums 2022
[Neue Funktion]	Im IT-Grundschutz-Check können die Bausteine und Absicherungsarten ↪auf- und zugeklappt werden, der Zustand wird in den persönlichen Usersettings ↪gespeichert
[Verbesserung]	Bearbeitung des Schutzbedarfes am Objekt jetzt per Inline-Editung ↪möglich
[Verbesserung]	Die Editierrechte für die Kategorie Schutzbedarf werden jetzt überall ↪berücksichtigt
[Verbesserung]	Verlinkung des Baustein-Objektes im IT-Grundschutz-Check
[Verbesserung]	Beim Import des Kompendiums wird die Schicht im Baustein mit ↪übernommen
[Verbesserung]	Bereinigung fehlerhafte Einträge in der Kategorie Schutzbedarf
[Änderung]	Die Buttons "Übernehmen" und "Anpassen" in der Kategorie Schutzbedarf ↪wurden entfernt
[Bug]	Geänderte Bausteinnamen wurden beim Kompendiums-Import nicht im ↪Objektnamen aktualisiert
[Bug]	Listeneditierung des Schutzbedarfs konnte zu fehlerhaften ↪Datenbankeinträgen führen
[Bug]	Beim Import des Kompendiums wurden teilweise keine Logbucheinträge ↪geschrieben
[Bug]	Rechtschreibfehler in deutscher Übersetzung wurde behoben

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

[Bug]	Der Menüpunkt "Schutzbedarfsfeststellung" überprüfte das falsche ↵ ↵Benutzerrecht
[Bug]	Es kam zu Fehlern beim Import des Kompendiums, wenn eigene Bausteine, ↵ ↵Anforderungen oder Gefährdungen vorhanden waren
[Bug]	Die Umsetzung der Anforderungen im IT-Grundschutz-Check verloren beim ↵ ↵Speichern Formatierungen und Zeilenumbrüche

15.4.2 English

[New function]	Support of new format of the IT-Grundschutzkompendiums 2022
[New function]	Modules and requirement groups can now be folded and unfolded in the ↵ ↵it baseline protection check, the status is saved in the personal user settings
[Improvement]	Editing of the protection requirement of an object now with inline ↵ ↵editing possible
[Improvement]	Respect edit right of category protection requirement everywhere
[Improvement]	Module objects are now linke din the IT baseline protection check
[Improvement]	The layer of the module is now taken over during import of the ↵ ↵Kompendium
[Improvement]	Clean up wrong database entries of category protection requirement
[Change]	The buttons "Accept" and "Adapt" are removed from category protection ↵ ↵requirement
[Bug]	Changes module names were not updated during import of the Kompendium
[Bug]	List edit of protection requirements possibly led to wrong database ↵ ↵entries
[Bug]	During import of the Kompendium sometimes no log book entries were ↵ ↵wrote
[Bug]	Wrong spelling in german translation was fixed
[Bug]	The menu entry "Assessment of protection requirements" checked wrong ↵ ↵user permissions
[Bug]	The import of the Kompendium led to errors, if custom modules, ↵ ↵requirements or threats were present
[Bug]	The realization of requirements in the IT baseline protection check ↵ ↵lost its formattings and line breaks when saving

15.5 Version 3.1.3

15.5.1 Deutsch

[Bug]	Die Schutzbedarfsfeststellung funktionierte auf einigen Systemen mit ↵ ↵i-doit 1.16 nicht
-------	--

15.5.2 English

[Bug]	The protection requirements didn't work on some systems with i-doit 1. ↵ ↵16
-------	---

15.6 Version 3.1.2

15.6.1 Deutsch

```
[Verbesserung] Neuer Benutzerabhängige Report "Meine mir zugewiesenen Anforderungen"
[Verbesserung] Anpassung der primären Zugriffs-URL an den neuen Aufbau der BSI-
↳ Webseite
[Verbesserung] Neue Icons für das Extra-Menü
[Verbesserung] VIVA2-Objekttypen-Bilder und -icons in den i-doit-Bilderordner
↳ verschoben
[Verbesserung] "Umsetzungsdatum" umbenannt nach "Umsetzung bis"
[Bug] Die Beschreibung des VIVA2-Upload-Ordner in den
↳ Mandanteneinstellungen war falsch
[Bug] Das Attribut "Beschreibung" in der Kategorie IT-Grundschutz
↳ (Informationsverbund) -> IT-Grundschutz-Check wurde nicht gespeichert
```

15.6.2 English

```
[Improvement] New user-dependent report "Requirements assigned to mir"
[Improvement] Adapt primary access URL to new layout of BSI website
[Improvement] New icons in the "Extra" menu
[Improvement] Moved VIVA2 object images and icons into i-doit image folder
[Improvement] Renamed "Implementation date" to "Implementation until"
[Bug] The label of the viva2 upload folder in the tenant settings was wrong
[Bug] The attribute "description" of the category IT baseline protection
↳ (scope) -> IT baseline protection check wasn't saved
```

15.7 Version 3.1.1

15.7.1 Deutsch

```
[Verbesserung] Anpassungen für den Import des Grundschutz-Kompandiums 2020
[Verbesserung] Die Reports "Verantwortlichkeiten" und "Fehlende Verantwortlichkeiten
↳ " überarbeitet und verbessert
[Verbesserung] Doppelt vorhandene Rollen konvertiert und entfernt
[Bug] Kategorie IT-Grundschutz Check funktionierte nicht wenn die Datenbank
↳ nicht „idoit_data“ heißt
[Bug] Profile ließen sich nicht anlegen, wenn der Ordner "exports" nicht im
↳ VIVA2 Addon Ordner vorhanden war
[Bug] Die Druckansicht des variablen Reports "IT-Grundschutz-Check" blieb
↳ leer
```

15.7.2 English

```
[Improvement] The Kompandium 2020 can now be imported
[Improvement] The reports "Responsibilities" and "Missing Responsibilities" are
↳ revised and improved
[Improvement] Duplicate roles are converted and removed
[Bug] Category "IT-Baseline protetion chec" didn't work when the name of
↳ the tenant database wasn't "idoit_data"
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
[Bug] Profiles could not be created when the folder "exports" didn't exist
↳in viva2 addon folder
[Bug] The print view of variable report "IT baseline protection check" was
↳empty
```

15.8 Version 3.1

15.8.1 Deutsch

```
[Neue Funktion] Neuer Objekttyp "Kommunikationsverbindung"
[Neue Funktion] Vererbung des Schutzbedarfs über die neue Beziehung
↳"Kommunikationsverbindung"
[Neue Funktion] Die grafische Darstellung der Schutzbedarfsfeststellung kann jetzt
↳gefiltert werden
[Neue Funktion] Die Begründung für die Schutzbedarfsfeststellung kann in der
↳grafischen Darstellung eingetragen werden
[Verbesserung] Die Begründung für die Schutzbedarfsfeststellung ist jetzt auch im
↳CSV-Export enthalten
[Verbesserung] Rollen, die durch das Grundschutzkompendium hinzugefügt werden,
↳werden jetzt auch deinstalliert
[Verbesserung] Die aktualisierte Dokumentation zum VIVA2-Addons ist ab jetzt hier zu
↳finden: https://viva2.readthedocs.io
[Bug] Übersetzungen für "SVG-Datei" und "PNG-Datei" sind in der 1.14.1
↳nicht mehr vorhanden und werden jetzt durch das Addon geliefert
[Bug] Übersetzung vom "Bitte warten" Overlay der Schutzbedarfsfeststellung
↳wurde nur angezeigt, wenn das Raumplan-Addon installiert ist
[Bug] Die Schutzbedarfsfeststellung zeigte einen Fehler an, wenn die
↳angezeigten Zielobjekte keine Verbindung haben.
```

15.8.2 English

```
[New feature] New object type "communication link"
[New feature] The protection requirements will be inherited over the new relation
↳"communication link"
[New feature] It is now possible to set a filter in the graphical representation of
↳the assessment of protection requirements
[New feature] The reason for the assessment of the protection requirements can now
↳be edited in the graphical representation
[Improvement] The reason for the assessment of the protection requirements in
↳included now in the CSV export
[Improvement] Contact roles, which will be imported by the IT-Grundschutz
↳Compendium, will now be removed during deinstallation of the addon
[Improvement] The updated documentation for the VIVA2 addon can now be found here:
↳https://viva2.readthedocs.io (only in german yet)
[Bug] Translations for "CSV file" and "PNG file" were not available in 1.14.
↳1 anymore
[Bug] Translation of the "Please wait" Overlay in the assessment of
↳protection requirements was only shown, if floorplan addon was installed
[Bug] The assessment of the protection requirements has shown an error, if
↳the shown target objects didn't have any links
```

15.9 Version 3.0

15.9.1 Deutsch

[Neue Funktion] Der Umsetzungsstatus der Anforderungen wird jetzt an den Zielobjekten/
 ↳-gruppen gespeichert

[Neue Funktion] Komplette Überarbeitung des "IT-Grundschutz-Check"

[Neue Funktion] Neue Kategorie "Prozessbausteine" am Informationsverbund

[Verbesserung] Die IT-GS-Kategorien am Informationsverbund sind in einem Ordner_
 ↳zusammengefasst

[Verbesserung] Überarbeitung aller mitgelieferten Reports, Entfernen der Reports
 ↳"Nicht vom Informationsverbund abgedeckt" und "Nicht von Informationsverbänden_
 ↳abgedeckt"

[Verbesserung] Umbenennung von Zielgruppen und Zielobjektgruppen

[Verbesserung] Umbenennung der Rolle "Verantwortliche Stelle" zu "Grundsätzlich_
 ↳zuständig"

[Verbesserung] Alle bei der Installations des VIVA2-Addon hinzugefügten Rollen_
 ↳erhalten den Prefix "IT-GS:"

[Verbesserung] Vorbereitung für nächste Version zum Editieren der Begründung bei der_
 ↳Schutzbedarfsfeststellung

[Bug] Reports mit Kategorien aus VIVA2 führen zu einem SQL-Fehler (behoben_
 ↳ab 1.14.1)

[Bug] Nach dem Import des Kompendiums wird der Suchindex für die neuen/
 ↳geänderten Objekte nicht neu erstellt

[Bug] VIVA2-Deinstallation lässt die Objekttypgruppe im Menü

[Bug] Fehler bei der Listeneditierung der Kategorie IT-Grundschutz-Check

[Bug] Der "Durchsuchen"-Button fehlt in ->Informationsverbund->Bereinigter_
 ↳Netzplan

15.9.2 English

[New feature] The implementation status of the requirements is now saved on the_
 ↳target objects/groups

[New feature] Complete revision of the "IT baseline protection check" category

[New feature] New category "process modules" at the object type "scope"

[Improvement] The addon categories in the object type "scope" are summarized in a_
 ↳folder

[Improvement] Revision of all supplied reports, removal of the reports "Not covered_
 ↳by scope" and "Not covered by scopes"

[Improvement] Renaming target groups into target object groups

[Improvement] Renaming the role "responsible person" to "basically responsible"

[Improvement] All roles added during the installation of the VIVA2 addon are given_
 ↳the prefix "IT-BP:"

[Improvement] Preparation for the next version to edit the reason in the assessment_
 ↳of protection requirements

[Bug] Reports containing categories from VIVA2 led to an SQL error (only_
 ↳working in 1.14.1)

[Bug] After importing the compendium, the search index for the new/changed_
 ↳objects wasn't recreated

[Bug] VIVA2 deinstallation leaves the object type group in the menu

[Bug] Error when using the list edit for the category IT baseline protection

[Bug] The "Browse" button is missing in Scope -> IT baseline protection_
 ↳(Scope)-> Adjusted network plan

15.10 Version 2.0.3

15.10.1 Deutsch

```
[Neue Funktion] Schutzbedarfsfeststellung: Neue Exportmöglichkeit im CSV Format
[Neue Funktion] Schutzbedarfsfeststellung: Neue Exportmöglichkeit im JSON Format
[Verbesserung] Schutzbedarfsfeststellung: Services und deren Beziehungen werden nun
↳berücksichtigt
[Verbesserung] Vorbereitung auf kommendes Major-Realease: Anforderungstyp wird beim
↳Import des Kompendiums an der Anforderung gespeichert
[Bug] Englische Übersetzungen fehlten teilweise
[Bug] Beim Aktualisieren des Grundschutz-Kompendiums sollte es
↳"Benutzerdefinierte Anforderungen" und nicht "Benutzer-definierte Anforderungen"
↳heißen
[Bug] Reports wurden bei der Installation nicht korrekt angelegt
[Bug] Addon wird nicht ordnungsgemäß deinstalliert
```

15.10.2 English

```
[New feature] Assessment of protection requirements: New export option in CSV format
[New feature] Assessment of protection requirements: New export option in JSON format
[Improvement] Assessment of protection requirements: Services and their
↳relationships are now taken into account
[Improvement] Preperation for nect major release: Type of requirement is saved on
↳requirement when importing the IT baseline protection kompendium
[Bug] Some english translations were missing
[Bug] Small fix in german translation
[Bug] Reports were not created correctly during installation
[Bug] Uninstallation of addon does not work correctly
```

15.11 Version 2.0.2

15.11.1 Deutsch

```
[Verbesserung] Neue Icons und Bilder für VIVA2-Objekttypen
[Bug] Reports werden bei der Neuinstallation in i-doit 1.13.1 (und höher)
↳in die falsche Datenbank geschrieben
```

15.11.2 English

```
[Improvement] New icons and images for VIVA2 object types
[Bug] Reports are stored in the wrong database during a new installation in
↳i-doit 1.13.1 (or higher)
```

15.12 Version 2.0.1

15.12.1 Deutsch

[Bug]	YAML ungültig
[Bug]	Doppelte Anzeige von Informationsverbunde in der Migration
[Bug]	Gefährdungen im IT-Grundschutz werden nicht mehr angezeigt
[Bug]	Schutzbedarfsfeststellung lässt sich nicht direkt nach öffnen des Add- ↪Ons aufrufen
[Bug]	Migration von VIVA auf VIVA2 bei leeren Inhalten teilweise fehlerhaft
[Bug]	In Kategorie Zugwiesene Anforderungen wird eine Fehlermeldung, ↪ausgegeben wenn man auf einen Eintrag klickt
[Aufgabe]	VIVA 2 PHP 7.2 Kompabilität

15.12.2 English

[Bug]	Invalid YAML
[Bug]	Double display of information networks in the migration
[Bug]	Threats in basic IT protection are no longer displayed
[Bug]	Schutzbedarfsfeststellung doesn't open when selected right after, ↪opening the add-on
[Bug]	Migration from VIVA to VIVA2 sometimes faulty when using empty content
[Bug]	In category "Assigned requirements" an error message is displayed, ↪when clicking on an entry
[Task]	VIVA 2 PHP 7.2 Compability

KAPITEL 16

License

becon © 2013-2020 becon GmbH