opus i

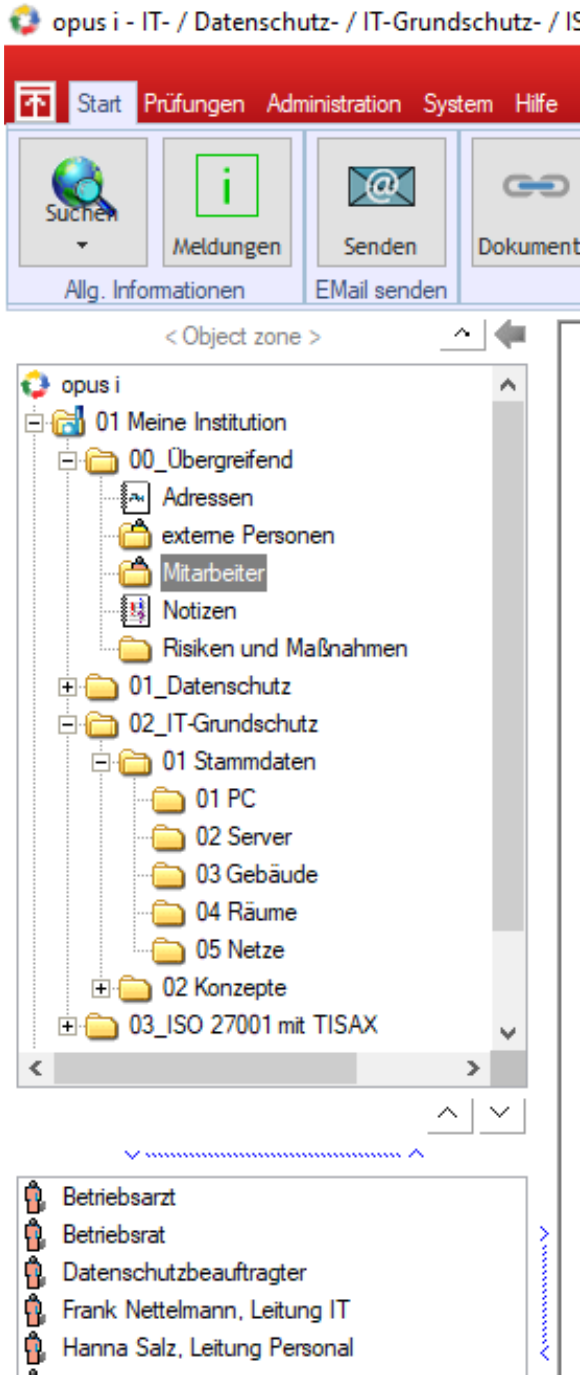
Kurzanleitung

BSI - IT-Grundschutz

umsetzen

opus i Version 8.1.303.1171
(Juli 2021)

Inhalt



Ribbon (Menüband)

Ordnerzone

Objektzone

1. Mitarbeiter erfassen

Erfassen Sie die Mitarbeiter, die Ihnen bei der Umsetzung der IT-Grundschutz-Anforderungen (IT-GS) zur Hilfe bereitstehen (Teammitglieder) in einem Mitarbeiter-Ordner des entsprechenden Mandanten-Ordners.

Hinterlegen Sie zu jedem Mitarbeiter nähere Informationen. Alle blau hinterlegten Felder sind Pflichtfelder und müssen ausgefüllt werden.

> *Hinweis: Sie können die Pflichtfelder selbst steuern. Editieren Sie in der Steuerdatei Database\SystemFiles\SystemINI\Mandatory\MandatoryFields.INI im Bereich [wMitarbeiter] die entsprechenden Felder. „0“ definiert das Feld als wahlfrei, bei „1“ wird es zum Pflichtfeld. Starten Sie nach der Anpassung opus i neu, damit die Änderungen übernommen werden. Blau hinterlegt sind nun nur noch die von Ihnen festgelegten Pflichtfelder.*

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild1.1.jpg

1 Navigieren Sie in der Ordnerzone zum Mandantenordner. Wählen Sie im Unterordner den Mitarbeiterordner aus

2 Fügen Sie in der Objektzone über „Rechtsklick > Neues Objekt (entsprechend dem Ordner)“ einen neuen Mitarbeiter hinzu

3 Öffnen Sie die Eigenschaften des Mitarbeiters über Doppelklick auf das Objekt

4 Hinterlegen Sie nähere Informationen zum Mitarbeiter. Beachten Sie dabei, dass die Pflichtfelder (blau hinterlegt) auf allen Registerkarten ausgefüllt sein müssen

5 Wiederholen Sie die Schritte 2-4 für jeden weiteren Mitarbeiter

Wenn Externe zu Ihrem Team gehören, können Sie auf der gleichen Stufe wie "Mitarbeiter" einen weiteren Ordner, speziell für "Personen, externe" anlegen und dort die Externen auf die gleiche Weise wie die Mitarbeiter erfassen.

Die involvierten Auftragsdatenverarbeiter, sind auch "Externe", werden aber bei den Asset-Stammdaten erfasst, also weder im Ordner Mitarbeiter, noch im Ordner Externe.

2. User erfassen

Legen Sie alle opus i-Benutzer im Ordner „User“ an. Hinterlegen Sie zu jedem Benutzer nähere Informationen. Alle blau hinterlegten Felder sind Pflichtfelder und müssen ausgefüllt werden.

Hinweis:

Sie können die Pflichtfelder selbst steuern. Editieren Sie in der Steuerdatei Database\SystemFiles\SystemINI\Mandatory\MandatoryFields.INI im Bereich [wBenutzer] die entsprechenden Felder. „0“ definiert das Feld als wahlfrei, bei „1“ wird es zum Pflichtfeld. Starten Sie nach der Anpassung opus i neu, damit die Änderungen übernommen werden. Blau hinterlegt sind nun nur noch die von Ihnen gewünschten Pflichtfelder

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild2.1.jpg

1 Wählen Sie in der Ordnerzone den Userordner

2 Fügen Sie in der Objektzone über „Rechtsklick > Neues Objekt (entsprechend dem Ordner)“ einen neuen opusi-User hinzu

3 Öffnen Sie die Eigenschaften des Users über Doppelklick auf das Objekt

4 Hinterlegen Sie nähere Informationen zum User. Beachten Sie dabei, dass die Pflichtfelder (blau hinterlegt) auf allen Registerkarten ausgefüllt sein müssen

5 Wiederholen Sie die Schritte 2-4 für jeden weiteren opusi-User

3. Zielobjekte und IT-Verbund (IT-Infrastruktur) anlegen

Legen Sie anschließend alle im späteren IT-Verbund notwendigen Zielobjekte an.

Hinweis:

Wenn Sie bereits heute wissen, dass Sie später genau einen (1) IT-Verbund betrachten und niemals einen zweiten oder dritten IT-Verbund benötigen, müssen Sie die Zielobjekte nicht als Stamm-Objekte anlegen, sondern können diese sofort im IT-Verbund neu anlegen

Bei Anwendungen unterscheidet opus i solche mit  *und ohne*  *Personenbezug*

Legen Sie den IT-Verbund in der folgenden Struktur an

- *IT-Verbund*
- *Gebäude*
- *Netzwerk*
- *Raum*
- *PC*
- *Anwendungen (keine personenbezogenen Daten) oder Verarbeitungen (personenbezogene Daten)*

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild3.1.jpg

1 Erfassen Sie im Mandantenordner unter 00_Stammdaten die Zielobjekte in den jeweiligen Kategorienordern

Dazu gehören auch die Auftragsdatenverarbeiter  , wie Reinigungsfirmen oder externe Systemhäuser.

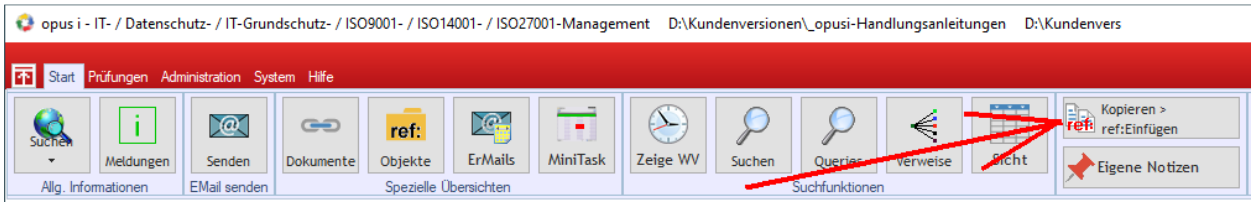
2 Erstellen Sie im Ordner 02_IT-Grundschutz (im Mandanten) über „Rechtsklick > Neuer Ordner > Allgemein“ einen neuen allgemeinen Ordner.
Vergeben Sie einen sprechenden Namen für Ihren neuen IT-Verbund – z.B. „IT-Verbund zum Scope A“

3 Damit der IT-Verbund später durch opus i als IT-Verbund erkannt werden kann, erstellen Sie in der Objektzone als erstes und oberstes Objekt wahlweise eine Organisationseinheit  , einen IT-Verbund  , einen Prozess  oder eine Fachaufgabe 

Erstellen Sie dieses Objekt über „Rechtsklick > Neues Objekt (alle Objekte) > IT-Grundschutz > Startelement IT-Verbund“ und Auswahl des Objekttyps

4 Fügen Sie Referenzierungen Ihrer Assets in den IT-Verbund ein, indem Sie in den Stammdaten das Objekt über Rechtsklick kopieren und im IT-Verbund nach Auswahl des übergeordneten Elements über „Rechtsklick > Einfügen als Referenzobjekt“ wieder einfügen

Schneller geht es so: Öffnen Sie das Fenster „schnelles Kopieren und Einfügen“ im Menü-Ribbon „Start“ über den Button „Kopieren > ref: Einfügen“ im rechten Bereich.
https://manual-images.kronsoft.de/kurzanl-ITGS/bild3.2.jpg



5 Wählen Sie im neuen Fenster aus, welche Objektart (Hauptobjekte/Nebenobjekte) Sie einfügen möchten und aus welchem Mandanten Sie die Objekte nehmen möchten

6 Wählen Sie zunächst in der Objektzone das übergeordnete Objekt aus

7 Fügen Sie die Referenzierung Ihres Assets per Doppelklick auf das Objekt im Fenster „Schnelles Kopieren…“ hinzu

8 Sie können Strukturen, die bereits im IT-Verbund vorhanden sind über Kopieren und Einfügen an anderer Stelle platzieren

4. BSI-Bausteine auf den IT-Verbund legen

Dokumentieren Sie für jedes Objekt die Einstellungen für Vertraulichkeit, Integrität und Verfügbarkeit. Ordnen Sie anschließend den Objekten die passenden Bausteine zu.

> *Hinweis:*
>
> *In den opus i Optionen kann festgelegt werden, dass nur Administratoren die Modellierung sehen dürfen. Nicht jeder User muss die Modellierung vornehmen bzw. ändern können*
>
> *Netzwerke sind i.d.R. „Netzwerk, nach außen". Dies trifft auch zu, wenn das Netzwerk hinter einer Firewall sitzt*

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild4.1.jpg

1 Öffnen Sie für jedes Objekt des IT-Verbunds mit Rechtsklick die „Eigenschaften IT-Grundschutz" (anstatt Rechtsklick auch SHIFT + Doppelklick)

2 Wechseln Sie auf die Registerkarte „IT-Grundschutz 200-x"

3 Legen Sie die Ausprägung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität fest

> *Hinweis:*
>
> *Sie können jedem Objekt grundsätzlich die Schutzbedarfe NORMAL zuordnen*
>
> *NUR den Objekten, die **Schutzbedarfsgeber** sind - das sind die Objekte, die keine Unterobjekte aufweisen - im Bild sind dies ref:Software, Mobiles-Verwaltung… und ref:Verarbeitungstätigkeit… - ordnen Sie den korrekten Schutzbedarf (für dieses Objekt selbst) zu*
>
> *Tatsächlich kann jeder Objekttyp (Notebook, Raum, Outsourcing-Auftragnehmer,…) zum Schutzbedarfsgeber werden, wenn das jeweilige Objekt keine Unterobjekte mehr hat*

4 Begründen Sie die gewählten Ausprägungen

5 Prüfen Sie in der mittleren Liste alle Fragestellungen (IT-Sicherheits*eigenschaften*) und kreuzen Sie alles Zutreffende an.
opus i markiert alle zum Objekttyp passenden Eigenschaften **grün.** Sie können auch andere Eigenschaften verwenden, auch solche, die nicht im grünen Bereich stehen

6 Klicken Sie auf „Übernehmen“

5. Schutzbedarf übertragen

Wählen Sie das oberste Element Ihres IT-Verbunds in der Objektzone aus (im Bild ist dies: „Unsere IT-Infrastruktur“). Über „Rechtsklick > Schutzbedarf innerhalb des Verbunds vererben“ werden die Schutzbedarfe übertragen.

Hinweis:

Fertigen Sie ein internes Backup an BEVOR Sie den Schutzbedarf vererben, damit Sie eventuell nochmal zurückgehen können und die vererbenden Schutzbedarfe überarbeiten (Ribbon/System/Backup)

Für unsere ISO 27001 - Anwender, bzw. unsere TISAX-Anwender endet diese Handlungsanleitung hier.
Gehen Sie jetzt über zur Anleitung „ISO 27001“.

Die IT-Grundschutz-Anwender arbeiten bitte weiter in dieser Anleitung.

6. Anforderungen bearbeiten

Der neue IT-Grundschutz 200 ist so entwickelt, dass mit „einem geringen Aufwand“ ohne eine Zertifizierung anzustreben eine grundlegende Sicherheit in der IT erreicht werden kann. Sie beginnen zuerst mit den Basisanforderungen. Siehe im Bild „B“. Die Spalte kann gefiltert werden (rechter Mausklick auf die Lupe).

Hinweis:

Wir empfehlen mit den Anforderungen des obersten Elementes (A) zu beginnen, danach Netz (C) und Netzelemente (z.B. Firewall und Switches; nicht im Bild dargestellt) zu bearbeiten

Mit der rechten Maustaste können Sie zu jeder Zeile der Anforderungstabelle die notwendigen Infos zur Anforderung abrufen

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild6.1.jpg

1 Wählen Sie in der Objektzone das oberste Element des IT-Verbundes aus

2 Öffnen Sie die Registerkarte „IT-Grundschutz-200 / Anforderungen bearbeiten“

3 Wählen Sie die Anforderung aus, die Sie bearbeiten und setzen Sie als erstes den Umsetzungsstatus (im Bild (A), APP.1.4.A2, teilweise). Fügen Sie die MINDESTINFORMATIONEN ein (im Bild (B). Speichern Sie

https://manual-images.kronsoft.de/kurzanl-ITGS/bild6.2.jpg

Hinweis zum Umsetzungsstatus:

JA	*Die Anforderung ist vollständig erfüllt*
TEILWEISE	*Die Umsetzung ist begonnen, die Anforderung ist noch nicht vollständig erfüllt. „Umzusetzen bis“ ist einzutragen.*
NEIN	*Die Anforderung ist zur Kenntnis aber noch nicht in Angriff genommen worden. „Nein“ ist der Umsetzungsstatus, der letztendlich NICHT MEHR vorhanden sein darf!* *Soll eine Anforderung nicht realisiert werden, ist „entbehrlich“ zu verwenden.*
ENTBEHRLICH	*Die Anforderung wird nicht umgesetzt, weil das Szenario bei Ihnen nicht gegeben ist.*

Die Anwender, die keine Zertifizierung nach IT-Grundschutz anstreben, können hier die Anleitung zur Seite legen und sich um das Realisieren der Anforderungen kümmern.

Die IT-Grundschutz-Anwender, die trotzdem mehr tun möchten oder eine Zertifizierung nach IT-Grundschutz anstreben, schauen sich jetzt noch die Risikoanalyse (nach 200-3) an und gehen danach an die Realisierung der offenen Anforderungen.

Zur Erreichung des IT-Grundschutz-Zertifikats sind alle Anforderungen zu realisieren. Umsetzungsstatus „Nein“ wird nicht akzeptiert. „Entbehrlich“ kann genutzt werden; ist dann aber auch zu begründen.
Nicht alle Anforderungen sind zur Zertifizierung vollständig mit „Ja“ zu realisieren – Auditoren akzeptieren auch „teilweise“, wenn ein „Umzusetzen bis“ avisiert wird.

7. Risikomatrix erstellen

Alle Anforderungen sind realisiert!

Schaffen Sie die Grundlagen für die Risikoanalyse, indem Sie die Risikomatrix erstellen und Eintrittswahrscheinlichkeiten und Schadensausmaßen definieren.

> *Hinweis: Mit Risikoanalyse ist hier diese nach BSI-Standard 200-3 gemeint, welche notwendig ist, wenn Sie in die Zertifizierung gehen möchten*

So geht es:

https://manual-images.kronsoft.de/kurzanl-ITGS/bild7.1.jpg

1 Wählen Sie in der Objektzone das oberste Element des IT-Verbundes aus

2 Erstellen Sie über Rechtsklick auf dem obersten Objekt ein neues Objekt „Risikomatrix für IT-Verbund (200-3)“

3 Wechseln Sie auf die Registerkarte „Risikomatrix“ und dort auf die Unterregisterkarte „Eintrittswahrscheinlichkeit und Schadenshöhe“ und passen dort die Vorgaben in der Spalte „Erläuterung“ an auf die für Ihre Institution gültigen Definitionen

4 Wechseln Sie auf die Unterregisterkarte „Risikomatrix“. Erstellen Sie dort die Risikomatrix mit den zur Verfügung stehenden Farben. Sie nehmen mindestens Grün, Gelb und Rot. Die gezeigte Grafik ist als Beispiel zu verstehen

https://manual-images.kronsoft.de/kurzanl-ITGS/bild7.2.jpg

8. Risikoanalyse durchführen

Wir betrachten zu jedem Objekt (Zielobjekt) unseres IT-Verbundes die Risiken. Dies sollte sinnvollerweise erst dann geschehen, wenn alle Anforderungen realisiert (JA) sind oder nicht betrachtet werden müssen (ENTBEHRLICH). Noch nicht vollständig realisierte Anforderungen werden wahrscheinlich vom Zertifizierer akzeptiert - allerdings dürfen es nicht so viele sein, dass das Konzept grundsätzlich in Frage zu stellen wäre.
Die Risikoanalyse ist im opusihandbuch.kronsoft.de ausführlich beschrieben.

So geht es:

Die Risikomatrix ist im IT-Verbund enthalten!

1 Öffnen Sie das zu betrachtende Objekt per Popup-Menü oder mit SHIFT + Doppelklick und schalten Sie die Registerkarte „IT-Grundschutz 200-x“ sowie die Unterregisterkarte „200-3“ in den Vordergrund

> *Hinweis: opus i schaltet die Registerkarte 200-3 nur dann sichtbar, wenn wenigstens einer der drei Grundwerte für Vertraulichkeit, Integrität und Verfügbarkeit auf HOCH oder SEHR HOCH steht*

2 Dokumentieren Sie zu jeder Gefährdung (die zum markierten Objekt wirkt, Buchstaben A), in der oberen Tabelle deren Eintrittswahrscheinlichkeit und Schadenshöhe (C), unter der Prämisse, dass alle vorgesehenen Anforderungen (Spalte B) realisiert/implementiert sind - aber KEINE ZUSÄTZLICHEN Maßnahmen (außer den vorgesehenen IT-Grundschutz-Anforderungen) ergriffen wurden
https://manual-images.kronsoft.de/kurzanl-ITGS/bild8.1.jpg

3 Sollten Sie zu diesem markierten Objekt noch WEITERE Gefährdungen/Risiken ermittelt haben (Buchstabe A), dokumentieren Sie dies in der unteren Tabelle (Schritt 2)
https://manual-images.kronsoft.de/kurzanl-ITGS/bild8.2.jpg

> *Hinweis: opus i zeigt Ihnen - der schnelleren Bearbeitung wegen - die bereits im Konzept berücksichtigten Anforderungen, die bereits umgesetzt sein sollten (Häkchen, Buchstaben A)*
>
> *und bietet Ihnen mögliche, weitere Gefährdungen/Risiken an (kein Häkchen, Buchstabe B), die Sie möglicherweise noch ermittelt und bearbeiten möchten, um die bestehende Gefährdungen noch weiter zu reduzieren*

4 Die IT-Sicherheit unterliegt dem PDCA-Kreislauf. Daraus resultiert eine immer wiederkehrende Verbesserung der Sicherheit - eine immer wiederkehrende Risikoreduzierung. Das dokumentieren Sie im Schritt 3 der opus i Risikoanalyse
https://manual-images.kronsoft.de/kurzanl-ITGS/bild8.3.jpg

> *Hinweis:*
>
> *Sie zeigen durch WEITERE REDUZIERUNG (Buchstabe A), dass Sie bestehende Risiken zukünftig weiter reduzieren werden*
>
> *und dass Risiken, die momentan ausreichend reduziert sind trotzdem noch unter BEOBACHTUNG bleiben, weil immer eine gewisse Unschärfe bei der Beurteilung eines Rest-Risikos bestehen kann (B)*

9. Referenzdokumente drucken

Letztendlich benötigen wir die Zertifizierungsreports.

Diese „Referenzdokumente“ werden so gedruckt.
https://manual-images.kronsoft.de/kurzanl-ITGS/bild9.1.jpg

Ende der Kurzanleitung