

opus i®

Informationssicherheit BSI-GS

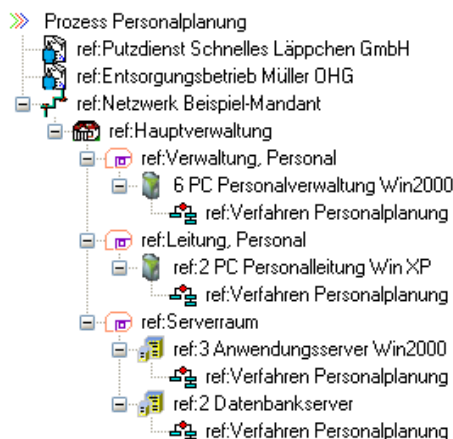
Informationsverbund anlegen

Legen Sie den Informationsverbund (IV) an, den Sie betrachten möchten. Dies kann die gesamte Organisation, ein Prozess, eine Fachaufgabe oder ein IT-Asset sein. Erstellen Sie die benötigten Objekte und fügen Sie sie in den IV ein. Die Struktur bestimmen Sie dabei selbst.



Referenz-Objekte:

Durch die Verwendung von Referenz-Objekten wird der Aufbau mehrerer IVs deutlich vereinfacht, z.B. zur getrennten Betrachtung verschiedener Prozesse.



In einer zentralen Struktur werden alle Original-Objekte abgelegt. Diese werden einfach in den neuen IV an der gewünschten Stelle eingefügt. Werden Original-Objekte verändert, sind diese Änderungen sofort im jeweiligen Prozess mit enthalten.

Modellierung des IVs

Für jedes Objekt wird eine oder mehrere IT-Sicherheits-Eigenschaften ausgewählt. Die Zuordnung der zutreffenden Bausteine erfolgt automatisch. Jeder vorgeschlagene Baustein kann sofort online eingesehen werden. Zusätzliche Bausteine können bei Bedarf manuell eingebunden werden.

Die Maßnahmen, die aus den Bausteinen resultieren werden separat aufgelistet und können ggf. manuell auf inaktiv gesetzt werden. Auch hier kann der volle Maßnahmentext direkt eingesehen werden.

Zu jeder gelisteten Maßnahme können zusätzlich die zugrunde liegenden Gefahren eingesehen werden.

Änderungen werden direkt in das Sicherheitskonzept übernommen.

Schutzbedarf der Objekte

Der Schutzbedarf (niedrig, mittel, hoch) wird innerhalb des IT-Verbundes automatisch vererbt.

| Vertraulichkeit | Integrität | Verfügbarkeit |
|-----------------|------------|---------------|
| hoch | normal | sehr hoch |

Die Schutzbedarfsvererbung erfolgt von unten nach oben im Baum. Nach der automatischen Vererbung kann der Schutzbedarf jederzeit manuell überarbeitet werden,

z.B. um Kumulations- und Verteilungseffekt zu berücksichtigen.

Sicherheitskonzept:

Nun ist das Sicherheitskonzept vollständig und entsprechend der Grundschtzvorgehensweise erstellt.

| BSI Nr. | Control/Maßnahme | Zertifikats-level | Lebenszyklus/ Phase | Umsetzungs-Status |
|---------|---|-------------------|------------------------------|-------------------|
| 1.29 | Geeignete Aufstellung eines IT-Systems | Z zusätzlich | 03 UM Umsetzung | unbearbeitet |
| 1.32 | Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern | B Aufbau | 03 UM Umsetzung | unbearbeitet |
| 1.33 | Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz | A Einstieg | 04 BT Betrieb | unbearbeitet |
| 1.46 | Einsatz von Diebstahl-Sicherungen | Z zusätzlich | 04 BT Betrieb | unbearbeitet |
| 1.59 | Geeignete Aufstellung von Archivsystemen | B Aufbau | 03 UM Umsetzung | unbearbeitet |
| 1.60 | Geeignete Lagerung von Archivmedien | A Einstieg | 04 BT Betrieb | unbearbeitet |
| 2.1 | Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz | A Einstieg | 01 PK Planung und Konzeption | unbearbeitet |
| 2.10 | Überprüfung des Software-Bestandes | C Zertifikat | 04 BT Betrieb | unbearbeitet |
| 2.11 | Regelung des Passwortgebrauchs | A Einstieg | 01 PK Planung und Konzeption | unbearbeitet |
| 2.110 | Datenschutzaspekte bei der Protokollierung | A Einstieg | 04 BT Betrieb | unbearbeitet |
| 2.111 | Bereithalten von Handbüchern | A Einstieg | 03 UM Umsetzung | unbearbeitet |
| 2.12 | Betreuung und Beratung von IT-Benutzern | C Zertifikat | 01 PK Planung und Konzeption | unbearbeitet |
| 2.13 | Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln | A Einstieg | 05 AS Aussonderung | unbearbeitet |
| 2.137 | Beschaffung eines geeigneten Datensicherungssystems | A Einstieg | 02 BE Beschaffung | unbearbeitet |
| 2.138 | Strukturierte Datenhaltung | B Aufbau | 03 UM Umsetzung | unbearbeitet |
| 2.14 | Schlüsselverwaltung | A Einstieg | 04 BT Betrieb | unbearbeitet |
| 2.154 | Erstellung eines Computer-Virenschutzkonzepts | A Einstieg | 01 PK Planung und Konzeption | unbearbeitet |
| 2.155 | Identifikation potentiell von Computer-Viren bedrohter IT-Systeme | A Einstieg | 01 PK Planung und Konzeption | unbearbeitet |
| 2.156 | Auswahl einer geeigneten Computer-Virenschutz-Strategie | A Einstieg | 01 PK Planung und Konzeption | unbearbeitet |

Eigene Gefährdungen / Maßnahmen / Bausteine:

Unter Umständen ist die Erweiterung des Informationssicherheitskonzeptes um eigene Gefährdungen, Maßnahmen und/oder Bausteine erforderlich. Dies ist speziell bei hohem oder sehr hohem Schutzbedarf der Fall. In opus i können diese Elemente entsprechend angelegt und ins Sicherheitskonzept übernommen werden.

Maßnahmen-Bearbeitung

Rollen:

Das BSI hat in jeder Maßnahme beispielhaft aufgezeigt, welche Funktionsträger für die Initiierung der Sicherheits-Maßnahmen (Freigabe zur Umsetzung) und welche für die Umsetzung (Realisierung, Implementierung) gewöhnlich in Betracht kommen. Von diesen Funktionsträgern, auch Rollen genannt, existieren mittlerweile mehr als 65 in den BSI-Sicherheitsmaßnahmen.

Maßnahmenzuordnung:

Aufgrund dieser Rollen-Vorschläge können die Maßnahmen zielgenau an die jeweils Zuständigen zur Bearbeitung delegiert werden. Es liegt in der Natur der Sache, dass in Institutionen mit wenigen Mitarbeitern nicht jede dieser Rollen verschiedenen Personen zugeordnet werden kann. Deshalb bietet opus i zwei Vorgehensweisen für die Maßnahmen-Zuordnung: Einzel- und Sammelzuweisung. Bei der Einzelzuweisung werden einzelne Maßnahmen einem Bearbeiter zugeordnet, bei der Sammelzuweisung erhält der Bearbeiter eine oder mehrere Rollen mit den entsprechenden Maßnahmen. Eine Kombination beider Vorgehensweisen ist ebenfalls möglich.

Maßnahmen-Status:

Bei der Umsetzung der Maßnahmen sind mehrere Status möglich, z.B. „entbehrlich“, „umgesetzt“, „unbearbeitet“. Diese können den einzelnen Maßnahmen zugeordnet werden.

Übergreifende Umsetzung:

Es gibt Maßnahmen, die innerhalb eines Informationsverbunds zwar für mehrere Objekte notwendig ist, aber durch eine einzige Umsetzung abgedeckt ist, z.B. erfordern Server Zutrittsbeschränkung. In einem Unternehmen gibt es oftmals mehrere Server (z.B. Web-Server und File-Server). Stehen diese in einem Serverraum, dessen Zutritt z.B. nur mit Chipkarte erfolgen kann, so ist diese Maßnahme für alle Server umgesetzt. Solche Maßnahmen können als „übergreifend umgesetzt“ markiert werden und haben somit bei jedem Objekt den Status „übergreifend umgesetzt“.

Datenschutzgebote:

Zu jeder Maßnahme kann das Datenschutzgebot aufgezeigt werden in das diese Maßnahme sachlich einzuordnen wäre.

ISO 27001-Zuordnung:

Zu ca. 600 Maßnahmen des Sicherheitskonzeptes kann angezeigt werden, in welchem ISO 27001-Kapitel diese Maßnahme sachlich einzuordnen wäre. Gleichzeitig können zu einem ISO-Kapitel alle entsprechenden Maßnahmen angezeigt werden. Die bereits im Sicherheitskonzept enthaltenen Maßnahmen werden dabei entsprechend markiert und können ggf. erweitert werden.

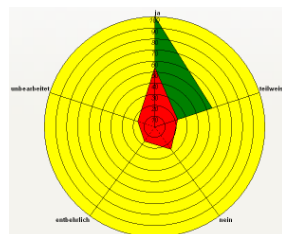
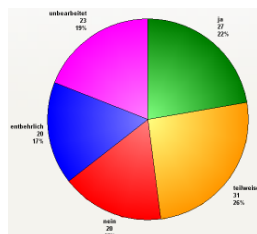
Referenz-Anzeige (Cross-Reference) von Objekten und Maßnahmen:

Objekte und Maßnahmen können über diese Funktion jederzeit schnell überprüft und nachverfolgt werden.

Auswertungen und Berichte

Grafische Auswertungen:

Mit opus i können grafische Auswertungen als Balken-/Kreisdiagramm oder als Kivi-atgraph (Spinnendiagramm) erstellt werden. Hierfür stehen 12 vordefinierte Auswertekriterien zur Verfügung. Innerhalb eines Auswertekriteriums können auch die zu betrachtenden Elemente ausgewählt werden.



Präsentationsreport:

Der Präsentationsreport ermöglicht es verschiedene Reports zum IT-Verbund und somit zum Informationssicherheitskonzept zu erstellen. Der Anwender kann sich aus 40 vordefinierten Sektionen unterschiedliche Reports zusammenstellen, dauerhaft speichern und bei Bedarf drucken. Folgende vordefinierte Reports werden mitgeliefert:

- ❖ Zusammenfassung für Management
- ❖ Jahresdokumentation ISMS
- ❖ Zertifizierungsunterlagen
- ❖ Dokumentation für Partner und Kunden
- ❖ Kostennachweis für Controller
- ❖ Jährlicher Dokumentencheck
- ❖ Datenschutz und ISO nach Maßnahme
- ❖ Maßnahme nach Datenschutz und ISO

Einbinden von Mitarbeitern:

Mit opus i kann ein Aufgabenplan für „Initierer“ und „Umsetzer“ gedruckt werden. Dieser kann auch die vollständigen Texte der Maßnahmen, Gefahren und Bausteine enthalten, damit diese dem Empfänger der Aufgaben bekannt sind.

Zertifikat und Audit:

Versionenvergleich:

Das BSI veröffentlicht jährlich Ergänzungslieferungen des Grundschutzhandbuchs. Der „Versionenvergleich“ zeigt übersichtlich die Änderungen in den Bausteinen-, Gefahren- und Maßnahmentexten zwischen zwei „Ergänzungslieferungen“.

Zertifizierungs-Dokumente:

Bei einer vorgesehenen Zertifizierung werden vom BSI bestimmte Dokumente angefordert. Alle für die Zertifizierung (vom BSI) vorgeschriebenen Dokumente werden durch opus i in die Systemdokumentation eingefügt. Diese Dokumente sind nun zentral (übergreifend und prozessbezogen) in einem separaten Ordner abgelegt. Alle Dokumente werden vorgefertigt mitgeliefert. Die meisten dieser Dokumente werden durch opus i automatisch erstellt und fortgeschrieben.

Import / Export:

Ein Informationsverbund (IV) kann exportiert und auch wieder importiert werden. Dies bietet sich speziell an um:

- ❖ an anderer Stelle am IV weiter zu arbeiten.
- ❖ dem Auditor den IV zur Vorbereitung einer Prüfung zu senden.
- ❖ dem Auditor den IV zur Überprüfung zuzusenden.

Funktionsübersicht:

Informationssicherheits-Bearbeitung:

- ❖ Erstellung von Sicherheitskonzepten
- ❖ IT-Strukturanalyse (Übersicht der vorhandenen Informationstechnologie: Infrastruktur, Hardware, Einsatzorte und die unterstützten IT-Anwendungen)
- ❖ Modellierung der Objekte des Verbundes (Organisationseinheit / IT-Asset / Prozess / Fachaufgabe)
- ❖ Schutzbedarfshinterlegung und Schutzbedarfsvererbung
- ❖ Basissicherheitscheck
- ❖ Unterstützung des Soll-Ist-Vergleichs
- ❖ Kostenbearbeitung
- ❖ Revisionsunterstützung
- ❖ Unterstützung der ergänzenden Sicherheitsanalyse
- ❖ automatische Zuordnung zu allen/ Einzelzuordnung der Controls / Maßnahmen zu Initiierer und Umsetzer
- ❖ automatische Zuordnung der Controls / Maßnahmen zu ISO27001 und 27002
- ❖ automatische Zuordnung der Controls / Maßnahmen zu den Datenschutzgebieten
- ❖ Eigene Gefährdungen / Maßnahmen / Bausteine erstellen und einbringen
- ❖ Arbeitsplan für Teammitglieder
- ❖ verschiedene Sichten auf das Sicherheitskonzept (Initiierer, Umsetzer, Einstieg, Aufbau, Zertifikat, Schichten, Lebenszyklen, „meine“, alle)
- ❖ Versionsvergleich (Vergleich zweier Grundschutzkatalog-Versionen. Bausteine, Gefahren, Maßnahmen.)
- ❖ ausführliche Dokumentation aller Objekte und Tätigkeiten

Produktiv-Unterstützung:

- ❖ integrierte Datenschutzbearbeitung (alle Datenschutzgesetze)
- ❖ unbegrenzte Dokumentationstiefe (eigene Eingabefelder)
- ❖ freie Zuordnung von Eigenschaften (auf Textbaustein-Basis)
- ❖ Referenzierung von Objekten, Mitarbeiter und Personen
- ❖ Import von Hard- und Software usw. Import von Mitarbeitern und Personen.
- ❖ automatische Aktualitätsprüfung des Datenbestandes
- ❖ integrierte Mail-Funktion (SMTP / Outlook / Lotus Notes) mit Protokollführung

- ❖ integrierte Faxfunktion mit Protokollführung
- ❖ Notizen
- ❖ Termin-Management
- ❖ Wiedervorlage-Management
- ❖ Gruppenbe- und -verarbeitung
- ❖ Personen- und Mitarbeiter-Management
- ❖ Adress-Management
- ❖ Beauftragten-Management, Anfragen, Fachkunde, Tätigkeiten, Planungen
- ❖ interne und externe Suchfunktion
- ❖ Komplettdarstellung der Dokumentation auch in Tabellenfunktion

Management-Funktionen:

- ❖ detaillierte Zugriffsprotokollierung (Einsehen, Ändern, Löschen) mit manueller und automatischer Archivierung der Protokolle
- ❖ Prozess- und Abhängigkeitsdarstellung
- ❖ detaillierte Auswertemöglichkeiten mit automatischer Berichterstellung (12 Sichten) mit vorgefertigten grafischen Auswertungen (Kreis- und Balkendiagramm sowie Kiviagraph)
- ❖ Präsentationsreport (40 Sektionen vom Anwender anpassbar)
- ❖ Komplette Archivierung des Datenbestandes zu einem Stichtag; Revisions-sichere Archivführung inklusive Wieder-einspielung
- ❖ Verwaltung externer Dokumente (mit Zugriffsnachweis)
- ❖ integriertes Backup und Restore
- ❖ Wiederherstellen gelöschter Objekte
- ❖ Export / Import des Informationsverbundes
- ❖ Mandanten-Verwaltung
- ❖ User-Verwaltung
- ❖ Objekte nach IT, Datenschutz, GDPdU, Informationssicherheit

Individuell konfigurierbar:

- ❖ Individuell konfigurierbar:
- ❖ beliebige Fremd-Datenbanken (MS SQL-Server {SQL-/Win-Authentifizierung}, MySQL, Oracle, DB2, SYBASE, INFORMIX, PROGRESS)
- ❖ Beliebiger Aufbau der Dokumentations-Struktur (Informationsverbundes)
- ❖ alle Parameter frei konfigurierbar
- ❖ individuell anpassbare Menüs