

Österreichisches Sicherheitshandbuch

Projekt Relaunch 2010



Zentrum für sichere Informationstechnologie - Austria

Akkreditierte Inspektionsstelle



Österreichische IT-Sicherheitshandbuch Version 2.3

Das Österreichische Informationssicherheitshandbuch ist im **April 2007** in Buchform sowie in .pdf und .xml Formaten erschienen.

Herausgeber: Bundeskanzleramt

OCG-Schriftenreihe,
ISBN 978-3-85403-226

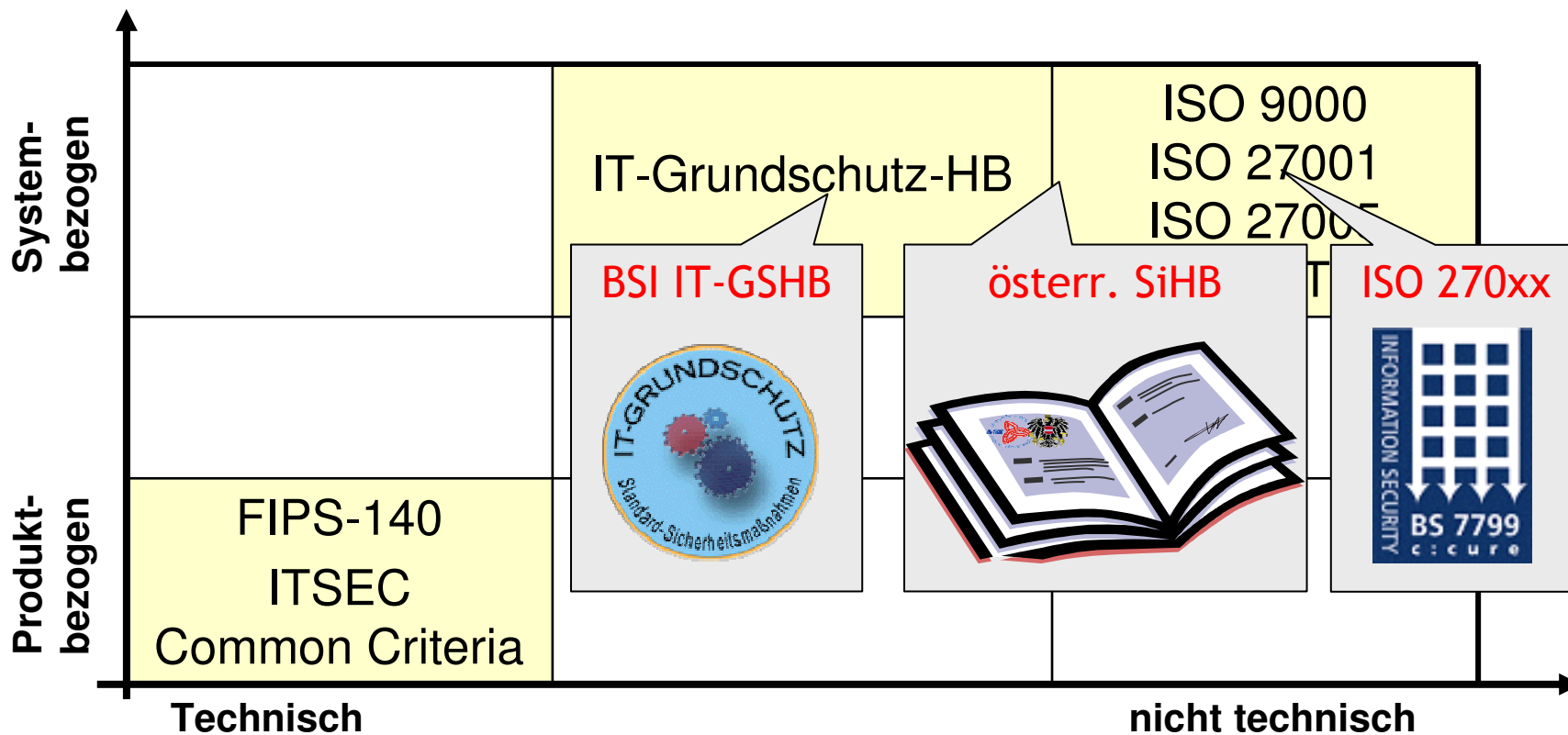


Zentrum für sichere Informationstechnologie - Austria

Akkreditierte Inspektionsstelle



Position



Informationssicherheitshandbuch

SiHB 1998 (BMI)

Das Österreichische Sicherheitshandbuch erschien in seiner ersten Version 1998.

SiHB 2001
(BMÖLS-ASIT)

Über die Zeit erscheinen weitere Versionen mit dem Ziel immer größer werdenden Anforderungen gerecht zu werden.

SiHB 2003
(BKA-ASIT)

Das letzte Update erschien 2007 in dem das „IT-Sicherheitshandbuch“ zum „Informationssicherheitshandbuch“ wurde und strukturell umgebaut wurde.

SiHB 2007
(BKA-ASIT)

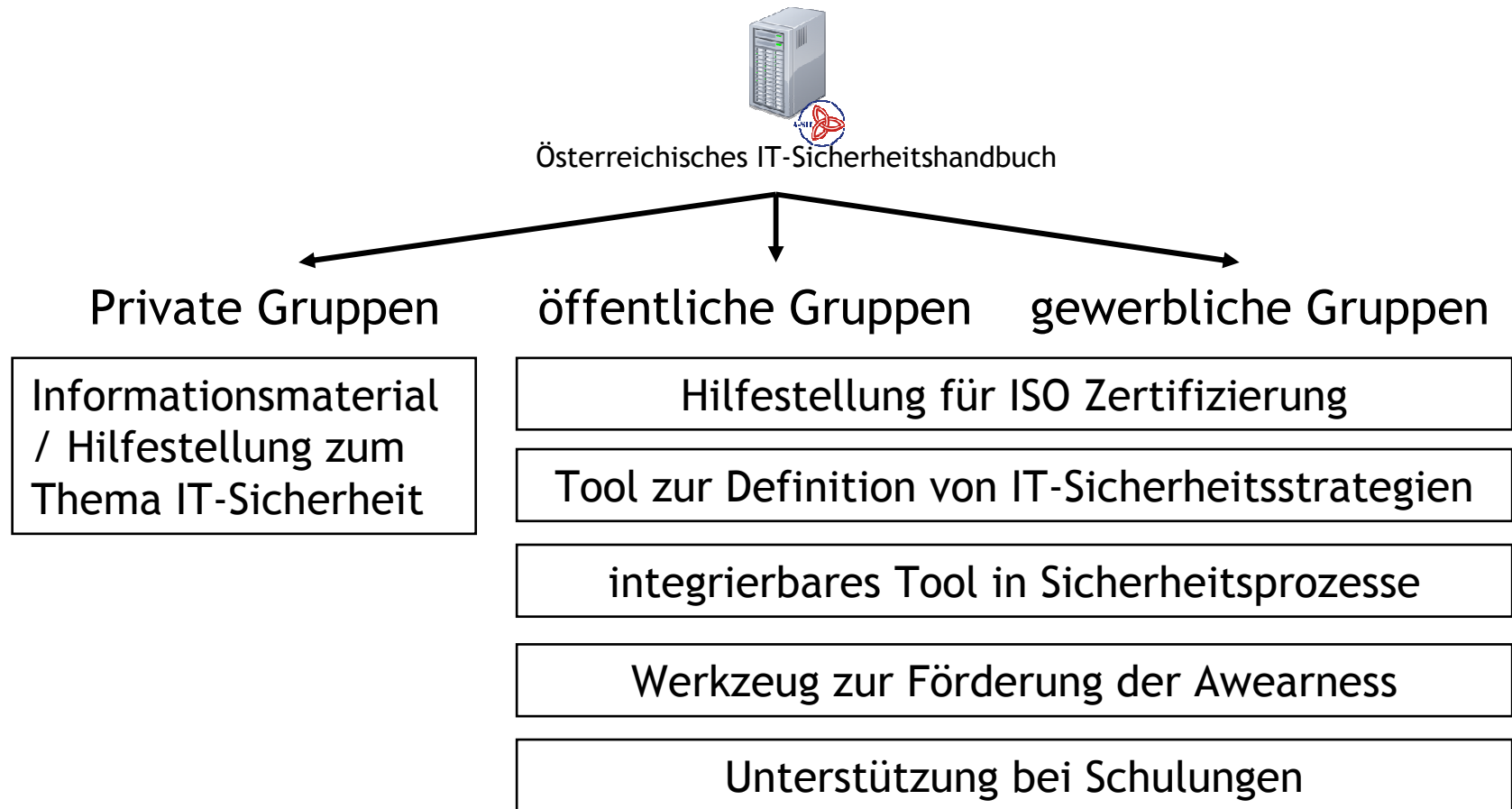
Ende 2009 startete eine erneute umfangreiche Überarbeitung des Österreichischen Informationssicherheitshandbuches

SiHB 2010
(BKA-ASIT)

Schwerpunkte des Relaunch

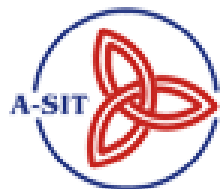
- Neuer Hauptzweck
 - Implementierungshilfe hinsichtlich ISO 27xxx
 - „Lückenschluss für KMUs“
- Aktualisierung der Inhalte und Strukturen
- Personalisierung nach unterschiedlichen Zielgruppen
- Realisierung von unterstützenden Tools
- Autorengruppen
- Exportierbare Versionen als CD oder Buch
 - Bereitstellung von PDFs

Einsatzgebiet

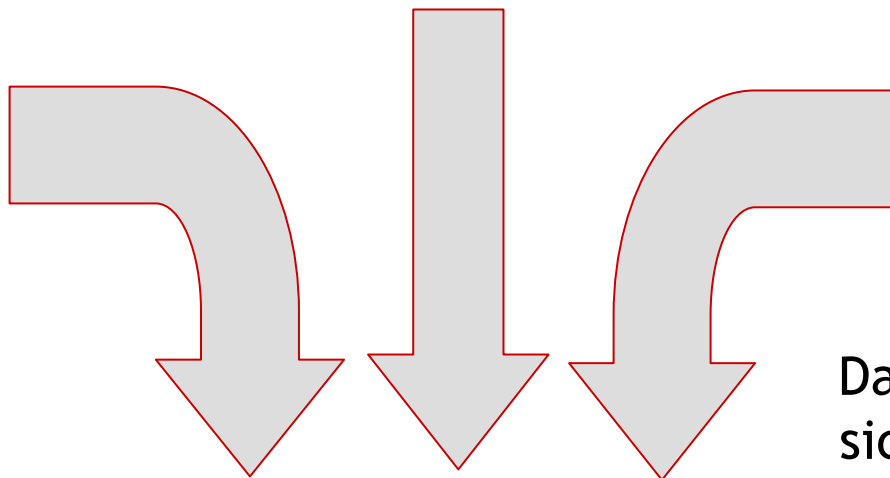


Informationssicherheitshandbuch

BUNDESKANZLERAMT  ÖSTERREICH
Österr. Bundeskanzleramt



A-SIT



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatikstrategieorgan Bund ISB

ISB - Schweiz

Das neue Informations-
sicherheitshandbuch in
der Version 3.0 entsteht
aus einer
Zusammenarbeit dreier
Partner



Informationssicherheitshandbuch

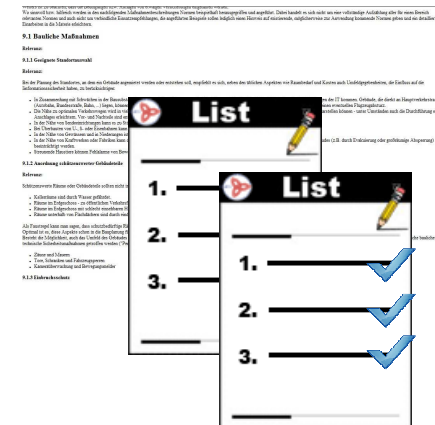
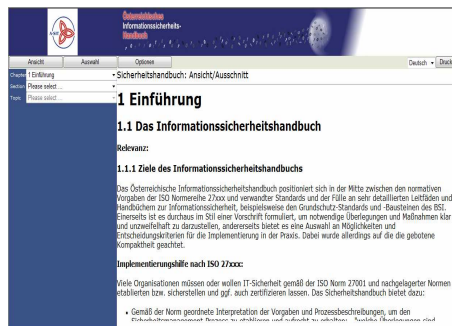


Zentrum für sichere Informationstechnologie - Austria

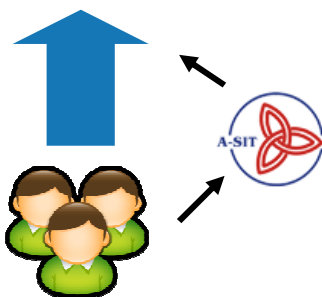
Akkreditierte Inspektionsstelle



Umsetzung



Wissensbasis (.xml)



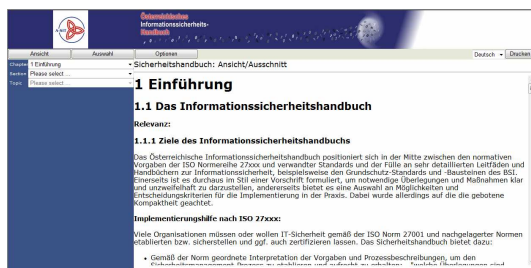
Autorengruppe(n)

(Online) Tool

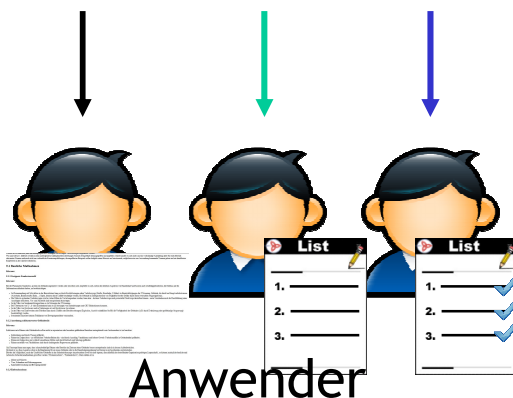


Anwender

Umsetzung



(Online) Tool

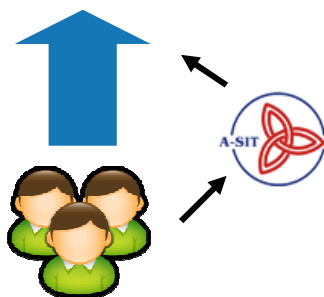


- Erstellung von „Auswahlen“
 - Querschnittsmaterien
 - Checklisten
- Automatische bzw. manuelle Updates
- Individuell erweiterbarer Datenbestand
- Individuelle Bearbeitung von Kommentaren
- Ausgabe in Standardformaten (z.B. HTML, PDF)
- Oberfläche
 - Intuitiv („So viel Funktionalität wie möglich. So wenig ‚Oberfläche‘ wie nötig)
 - Nach internationalen Standards

Umsetzung



Wissensbasis (.xml)



Autorengruppe(n)

- Inhaltliche (Neu-)Strukturierung
 - Anpassung an ISO 27xxx (hinsichtlich Implementierungshilfe)
 - Landesspezifische Maßnahmen
 - Zielgruppenorientierte Personalisierung
- (kontinuierliche) Kontrolle aller Inhalte
 - Rasante Weiterentwicklung von Technologie
 - z.B. Mobile Technologie, Clouding, Social Networks,
 - Gesetzliche Veränderungen
- Einführung von Autorengruppe(n)

Umsetzung



Autorengruppe(n)

- Autorengruppe(n)
 - Ausgewählte Anwender die spezifisches Know-How (bspw. Brandschutz) zur Verfügung stellen
 - Infrastruktur wird von der A-SIT bereitgestellt
 - Tool zur Erzeugung von Inhalten
 - A-SIT übernimmt die Rolle des „Wissensmanagers“
 - Vorgaben
 - Kontrolle der Inhalte

Umsetzung

Anpassung der Struktur an die der ISO 27000 Norm

Sicherheitshandbuch 2.3



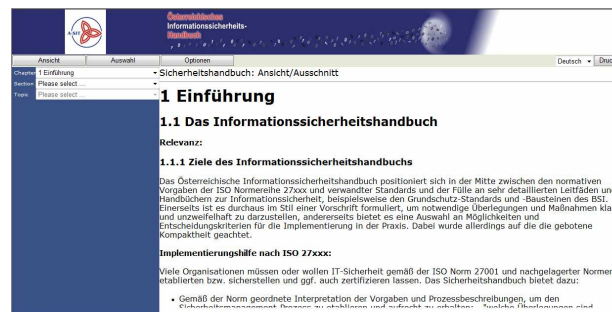
Teil 1

6 Kapitel + Anhänge

Teil 2

7 Kapitel + Anhänge

Sicherheitshandbuch 3.0



15 Kapitel + Anhänge

Umsetzung

Anpassung der Struktur an die der ISO 27000 Norm

Sicherheitshandbuch 2.3

Informationssicherheits-
management-Prozeß



organisationsweiten
Sicherheitspolitik



Risikoanalyse

Erstellung von
Sicherheitskonzepten



...

Bauliche & infrastrukturelle
Maßnahmen
Personelle Maßnahmen



...

Sicherheitshandbuch 3.0

Vorwort & Einführung
Informationssicherheits- /Managementsysteme

Management-Verantwortung und Aufgaben

Risikoanalyse

Entwicklung einer organisationsweiten
Informationssicherheitspolitik

Organisation

Vermögenswerte und Klassifizierung von
Objekten

Physische und umgebungsbezogene Sicherheit

Personelle Sicherheit

...

Umsetzung

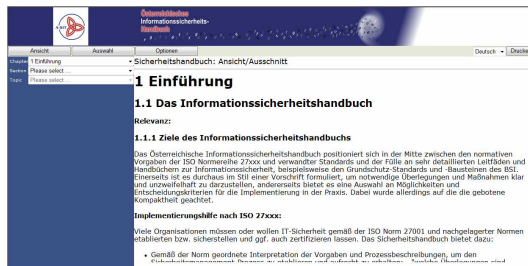
Das Tool Sicherheitshandbuch soll das Arbeiten mit dem Informationssicherheitshandbuch vereinfachen.



Laie



Buchhaltung



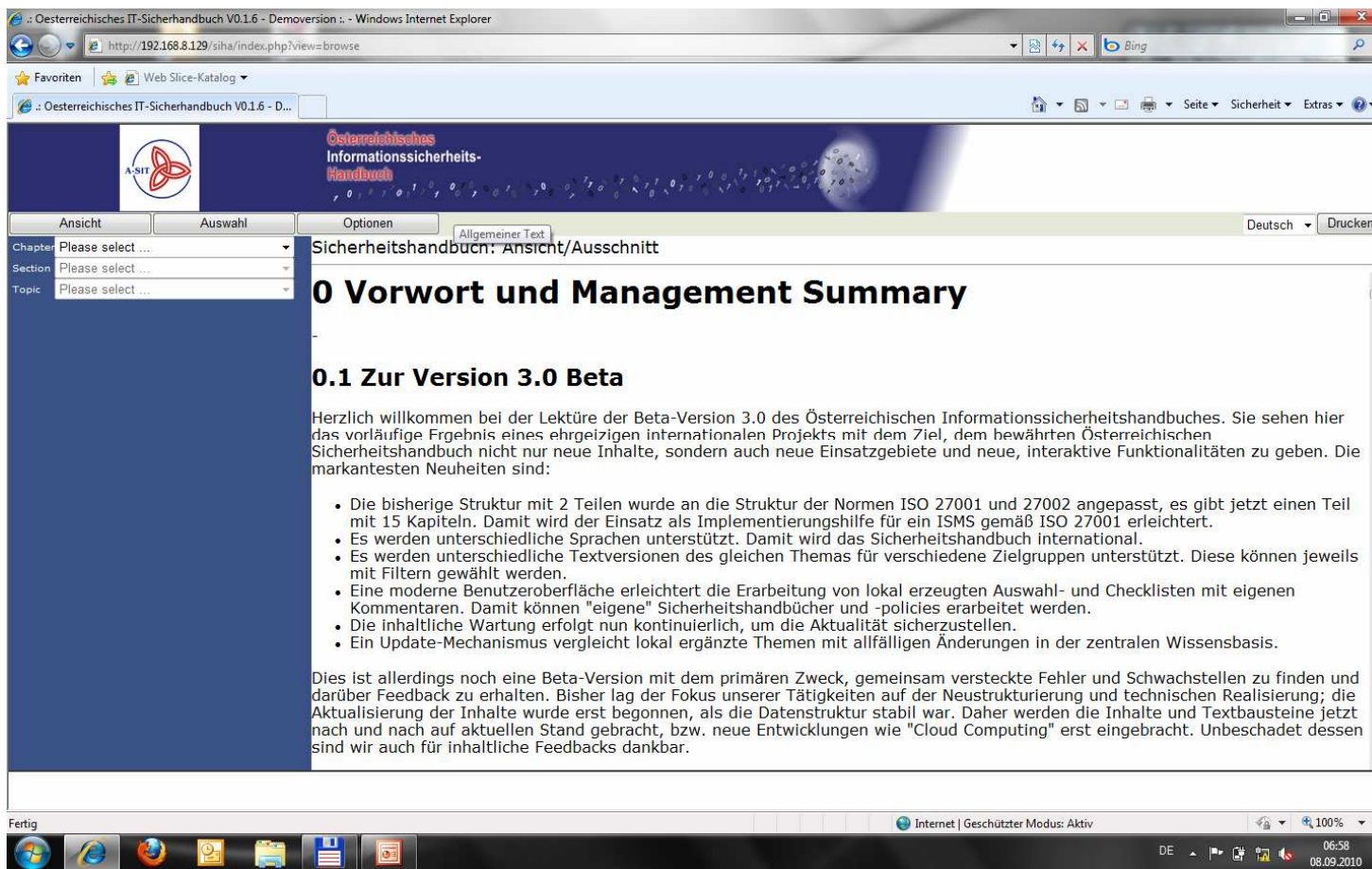
Experte, englisch



Anwender, Gemeindeamt

Die Anwender des Sicherheitshandbuches setzen sich aus unterschiedlichsten Bereichen zusammen. Der Unterschied in IT-Erfahrung und Know-How kann enorm sein.

Anwendung



Österreichisches Informationssicherheits-Handbuch

Sicherheitshandbuch: Ansicht/Ausschnitt

0 Vorwort und Management Summary

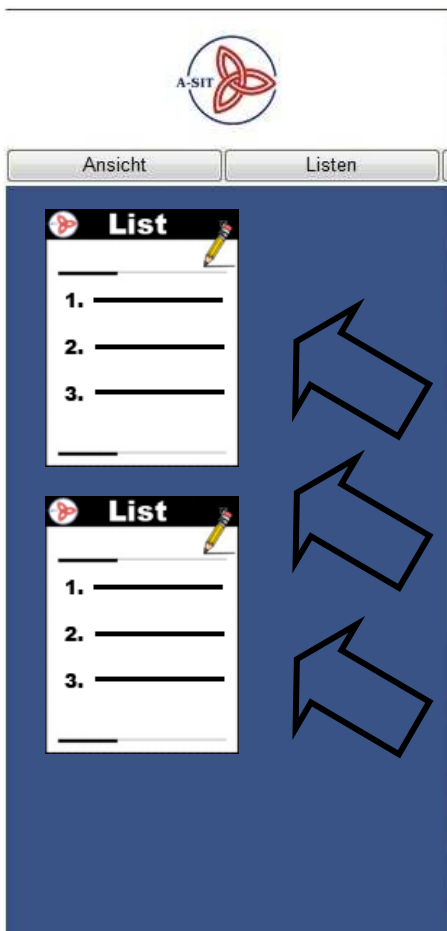
0.1 Zur Version 3.0 Beta

Herzlich willkommen bei der Lektüre der Beta-Version 3.0 des Österreichischen Informationssicherheitshandbuches. Sie sehen hier das vorläufige Ergebnis eines ehrgeizigen internationalen Projekts mit dem Ziel, dem bewährten Österreichischen Sicherheitshandbuch nicht nur neue Inhalte, sondern auch neue Einsatzgebiete und neue, interaktive Funktionalitäten zu geben. Die markantesten Neuheiten sind:

- Die bisherige Struktur mit 2 Teilen wurde an die Struktur der Normen ISO 27001 und 27002 angepasst, es gibt jetzt einen Teil mit 15 Kapiteln. Damit wird der Einsatz als Implementierungshilfe für ein ISMS gemäß ISO 27001 erleichtert.
- Es werden unterschiedliche Sprachen unterstützt. Damit wird das Sicherheitshandbuch international.
- Es werden unterschiedliche Textversionen des gleichen Themas für verschiedene Zielgruppen unterstützt. Diese können jeweils mit Filtern gewählt werden.
- Eine moderne Benutzeroberfläche erleichtert die Erarbeitung von lokal erzeugten Auswahl- und Checklisten mit eigenen Kommentaren. Damit können "eigene" Sicherheitshandbücher und -policies erarbeitet werden.
- Die inhaltliche Wartung erfolgt nun kontinuierlich, um die Aktualität sicherzustellen.
- Ein Update-Mechanismus vergleicht lokal ergänzte Themen mit allfälligen Änderungen in der zentralen Wissensbasis.

Dies ist allerdings noch eine Beta-Version mit dem primären Zweck, gemeinsam versteckte Fehler und Schwachstellen zu finden und darüber Feedback zu erhalten. Bisher lag der Fokus unserer Tätigkeiten auf der Neustrukturierung und technischen Realisierung; die Aktualisierung der Inhalte wurde erst begonnen, als die Datenstruktur stabil war. Daher werden die Inhalte und Textbausteine jetzt nach und nach auf aktuellen Stand gebracht, bzw. neue Entwicklungen wie "Cloud Computing" erst eingebracht. Unbeschadet dessen sind wir auch für inhaltliche Feedbacks dankbar.

Umsetzung



Auswahlen können mit beliebigen Inhalten aus dem Handbuch gefüllt werden.

Weiters ist zu beachten, dass die Bedingungen bzw. Aussagen von etwaigen Versicherungen eigenmächtig werden.
Wo sinnvoll bzw. hilfreich werden in den nachfolgenden Maßnahmenbeschreibungen Normen beispielhaft herausgegriffen und angeführt. Dabei handelt es sich nicht um eine vollständige Aufzählung aller für einen Bereich relevanten Normen und auch nicht um verbindliche Einsatzempfehlungen, die angeführten Beispiele sollen lediglich einen Hinweis auf existierende, möglicherweise zur Anwendung kommende Normen geben und ein detailliertes Einarbeiten in die Materie erleichtern.

9.1 Bauliche Maßnahmen

Relevanz:

9.1.1 Geeignete Standortauswahl

Relevanz:

Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen. Gebäude, die direkt an Hauptverkehrsstrassen (Autobahn, Bundesstraße, Bahn, ...) liegen, können durch Unfälle beschädigt werden, für Gebäude in Einflugschneisen von Flughäfen besteht Gefahr durch einen eventuellen Flugzeugabsturz.
- Die Nähe zu optimalen Verkehrswegen wird in vielen Fällen als Vorteil angesehen werden, kann aber - da diese Verkehrswege auch potentielle Fluchtwege darstellen können - unter Umständen auch die Durchführung eines Anschlages erleichtern. Vor- und Nachteile sind entsprechend abzuwägen.
- In der Nähe von Sendeanlagen kann es zu Störungen der IT kommen.
- Bei Überbauten von U-, S- oder Eisenbahnen kann es zu Störungen von Datenleitungen und CRT-Bildschirmen kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z.B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.
- Streunende Haustiere können Fehlalarme von Bewegungsmeldern verursachen.

9.1.2 Anordnung schützenswerter Gebäudeteile

Relevanz:

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudnähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

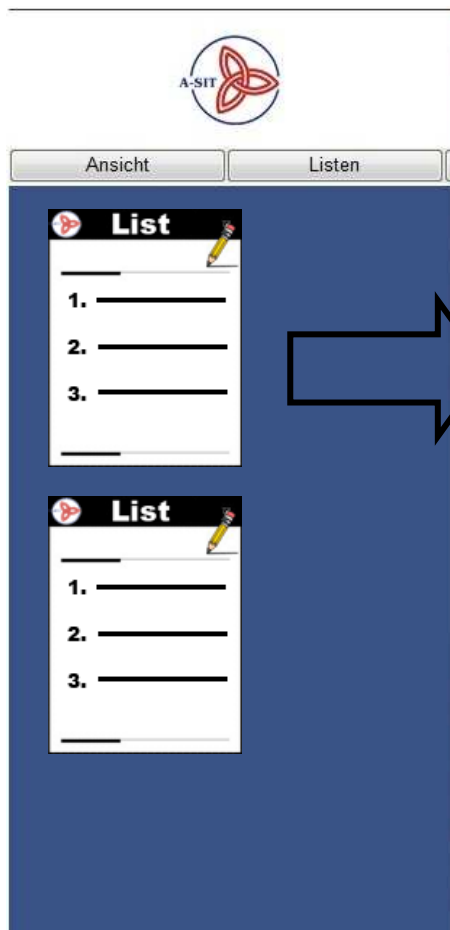
Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen.

Besteht die Möglichkeit, auch das Umfeld des Gebäudes in das Sicherheitskonzept einzubeziehen (etwa bei einer eigenen, ausschließlich der betreffenden Organisation gehörigen Liegenschaft), so können zusätzliche bauliche und technische Sicherheitsmaßnahmen getroffen werden ("Perimeterschutz", "Freilandschutz"). Dazu zählen etwa:

- Zäune und Mauern
- Tore, Schranken und Fahrzeugsperrern
- Kamerasüberwachung und Bewegungsmelder

9.1.3 Einbruchschutz

Umsetzung



Aus diesen Listen können Checklisten generiert werden.

9.1.1 Geeignete Standortauswahl

Relevanz:

Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen. Gebäude, die direkt an Hauptverkehrsstrassen (Autobahn, Bundesstraße, Bahn, ...) liegen, können durch Unfälle beschädigt werden, für Gebäude in Einflogschneisen von Flughäfen besteht Gefahr durch einen eventuellen Flugzeugabsturz.
- Die Nähe zu optimalen Verkehrswegen wird in vielen Fällen als Vorteil angesehen werden, kann aber - da diese Verkehrswege auch potentielle Fluchtwege darstellen können - unter Umständen auch die Durchführung eines Anschlages erleichtern. Vor- und Nachteile sind entsprechend abzuwägen.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- Bei überbauten von U-, S- oder Eisenbahnen kann es zu Störungen von Datenleitungen und CRT-Bildschirmen kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z.B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.
- Streunende Haustiere können Fehlalarme von Bewegungsmeldern verursachen.

9.1.2 Anordnung schützenswerter Gebäudeteile

Relevanz:

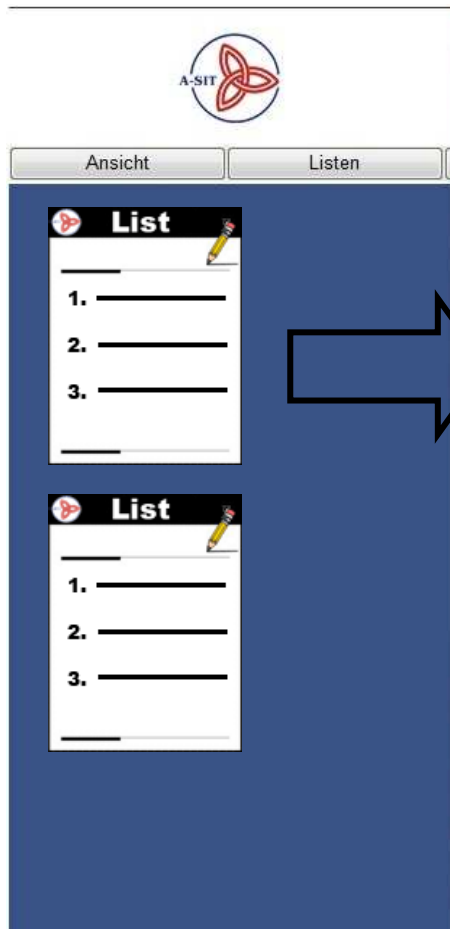
Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

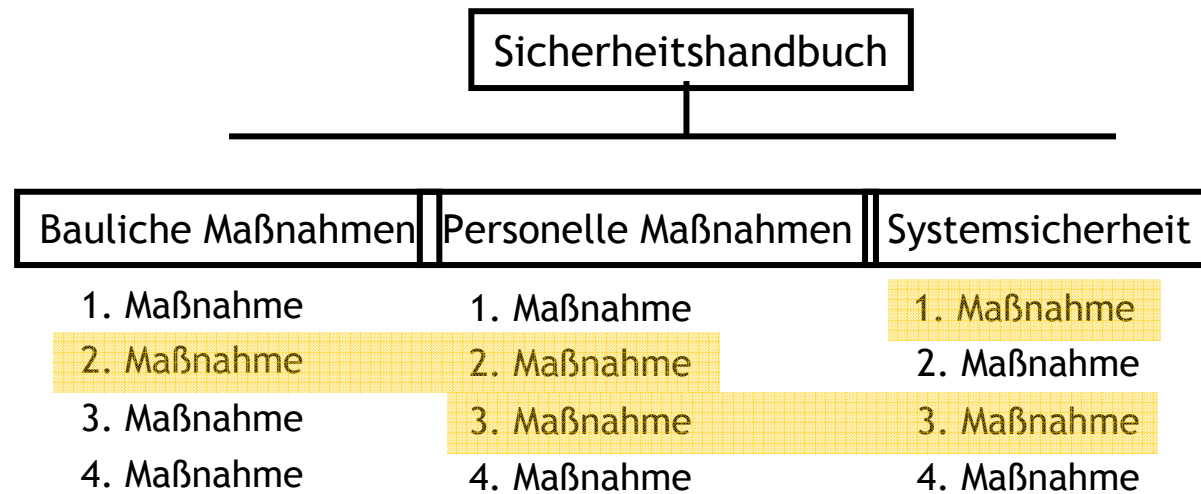
Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen. Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelagungsplanung bei Einzug in ein bestehendes einzubeziehen. Besteht die Möglichkeit, auch das Umfeld des Gebäudes in das Sicherheitskonzept einzubeziehen (etwa bei einer eigenen, ausschließlich der betreffenden Organisation gehörigen Liegenschaft), so können zusätzliche bauliche und technische Sicherheitsmaßnahmen getroffen werden ("Perimeterschutz", "Freilandschutz"). Dazu zählen etwa:

- Zäune und Mauern
- Tore, Schranken und Fahrzeugsperrern
- Kameraüberwachung und Bewegungsmelder

Umsetzung

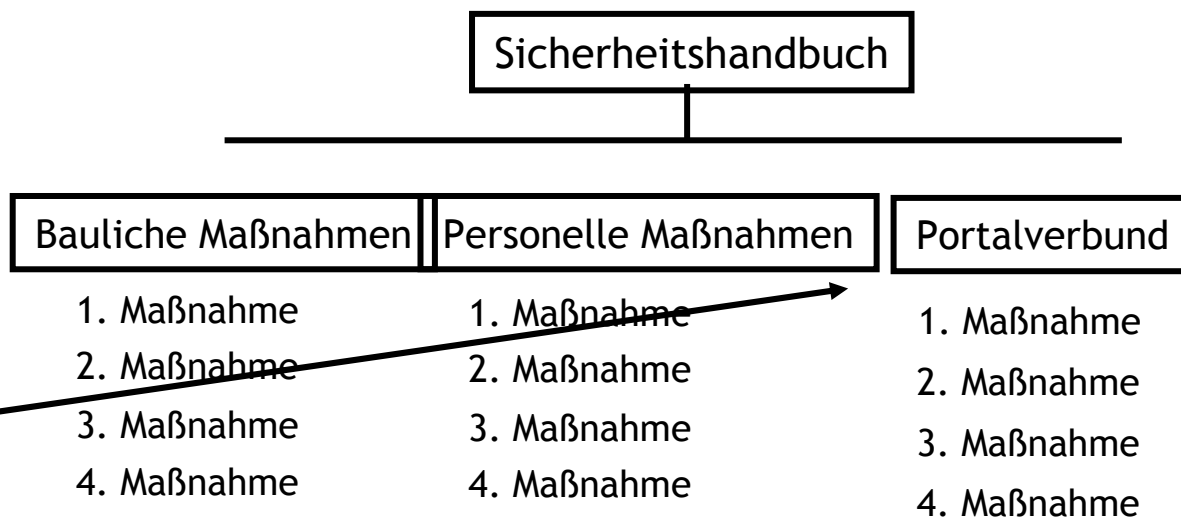
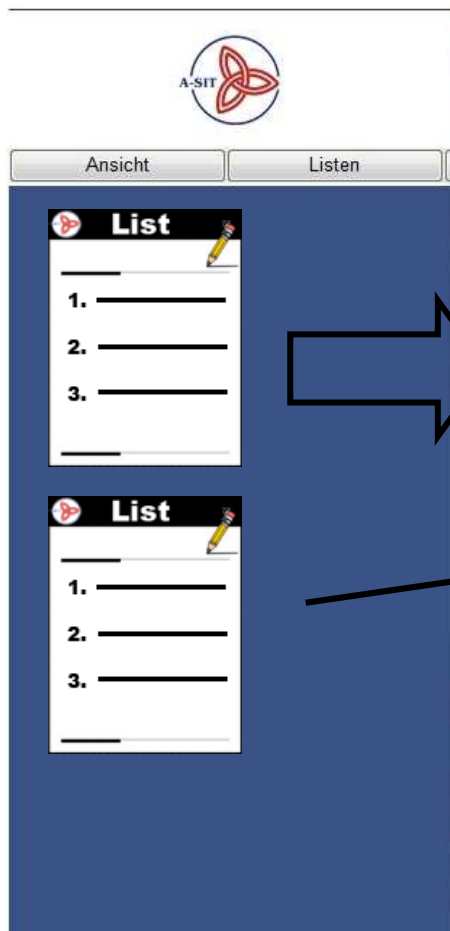


Diese Listen können als Querschnittsmaterien verwendet werden



Umsetzung

Diese Auswahlen können als Erweiterung in ein individualisiertes Handbuch eingegliedert werden



Zusammenfassung

- Ende 2009 Notwendigkeit eines Updates festgestellt
 - Neue Schwerpunkte
- Neue Struktur
 - Wissensbasis
 - Anwendung
 - Autorengruppe(n)
- Neuer Zugang
 - Online Tool
 - Filter
 - Auswahlen / Listen

Vielen Dank für ihre Aufmerksamkeit

Weitere Informationen unter:
<http://www.a-sit.at>