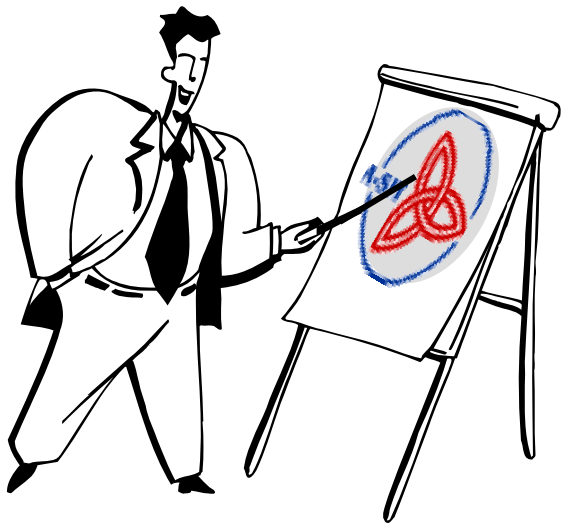
Risikomanagement

Nationale / Internationale Methoden

Herbert.Leitold@a-sit.at

Inhalte



- Einleitung
  - Vorgaben des Rates zu klassifizierten Informationen
- International
  - CRAMM, EBIOS, GSHB
- National
  - IT Sicherheitshandbuch
  - Status „SIHA Teil 3“
- Zusammenfassung

Internationale Vorgaben *(1/2)*

Sicherheitsvorschriften des Rates

Anmerkung in Abschnitt XI (*), Kapitel II, Pkt. 24.

[…] Die Akkreditierung sollte in der Regel auf der Grundlage der SSRS (**) erfolgen und Folgendes umfassen:

(a) […]

(b) Bestandsaufnahme **des Risikomanagements**, in der Bedrohungen und Schwachstellen benannt und entsprechende Gegenmaßnahmen dargelegt werden;

etc.

(*) Behandelt Schutz von Informationen in informationstechnischen Systemen und Kommunikationssystemen

(**) SSRS: Systemspezifische Sicherheitsanforderungen

Internationale Vorgaben *(2/2)*

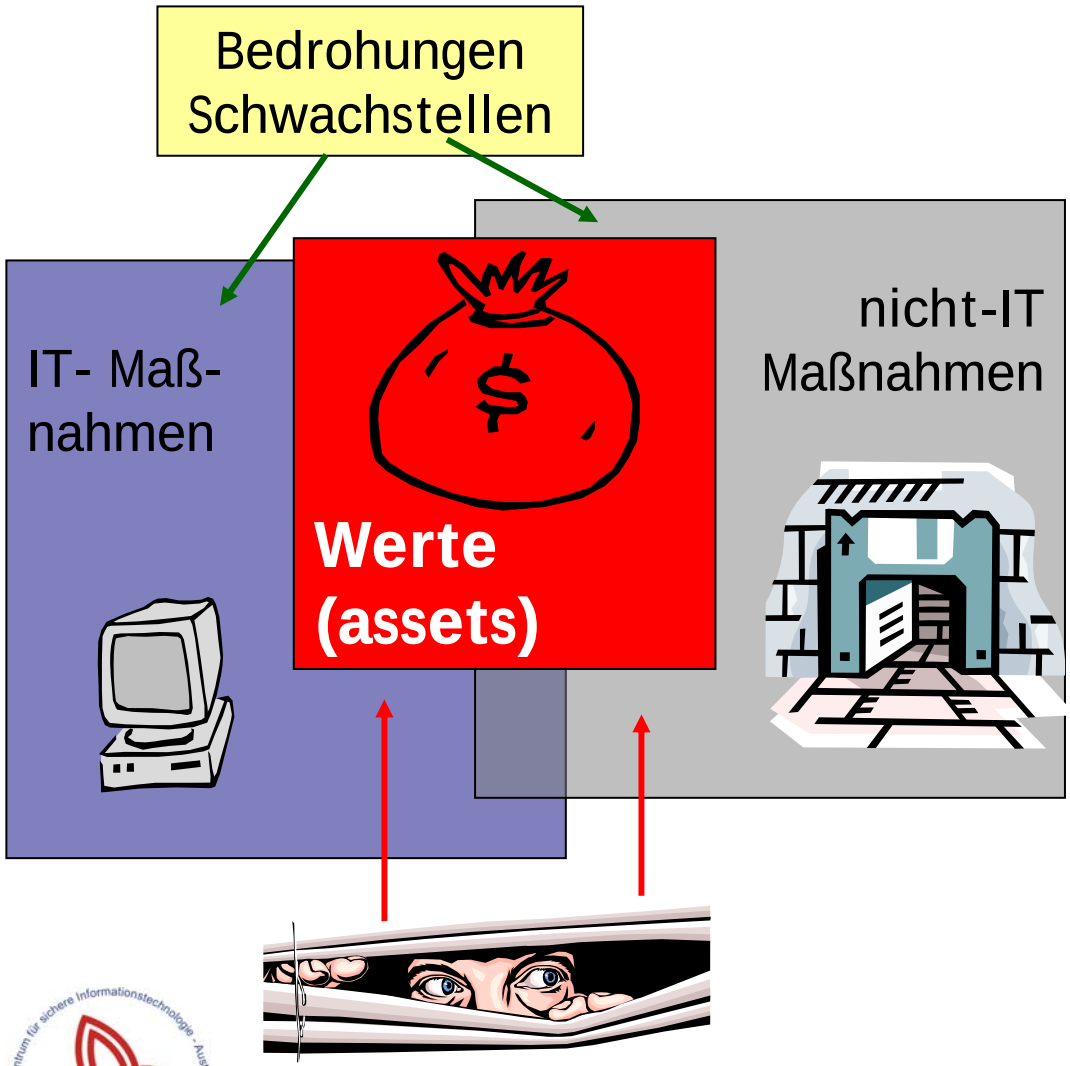
SSRS

Abschnitt XI (*), Kapitel I, Pkt. 12.

Die SSRS (*) ist eine vollständige und ausführliche Festlegung der einzuhaltenden Sicherheitsgrundsätze und der zu erfüllenden detaillierten Sicherheitsanforderungen.
Sie beruht auf dem Sicherheitskonzept und der **Risikobewertung des Rates** bzw. wird von Faktoren des betrieblichen Umfelds bestimmt, vom niedrigsten Berechtigungsstatus [... etc. etc. …]

(*) SSRS: Systemspezifische Sicherheitsanforderungen;
verpflichtend ab CONFIDENTIEL UE, oder schon ab RESETRINT UE, wenn die Verfügbarkeit der Information als kritisch anzusehen ist.

Grundsätze zu Methodik



- Identifikation der Werte
  - Vollständigkeit
- Bedrohungsanalyse
  - Vollständigkeit
  - Threat-Kataloge
- Maßnahmen
  - Sollen Bedrohungen bedecken
  - Systematische Auswertung möglich
- Oft bestehende Infrastruktur
  - Zuerst Analyse des IST-Stands

Grundprinzipien

Strukturierter, methodischer Zugang

ISP Guidelines Risk Management

- identification of the scope and objective of the risk assessment;
- determination of the information assets and (if possible) of the physical assets;
- determination of the value of the physical and information assets;
- selection of the relevant threats and associated vulnerabilities.
- impact of the identified threats and vulnerabilities on the system.
- identification of existing countermeasures;
- determination of the necessary countermeasures and a comparison with existing measures;
- review of the risks and the recommended countermeasures;
- development of a Risk Management Report, including a description of the countermeasures to be implemented, and a description of the residual risk.

AT Sicherheitshandbuch Teil 1: Detaillierte Risikoanalyse (Schritte)

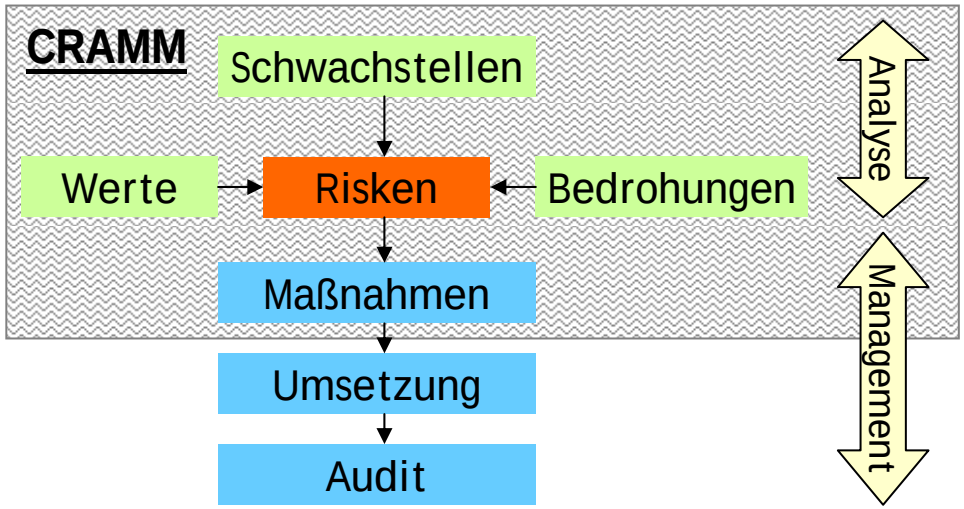
1. Abgrenzung des Analysebereichs
2. Identifikation der bedrohten Werte
3. Wertanalyse
4. Bedrohungsanalyse
5. Schwachstellenanalyse
6. Identifikation bestehender Maßnahmen
7. Risikobewertung
8. Auswertung und Aufbereitung

International

- Ein Vielzahl an Methoden
  - vgl. ENISA www.enisa.europa.eu/rmra/rm_home.html
- Überblick und Tools an einigen Beispielen
  - CRAMM
  - EBIOS
  - GSHB

CRAMM - Grundlagen

- CCTA (*) Risk Analysis and Management Method
  - 1985 aus UK Government Best Practices entwickelt
  - dzt. Version 5 (2003)
- Bevorzugte UK Methode



Bewertung ENISA Arbeitsgruppe						
Risk Identification	Risk Analysis	Risk Evaluation	Risk Assessment	Risk Treatment	Risk Acceptance	Risk Communication
***	***	***				

(*) CCTA: Central Communication and Telecommunication Agency, nun: Office of Government Commerce www.ogc.gov,uk

CRAMM - Tool

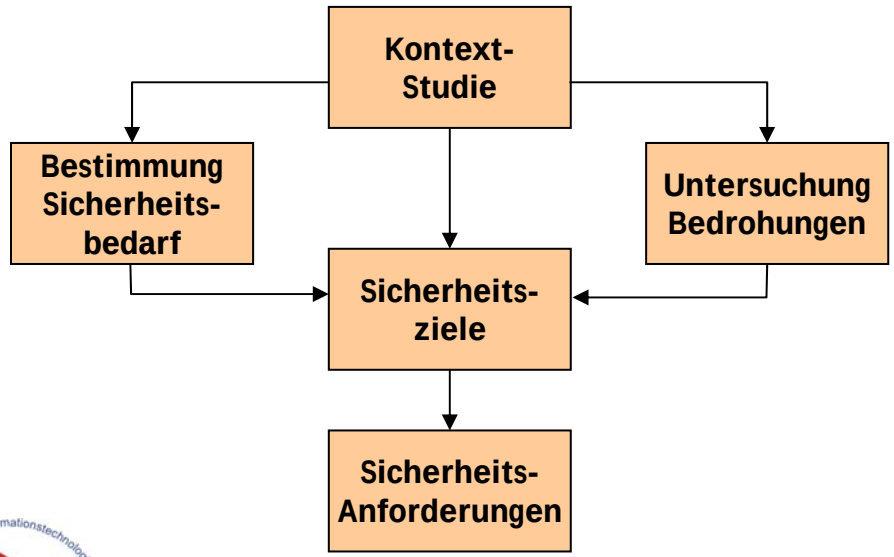
- Kommerzielles Tool
  - Expert : £2950 + £875 p.a.
  - Express: £1500 + £250 p.a.
  - www.cramm.com
- Für Verwendung CRAMM ist Tool praktisch notwendig
  - Modellierung Werte
  - Bedrohungs- und Schwachstellenanalyse
  - Risikobewertung
  - Identifikation von Maß-nahmen (controls)

- Beispiel eines MOR Reports

Threat	Threat level	Vulnerability level	Measure of risk
Introduction of Damaging or Disruptive Software	Very High	High	6
Embedding of Malicious Code	Very High	High	6
Masquerading of User Identity by Contracted Service Providers	Medium	High	5
Masquerading of User Identity by Outsiders	Medium	High	5
[illegible] peration			
Technical Failure of Network Interface	Low	Low	3
Hardware Maintenance Error	Very Low	Medium	3
Software Maintenance Error	Very Low	Low	3
Wilful Damage by Outsiders	Very Low	Medium	3
Terrorism	Very Low	Medium	3

EBIOS - Grundlagen

- Expression des Besoins et Identification des Objectifs de Sécurité
  - 1995 durch DCSSI (*) entwickelt
  - dzt. Version 2 (2004)

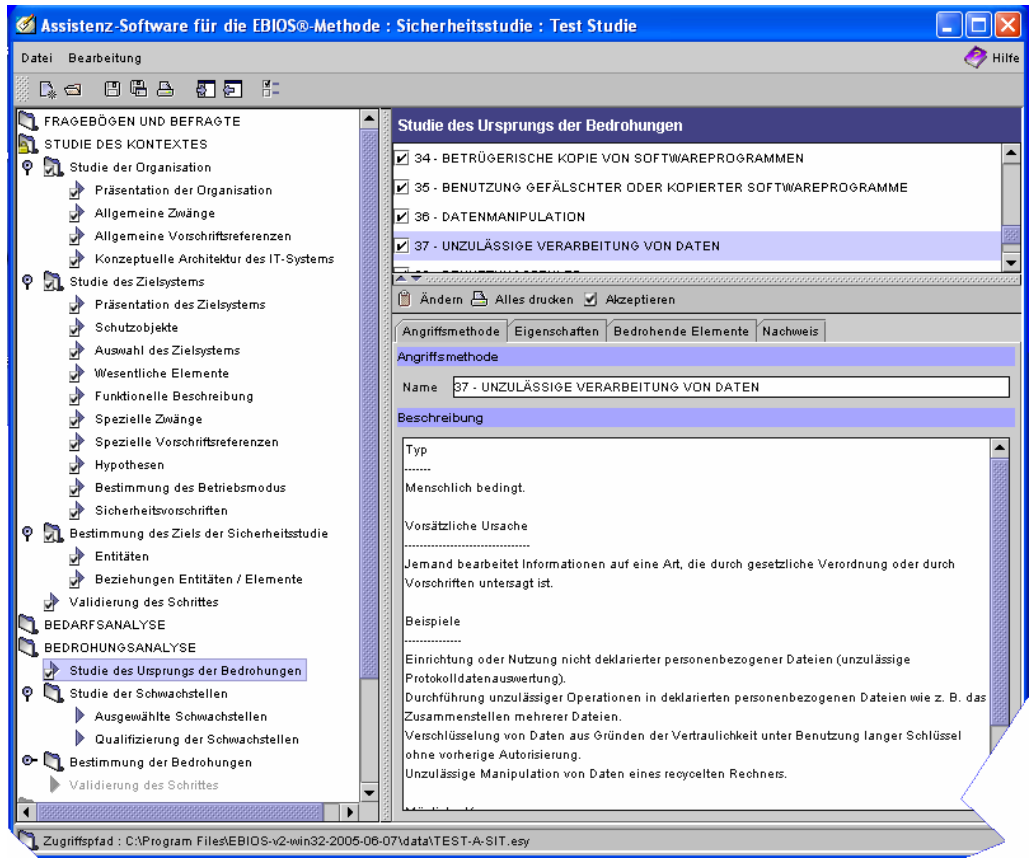


Bewertung ENISA Arbeitsgruppe						
Risk Identification	Risk Analysis	Risk Evaluation	Risk Assessment	Risk Treatment	Risk Acceptance	Risk Communication
***	***	***	***	***	***	***

(*) DCSSI: Direction Centrale de la Sécurité des Systémes d'Information, www.ssi.gouv.fr

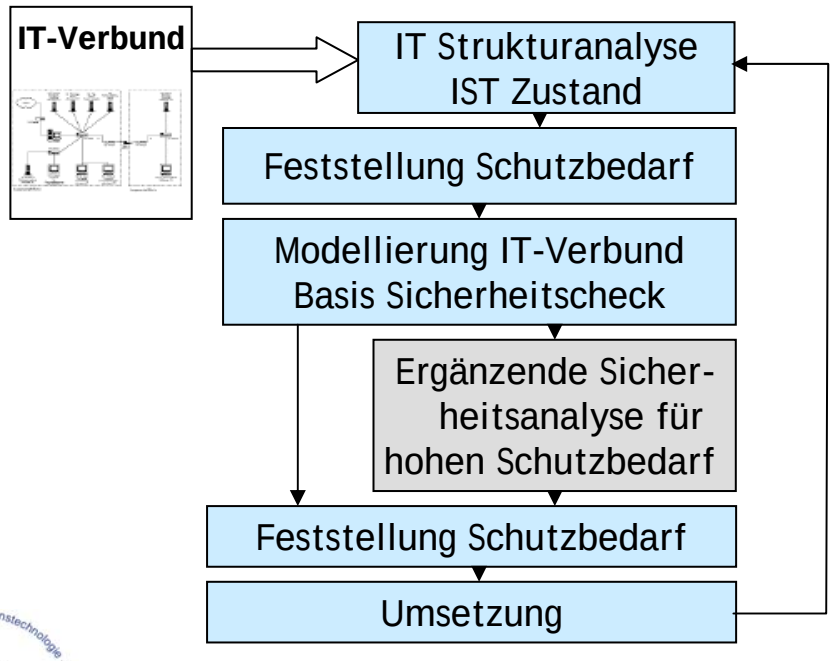
EBIOS - Tool

- Frei verfügbares Tool
  - Windows, Linux, Solaris
  - Open Source
  - auch deutsch / englisch
  - www.ssi.gouv.fr/de/vertrauen/ebiospresentation.html
- Umfasst
  - Definition des Systems
  - Bedrohungsanalyse
  - Definition der Sicherheitsziele
  - Festelegen der Sicherheitsanforderrungen
  - Synthesefunktionen, u.a.
    - CC-PP, CC-ST, SSRS, …



Grundschutzhandbuch - Grundlagen

- IT Grundschutzhandbuch
  - 1994 durch BSI (*) entwickelt
  - laufend aktualisiert (2005)



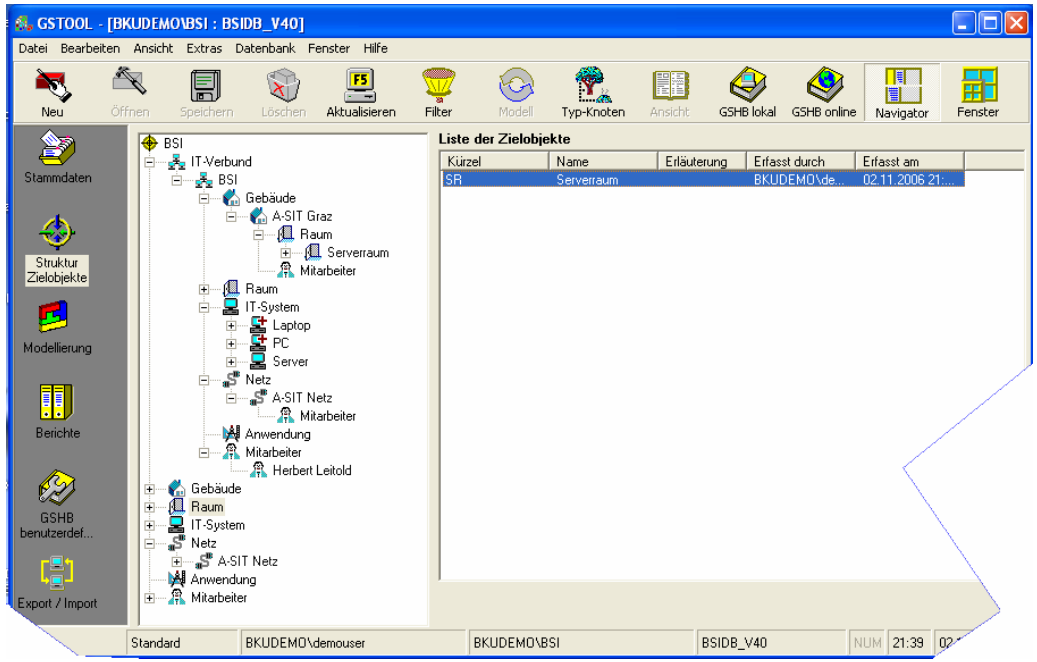
Bewertung ENISA Arbeitsgruppe						
Risk Identification	Risk Analysis	Risk Evaluation	Risk Assessment	Risk Treatment	Risk Acceptance	Risk Communication
***	***	***	***	***	***	***

(*) Bundesamt für Sicherheit in der Informationstechnologie, www.bsi.bund.de

Grundschutzhandbuch - Tool

- Kommerzielles Tool
  - Kostenlos für deutsche Behörden
  - 1-Platz Lizenz ca. € 1000
  - www.bsi.bund.de/gstool/
- Umfasst u.a.
  - Erfassung der IT Systeme
  - Modellierung
  - Basis-Sicherheitscheck
- Weitere Tools:
  - HiScout SME, SAVe, IGSDoku, Secu-Max, …

- Beispiel



National

- IT Sicherheitshandbuch
  - Anpassung 2002/2003
    - Checklisten
  - „Teil 3“

Österreichisches IT-Sicherheitshandbuch

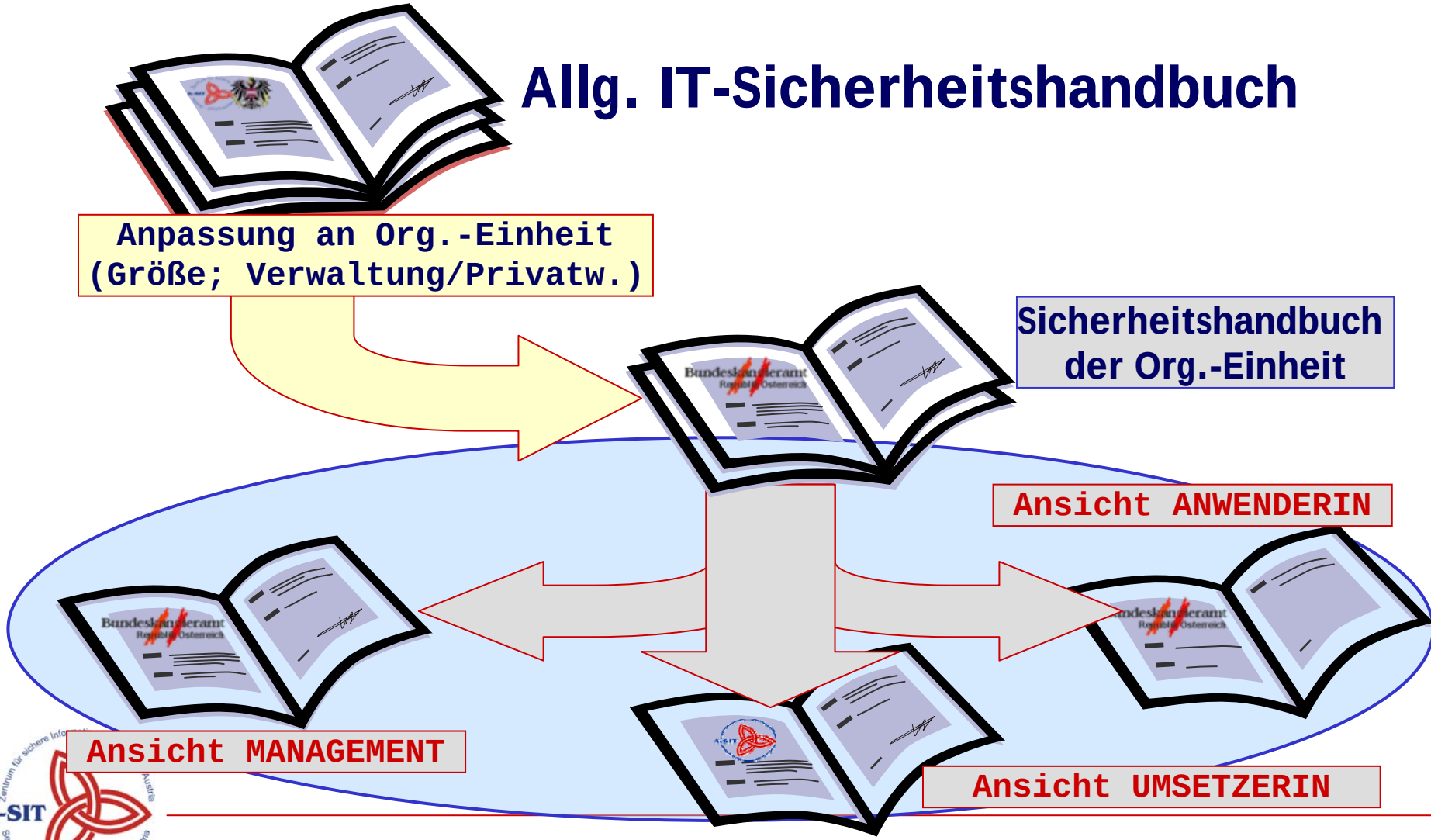
- SIHA
  - Teil 1: Sicherheitsmanagement
  - Teil 2: Maßnahmen
- Ziele der XML-Struktur
  - Unterstützung bei Umsetzung
  - Verschiedene Ansichten
  - Vorarbeiten für Tools
- Historie
  - 1998 BMI
  - 2001 Erweiterungen
  - 2003 XML-Struktur
  - 2006 - Aktualisierung, „Teil 3“

Bewertung ENISA Arbeitsgruppe						
Risk Identification	Risk Analysis	Risk Evaluation	Risk Assessment	Risk Treatment	Risk Acceptance	Risk Communication
**	*	*	***	***	***	***

XML-Struktur: Zielgruppenorientierung

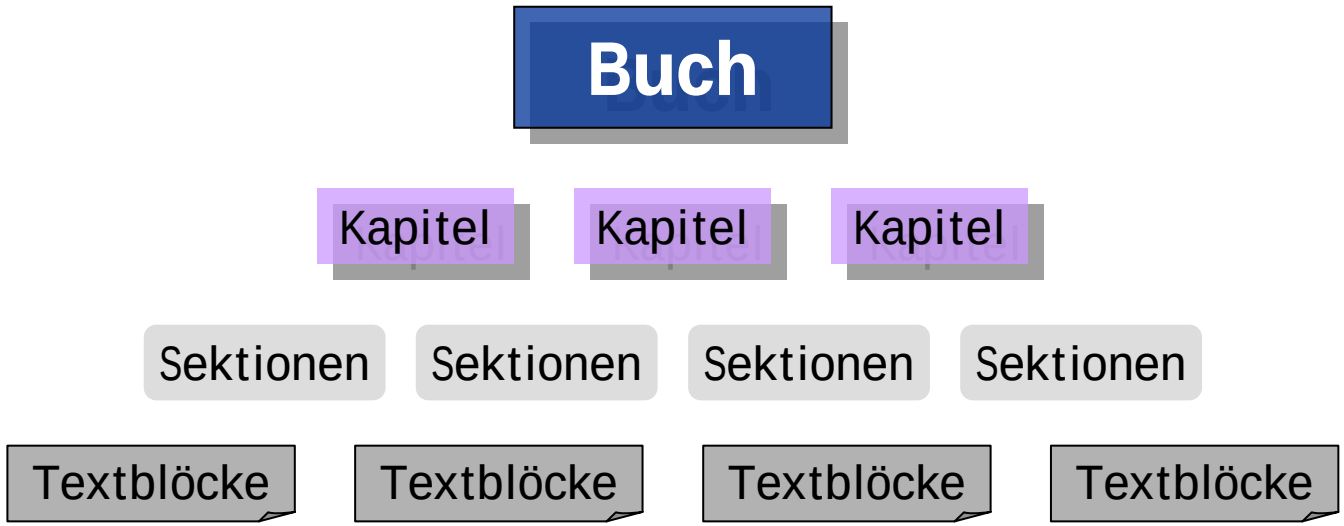
- Sicherheitshandbuch soll an die Gegebenheit der Organisationseinheit „personalisierbar“ sein
  - Größe der Organisationseinheit
  - Umfeld öffentl. Verwaltung vs. Privatwirtschaft
- Spezifische Ansichten
  - Management, Umsetzung/Wartung, AnwenderIn
  - Checklisten

Personalisierung / Konzept

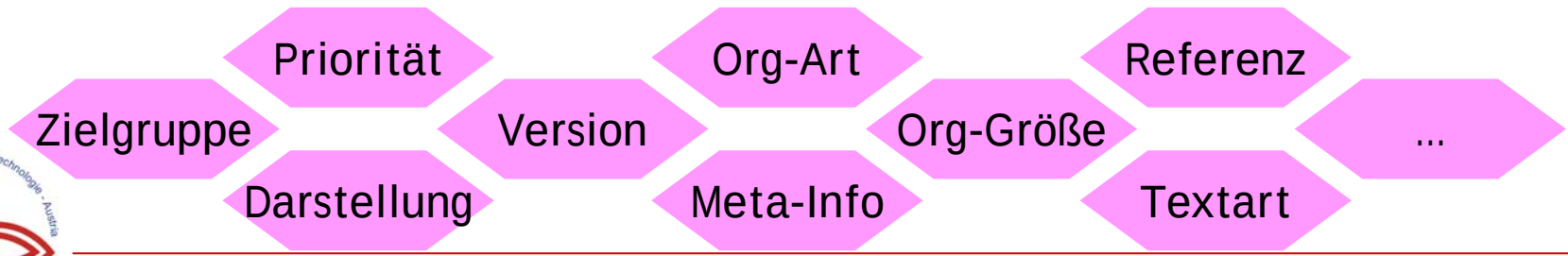


Das XML-Schema

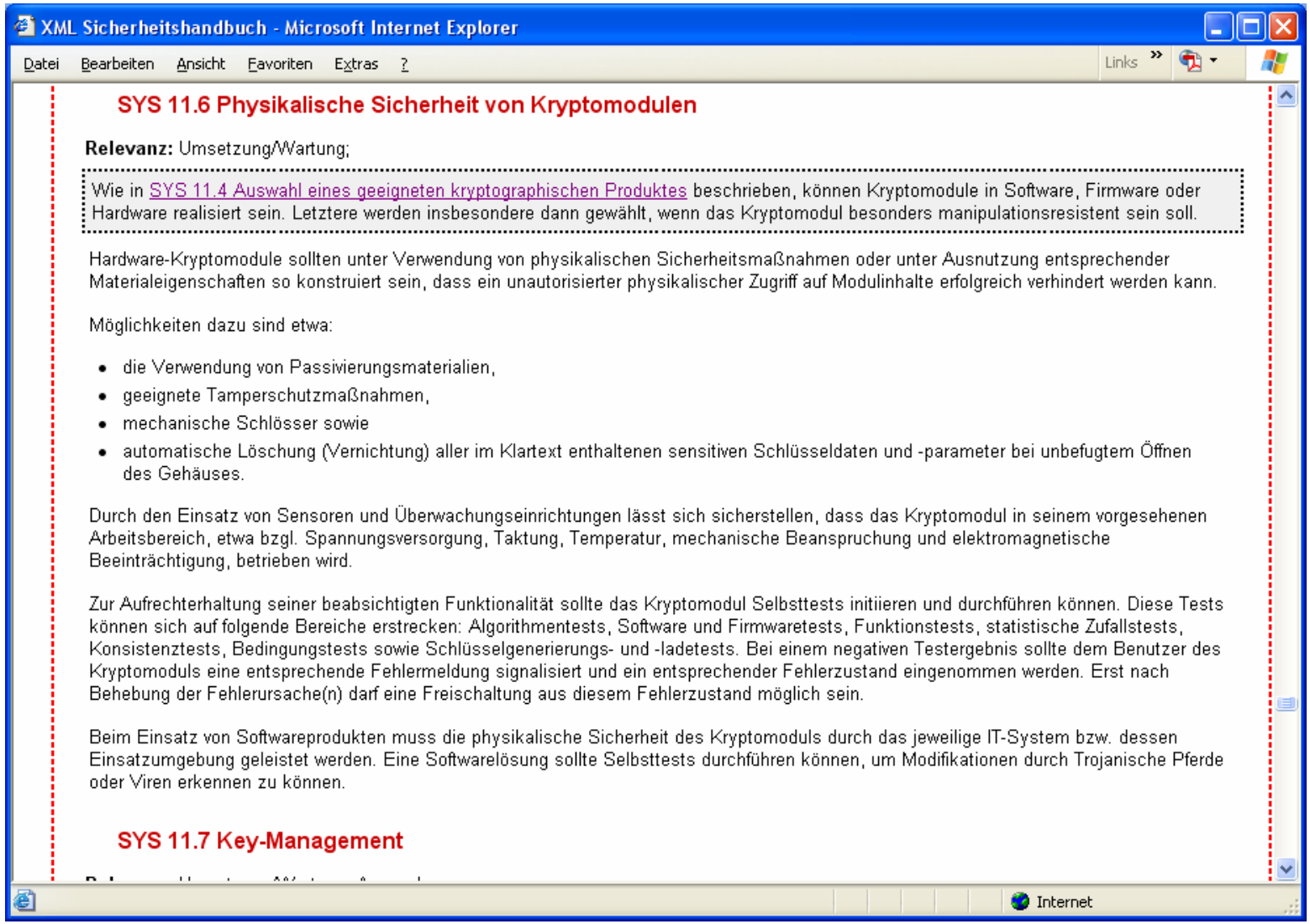
- Struktur:



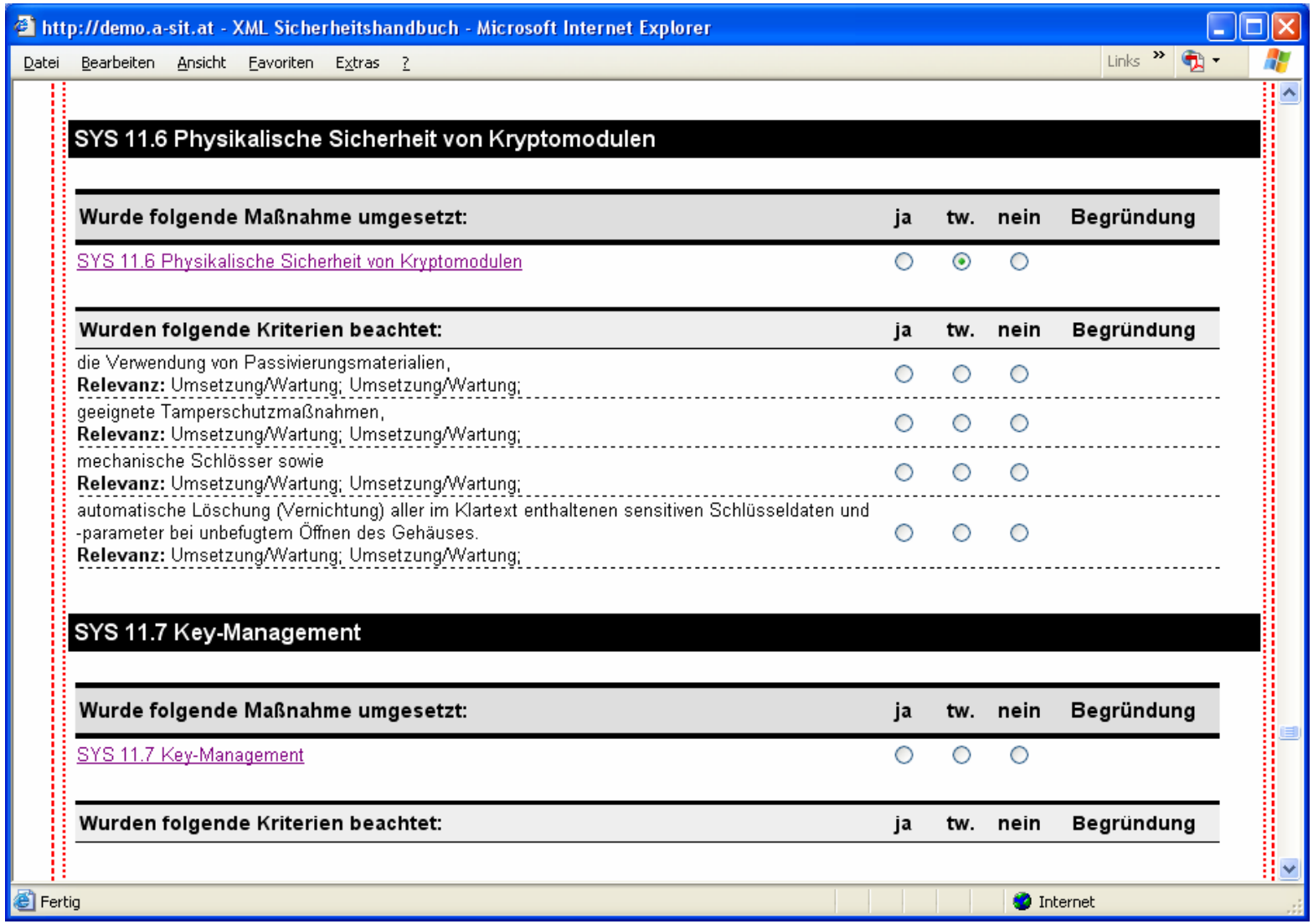
- Zusatzinformationen:



Beispiel Gesamtansicht



Beispiel Checklisten

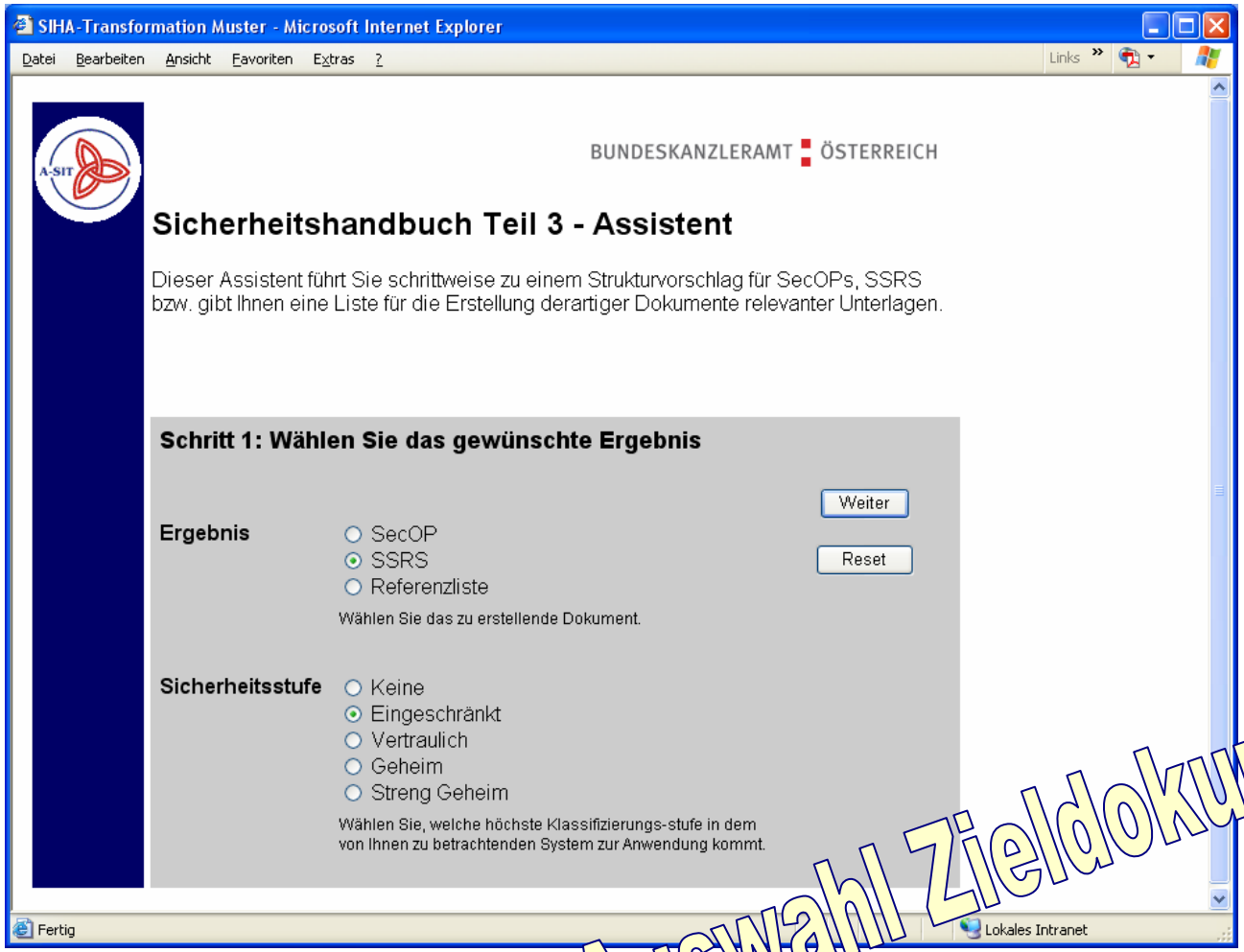


SIHA Teil 3

- Aktuell wird ein „Teil 3“ erstellt
  - Unterstützung ITSOA (*) / INFOSEC Stelle
    - Vorlage zur Erstellung von SSRS (**) und SecOPs (***)
      - Assistenten-gestütztes Generieren der Dokumentenvorlage
      - Hinweise auf relevante Dokumente (z.B. ISP)
    - Liste relevanter Unterlagen mit Kurzbeschreibungen
- Teil 3 selbst klassifiziert (Teile)

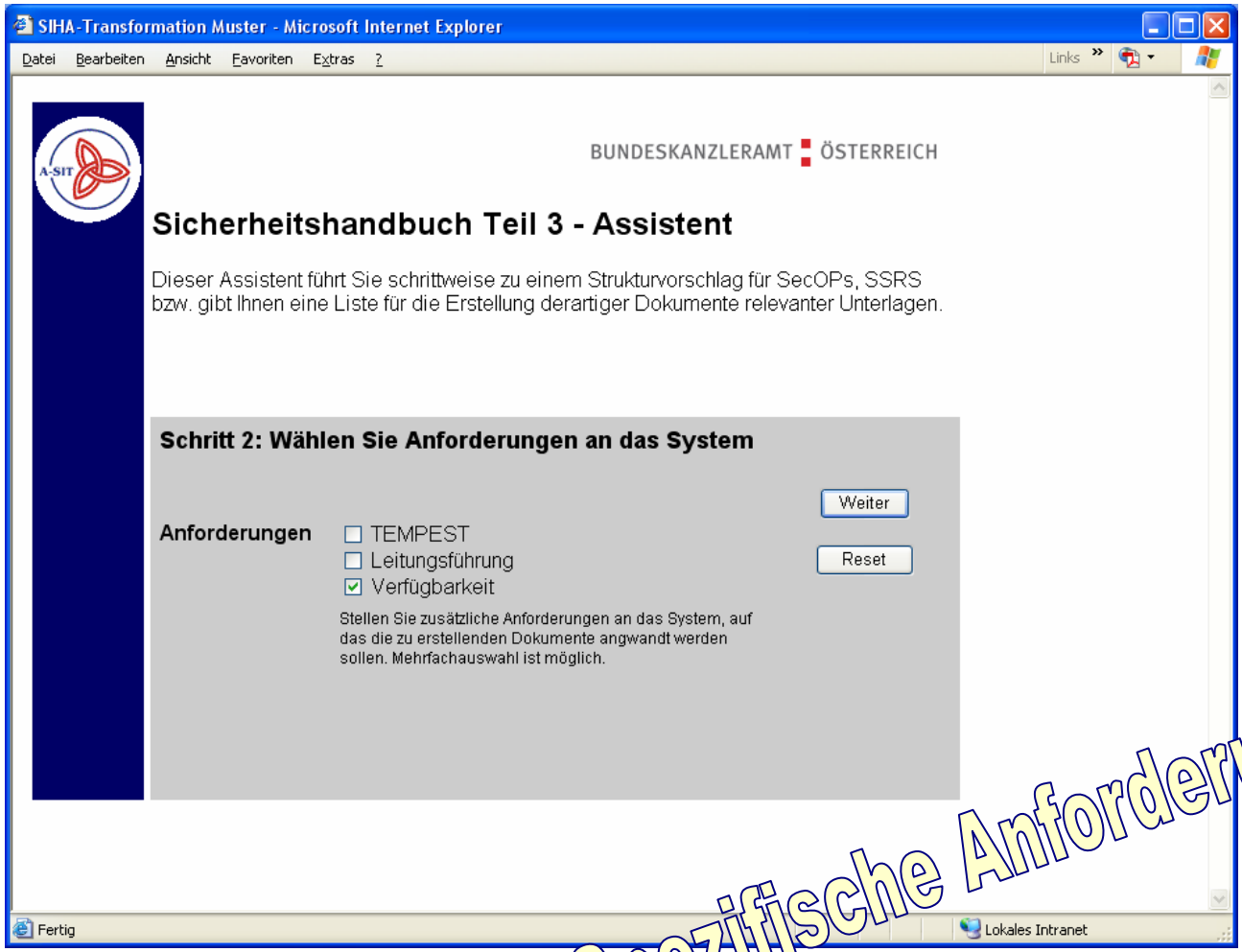
(*) ITSOA: Zuständige Stelle für Betrieb des IT-Systems
(**) SSRS: Systemspezifische Sicherheitsanforderungen
(***) SecOPs: Sicherheitsrelevante Betriebsverfahren

Assistent Teil 3 *(1/5)* exemplarisch



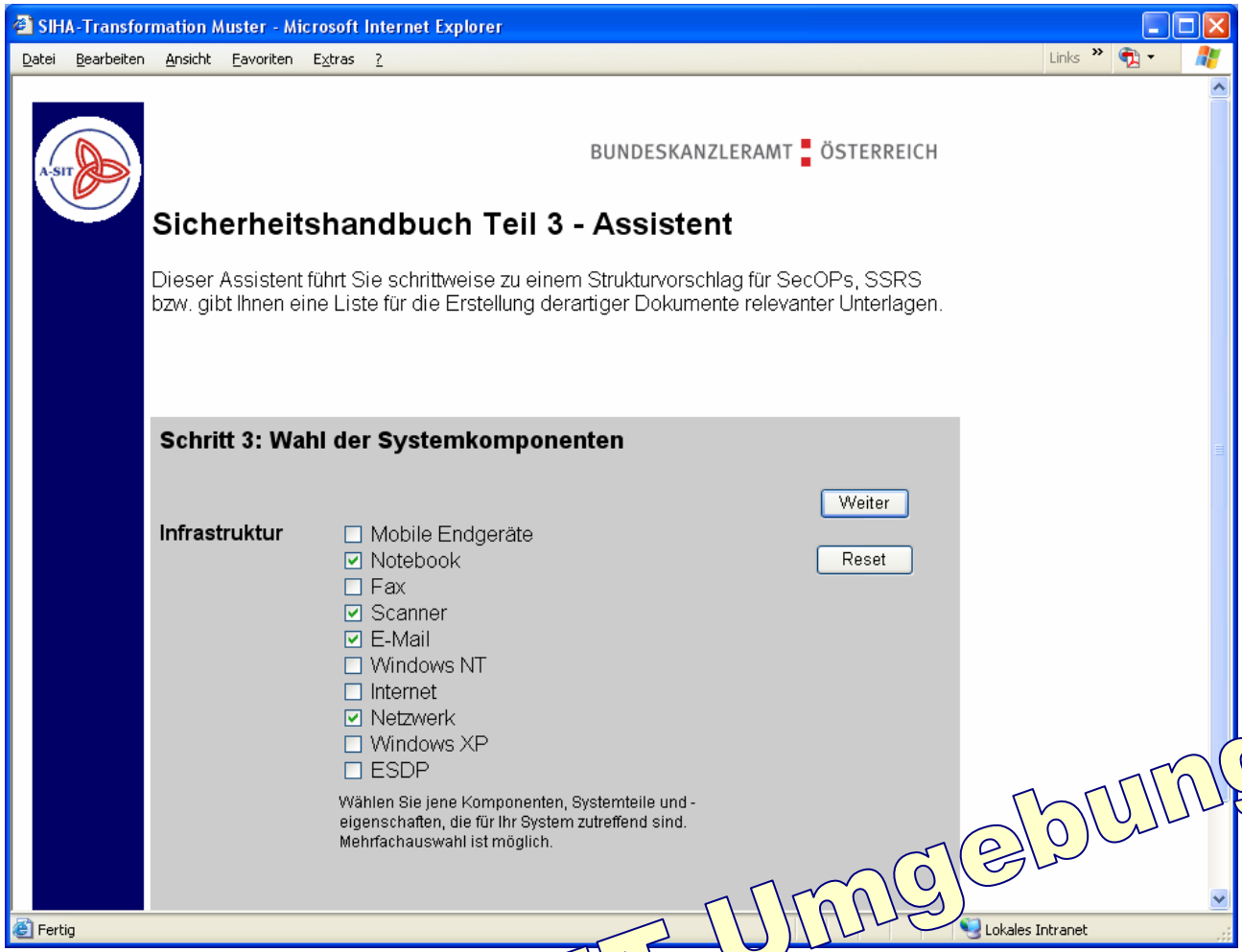
Auswahl Zieldokument

Assistent Teil 3 *(2/5)* exemplarisch



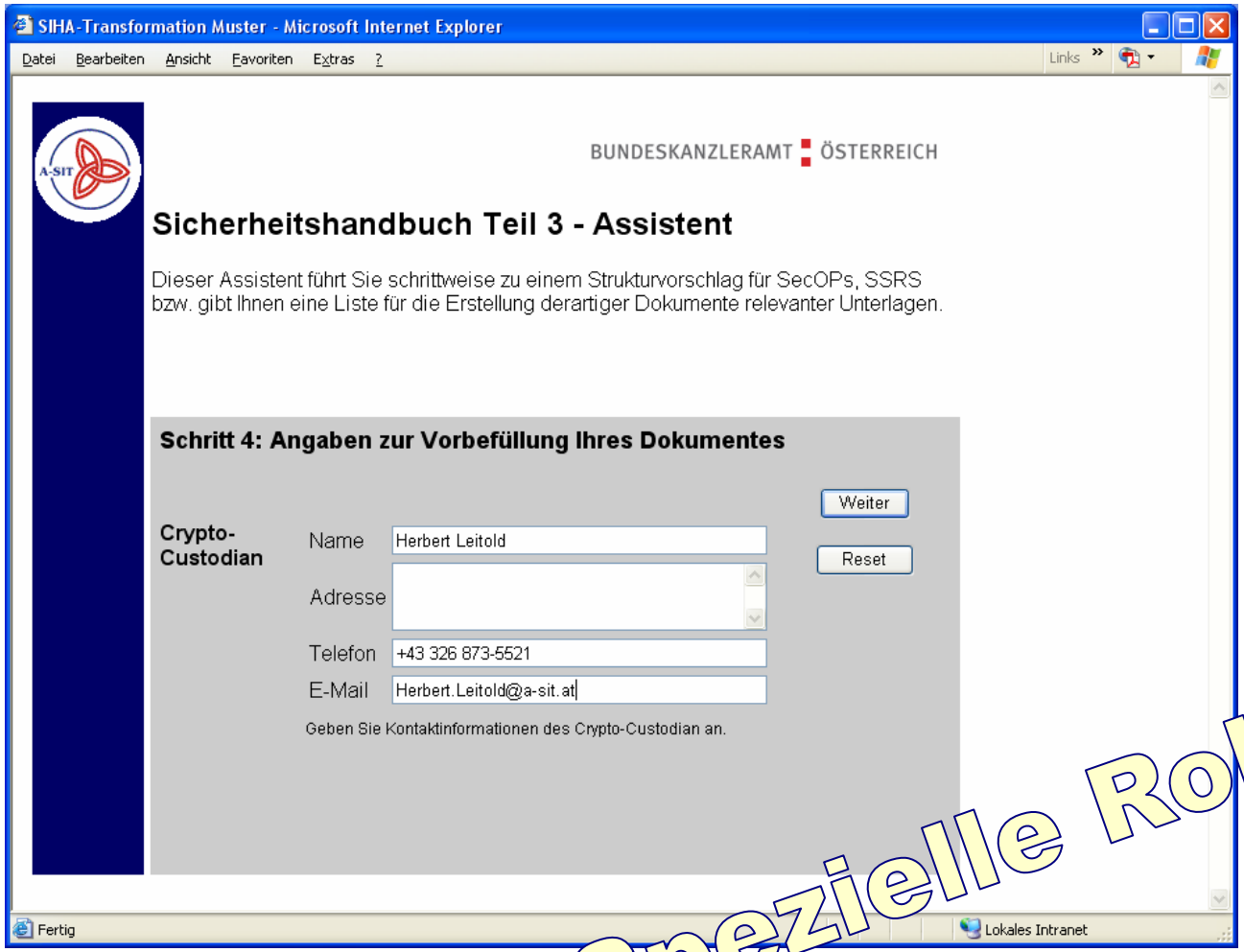
Spezifische Anforderungen

Assistent Teil 3 *(3/5)* exemplarisch



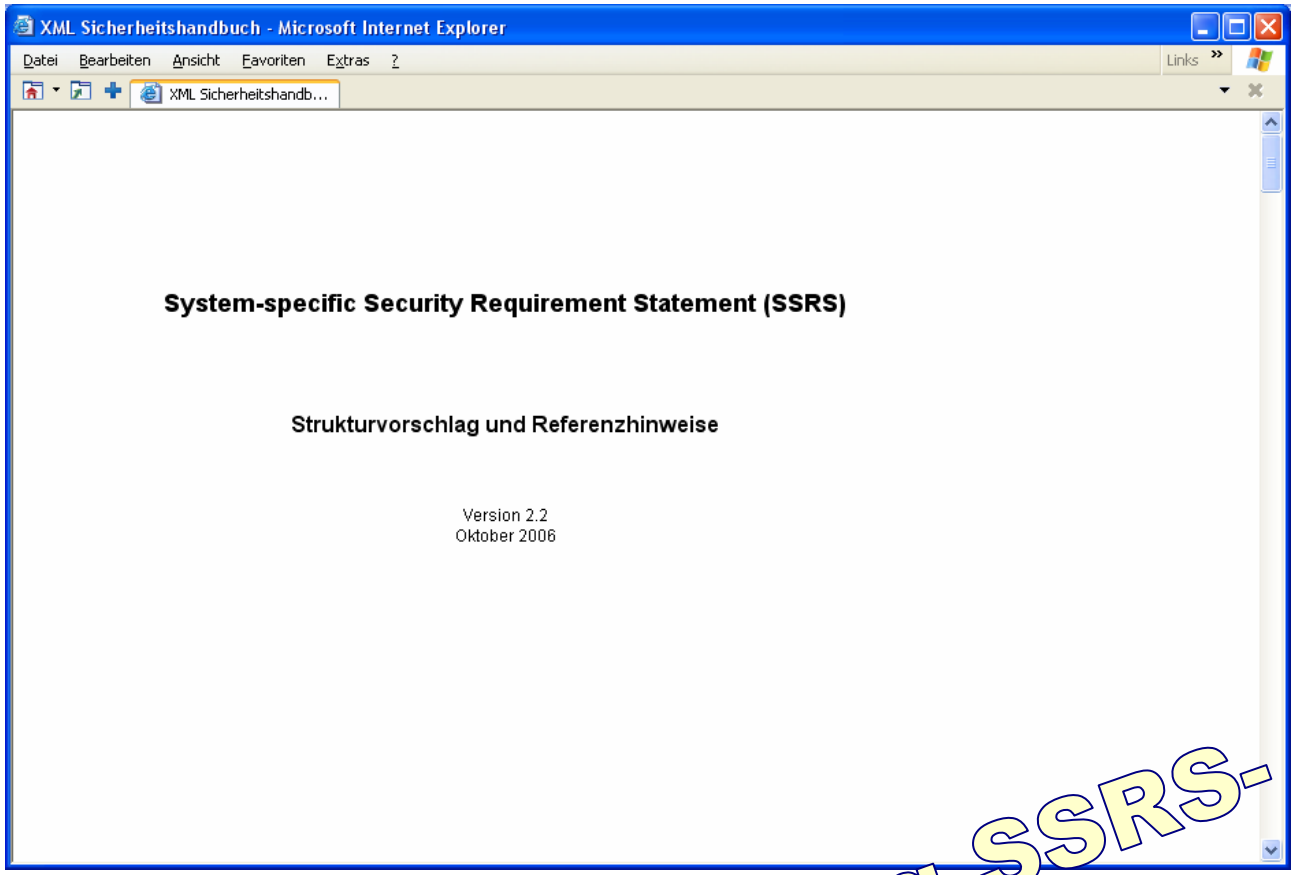
IT Umgebung

Assistent Teil 3 *(4/5)* exemplarisch



Spezielle Rollen

Assistent Teil 3 *(5/5)* exemplarisch



Auszug SSRS-Vorlage

Zusammenfassung

- Vielzahl an Methoden / Tools
  - Bsp. CRAMM, EBIOS, GSHB
- IT Sicherheitshandbuch
  - Teil 1 erläutert IT Sicherheits-managementprozess
  - Maßnahmen in Teil 2
  - Teil 3 in Arbeit
    - Unterstützung bei Erstellung von SSRS und SecOPs
    - Unterstützung zu „Industrieller Sicherheit“

Danke für die Aufmerksamkeit!

http://www.a-sit.at

http://demo.a-sit.at/it_sicherheit/it_siha/

Herbert.Leitold@a-sit.at