

# **Governance-Mapping für den KRITIS-Sektor: Finanz- und Versicherungswesen**

22. März 2018

Tatjana Anisow

SerNet GmbH, Göttingen - Berlin

---

## Agenda

---

- SerNet GmbH
  - KRITIS-Sektor: Finanz- und Versicherungswesen
  - Governance-Mapping
  - Umsetzung in verinice
-

- **SerNet GmbH**
  - KRITIS-Sektor: Finanz- und Versicherungswesen
  - Governance-Mapping
  - Umsetzung in verinice
-

- gegründet 1997
- Büros in Göttingen und Berlin
- Themen: Informationssicherheit und Datenschutz
- spezialisiert auf Open Source Software
- verinice.: Open Source ISMS Tool
- SAMBA: Windows/Linux-Interoperabilität, Clustering und Private Clouds
- Zertifizierungen und Audits, IT-Grundschutz und ISO 27001
- Firewalls und VPN-Lösungen für mittlere und große Einrichtungen
- Old Economy: kein Risiko-Kapital, keine Bank-Kredite
- über 1500 Bestandskunden in DE, EU, US

## Agenda

---

- SerNet GmbH
  - **KRITIS-Sektor: Finanz- und Versicherungswesen**
  - Governance-Mapping
  - Umsetzung in verinice
-



- Banken
  - Börsen
  - Versicherungen
  - Finanzdienstleister
-

- Banken
- Börsen
- Versicherungen
- Finanzdienstleister
- ...Gefährdungen insbesondere im Teilsektor Banken und Börsen wirken sich auf alle Akteure in Staat, Wirtschaft und Gesellschaft aus. Insbesondere Störungen im Zahlungsverkehr können erhebliche Rückwirkungen bis hin zu Beeinträchtigungen der Versorgungsleistung mit sich bringen.





## Anforderungen an die Banken

---

- ISO 27001: Implementierung und Betrieb eines ISMS
  - MaRisk: Mindestanforderungen an das Risikomanagement
  - MaSI: Mindestanforderungen an die Sicherheit von Internetzahlungen
  - BAIT: Bankenaufsichtliche Anforderungen an die IT
  - SWIFT CSP: SWIFT Customer Security Controls Framework
  - ...
-

## Agenda

---

- SerNet GmbH
  - KRITIS-Sektor: Finanz- und Versicherungswesen
  - **Governance-Mapping**
  - Umsetzung in verinice
-

- Schwierigkeit: Gleiche Inhalte bei mehreren Standards
-

- Schwierigkeit: Gleiche Inhalte bei mehreren Standards
  - Lösung: Modul-Katalog
-

- Schwierigkeit: Gleiche Inhalte bei mehreren Standards
  - Lösung: Modul-Katalog
  - Inhalt:
    - Standards als eigene „Verbünde“ mit den entsprechenden Maßnahmen
    - Zuordnung der gleichen Maßnahmen in unterschiedlichen Standards
-

- Schwierigkeit: Gleiche Inhalte bei mehreren Standards
- Lösung: Modul-Katalog
- Inhalt:
  - Standards als eigene „Verbünde“ mit den entsprechenden Maßnahmen
  - Zuordnung der gleichen Maßnahmen in unterschiedlichen Standards

---

- Vererbung des Umsetzungsstatus
- Bericht

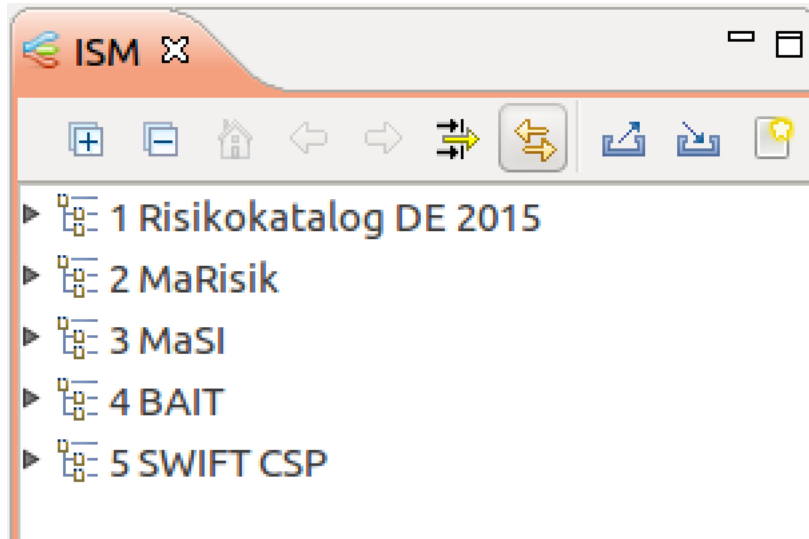
## Agenda

---

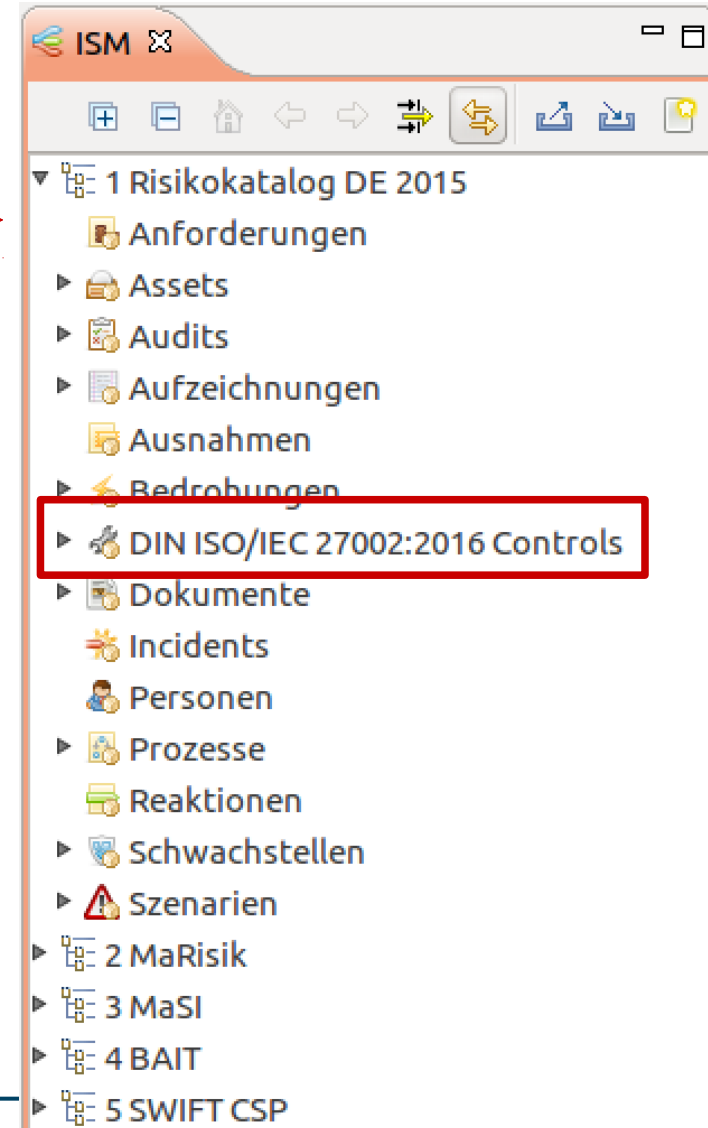
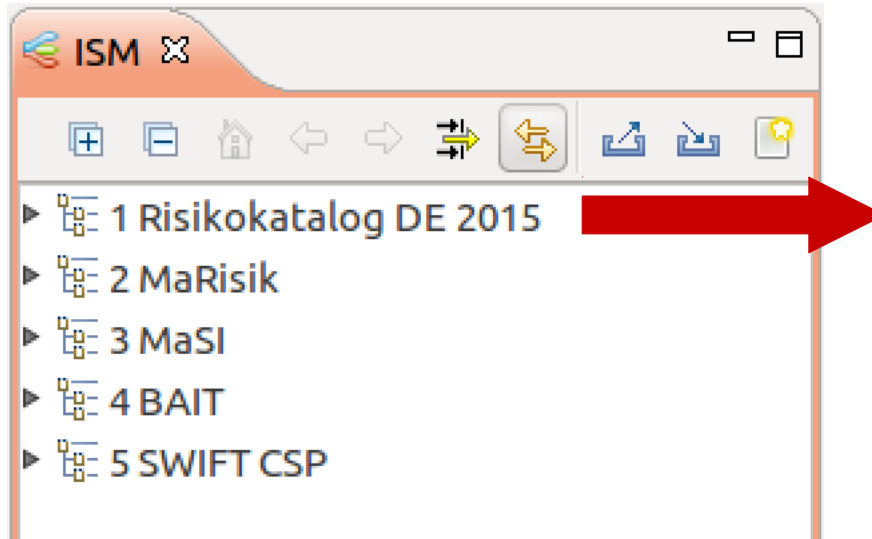
- SerNet GmbH
  - KRITIS-Sektor: Finanz- und Versicherungswesen
  - Governance-Mapping
  - **Umsetzung in verinice**
-

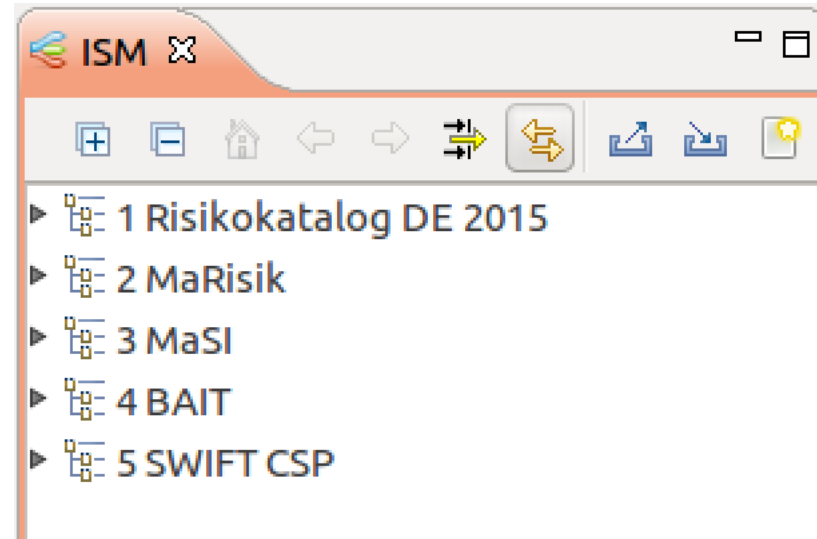


## Umsetzung in verinice

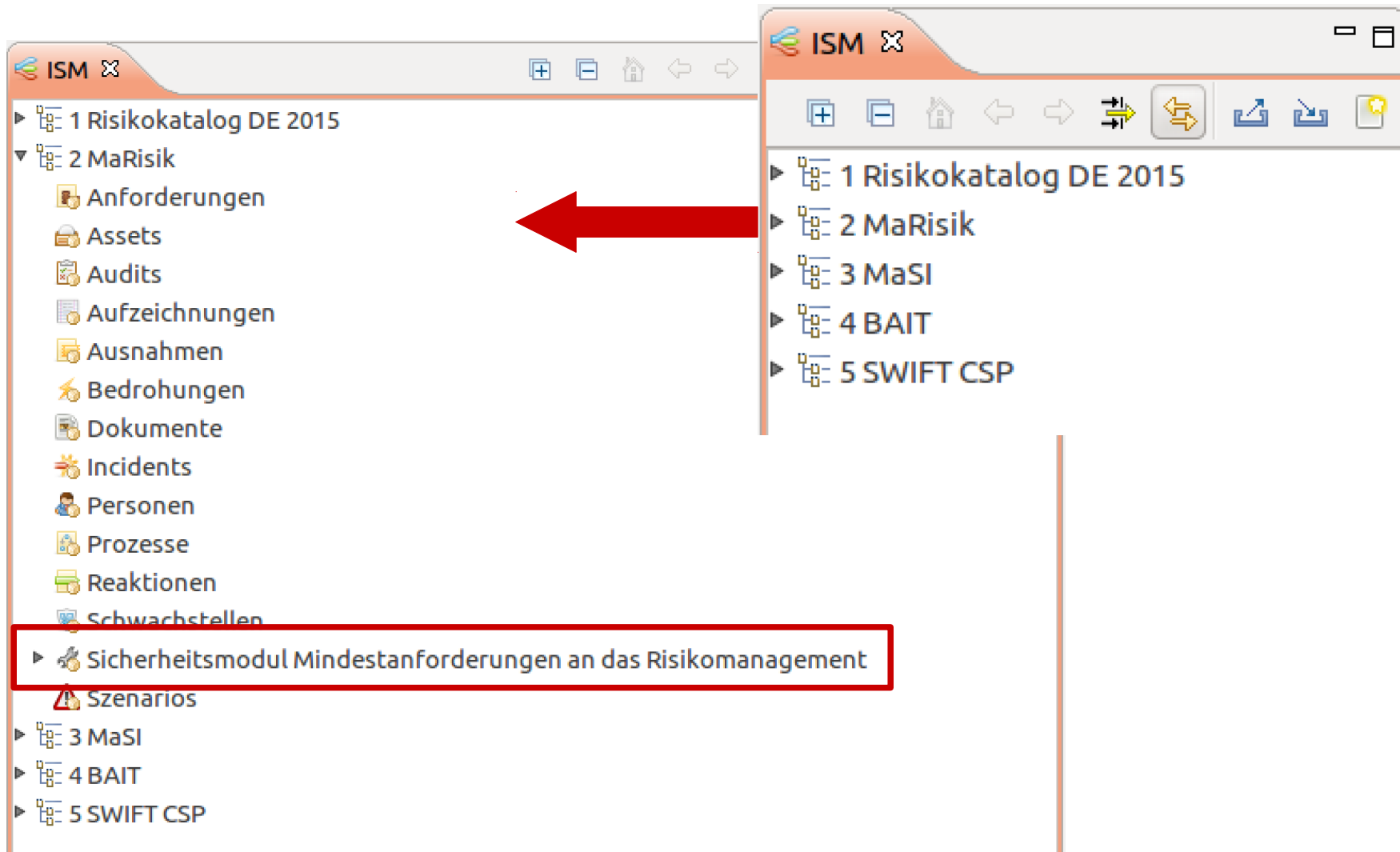


# Umsetzung in verinice

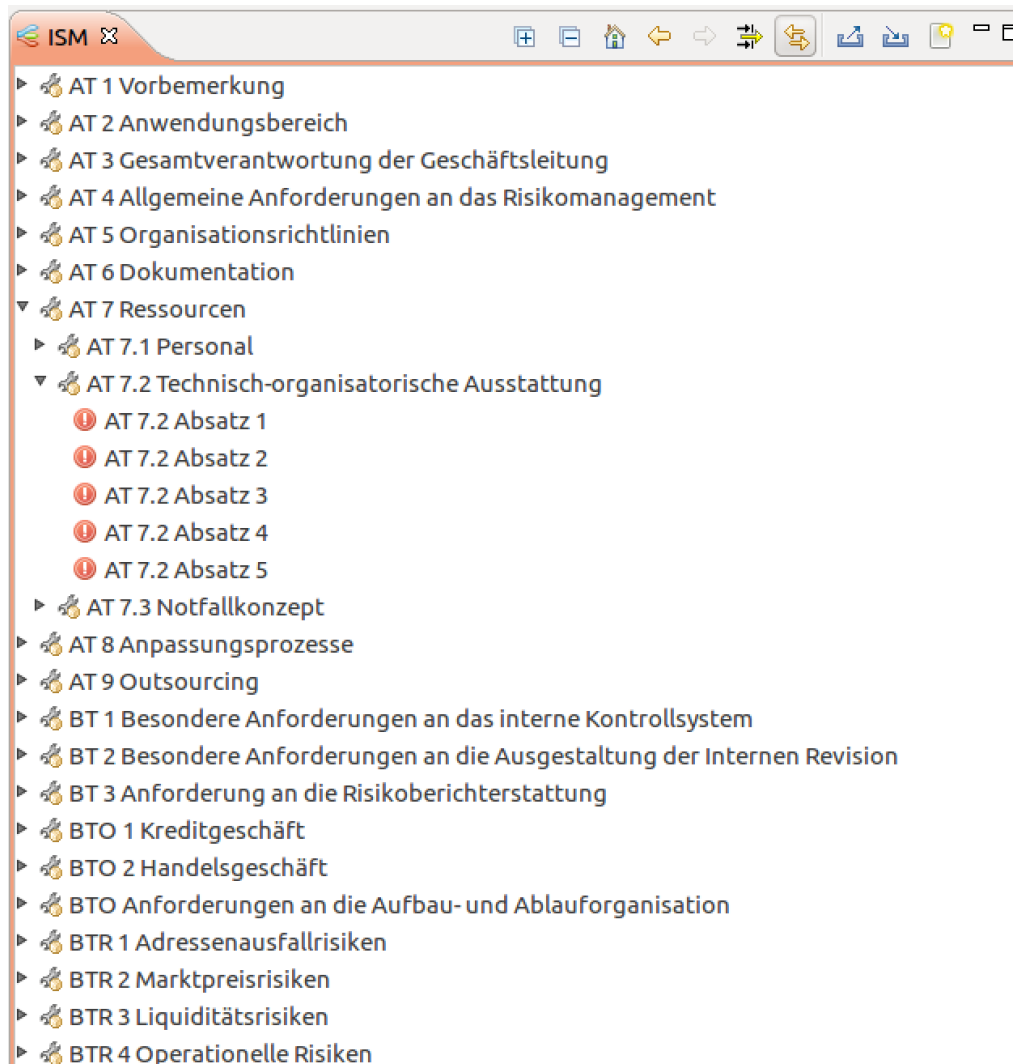




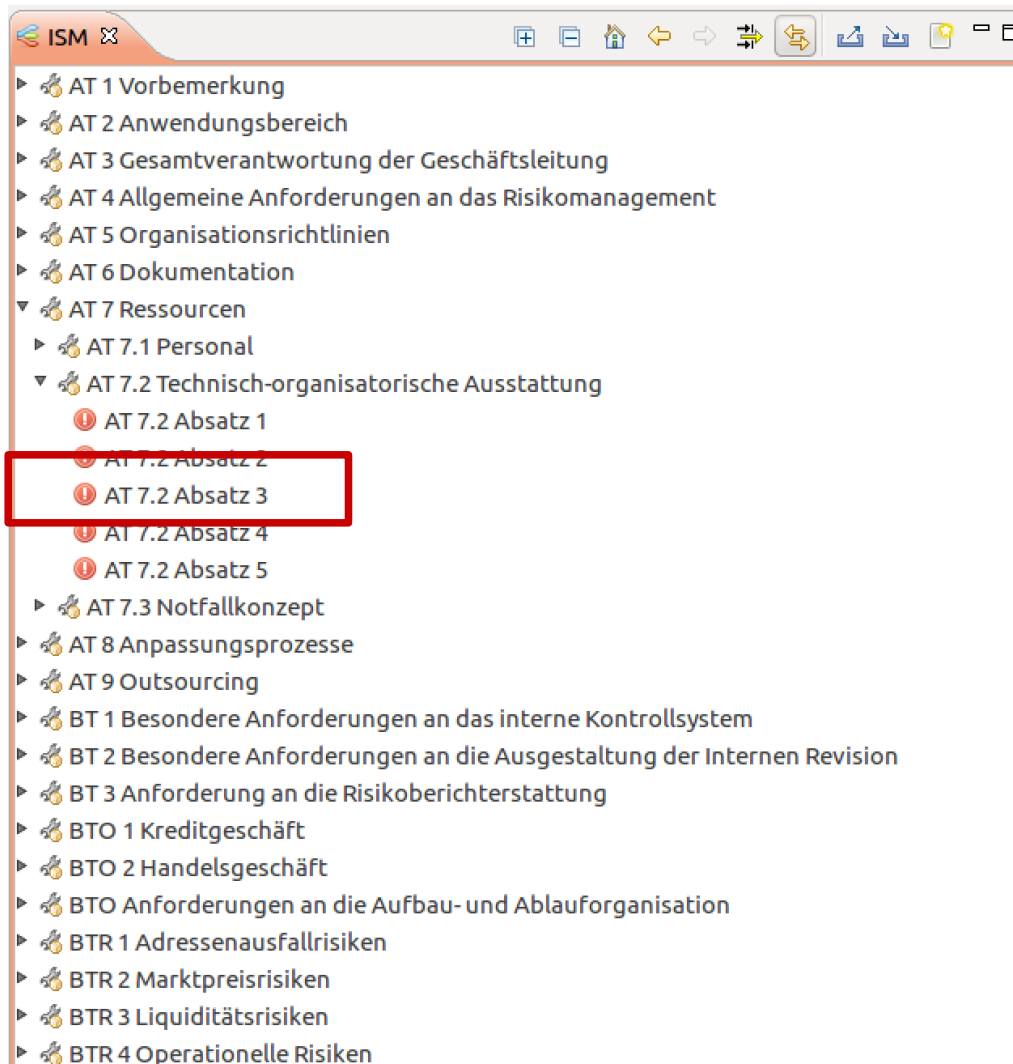
# Umsetzung in verinice



# Umsetzung in verinice



# Umsetzung in verinice



<> Objektbrowser ☒



## AT 7.2 Absatz 3

Die IT-Systeme sind vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Hierfür ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse zu etablieren. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen.

**Veränderungen an IT-Systemen** Bei der Beurteilung der Wesentlichkeit von Veränderungen ist nicht auf den Umfang der Veränderungen, sondern auf die Auswirkungen, die eine Veränderung auf die Funktionsfähigkeit des betroffenen IT-Systems haben kann, abzustellen.

**Abnahme durch die technisch und fachlich zuständigen Mitarbeiter** Bei der Abnahme durch die fachlich und die technisch zuständigen Mitarbeiter steht die Eignung und Angemessenheit der IT-Systeme für die spezifische Situation des jeweiligen Kreditinstituts im Mittelpunkt. Gegebenenfalls vorliegende Testate Dritter können bei der Abnahme berücksichtigt werden, sie können die Abnahme jedoch nicht vollständig ersetzen.

# Umsetzung in verinice

AT 7.2 Absatz 3

Titel: AT 7.2 Absatz 3

Abkürzung:

Tags:

Beschreibung:

Dokument:

Implementation

Implementiert: unbearbeitet

Erklärung:

Verknüpfungen: Control spezifiziert

Verknüpfung	Titel	Scope
spezifiziert	12.6.1 Handhabung von technischen Schwachstellen	1 Risikokatalog DE 2015
spezifiziert	14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen	1 Risikokatalog DE 2015
spezifiziert	14.2.9 Systemabnahmetest	1 Risikokatalog DE 2015
spezifiziert	8.2.1 Klassifizierung von Information	1 Risikokatalog DE 2015
spezifiziert	8.2.3 Handhabung von Werten	1 Risikokatalog DE 2015
spezifiziert	9.1.1 Zugangssteuerungsrichtlinie	1 Risikokatalog DE 2015



**Tatjana Anisow, [ta@sernet.de](mailto:ta@sernet.de)**

**SerNet GmbH**

**Bahnhofsallee 1b**

**37081 Göttingen**

**Torstraße 6**

**10119 Berlin**

**tel +49 551 370000-0**

**+49 30 5 779 779 0**

**fax +49 551 370000-9**

**+49 30 5 779 779 9**

**<http://www.sernet.de>**