Umsetzung des ISMS bei DENIC

Boban Krsic, DENIC eG

Berlin, den 16.09.2015

Agenda

- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- Business Continuity Management
- Ausblick

Agenda

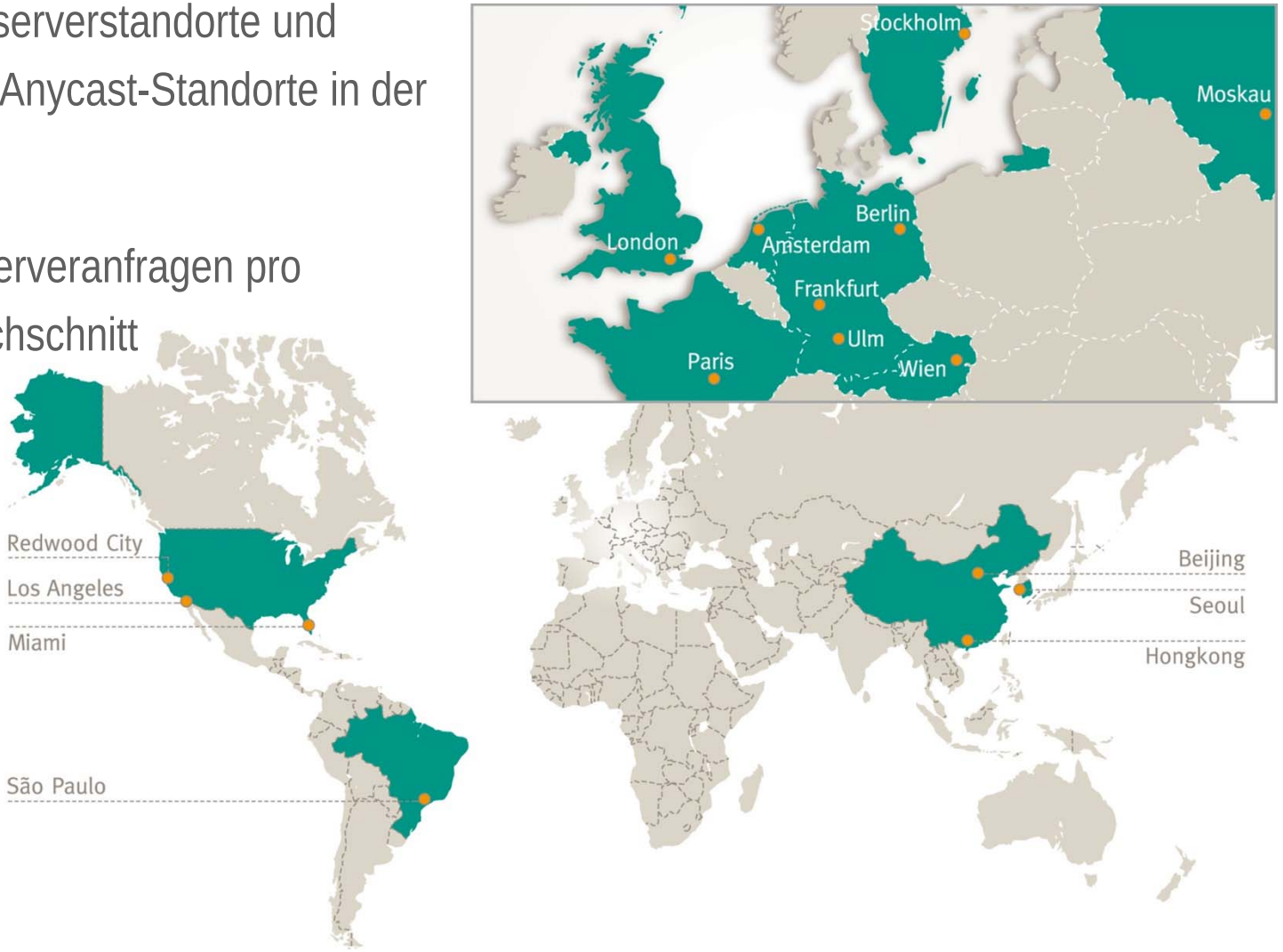
- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- Business Continuity Management
- Ausblick

Kurzvorstellung - DENIC eG

- Eingetragene Genossenschaft mit Sitz in Frankfurt am Main, gegründet 1996.
- Zentrale Registrierungsstelle für alle Domains unterhalb der länderbezogenen Top Level Domain .de sowie für ENUM-Domains (E.164 NUmber Mapping) unter .9.4.e164.arpa, dem deutschen Rufnummernraum.
- Selbstverständnis als neutraler, diskriminierungsfreier, Not-for-Profit-Dienstleister für die Internet Community, der seiner Verantwortung gemeinsam mit den mehr als 320 Mitgliedern (Registrare, ISP) der Genossenschaft nachkommt.
- Aufgaben und Tätigkeitsbereiche:
  - Betrieb des Nameservices für .de und für .9.4.e164.arpa.
  - Betrieb eines automatischen Registrierungssystems und der Domaindatenbank sowie Bereitstellung von Auskunftsdiensten und einer Service Hotline.
  - Aktive Mitgestaltung der Weiterentwicklung des Internets und von Internet-Standards (RFC) in internationalen Gremien (ICANN, RIPE, IETF, CENTR).

Kurzvorstellung - DENIC eG - Nameservice für .de

- 18 eigene Nameserverstandorte und 35+ ergänzende Anycast-Standorte in der ganzen Welt
- > 40.000 Nameserveranfragen pro Sekunde im Durchschnitt



Agenda

- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- Business Continuity Management
- Ausblick

ISMS bei DENIC – Ausgestaltung

- Ganzheitliche Ausrichtung des Managementsystems in einem integrierten Ansatz (ISO/IEC 27001:2013 ISMS , ISO/IEC 27005:2011 RM und ISO 22301:2012 BCMS)
- Scope des ISMS: Gesamtes Unternehmen inkl. aller erbrachten Dienste
- Aufbau des ISMS unter Berücksichtigung der strategischen Unternehmensziele*
  - Operational Excellence - Stärkung des operativen Kerngeschäftes durch Verbesserung der Effizienz sowie Erhöhung der Qualität und Skalierbarkeit der Dienste
  - Gestaltung von und Weiterentwicklung der DENIC-Aufgaben in neue Bereiche, die die Bereitstellung neutraler Internet-Infrastrukturdienste benötigen
  - Stärkung des Modells der industriellen Selbstverwaltung
- Steuerung des ISMS unter Verwendung von Key Performance Indikatoren (KPIs), die unter Zuhilfenahme von COBIT 5 for Information Security abgeleitet wurden
- Toolgestützte Umsetzung normativer Anforderungen

TÜV NORD
TÜV NORD CERT GmbH
ISO/IEC 27001

* vgl. hierzu Strategiepapier der DENIC eG, S.1 ff. vom März 2008

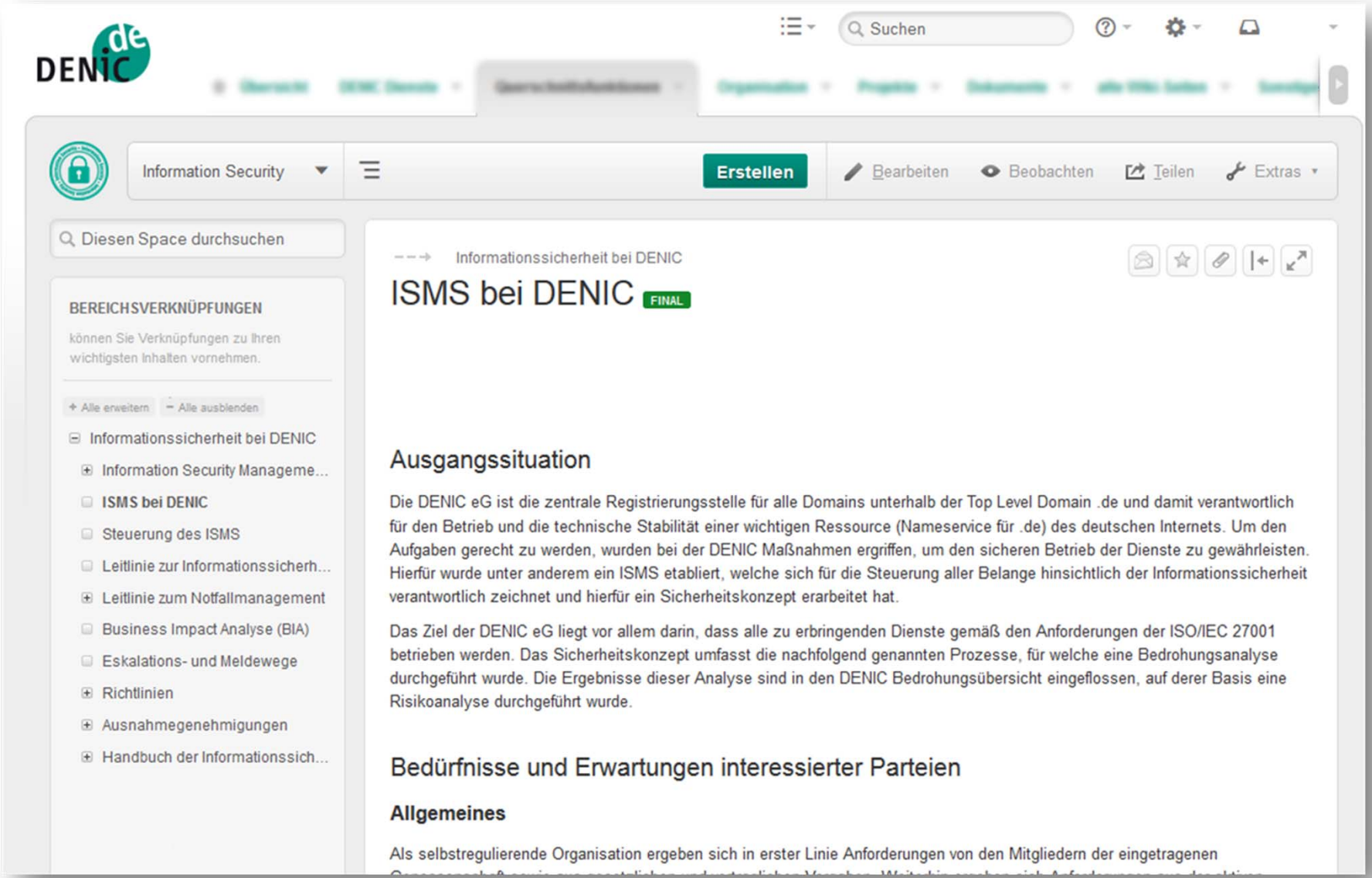
ISMS bei DENIC – Toolgestützte Umsetzung

- Begonnen hat alles mit….

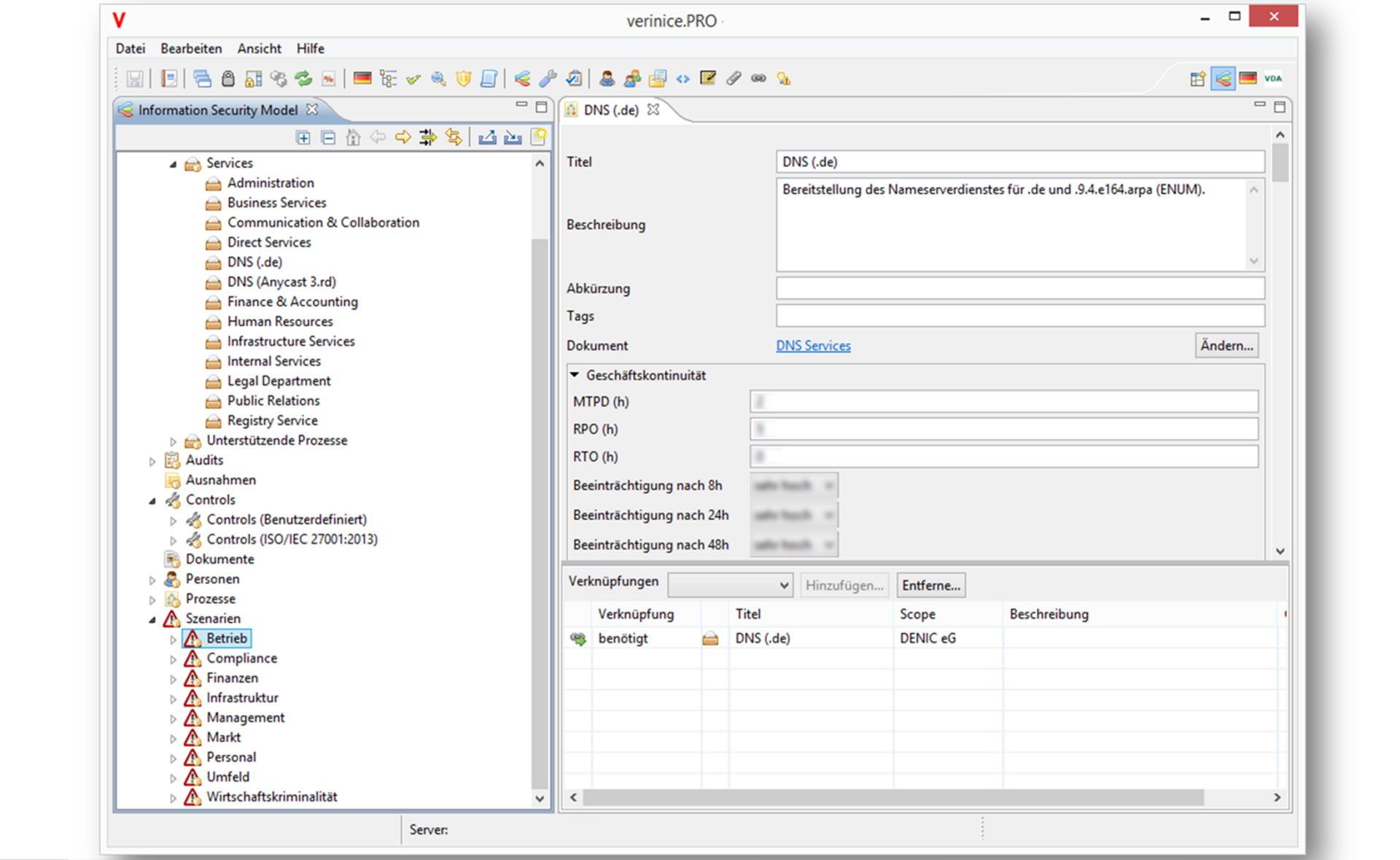
  Excel ;-)

- Folgende Tools aktuell im Einsatz:
  - Confluence (ISMS Dokumentation)
  - Greenbone (Schwachstellenmanagement)
  - JIRA (Tracking von Maßnahmen und Aufgaben)
  - OTRS (Mailing, Ticketing)
  - verinice.PRO (ISMS Modellierung, Risikoanalyse, Datenschutz, Reporting)

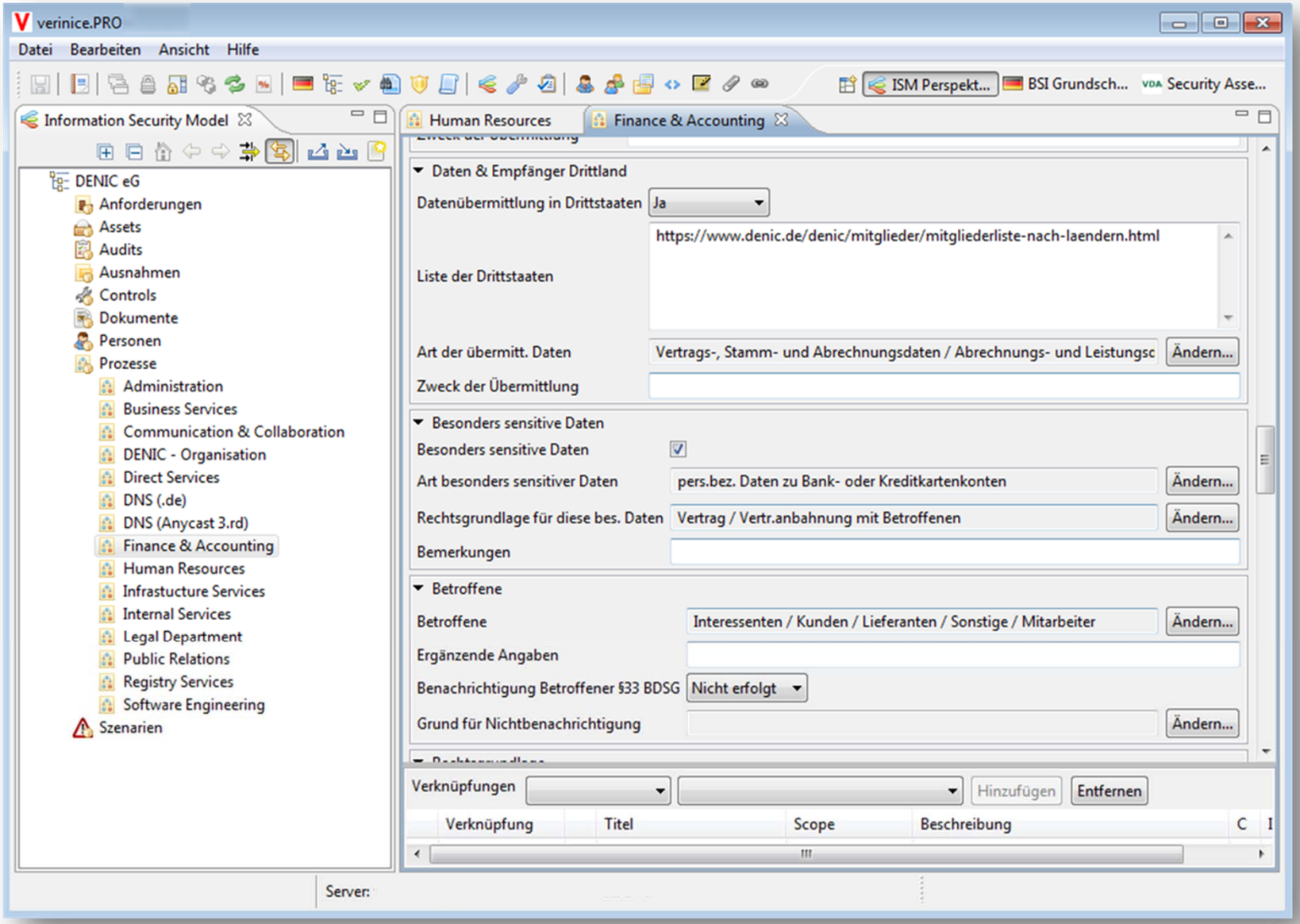
ISMS bei DENIC – Darstellung und Inhalte



ISMS bei DENIC – Scoping im verinice



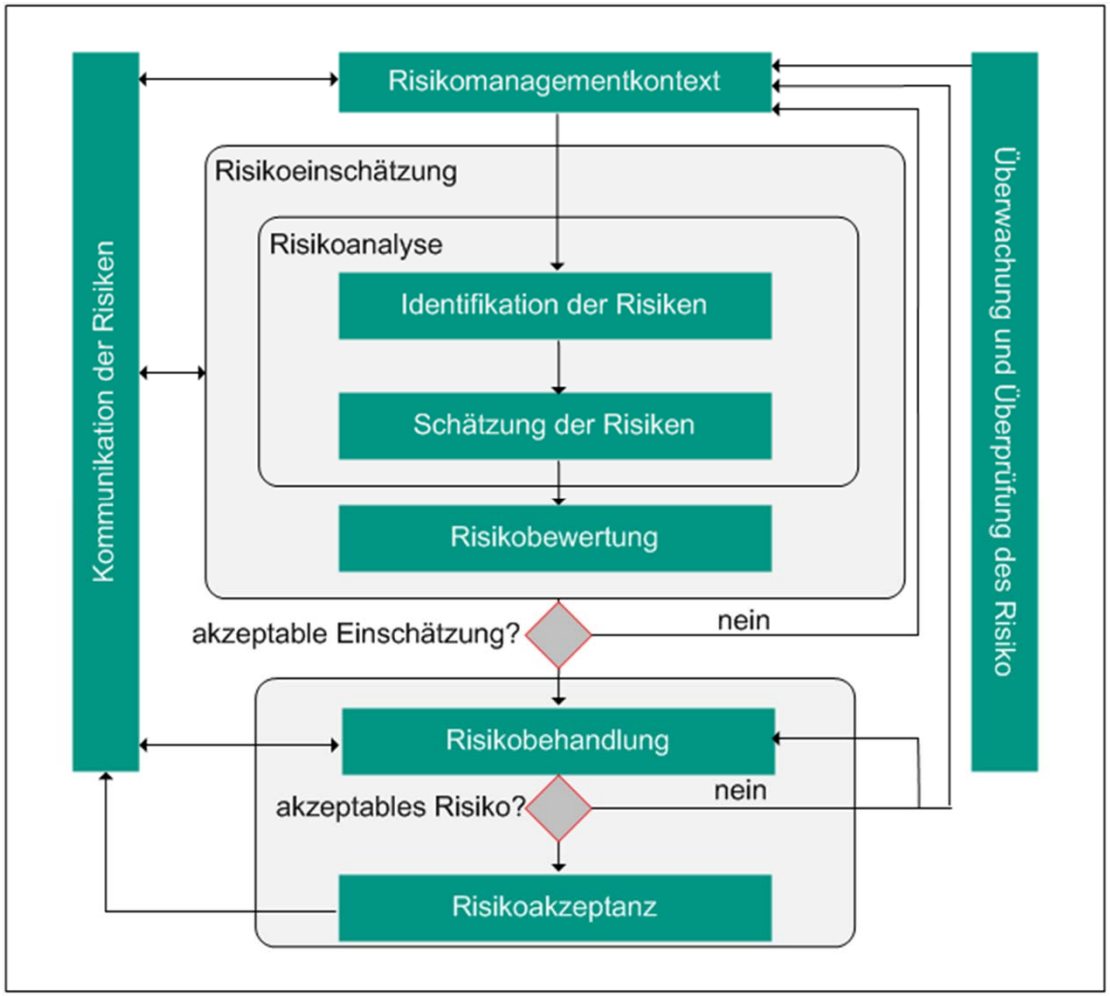
ISMS bei DENIC – Datenschutzrelevante Anforderungen



Agenda

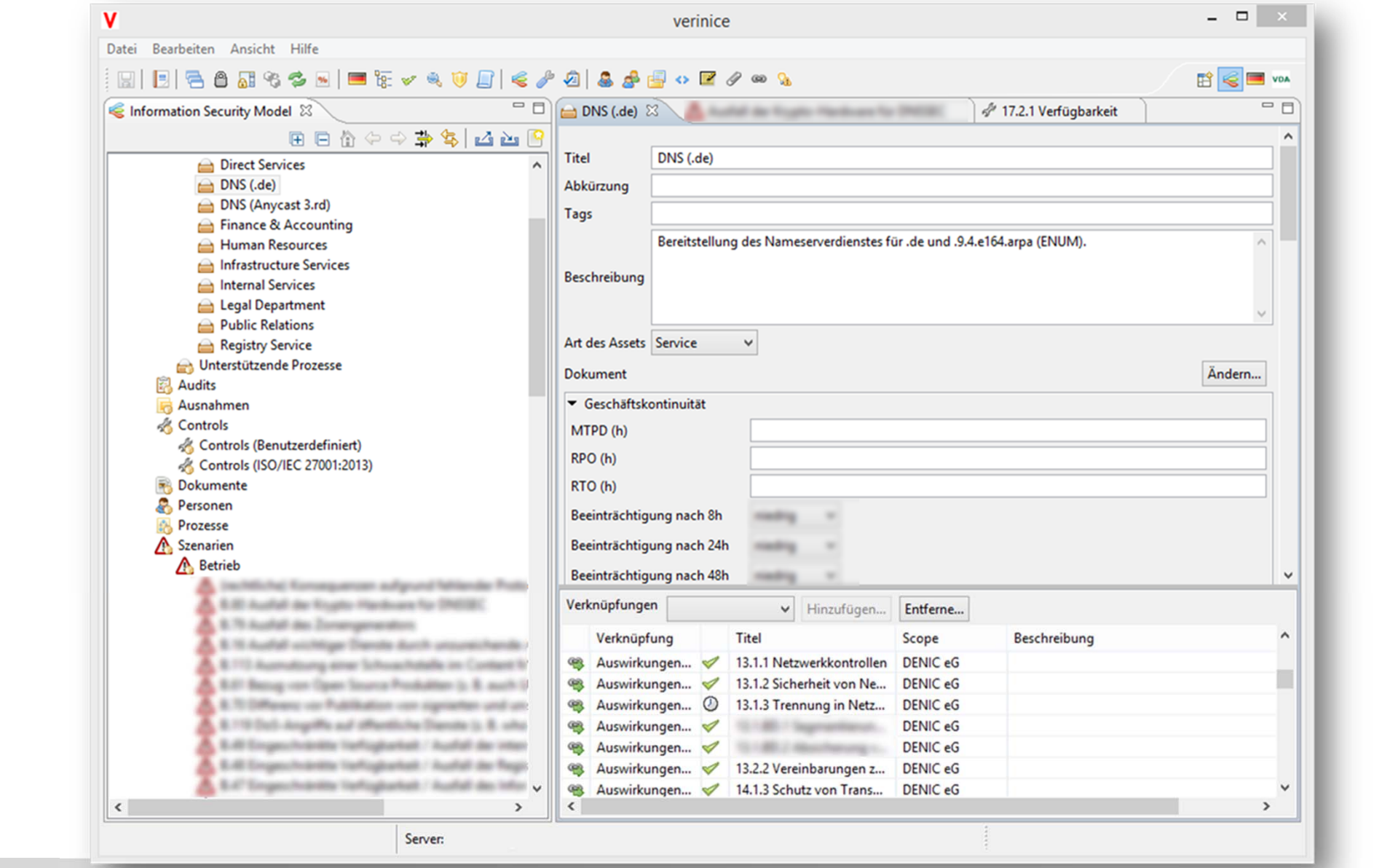
- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- Business Continuity Management
- Ausblick

Risikomanagement im Bereich Information Security bei DENIC

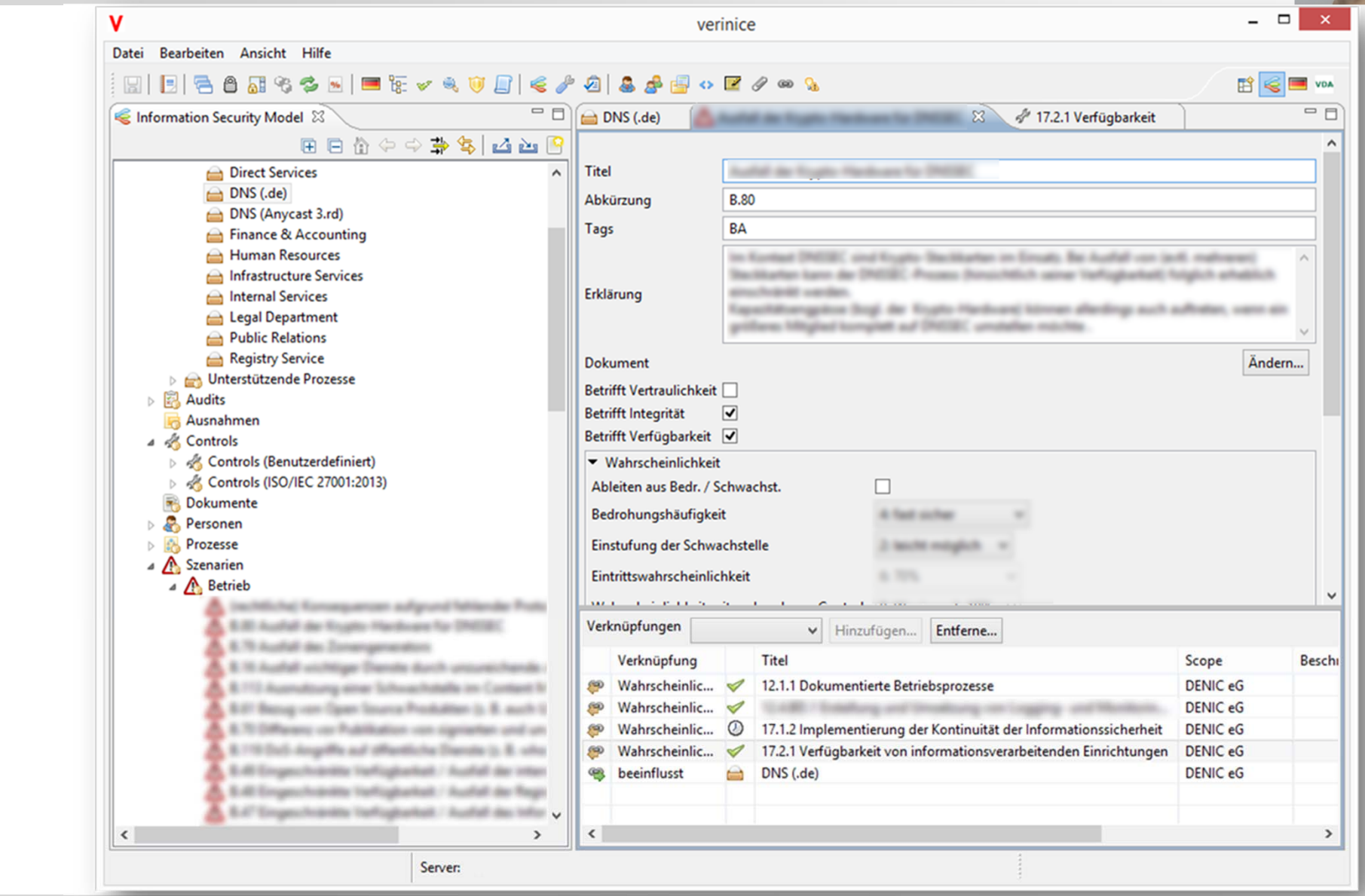


- Orientierung an ISO/IEC 27005
- Prozessuale Einbindung in das übergreifende Risikomanagement bei DENIC
- Kontext deckungsgleich mit ISMS
- Beteiligte Akteure / Rollen:
  - Risikomanager
  - Risikomanagementkreis
  - Risikoverantwortliche
- Ermittlung der Risiken durch:
  - Workshops mit Produktteams
  - Bedrohungsmodellierung
  - Bedrohungskataloge

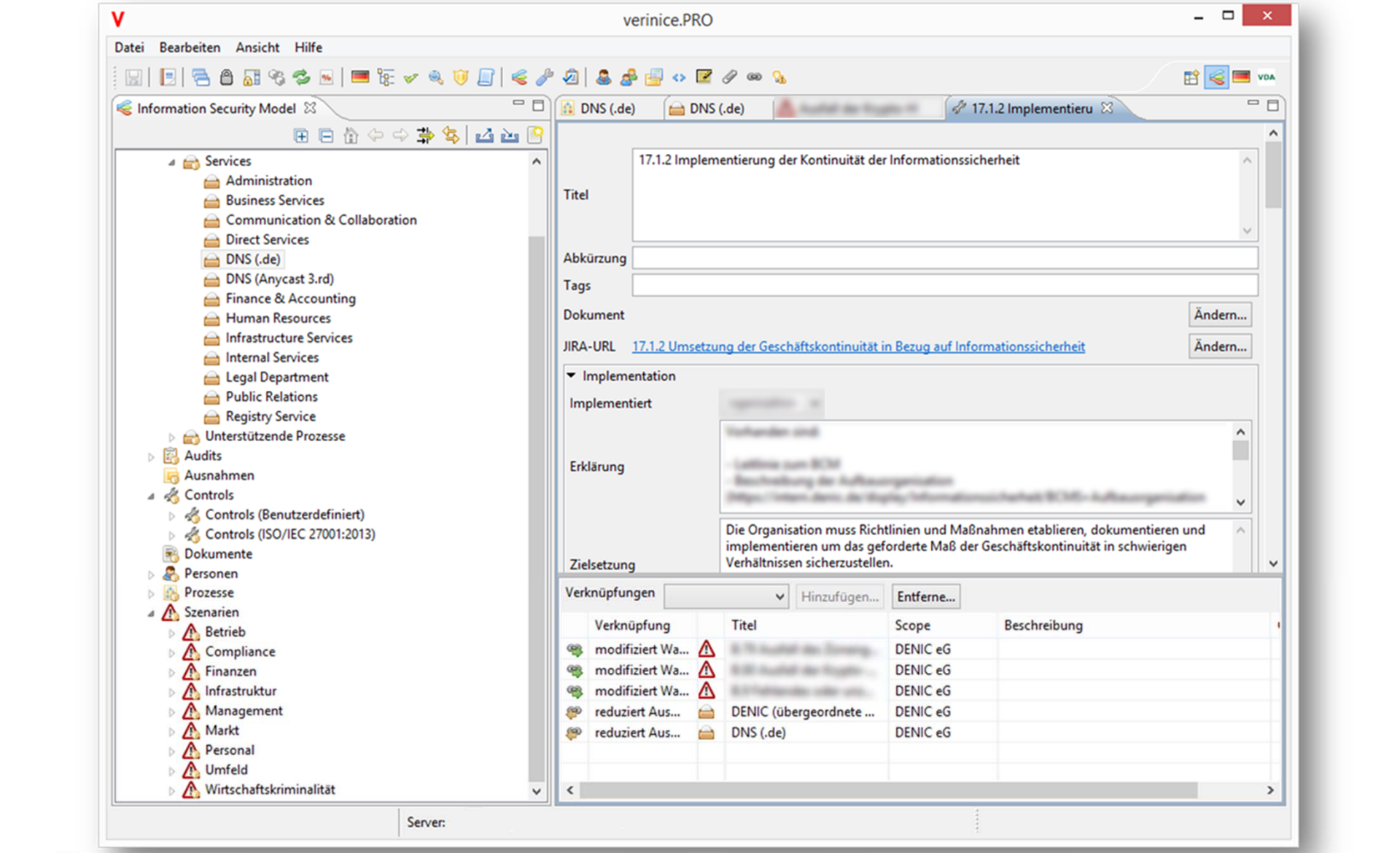
Risikomanagement im Rahmen des ISMS – Bedrohungsszenarien



Risikomanagement im Rahmen des ISMS – Bedrohungsszenarien



Risikomanagement im Rahmen des ISMS – Maßnahmen



Risikomanagement im Rahmen des ISMS – Maßnahmen

JIRA Startseite Projekte Vorgänge Tempo Agile Erstellen Suche

Information Security / SEC-69

17.1.2 Umsetzung der Geschäftskontinuität in Bezug auf Informationssicherheit

Bearbeiten | Kommentar | Zuweisen | Weitere Aktionen | Open | In Progress | Arbeitsablauf | Email | Exportieren

Details

Typ:	Aufgabe	Status:	
Priorität:	↑	Lösung:	
betrifft Version(en):	Keine	Lösungsversion(en):	
Stichwörter:	Keine		
Umgebung:	DENIC Sicherheitskonzept		
Epic Link:	ISMS		
Sprint:	2015-8		
Rank:	0|hzzzii:r		
Rank (Veraltet):	6038		

Beschreibung

BCM Leitlinie ist veröffentlicht.

Verknüpfungen +

hängt zusammen mit

Personen

Bearbeiter: Mir zuweisen

Autor:

Beobachter verwalten: 2 Beobachten beenden

Daten

Erstellt:	08.07.2014
Aktualisiert:	Jetzt

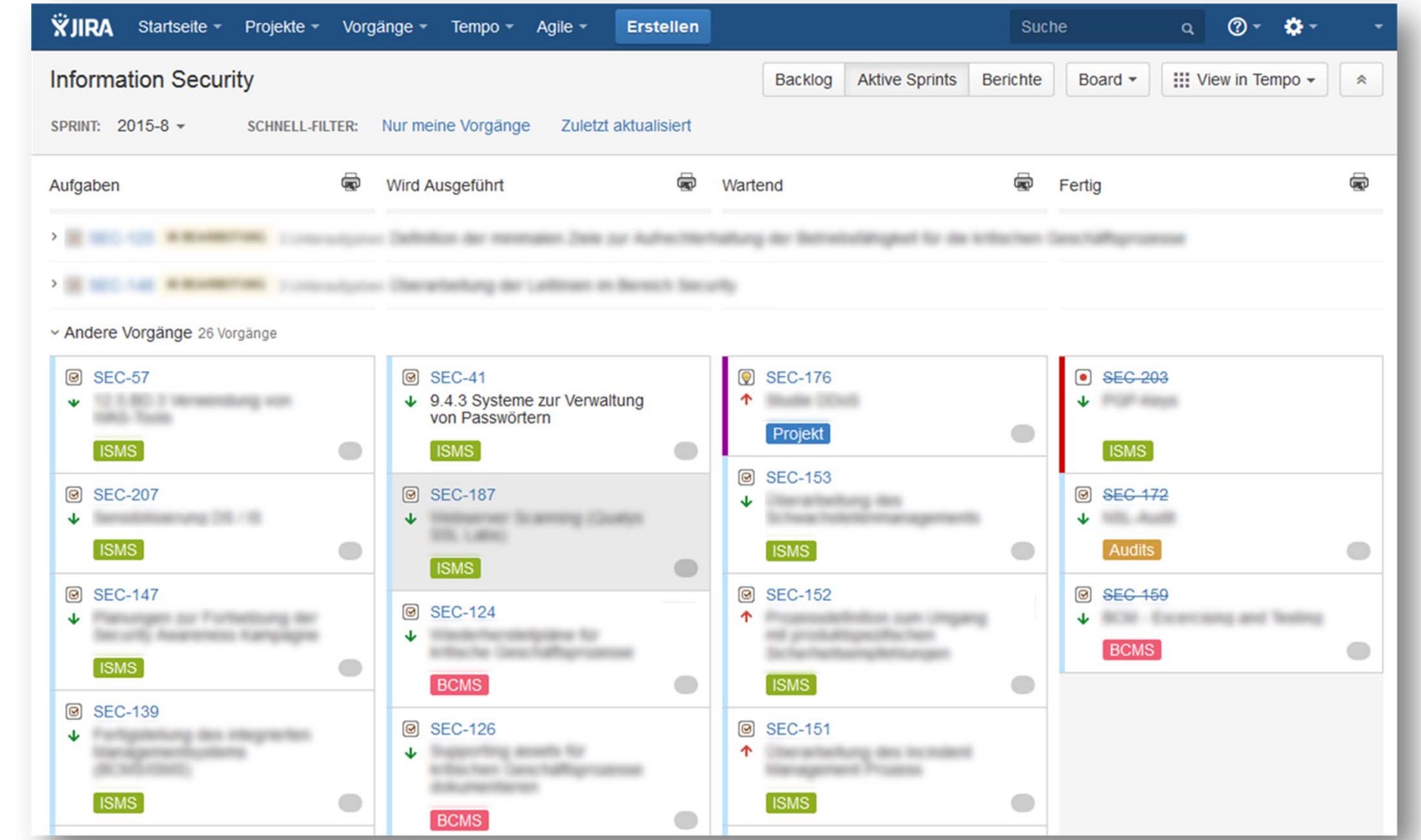
Drag and Drop

Dateien hier hinziehen zum anhängen
oder
Wählen Sie die Dateien

Agil

Aktiv Sprint: 2015-8

Risikomanagement im Rahmen des ISMS – Maßnahmen



Risikomanagement im Rahmen des ISMS – Reporting

Bericht zur Informationssicherheitsrisikoeinschätzung

DNS (.de)

vertraulich

Abteilung:	Information Security		IS
Dok.-Version:	1.0	**Dok.-Status:**	Finale Version
Dok.-Stand:	01.09.2014	**Dok.-Name:**	Bericht.IS.RA-DNS (.de)-V1.0

Inhalt

Risikomanagement im Rahmen des ISMS – Reporting

Scenario		Likelihood				
[redacted]		6	0	0	9	
Controls affecting scenario	**Effectiveness**	**Implemented**				
[redacted]	2	Ja				
[redacted]	2	Ja				
[redacted]	2	Ja				
[redacted]	3	Ja				
Residual Risk			**0**	**0**	**3**	**3**
Scenario		**Likelihood**				
[redacted]		5	7	7	8	
Controls affecting scenario	**Effectiveness**	**Implemented**				
[redacted]	2	Ja				
[redacted]	2	Ja				

Kategorie	Tolerierbarer Risikowert
Vertraulichkeit	6
Integrität	7
Verfügbarkeit	6

Tabelle 12: Risikoakzeptanzvorgabe

Anhang A - Klassifizierungsstufen

A.1 Klassifizierungsstufen - Grundwerte des Assets - Vertraulichkeit

#	Stufe	Beschreibung
0	offen	Informationen, bei deren Verlust oder Kenntnisnahme durch Dritte mit keinem Schaden für DENIC zu rechnen ist oder gegen keine vorgegebene Auflagen verstoßen (z.B. Datenschutz) wird.
1	intern	Informationen, die für einen breiten Verteilerkreis bei DENIC und den Mitgliedern der Genossenschaft bestimmt sind.
2	vertraulich	Informationen, die für einen beschränkten Verteilerkreis bei DENIC bestimmt sind.
3	geheim	Informationen, die bei vorzeitiger Veröffentlichung einen Schaden für DENIC bedeuten oder gegen vorgegebene Auflagen verstoßen.

Tabelle 7: Grundwerte des Assets – Vertraulichkeit

A.2 Klassifizierungsstufen - Grundwerte des Assets - Integrität

#	Stufe	Beschreibung
0	gering	kein erhöhter Integritätsschutz: Hierbei handelt es sich um allgemeine Informationen, deren Verfälschung keine nennenswerten Schäden hervorrufen können. Für diese Art von Informationen sind keine spezifischen Anforderungen zu erfüllen.
1	mittel	kein erhöhter Integritätsschutz: Hierbei handelt es sich um allgemeine Informationen, deren Verfälschung nennenswerten Schäden hervorrufen können. Für diese Art von Informationen sind keine spezifischen Anforderungen zu erfüllen.
2	hoch	erhöhter Integritätsschutz: Hierbei handelt es sich um Informationen, deren Verfälschung größere Schäden für DENIC hervorrufen können.
3	sehr hoch	erhöhter Integritätsschutz: Hierbei handelt es sich um Informationen, deren Verfälschung massive Schäden für DENIC hervorrufen können.

Tabelle 8: Grundwerte des Assets – Integrität

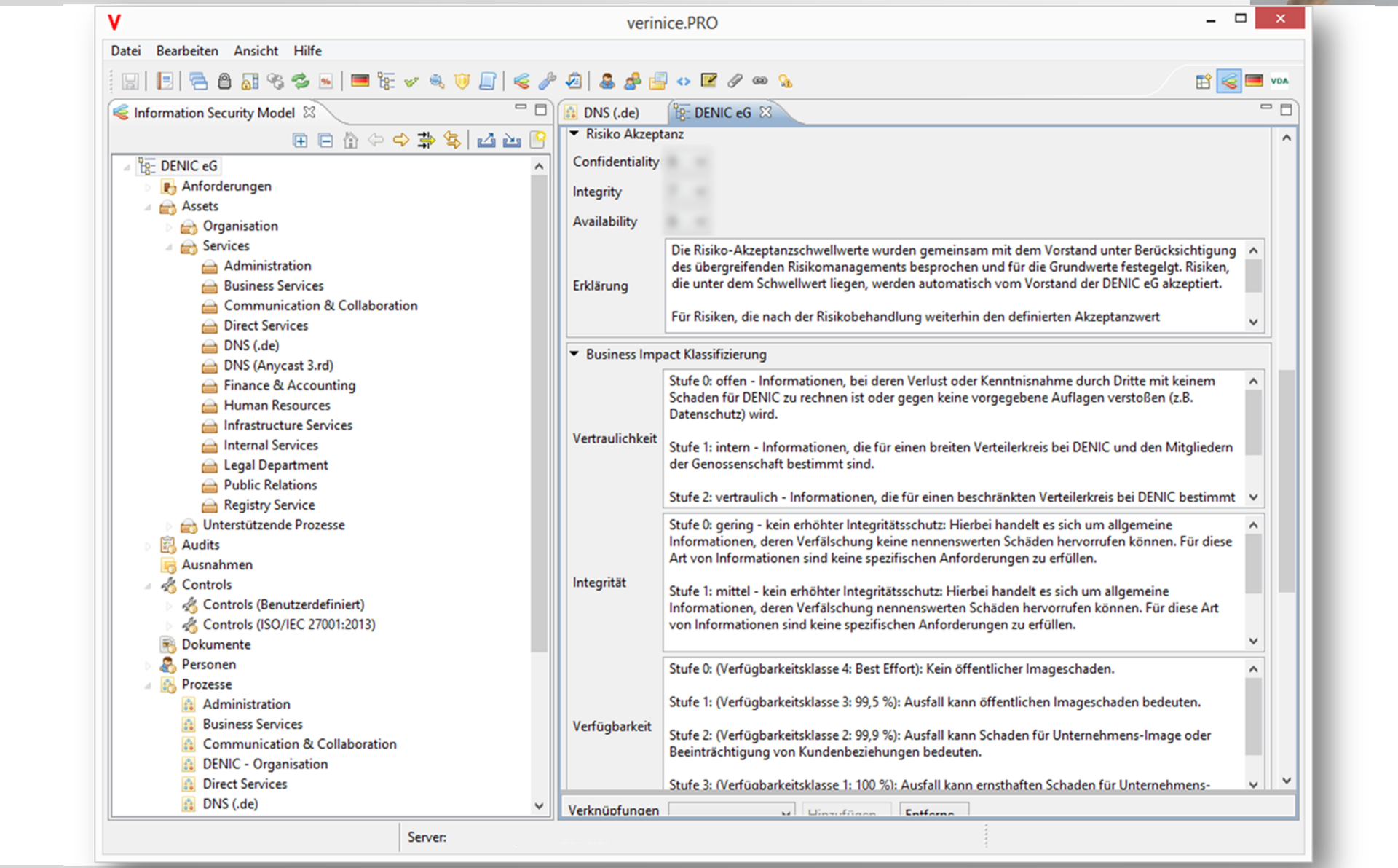
Agenda

- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- **Business Continuity Management**
- Ausblick

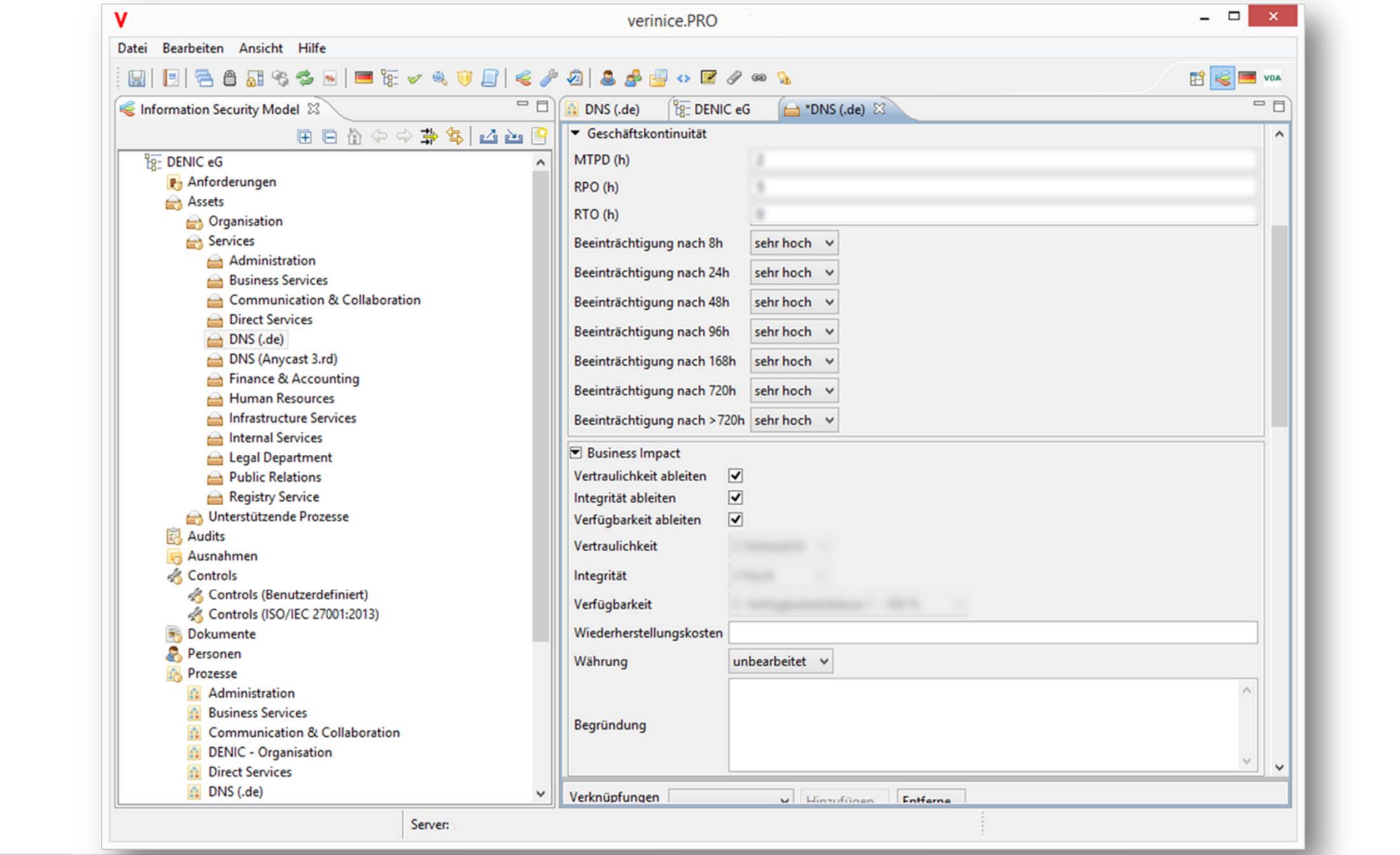
Business Continuity Management

- Umsetzung als integrierter Ansatz ISO 22301 und ISO/IEC 27001
  - BCM Verantwortung beim CISO
  - Aufbauorganisation analog zum ISMS bis auf Public Relations und Product Owner
  - Scope der Risikoanalyse deckungsgleich mit dem Scope des ISMS
  - Nutzung von Synergien im Kontext der Bedrohungsanalyse
  - Gemeinsame Betrachtung mit dem ISMS von verfügbarkeitsrelevanten Maßnahmen
- Business Impact Analyse (BIA) zur Bestimmung der Kritikaliät der Geschäftsprozesse
- Wiederanlauf- und Kontinuitätspläne für kritische Geschäftsprozesse
- Durchführung von regelmäßigen Notfallübungen

Business Continuity Management - Übersicht



Business Continuity Management - Übersicht



Agenda

- Kurzvorstellung
- ISMS bei DENIC
- Risikomanagement im Rahmen des ISMS
- Business Continuity Management
- Ausblick

Ausblick

- Abbildung der datenschutzrelevanten Aspekte
- Abbildung der KPI (Prozessziele und Metriken)
- Gewichtung von Umsetzungsstatus (Ja, Nein, Teilweise)
- Verknüpfung Schwachstellenmanagement (Greenbone, verinice)

Fragen?

Vielen Dank!

Boban Krsic, DENIC eG
Chief Information Security Officer

e-mail: <krsic@denic.de>
phone: +49 69 272 35 – 120

PGP Key-ID: 0x43C89BA9