



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



- 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



- 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



* 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



The screenshot displays the DENIC website interface. At the top left is the DENIC logo. A search bar with the text 'Suchen' is located at the top right. Below the logo, there is a navigation menu with items like 'Startseite', 'ISMS bei DENIC', 'Geschäftsstrukturen', 'Organisation', 'Prozesse', 'Dokumente', 'alle Web-Sites', and 'Sonstige'. The main content area is titled 'Information Security' and features a green 'Erstellen' button and icons for 'Bearbeiten', 'Beobachten', 'Teilen', and 'Extras'. A search bar on the left side of the main area contains the text 'Diesen Space durchsuchen'. The left sidebar is titled 'BEREICHsverknüpfungen' and lists various links under the heading 'Informationssicherheit bei DENIC', including 'Information Security Manageme...', 'ISMS bei DENIC', 'Steuerung des ISMS', 'Leitlinie zur Informationssicherh...', 'Leitlinie zum Notfallmanagement', 'Business Impact Analyse (BIA)', 'Eskalations- und Meldewege', 'Richtlinien', 'Ausnahmegenehmigungen', and 'Handbuch der Informationssich...'. The main content area shows the title 'ISMS bei DENIC' with a 'FINAL' badge. Below the title is the section 'Ausgangssituation' with a paragraph of text. The next section is 'Bedürfnisse und Erwartungen interessierter Parteien' followed by 'Allgemeines' and a paragraph of text.

Information Security

Erstellen

Bearbeiten

Beobachten

Teilen

Extras

Diesen Space durchsuchen

Informationssicherheit bei DENIC

ISMS bei DENIC FINAL

Ausgangssituation

Die DENIC eG ist die zentrale Registrierungsstelle für alle Domains unterhalb der Top Level Domain .de und damit verantwortlich für den Betrieb und die technische Stabilität einer wichtigen Ressource (Nameservice für .de) des deutschen Internets. Um den Aufgaben gerecht zu werden, wurden bei der DENIC Maßnahmen ergriffen, um den sicheren Betrieb der Dienste zu gewährleisten. Hierfür wurde unter anderem ein ISMS etabliert, welche sich für die Steuerung aller Belange hinsichtlich der Informationssicherheit verantwortlich zeichnet und hierfür ein Sicherheitskonzept erarbeitet hat.

Das Ziel der DENIC eG liegt vor allem darin, dass alle zu erbringenden Dienste gemäß den Anforderungen der ISO/IEC 27001 betrieben werden. Das Sicherheitskonzept umfasst die nachfolgend genannten Prozesse, für welche eine Bedrohungsanalyse durchgeführt wurde. Die Ergebnisse dieser Analyse sind in den DENIC Bedrohungsübersicht eingeflossen, auf derer Basis eine Risikoanalyse durchgeführt wurde.

Bedürfnisse und Erwartungen interessierter Parteien

Allgemeines

Als selbstregulierende Organisation ergeben sich in erster Linie Anforderungen von den Mitgliedern der eingetragenen

ISMS bei DENIC – Scoping im verinice



The screenshot displays the 'verinice.PRO' application window. On the left, a tree view shows the 'Information Security Model' structure, with 'DNS (.de)' selected under 'Services'. The main area shows the configuration for this service:

- Titel:** DNS (.de)
- Beschreibung:** Bereitstellung des Nameserverdienstes für .de und .9.4.e164.arpa (ENUM).
- Abkürzung:** (empty)
- Tags:** (empty)
- Dokument:** [DNS Services](#) (with an 'Ändern...' button)
- Geschäftskontinuität:** A section with input fields for MTPD (h), RPO (h), and RTO (h), and dropdown menus for 'Beeinträchtigung nach 8h', 'Beeinträchtigung nach 24h', and 'Beeinträchtigung nach 48h'.
- Verknüpfungen:** A table showing a link between 'benötigt' and 'DNS (.de)' with a scope of 'DENIC eG'.

Verknüpfung	Titel	Scope	Beschreibung
benötigt	DNS (.de)	DENIC eG	

ISMS bei DENIC – Datenschutzrelevante Anforderungen



The screenshot displays the 'verinice.PRO' application window. The left sidebar shows a tree view of 'Information Security Model' with categories like 'Anforderungen', 'Assets', 'Audits', etc., and a sub-tree for 'DENIC eG' with various service categories. The main area is titled 'Human Resources' and 'Finance & Accounting'. It contains several sections for configuring data transfer requirements:

- Daten & Empfänger Drittland:** 'Datenübermittlung in Drittstaaten' is set to 'Ja'. A URL is provided: <https://www.denic.de/denic/mitglieder/mitgliederliste-nach-laendern.html>. 'Liste der Drittstaaten' is empty. 'Art der übermitt. Daten' is 'Vertrags-, Stamm- und Abrechnungsdaten / Abrechnungs- und Leistungsc'. 'Zweck der Übermittlung' is empty.
- Besonders sensitive Daten:** 'Besonders sensitive Daten' is checked. 'Art besonders sensibler Daten' is 'pers.bez. Daten zu Bank- oder Kreditkartenkonten'. 'Rechtsgrundlage für diese bes. Daten' is 'Vertrag / Vertr.anbahnung mit Betroffenen'.
- Betroffene:** 'Betroffene' is 'Interessenten / Kunden / Lieferanten / Sonstige / Mitarbeiter'. 'Ergänzende Angaben' is empty. 'Benachrichtigung Betroffener §33 BDSG' is 'Nicht erfolgt'. 'Grund für Nichtbenachrichtigung' is empty.
- Rechtsgrundlagen:** A table for 'Verknüpfungen' with columns 'Verknüpfung', 'Titel', 'Scope', and 'Beschreibung'. It includes 'Hinzufügen' and 'Entfernen' buttons.

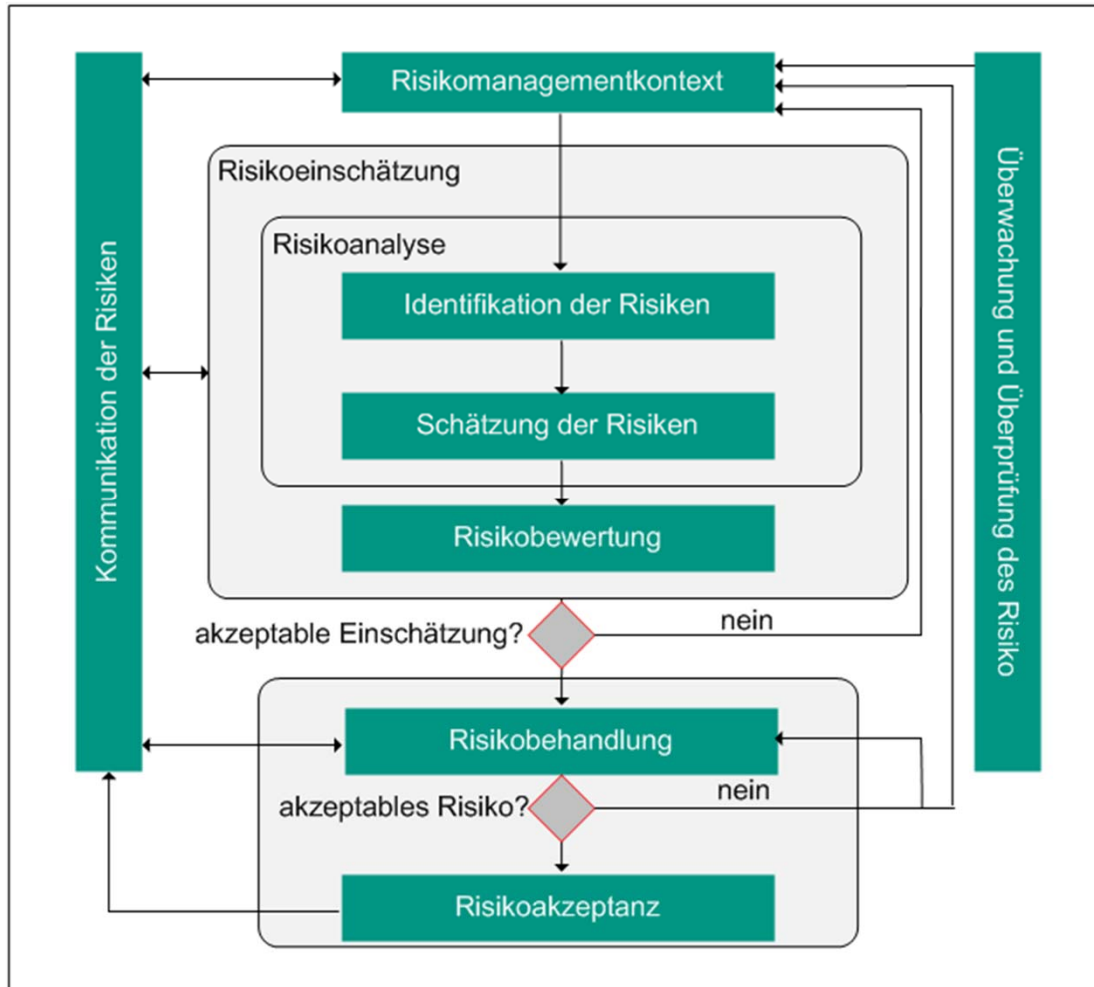
At the bottom, a 'Server:' label is visible.

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



verinice

Information Security Model

- Direct Services
 - DNS (.de)
 - DNS (Anycast 3.rd)
 - Finance & Accounting
 - Human Resources
 - Infrastructure Services
 - Internal Services
 - Legal Department
 - Public Relations
 - Registry Service
- Unterstützende Prozesse
- Audits
- Ausnahmen
- Controls
 - Controls (Benutzerdefiniert)
 - Controls (ISO/IEC 27001:2013)
- Dokumente
- Personen
- Prozesse
- Szenarien
- Betrieb

DNS (.de) 17.2.1 Verfügbarkeit

Titel: DNS (.de)

Abkürzung:

Tags:

Beschreibung: Bereitstellung des Nameserverdienstes für .de und .9.4.e164.arpa (ENUM).

Art des Assets: Service

Dokument: [Ändern...](#)

Geschäftskontinuität

MTPD (h):

RPO (h):

RTO (h):

Beeinträchtigung nach 8h:

Beeinträchtigung nach 24h:

Beeinträchtigung nach 48h:

Verknüpfungen

Verknüpfung	Titel	Scope	Beschreibung
Auswirkungen...	13.1.1 Netzwerkkontrollen	DENIC eG	
Auswirkungen...	13.1.2 Sicherheit von Ne...	DENIC eG	
Auswirkungen...	13.1.3 Trennung in Netz...	DENIC eG	
Auswirkungen...	13.1.4 ...	DENIC eG	
Auswirkungen...	13.1.5 ...	DENIC eG	
Auswirkungen...	13.2.2 Vereinbarungen z...	DENIC eG	
Auswirkungen...	14.1.3 Schutz von Trans...	DENIC eG	

Server:



Risikomanagement im Rahmen des ISMS – Bedrohungsszenarien

The screenshot shows the Verinice software interface. The left sidebar displays a tree view of the Information Security Model, with 'Szenarien' (Scenarios) expanded to 'Betrieb' (Operation). The main window shows a detailed view of a threat scenario titled 'Ausfall der Haupt-Hardware für DNS(.de)'. The scenario details include:

- Abkürzung:** B.80
- Tags:** BA
- Erklärung:** Im Kontext DNS(.de) sind Haupt-Servern im Einsatz. Bei Ausfall von zwei weiteren Servern kann der DNS(.de) Prozess hinsichtlich seiner Verfügbarkeit negativ erheblich erschüttert werden. Kapazitätsengpässe trotz der Haupt-Hardware können allerdings auch auftreten, wenn ein großes Maßstab komplett auf DNS(.de) umstellen muss.
- Dokument:** Includes checkboxes for 'Betrifft Vertraulichkeit' (unchecked), 'Betrifft Integrität' (checked), and 'Betrifft Verfügbarkeit' (checked).
- Wahrscheinlichkeit:** Includes dropdown menus for 'Bedrohungshäufigkeit' (set to '4 mal wöchentlich') and 'Einstufung der Schwachstelle' (set to '2 hoch möglich').

At the bottom, a 'Verknüpfungen' (Links) table shows the following connections:

Verknüpfung	Titel	Scope	Beschreibung
Wahrscheinlich...	12.1.1 Dokumentierte Betriebsprozesse	DENIC eG	
Wahrscheinlich...	12.1.2 Implementierung der Kontinuität der Informationssicherheit	DENIC eG	
Wahrscheinlich...	17.1.2 Verfügbarkeit von informationsverarbeitenden Einrichtungen	DENIC eG	
beeinflusst	DNS (.de)	DENIC eG	

Risikomanagement im Rahmen des ISMS – Maßnahmen



verinice.PRO

Information Security Model

- Services
 - Administration
 - Business Services
 - Communication & Collaboration
 - Direct Services
 - DNS (.de)
 - DNS (Anycast 3.rd)
 - Finance & Accounting
 - Human Resources
 - Infrastructure Services
 - Internal Services
 - Legal Department
 - Public Relations
 - Registry Service
- Unterstützende Prozesse
- Audits
- Ausnahmen
- Controls
 - Controls (Benutzerdefiniert)
 - Controls (ISO/IEC 27001:2013)
- Dokumente
- Personen
- Prozesse
- Szenarien
 - Betrieb
 - Compliance
 - Finanzen
 - Infrastruktur
 - Management
 - Markt
 - Personal
 - Umfeld
 - Wirtschaftskriminalität

17.1.2 Implementierung der Kontinuität der Informationssicherheit

Titel

Abkürzung

Tags

Dokument

JIRA-URL [17.1.2 Umsetzung der Geschäftskontinuität in Bezug auf Informationssicherheit](#)

Implementation

Implementiert

Erklärung

Zielsetzung

Die Organisation muss Richtlinien und Maßnahmen etablieren, dokumentieren und implementieren um das geforderte Maß der Geschäftskontinuität in schwierigen Verhältnissen sicherzustellen.

Verknüpfungen

Verknüpfung	Titel	Scope	Beschreibung
modifiziert Wa...	...	DENIC eG	
modifiziert Wa...	...	DENIC eG	
modifiziert Wa...	...	DENIC eG	
reduziert Aus...	DENIC (übergeordnete ...	DENIC eG	
reduziert Aus...	DNS (.de)	DENIC eG	

Server:

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:	0jhzzii:r		
Rank (Veraltet):	6038		

Personen

Bearbeiter: [Mir zuweisen](#)

Autor: [2 Beobachten beenden](#)

Beobachter verwalten:

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

Beschreibung

BCM Leitlinie ist veröffentlicht.

Verknüpfungen

hängt zusammen mit

- [SEC-108 Definition der minimalen Daten zur Aufrechterhaltung der Geschäftsprozesse](#) ⚠
- [SEC-104 Wiederherstellungspläne für kritische Geschäftsprozesse](#) ✅
- [SEC-106 Supporting assets for kritischen Geschäftsprozesse](#) ✅



Risikomanagement im Rahmen des ISMS – Maßnahmen

JIRA Startseite ▾ Projekte ▾ Vorgänge ▾ Tempo ▾ Agile ▾ **Erstellen** Suche 🔍 ? ⚙️ ▾

Information Security Backlog Aktive Sprints Berichte Board ▾ View in Tempo ▾

SPRINT: 2015-8 ▾ SCHNELL-FILTER: Nur meine Vorgänge Zuletzt aktualisiert

Aufgaben Wird Ausgeführt Wartend Fertig

> **SEC-105** **ISMS** Fortschreiten Definition der minimalen Ziele zur Aufrechterhaltung der Betriebsfähigkeit für die kritischen Geschäftsprozesse

> **SEC-146** **ISMS** Fortschreiten Überarbeitung der Leitlinien im Bereich Security

▾ Andere Vorgänge 26 Vorgänge

<input checked="" type="checkbox"/> SEC-57 ↓ 9.4.2 Verwaltung von ISMS Tools ISMS	<input checked="" type="checkbox"/> SEC-41 ↓ 9.4.3 Systeme zur Verwaltung von Passwörtern ISMS	<input checked="" type="checkbox"/> SEC-176 ↑ Risiko (Hoch) Projekt	<input checked="" type="checkbox"/> SEC-203 ↓ PDP Maps ISMS
<input checked="" type="checkbox"/> SEC-207 ↓ Implementierung IS-10 ISMS	<input checked="" type="checkbox"/> SEC-187 ↓ Implementierung Security Center (IS, L&S) ISMS	<input checked="" type="checkbox"/> SEC-153 ↓ Überarbeitung des ISMS-Risikomanagements ISMS	<input checked="" type="checkbox"/> SEC-172 ↓ ISMS Audit Audits
<input checked="" type="checkbox"/> SEC-147 ↓ Fortschritt der Fortsetzung der Security Awareness Kampagne ISMS	<input checked="" type="checkbox"/> SEC-124 ↓ Implementierung von ISMS-Tools für kritische Geschäftsprozesse BCMS	<input checked="" type="checkbox"/> SEC-152 ↑ Prozessdefinition zum Umgang mit produktionskritischen Sicherheitsverletzungen ISMS	<input checked="" type="checkbox"/> SEC-159 ↓ ISMS - Governance and Training BCMS
<input checked="" type="checkbox"/> SEC-139 ↓ Fortschritt der Integration von ISMS-Tools in die ISMS-Strategie ISMS	<input checked="" type="checkbox"/> SEC-126 ↓ Implementierung von ISMS-Tools für kritische Geschäftsprozesse BCMS	<input checked="" type="checkbox"/> SEC-151 ↑ Überarbeitung des Incident Management Prozess ISMS	

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

Tabellenverzeichnis	4
1 Zweck des Dokumentes	5
2 Grundwerte des Assets	6
3 Bericht zur Risikoeinschätzung	7
3.1 Allgemeines Vorgehen	7
3.2 Einzelaufistung der Bedrohungsszenarien	8
3.3 Summe aller Risikowerte („Total Risk“).....	18
3.4 Übersicht Maßnahmen	18
4 Risikoakzeptanz	21
5 Änderungshistorie des Dokuments	22
Anhang A - Klassifizierungsstufen	23
A.1 Klassifizierungsstufen - Grundwerte des Assets - Vertraulichkeit.....	23
A.2 Klassifizierungsstufen - Grundwerte des Assets - Integrität	23
A.3 Klassifizierungsstufen - Grundwerte des Assets - Verfügbarkeit	23
A.4 Klassifizierungsstufen - Bedrohungshäufigkeit	24
A.5 Klassifizierungsstufen - Einstufung der Schwachstelle.....	24
Anhang B - Vorgaben Risikoakzeptanz	26

Risikomanagement im Rahmen des ISMS – Reporting



Scenario	Likelihood	0	0	9	
Informationelle Verfügbarkeit: Ausfall des Netzwerkes durch unautorisierte Manipulation	6				
Controls affecting scenario	Effectiveness	Implemented			
...	2	Ja			
...	2	Ja			
...	2	Ja			
...	3	Ja			
Residual Risk		0	0	3	3
Scenario	Likelihood	7	7	8	
Informationelle Integrität: Verlust der Vertraulichkeit	5				
Controls affecting scenario	Effectiveness	Implemented			
...	2	Ja			
...	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



- 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 Kritikalität der Geschäftsprozesse
- Wiederanlauf- und Kontinuitätspläne für kritische Geschäftsprozesse
- Durchführung von regelmäßigen Notfallübungen

Business Continuity Management - Übersicht



verinice.PRO

Information Security Model

- DENIC eG
 - Anforderungen
 - Assets
 - Organisation
 - Services
 - Administration
 - Business Services
 - Communication & Collaboration
 - Direct Services
 - DNS (.de)
 - DNS (Anycast 3.rd)
 - Finance & Accounting
 - Human Resources
 - Infrastructure Services
 - Internal Services
 - Legal Department
 - Public Relations
 - Registry Service
 - Unterstützende Prozesse
 - Audits
 - Ausnahmen
 - Controls
 - Controls (Benutzerdefiniert)
 - Controls (ISO/IEC 27001:2013)
 - Dokumente
 - Personen
 - Prozesse
 - Administration
 - Business Services
 - Communication & Collaboration
 - DENIC - Organisation
 - Direct Services
 - DNS (.de)

DNS (.de) DENIC eG

Risiko Akzeptanz

Confidentiality

Integrity

Availability

Erklärung

Die Risiko-Akzeptanzschwellwerte wurden gemeinsam mit dem Vorstand unter Berücksichtigung des übergreifenden Risikomanagements besprochen und für die Grundwerte festgelegt. Risiken, die unter dem Schwellwert liegen, werden automatisch vom Vorstand der DENIC eG akzeptiert.

Für Risiken, die nach der Risikobehandlung weiterhin den definierten Akzeptanzwert

Business Impact Klassifizierung

Vertraulichkeit

Integrität

Verfügbarkeit

Verknüpfungen

Server:

Business Continuity Management - Übersicht



verinice.PRO

Information Security Model

- DENIC eG
 - Anforderungen
 - Assets
 - Organisation
 - Services
 - Administration
 - Business Services
 - Communication & Collaboration
 - Direct Services
 - DNS (.de)
 - DNS (Anycast 3.rd)
 - Finance & Accounting
 - Human Resources
 - Infrastructure Services
 - Internal Services
 - Legal Department
 - Public Relations
 - Registry Service
 - Unterstützende Prozesse
 - Audits
 - Ausnahmen
 - Controls
 - Controls (Benutzerdefiniert)
 - Controls (ISO/IEC 27001:2013)
 - Dokumente
 - Personen
 - Prozesse
 - Administration
 - Business Services
 - Communication & Collaboration
 - DENIC - Organisation
 - Direct Services
 - DNS (.de)

DNS (.de) | DENIC eG | *DNS (.de)

Geschäftskontinuität

MTPD (h)

RPO (h)

RTO (h)

Beeinträchtigung nach 8h

Beeinträchtigung nach 24h

Beeinträchtigung nach 48h

Beeinträchtigung nach 96h

Beeinträchtigung nach 168h

Beeinträchtigung nach 720h

Beeinträchtigung nach >720h

Business Impact

Vertraulichkeit ableiten

Integrität ableiten

Verfügbarkeit ableiten

Vertraulichkeit

Integrität

Verfügbarkeit

Wiederherstellungskosten

Währung

Begründung

Verknüpfungen

Server:

Agenda



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