Information Security Management bei DENIC

Umsetzung von Anforderungen aus dem IT-Sicherheitsgesetz

Boban Krsic, DENIC eG

Frankfurt, den 13.11.2015

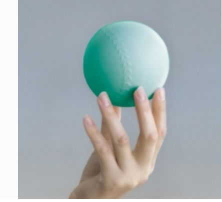
Agenda

- Kurzvorstellung
- Gesetzliche Anforderungen
- Überlegungen zur Umsetzung
- Security Management bei DENIC
- Ausblick

Agenda

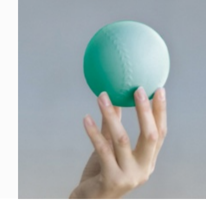
- **Kurzvorstellung**
- Gesetzliche Anforderungen
- Überlegungen zur Umsetzung
- Security Management bei DENIC
- Ausblick

Kurzvorstellung - DENIC eG

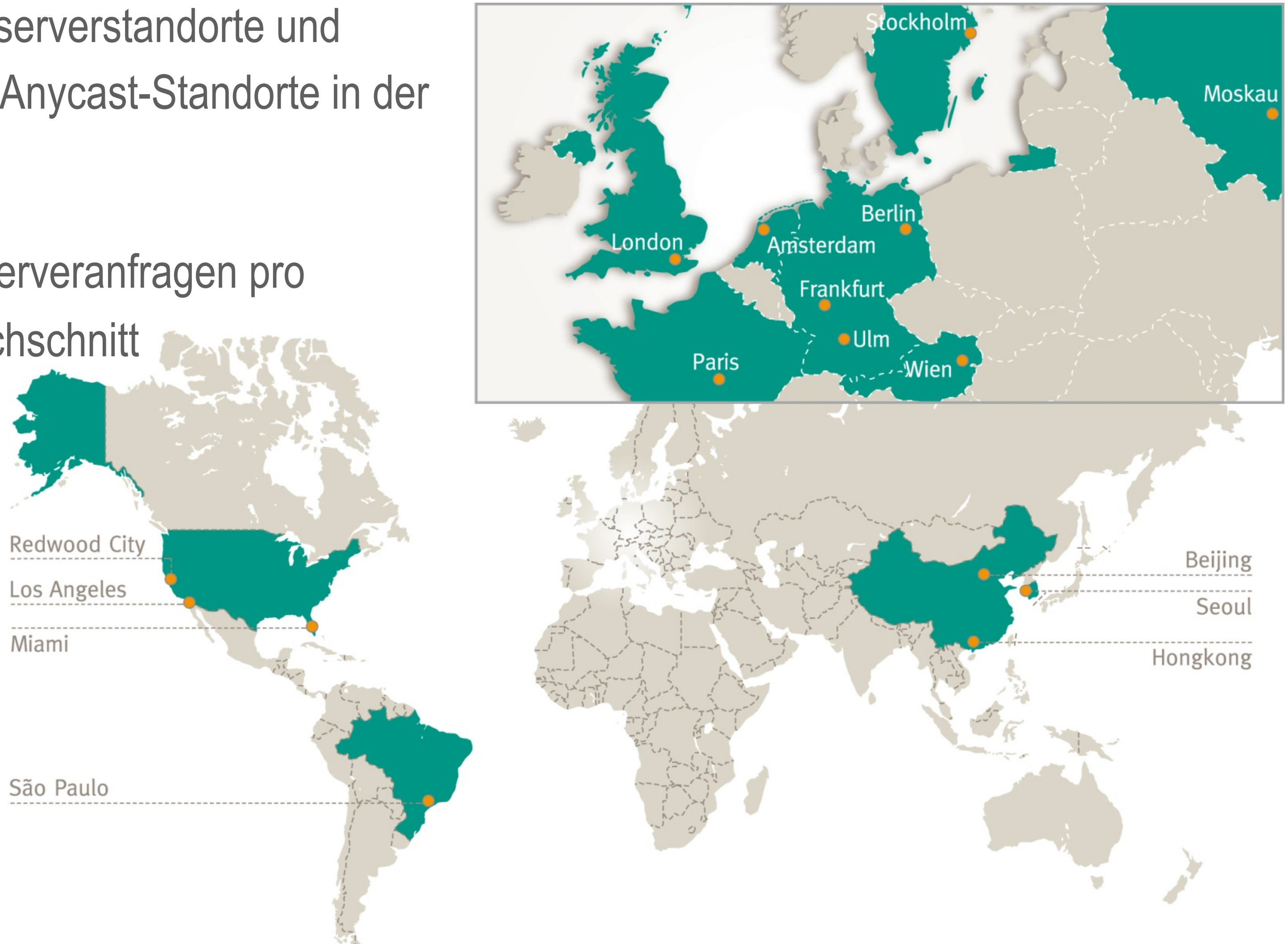


- Eingetragene Genossenschaft mit Sitz in Frankfurt am Main, gegründet 1996.
- Zentrale Registrierungsstelle für alle Domains unterhalb der länderbezogenen Top Level Domain .de sowie für ENUM-Domains (**E**.164 **NU**mber **M**apping) unter .9.4.e164.arpa, dem deutschen Rufnummernraum.
- Selbstverständnis als neutraler, diskriminierungsfreier, Not-for-Profit-Dienstleister für die Internet Community, der seiner Verantwortung gemeinsam mit den mehr als 320 Mitgliedern (Registrare) der Genossenschaft nachkommt.
- Aufgaben und Tätigkeitsbereiche:
  - Betrieb des Nameservices für .de und für .9.4.e164.arpa
  - Betrieb eines automatischen Registrierungssystems und der Domaindatenbank
  - Bereitstellung von Auskunftsdiensten (whois) und einer Service Hotline

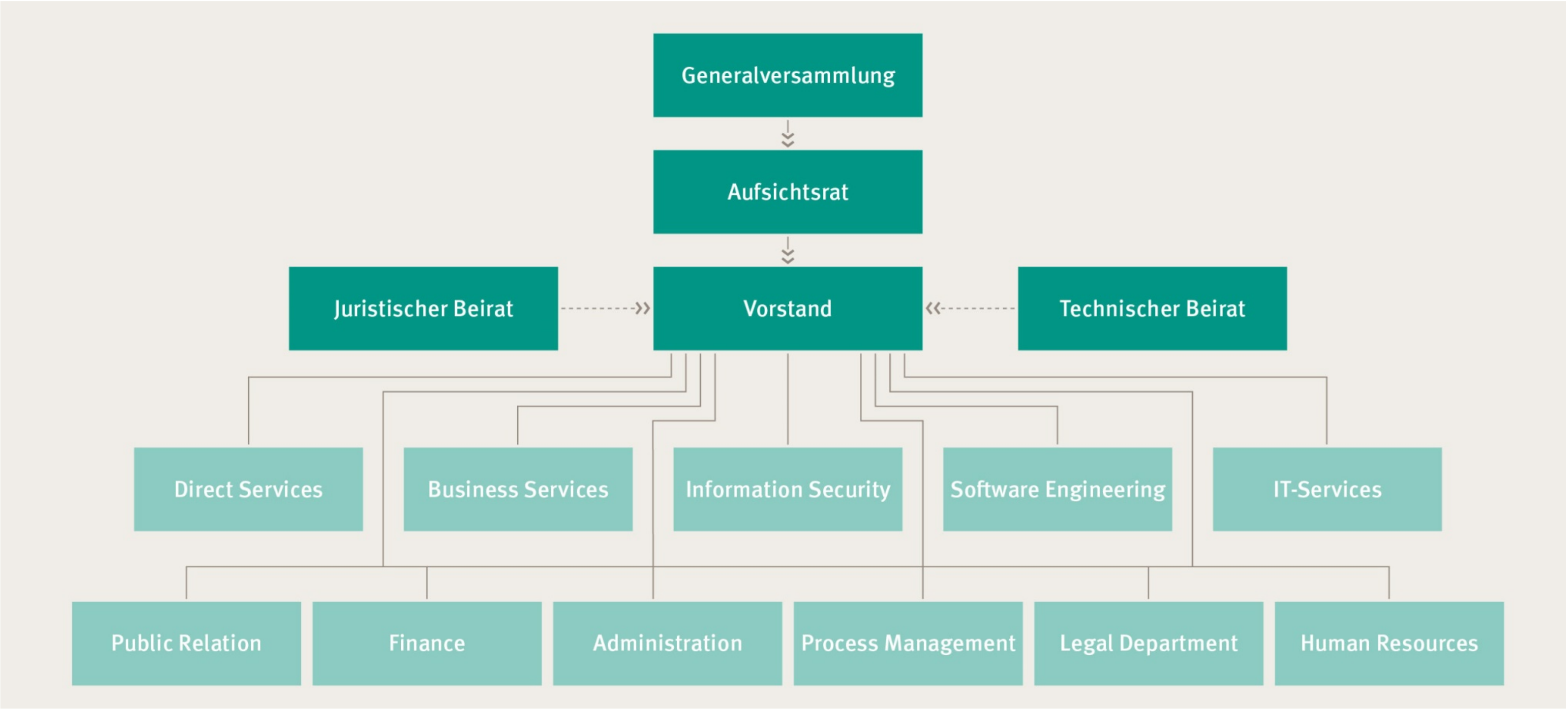
Kurzvorstellung - DENIC eG - Nameservice für .de



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



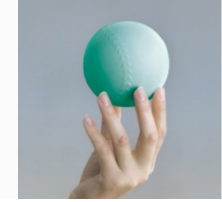
Kurzvorstellung - DENIC eG - Struktur



Kurzvorstellung - DENIC eG - Zusammenarbeit und Kooperationen

- Aktive Mitgestaltung an der Weiterentwicklung des Internets in diversen Gremien:
  - Council of European TLD-Registries (CENTR)
  - Deutscher CERT-Verbund
  - DNS-Operations, Analysis and Research Center (DNS-OARC)
  - Internet Corporation for Assigned Names and Numbers (ICANN)
  - Internet Governance Forum (IGF)
  - Internet Engineering Task Force (IETF)
  - Internet Society (ISOC)
  - RIPE Network Coordination Centre (RIPE NCC)
- Weiterentwicklung von Internetstandards
- Unterstützung bei der Zusammenarbeit der ccTLDs

Kurzvorstellung - DENIC eG - Mitarbeit bei UP KRITIS



- Aktive Mitarbeit am UP KRITIS seit 2011
- Mitglied im Plenum des UP KRITIS
- Leiter / Sprecher des Branchenarbeitskreises Internet-Infrastruktur
  - Mitglieder: Organisationen, Verbände und öffentliche Verwaltung
  - Primäres Ziel: Vernetzung, vertrauensvoller Informationsaustausch sowie Entwicklung gemeinsamer Positionen und Dokumente für die Branche
  - Aktuelle Aufgaben: Umgang / Umsetzung von gesetzlichen Anforderungen
- Mitarbeit im Kernteam mit weiteren BAK-Leitern und dem BMI zur
  - Beschreibung der sektorspezifischen Dienstleistungen,
  - qualitativen (Anlagen) und quantitativen (Schwellenwerte) Kriterien

  als Grundlage für die BSI-KritisV.

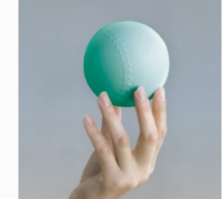
Agenda

- Kurzvorstellung
- **Gesetzliche Anforderungen**
- Überlegungen zur Umsetzung
- Security Management bei DENIC
- Ausblick

Gesetzliche Anforderungen

- § 8a
  - Treffen von angemessenen organisatorischen und technischen Vorkehrungen
  - Stand der Technik ist zu berücksichtigen
  - Betreiber können einen Branchenspezifischen Sicherheitsstandard (B3S) vorschlagen
  - Nachweispflicht durch Audits alle 2 Jahre gegenüber dem BSI
- § 8b
  - BSI als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen
  - Kontinuierliches Lagebild mit Pflicht zur unverzüglichen Weitergabe an Betreiber
  - Alarmierungskontakt ist innerhalb von 6 Monaten zu benennen
  - Verpflichtung zur Meldung von Sicherheitsvorfällen
- § 10
  - Rechtsverordnung zur Identifikation Kritischer Infrastrukturen

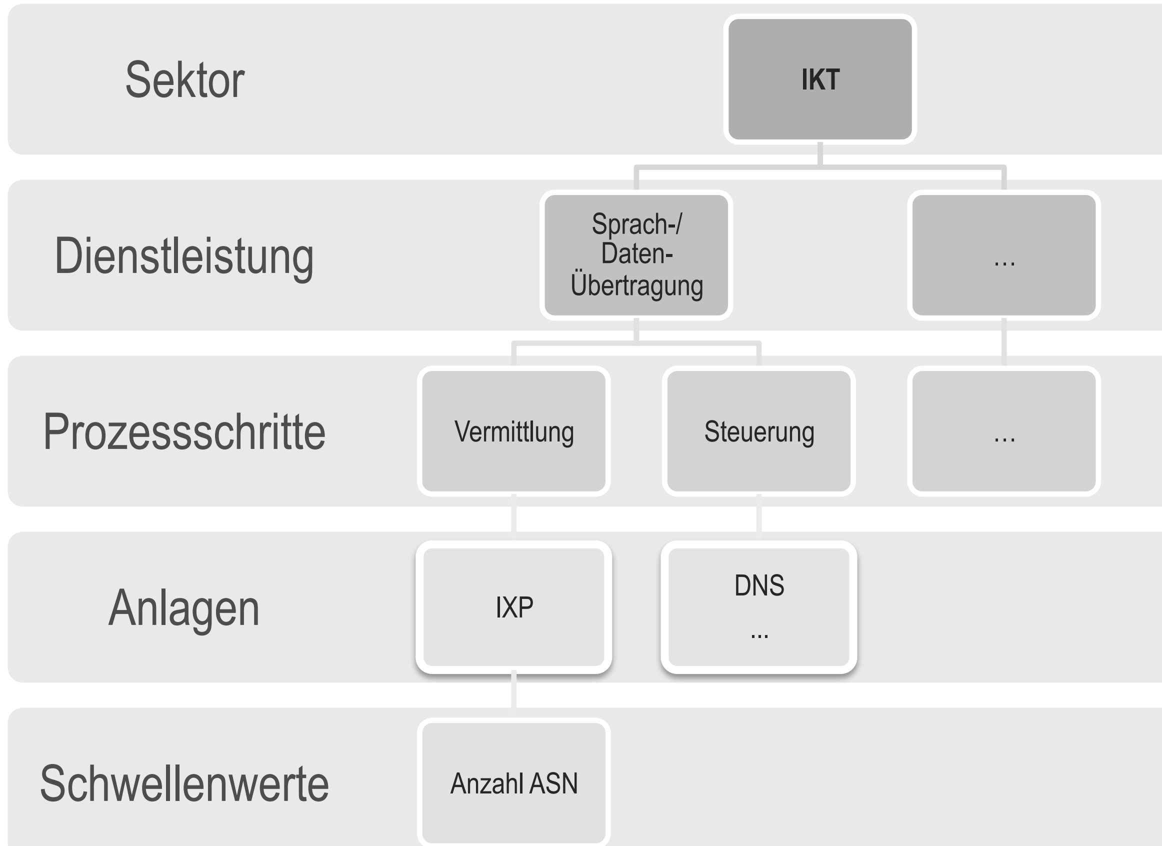
Gesetzliche Anforderungen - BSI-KritisV - Vorgehensweise



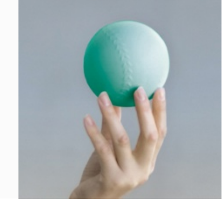
Versorgung der Gesellschaft mit wichtigen Dienstleistungen

Qualität: Dienstleistungen in den KRITIS-Sektoren, die für die Versorgungskette relevant sind und abstrakte Anlagen

Quantität: Schwellenwerte innerhalb dieser Dienstleistungen



Agenda



- Kurzvorstellung
- Gesetzliche Anforderungen
- **Überlegungen zur Umsetzung**
- Security Management bei DENIC
- Ausblick

Überlegungen zur Umsetzung von § 8a IT-Sicherheitsgesetz

- Was sind die kritischen Dienstleitungen und damit verbundene Schutzziele?
- Welche Gefährdungslage ist innerhalb der Branche zu beobachten?
- Was ist der Reifegrad zur Umsetzung von sicherheitsrelevanten Anforderungen innerhalb der Branche?
- Wie ist der Umsetzungsstatus von getroffenen Maßnahmen?
- Sind eventuell Zertifizierungen, die das Schutzziel umfassen, vorhanden?
- Wollen wir einen eigenen (internationalen) Standard entwickeln?
- Sollen wir den Weg der Normierung einschlagen?

→ Umsetzung von § 8a in Anlehnung an internationale Normen

Überlegungen zur Umsetzung von § 8a und § 8b

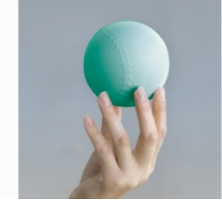
- Erstellung eines Rahmendokumentes
  - Definition und Beschreibung der Kritischen Dienstleistung und der IT-Systeme
  - Konsequente Etablierung:
    - eines Information Security Management Systems nach ISO/IEC 27001:2013,
    - eines Business Continuity Management Systems nach ISO 22301,
    - eines Risikomanagement-Prozesses nach ISO/IEC 27005

    in einem integrierten Ansatz unter Berücksichtigung der strategischen Ausrichtung der jeweiligen Organisation
  - Betrachtung von branchenspezifischen Bedrohungen und Umsetzung von Best Practices
  - Umsetzung des Meldewesens und Benennung der Kontaktstellen
  - Definition von Kriterien zur Meldung von Sicherheitsvorfällen nach ISO/IEC 27035:2011
  - Auditierung des ISMS und Nachweis gegenüber dem BSI

Agenda

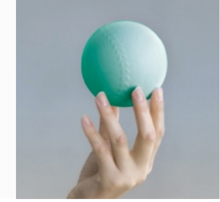
- Kurzvorstellung
- Gesetzliche Anforderungen
- Überlegungen zur Umsetzung
- **Security Management bei DENIC**
- Ausblick

Security Management 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 iMS: Gesamtes Unternehmen inkl. aller erbrachten Dienste
- Aufbau des iMS 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 iMS unter Verwendung von Key Performance Indikatoren (KPIs), die unter Zuhilfenahme von COBIT 5 for Information Security abgeleitet wurden
- Risikomanagement der Informationssicherheit nach ISO/IEC 27005:2011
- Business Continuity Management nach ISO 22301:2012

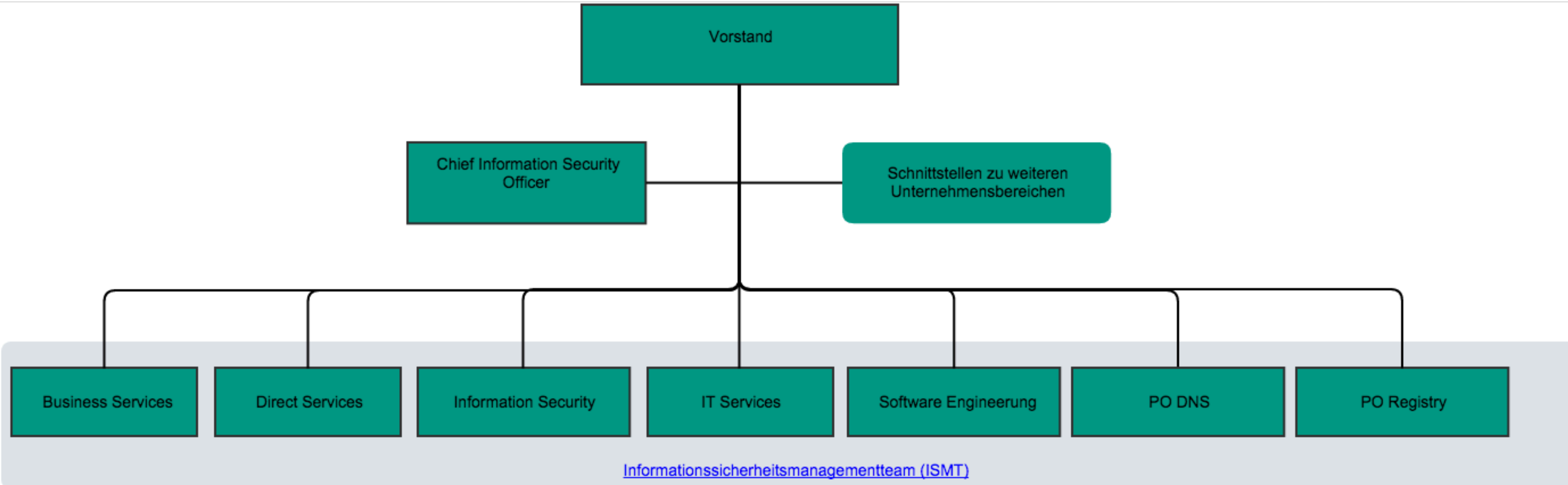
* vgl. hierzu Strategiepapier der DENIC eG, S.1 ff. vom März 2008



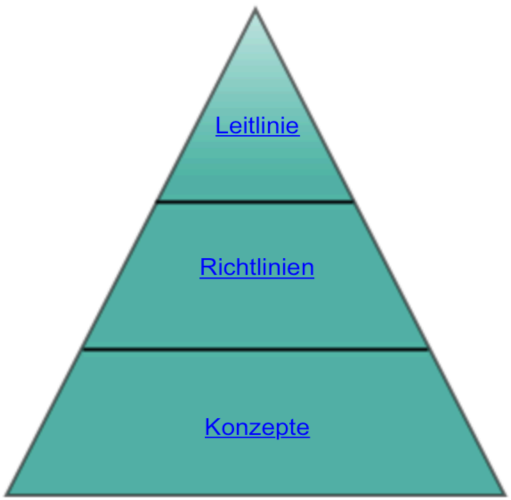
Security Management bei DENIC – Scope im Detail

Name	Beschreibung	Owner
Administration	Administration umfasst den Empfang, Bewirtungen, Reisebuchungen und -abrechnungen sowie die Poststelle bei DENIC.	CFO
Business Services	Business Services umfasst die Betreuung (Loginverwaltung, Problemlösungen, etc.) von Genossenschaftsmitgliedern.	AL (DBS)
Communication & Collaboration	Der Service Communication & Collaboration umfasst hausinterne Anwendungen wie Groupware (Lotus Notes, OTRS), Intranet (Confluence), Office Productivity (Fileserver, Software, Office-Umgebungen) sowie Telefonie und FAX.	AL (ITS)
Direct Services	Direct Services umfasst den hauseigenen Provider DENICdirect (Registrar), Endkundensupport sowie das TRANSIT Service Center zur Bearbeitung von Vorgängen zur weiteren Verfahrensweise mit .de-Domains.	AL (DS)
DNS (Anycast 3.rd)	Der Service DNS (Anycast 3.rd) umfasst den Vertrieb sowie die Bereitstellung des Produktes Anycast für Dritte (ccTLD).	AL (DBS)
DNS (.de)	Der Service DNS (.de) umfasst die Instandhaltung (z.B. Bugfixing), Weiterentwicklung, Betrieb (inkl. Monitoring), Prozessoptimierung und Kapazitätsplanung der IT-Systeme zur Erbringung der Name Services für .de und ENUM.	DNS-Services (PO)
Finance & Accounting	Der Service Finance & Accounting umfasst das Enterprise-Resource-Planning-System (ERP) sowie die Rechnungsstellung gegenüber den Mitgliedern.	AL (Finanzen)
Human Resources	Human Resources umfasst die Zeiterfassung, die Gehaltsabrechnung sowie die administrative Verwaltung der internen Public Key Infrastruktur (PKI) für die Mitarbeiterzertifikate.	AL (Personal)
Infrastucture Services	Infrastructure Services liefert Basisinfrastrukturdienste sowie Anwendungen zur Administration und zum Systems Management. Dazu zählen u.a. Backup, Monitoring und Logging sowie diverse Methoden und Werkzeuge zur Automatisierung der Systemlandschaft.	Infrastructure Services (PO)
Internal Services	Internal Services ist für die Planung und Koordination der Basisinfrastrukturdienste im Bürogebäude und den RZ-Standorten sowie für die anfälligen Wartungs- und Installationstätigkeiten zuständig.	AL (ITS)
Legal Department	Legal Services umfasst die Rechtsverteidigung der DENIC eG sowie die rechtliche Bearbeitung von Domains, Domainstreitigkeiten (Dispute) und Verstößen.	AL (Recht)
Public Relations	Public Realtions umfasst die Betreuung der Öffentlichkeit, Übersetzungsservice, Planung von Veranstaltungen, Newsletter und die Pflege des Internetauftritts.	Verantwortliches Vorstandsmitglied
Registry Service	Der Registry Service umfasst das Registrierungssystem mit seinen Schnittstellen Mail Registry Interface (MRI) und Real Time Registry Interfaces (RRI) sowie die Auskunftsdienste (whois und Statusabfragen (INFO und CHECK)) des Registrierungssystems. Weiterhin findet sich das Registry Administration Interface (RAI) ebenfalls in der Verantwortung des Registry Services.	Registry Services (PO)

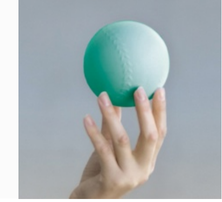
Security Management bei DENIC – Aufbauorganisation / Regelwerk



- Leitlinie bildet strategische Grundlage
- Aufbauend auf der Leitlinie dienen Richtlinien zur Konkretisierung der Vorgaben
- Umsetzung von konkreten Maßnahmen zur Erfüllung der Anforderungen werden in Sicherheits- und Betriebskonzepten dokumentiert



Strategische Ausrichtung und Steuerung

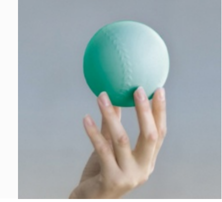


- Unter Berücksichtigung der strategischen Unternehmensziele wurden die nachfolgenden generischen Ziele zur Ausrichtung aller Aktivitäten des iMS auf gemeinsame Ziele relevanter Interessengruppen anhand einer Scorecard identifiziert:
  - Finanzen
    - 2. Portfolio wettbewerbsfähiger Produkte und Services
    - 3. Gemanagtes Unternehmensrisiko (Sicherung der Betriebsmittel)
  - Kunden (Mitglieder)
    - 7. Kontinuität und Verfügbarkeit von Services
    - 10. Optimierung der Kosten für die Serviceerbringung
  - Prozesse
    - 11. Optimierung der Funktionalität von Geschäftsprozessen
    - 12. Optimierung der Geschäftsprozesskosten
  - Mitarbeiter
    - 16. Kompetente und motivierte Mitarbeiter

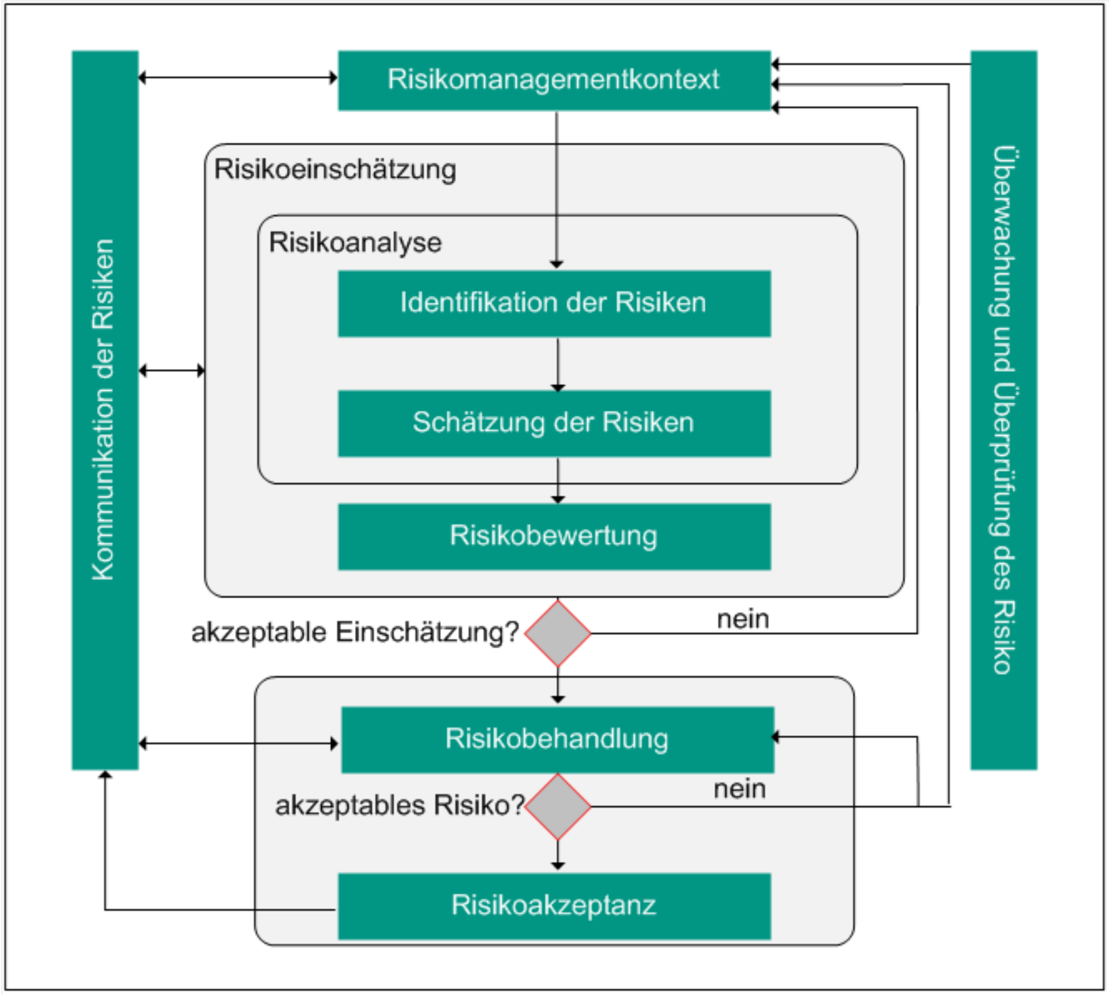
Strategische Ausrichtung und Steuerung des ISMS II

- Unter Anwendung der Zielkaskadierung von „COBIT 5 for Information Security“ wurden die nachfolgenden sicherheitsspezifischen Prozessziele und dazugehörigen Metriken zur Steuerung des ISMS abgeleitet.

ID	Security-specific process goal	Metric	Frequency	Minimum	Maximum
01	Information security requirements are considered and incorporated in all programmes and projects.	Percent of programmes and projects that have a security risk assessment and an information security plan to adress the risk	annually	80%	90%
02	Suppliers and contracts are assessed regularly and appropriate risk mitigation plans are provided	Number of independent information security reviews of suppliers	annually	0	1
03	HR capabilities and processes are aligned with information security requirements	Percent of employees provided security introduction	annually	60%	90%
04	A security plan has been established, accepted and communicated throughout the enterprise	Level of stakeholder satisfaction with the security plan throughout the enterprise	annually	60%	80%
05	Information security solutions are implemented and operated consistently throughout the enterprise	Percent of critical services with confirmed alignment to the security plan	annually	95%	100%
06	Operational information security quality requirements for information security services are defined and implemented	Frequency of reporting (weekly, monthly, quarterly, annually)	annually	0	1
07	An effective information security incident response programme is established and maintained	Mean time (hours) to resolve critical information security incidents	monthly	1	2



Risikomanagement im Bereich Information Security bei DENIC



- Prozessuale Einbindung in das übergreifende Risikomanagement bei DENIC
- Full Scope Ansatz
- Beteiligte Akteure / Rollen:
  - Risikomanager
  - Risikomanagementkreis
  - Risikoverantwortliche
- Ermittlung der Risiken durch:
  - Workshops mit Produktteams
  - Bedrohungsmodellierung / -Kataloge
  - 134 Bedrohungsszenarien
  - 183 Controls

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 Bedrohungs- und Risikoanalyse
    - 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

Agenda

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

Ausblick

- Fertigstellung des Rahmendokumentes zur Umsetzung des Mindeststandards
- Einreichung des Dokumentes beim BSI bis Ende Q1 / 2016
- Durchführung einer GAP-Analyse zur organisationseigenen Ermittlung des Reifegrades unter Berücksichtigung des Rahmendokumentes
- Definition und Umsetzung eines Meldeverfahrens Q2 / 2016
- Benennung einer Kontaktstelle Q2 / 2016

Fragen?

Vielen Dank!

Boban Krsic, DENIC eG
Chief Information Security Officer

e-mail: <krsic@denic.de>
phone: +49 69 272 35 – 0

PGP Key-ID: 0x43C89BA9