T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013

Dr. Jochen Ruben (bridgingIT GmbH)

ISACA Germany Chapter e.V

Dr. Jochen Ruben – Management Consultant

Beratungsexpertise

- Informationssicherheit / IT-Security / Cyber-Security
- Integrierte Managementsysteme
- IT-Strategie / IT-GRC

Qualifikationen

- IT-Governance Manager (ISACA)
- CobiT Practitioner (ISACA)
- TÜViT ISMS-Auditor (nach ISO/IEC 27000 Informationssicherheits-Managementsystem)
- Cyber-Security Practitioner (ISACA)
- TOGAF 8
- ITIL Service Manager (V3.0)

Agenda

- Überblick über die ISO270xx Familie
- Vorstellung des Implementierungsleitfadens
- Diskussion

Agenda

- **Überblick über die ISO270xx Familie**
- Vorstellung des Implementierungsleitfadens
- Diskussion

Die ISO 270XX Familie

27000	• Terms and Definitions
27001	• Requirements
27002	• Code of Practice
27003	• Implemenation Guidance
27004	• Measurements
27005	• IS Risk Management

27006	• Req. For Certification Bodies
27007	• Guidelines to Auditing
27008	• Guidelines for Auditors
27010	• Inter sector inter org. comm.
27011	• Sector Telecommunication
27013	• Integ. Impl. Of 20000 & 27001
27014	• Governance of InfoSec
27015	• Sector Financial Services
27016	• Organisational Economics
27017	• Cloud Computing
27018	• Public Cloud Computing Serv.

Die ISO 270XX Familie – Die Verwandtschaft

27799	• Healthcare
27031	• ICT Readiness BC
27032	• Cyber Security
27033	• Network Security
27034	• Application Security
27035	• Information Security Inc. Mgmt.
27036	• Supplier Relationships
27037	• Digital Evidence
27039	• IDPS
27040	• Storage Security
27041 - 43	• Investigation
27044	• Sec. Inf. and Event Management

Die ISO 270XX Familie – Der Ursprung

- **ISO 27002 evolves out of the British Standard 17799**
  - Selection of IT Security procedures and guides
- **ISO 27001 is an IS Management Standard (certification)**
  - it includes the „Clauses“
    Requirements concerning the Management System
- **It includes the „Annex A“**
  - Risk oriented technical and organisational requirements within the organisation and organisation‘s partners (Short version of the ISO 27002)

Die ISO 270XX Familie
Neue Vorgehensweise 2013 / Wiederaufbau der Erde

Folgt dem in den ISO/IEC Direktiven (Annex SL) vorgeschlagenen Aufbau eines Managementstandards

Ziel: Vereinfachung integrierter Managementsysteme

Struktur der ISO27001:2013 - Clauses

4	• Kontext der Organisation
5	• Führung
6	• Planung
7	• Unterstützung
8	• Betrieb
9	• Bewertung der Leistung
10	• Verbesserung der Leistung

Struktur der ISO 27001:2013
Annex A und die ISO 27002

5	• Informationssicherheitsrichtlinien
6	• Organisation der Informationssicherheit
7	• Personalsicherheit
8	• Verwaltung der Werte
9	• Zugangssteuerung
10	• Kryptograhie
11	• Physische und umgebungsbezogene Sicherheit
12	• Betriebssicherheit
13	• Kommunikationssicherheit
14	• Anschaffung, […] und Instandhalten von Systemen
15	• Lieferantenbeziehungen
16	• Handhabung von Informationssicherheitsvorfällen
17	• Informationssicherheitsaspekte beim BCM
18	• Compliance

Agenda

- Überblick über die ISO270xx Familie
- **Vorstellung des Implementierungsleitfadens**
- Diskussion

Implementierungsleitfaden ISO/IEC 27001:2013

Erklärung eines ISMS in der Einleitung

Governance-Sicht:

- IT-Ziele und Informationssicherheitsziele, die aus den übergeordneten Unternehmenszielen abgeleitet sind (z. B. unterstützt nach COSO oder COBIT)

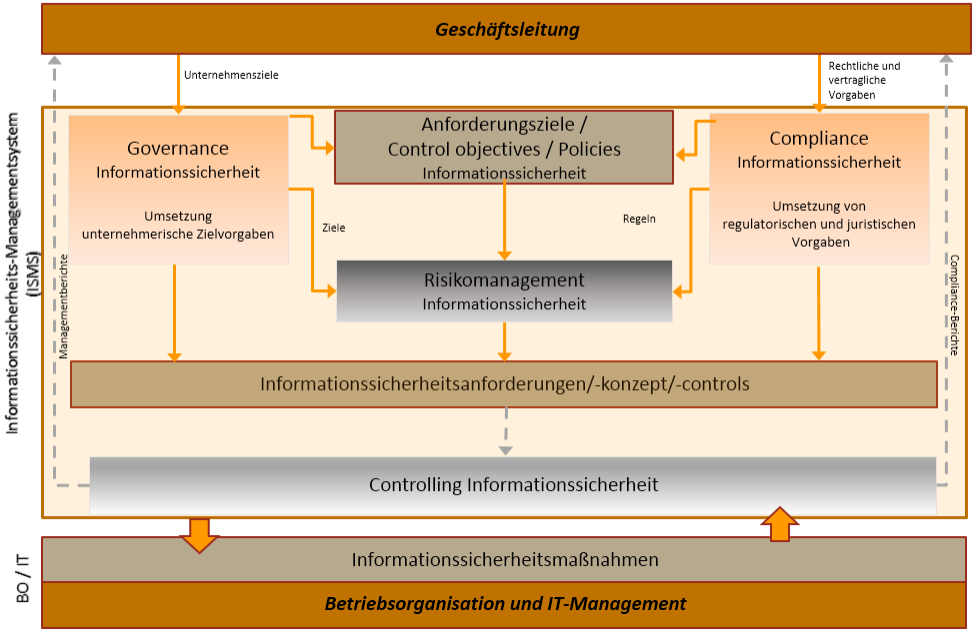
Risiko-Sicht:

- Schutzbedarf und Risikoexposition der Unternehmenswerte und IT-Systeme
- Risikoappetit des Unternehmens
- Chancen vs. Risiken

Compliance-Sicht:

- Externe Vorgaben durch Gesetze, Regulatoren und Normen
- Interne Vorgaben und Richtlinien
- Vertragliche Verpflichtungen

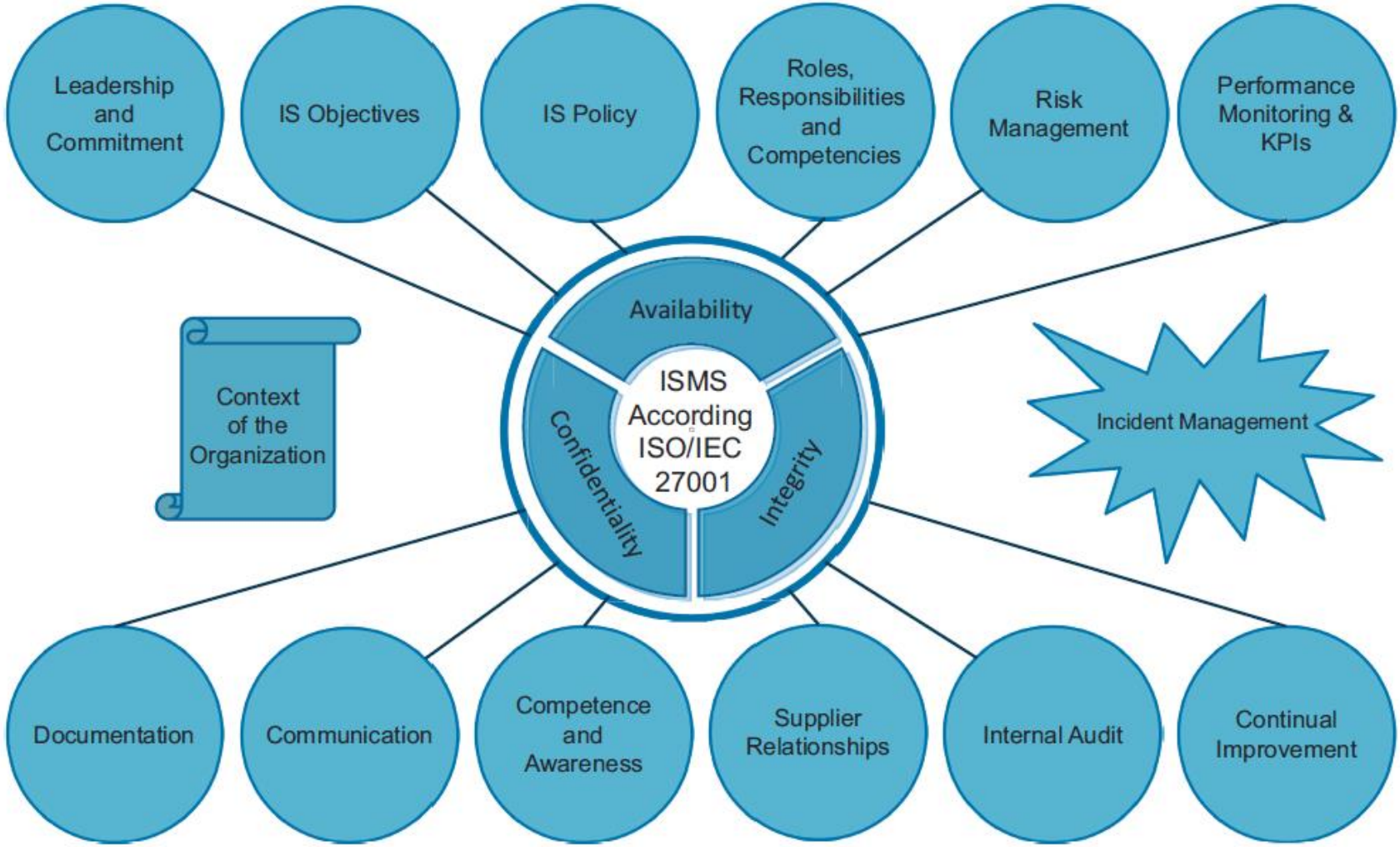
ISMS: Einbindung in die Unternehmenssteuerung



Informationssicherheit aus Praxissicht

- Der ISACA Implementierungsleitfaden enthält **praxisorientierte Anleitungen** und Hinweise für Organisationen, die ein Managementsystem für Informationssicherheit (ISMS) auf Basis von ISO/IEC 27001:2013 betreiben oder aufbauen wollen.
- Er betont die Vorteile eines ISMS, welches an die jeweilige Organisation angepasst wurde.
- Der Leitfaden enthält Expertentipps sowie Best-Practice-Beispiele, um verschiedene Anforderungen zu erfüllen.
- Der Leitfaden unterscheidet in normative Anforderungen und weitergehende Best-Practices.
- Der Leitfaden thematisiert auch oft kontrovers diskutierte Normauslegungen und nimmt Stellung dazu
  - → "stundenlange" Diskussionen bei der Erstellung, nicht selten mit finaler Klärung über Zertifizierungsstelle ;-)
- An der Erstellung des Leitfadens waren sowohl Security Manager aus Linienorganisationen als auch Berater und Auditoren beteiligt, weshalb die verschiedenen Sichten berücksichtigt wurden.

Aufbau des Leitfadens (14 Bausteine)



Implementierungsleitfaden ISO/IEC 27001:2013

Kapitelstruktur

Die einzelnen Kapitel sind jeweils gleich aufgebaut und in folgende drei Abschnitte gegliedert:

- **A. Erfolgsfaktoren aus der Praxis**
  Darstellung von – aus Sicht der Autoren – wesentlichen Erfolgsfaktoren für den Aufbau und Betrieb eines ISMS nach ISO/IEC 27001:2013

- **B. Anforderungen an die Dokumentation**
  Welche normativen Dokumentationsanforderungen gibt es und welche aus Sicht der Praxis?

- **C. Referenzen**
  Angabe der für den Themenbereich relevanten Kapitelnummern aus ISO/IEC 27001:2013 sowie weitere Quellenangaben, sofern erforderlich und sinnvoll

Implementierungsleitfaden ISO/IEC 27001:2013

Beispiel: Lieferantenbeziehung / Supplier Relationships

- Internationale Vernetzung und Standardisierung in der Informationsverarbeitung
  → Förderung des Einsatzes externer Dienstleister
- Sicherheitsrisiken beim Dienstleister haben Wirkung auf eigene Infrastruktur
  → belegt durch etliche öffentlichkeitswirksame Vorfälle der letzten Jahre
- Sicherheitsmängel bei Dienstleistern führten zu Datendiebstählen oder anderen Sicherheitsvorfällen prominenter Firmen.
- Definition "Dienstleister" bzw. "Lieferant"
  große Bandbreite von Geschäftsbeziehungen zu externen Firmen und Partnern aus den Bereichen Logistik, Versorgungseinrichtungen, IT-(Outsourcing) Dienstleister, Facility Management, Reinigungsdienstleister, Gehaltsabrechnung aber auch viele andere.

Implementierungsleitfaden ISO/IEC 27001:2013

Beispiel: Lieferantenbeziehung / Supplier Relationships

ISO/IEC 27036 und weitere relevante Standards

Deutlich detailliertere Betrachtung bietet die Norm ISO/IEC 27036 "Information Security in Supplier relationships".

- Betrachtet die notwendigen Prozesse und beschreibt die im jeweiligen Prozess notwendigen Aktivitäten.

  → konkrete Hilfestellungen zur Umsetzung der Prozessschritte

Beispiel: Lieferantenbeziehung / Supplier Relationships

Übersicht der in diesem Kontext relevanten Standards:

unterteilt in Überblick, Anforderungen und Leitfäden, sowie ergänzende Dokumente, die sich auf Prozesse und Techniken fokussieren:

Überblick	ISO/IEC 27036-1 Überblick und Konzepte	ISO/IEC 27000 Terminologie
Anforderungen	ISO/IEC 27036-2 IS-Anforderungen für Lieferantenbeziehungen	ISO/IEC 27001 ISMS
Leitfaden	ISO/IEC 15288 SDLC ISO/IEC 27036-3 Suppy Chain	ISO/IEC 27036-4 Cloud Services ISO/IEC 27002 Leitfaden ISMS
Prozesse/ Techniken	NIST SP-800-64 Systemlebenzyklus ISO/IEC 15026 System Zusicherung ISO/IEC 27034 – Applikationssicherheit Microsoft SDL SAFECode BSIMM	ISO/IEC 15408 Common Criteria OWASP Top 10 SANS Top 25 Secure Coding Checklists ...

Beispiel: Lieferantenbeziehung / Supplier Relationships

Erfolgsfaktoren aus der Praxis

- Ganzheitliche Risikobetrachtung
  - alle ausgelagerten Prozesse klar festgelegt und nachhaltig gesteuert
- Recht auf Auditierung (Größe spielt manchmal doch ein Rolle!)
- Zertifizierungen (Scope: Mind the gap!)
  - ISO/IEC 27001, ISMS
  - ISO/IEC 27018 für die Verarbeitung personenbezogener Daten in einer Cloud
  - ISAE 3402 „Assurance Reports on Controls at a Service Organization“.

Peril Sensitive Sunglasses
Joo Janta 200 Super-Chromatic Peril Sensitive Sunglasses have been specially designed to help people develop a relaxed attitude to danger.
At the first hint of trouble, they turn totally black and thus prevent you from seeing anything that might alarm you.
A double-pair is frequently worn by Zaphod Beeblebrox.

Beispiel: Lieferantenbeziehung / Supplier Relationships

Erfolgsfaktoren aus der Praxis

Kennzahlen

- Anzahl der Dienstleisterbeziehungen, die den definierten IS-Lieferantenprozess durchlaufen haben, im Verhältnis zu allen Dienstleisterbeziehungen
- Anzahl der Dienstleister, die IS-Maßnahmen vertraglich zusichern, im Verhältnis zu allen Dienstleistern
- Anzahl der Audits bei Dienstleistern in einem Jahr im Verhältnis zu allen Dienstleistern
- Anzahl der gemessenen Richtlinienverstöße durch Lieferanten
- Anzahl der Sicherheitsvorfälle bei Dienstleistern im vergangenen Berichtszeitraum

Implementierungsleitfaden ISO/IEC 27001:2013

Bezugsquelle / Download-Link:

https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_i_gesamt_web.pdf

Hinweis: Eine papiergebunde Version des Implemetierungsleitfadens wurde an alle ISACA-Mitglieder verschickt.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Jochen Ruben
Management Consultant
bridgingIT GmbH

www.bridging-it.de