HERZLICH WILLKOMMEN

Holger Schrader
Principal Consultant der CARMAO GmbH

Stellvertretender Leiter
der Fachgruppe Informationssicherheit
ISACA Germany Chapter

… seit 1998 tätig in den Themen
- IT Sicherheit
- Informationssicherheit
- Risikomanagement tätig

CISM, CRISC, Cyber Security Practitioner
und
Blutspender

FG Übersicht ISACA Germany Chapter

Experten nur ein Steinwurf entfernt

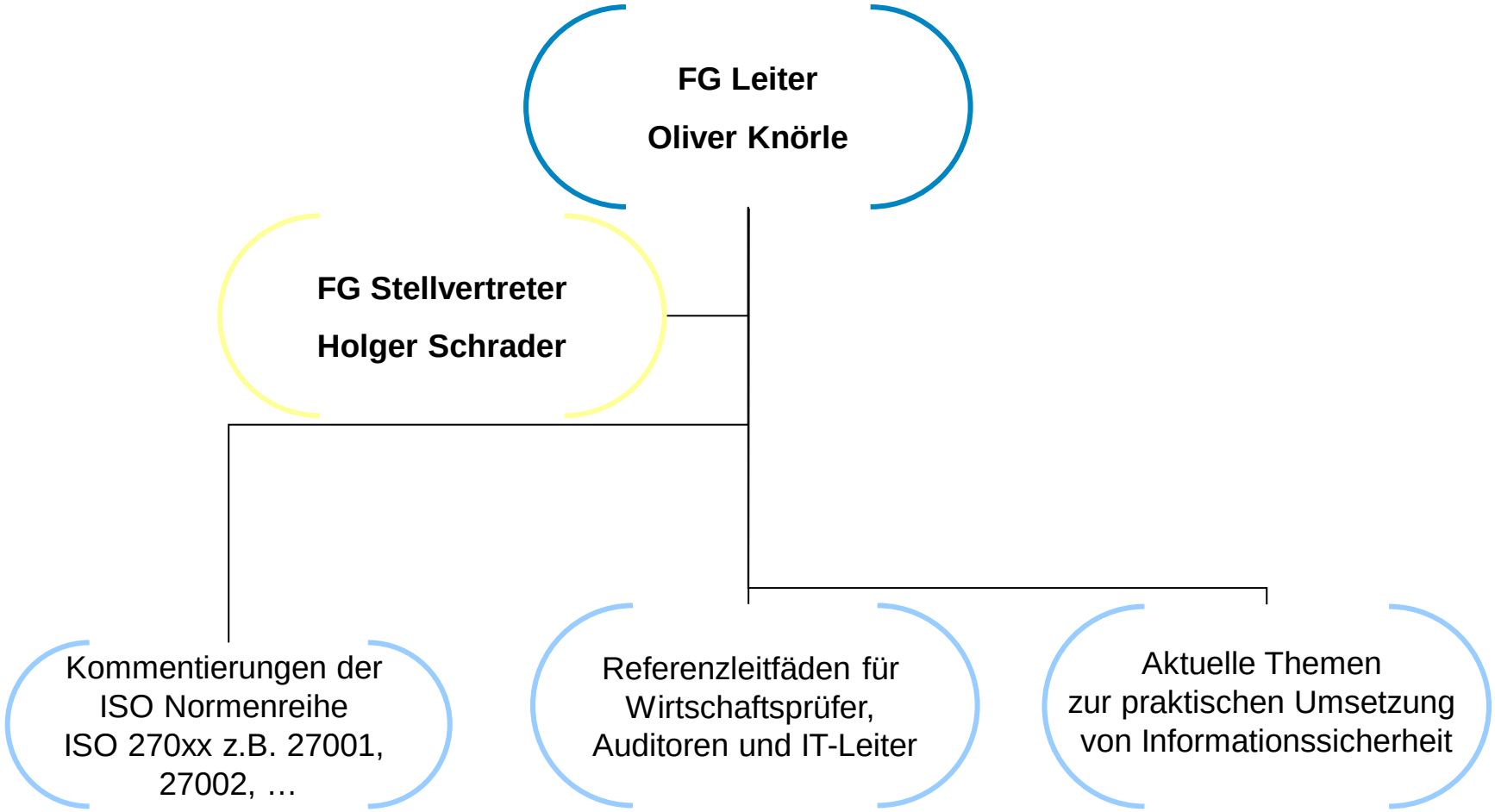
ISACA EXPERTS TOGETHER Germany Chapter

12 Fachthemen, die Sie mitbestimmen können

: Aus- und Weiterbildung
: Cloud Computing
: COBIT Dt. Rechnungslegung
: Datenschutz
: Datenanalyse
: GxP
: Informationssicherheit
: IT Governance
: IT-Revision
: IT-Risiko Management
: Linux Audit Group
: SAP

Die Fachgruppe Informationssicherheit

Übersicht



Die Fachgruppe Informationssicherheit

Fokus und Ziele

: Die Fachgruppe Informationssicherheit bildet sich aus Mitgliedern der ISACA und Gästen, die einen praktischen Bezug zur Informationssicherheit haben.

: Die Mitglieder sind im Rahmen Ihrer beruflichen Tätigkeit als Auditor, Informationssicherheitsbeauftragter, Berater oder IT-Leiter mit dem Themengebiet vertraut.

: **Was sind die wichtigsten Merkmale der Fachgruppe**
- Fachliche Arbeit an aktuellen Themen rund um die Informationssicherheit
- Erfahrungsaustausch zu Fachthemen
- Vorstellung von neuen Methoden, Prozessen und Tools
- Mehrwert für Dritte um die Informationssicherheit mehr in den Vordergrund zu rücken

: **Arbeitsmodi:**
- Physikalische Treffen alle 3-4 Monate zu Gast bei einem FG-Mitglied
- Virtuelle Treffen in Arbeitsgruppen via Telefonkonferenz

- - - - - - - - - - - - - -

: ISACA/Herr Teuscher - Mitwirkung und Kommentierung von ISO Standard
- The ISO Liaison Sub Committee (ILSC)

: ISACA/Herr Teuscher - Mitwirkung und Kommentierung von DIN Standard

Überblick über die ISO27001:2013

Der rote Faden

ISO 270**XX** Familie

ISO 27001 und ISO 27002

ISO Directives Annex SL

Der neue Aufbau der ISO/IEC 27001

Der neue Aufbau der ISO/IEC 27002

Transitions- und Implementierungsleitfaden

Überblick über die ISO27001:2013

Die ISO 270XX Familie

ISACA EXPERTS TOGETHER Germany Chapter

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 on Controls
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.

Überblick über die ISO27001:2013

Nahe Verwandte

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. Inform. and Event Management

Überblick über die ISO27001:2013

Am Anfang war das Wort

: ISO 27002 entstanden aus British Standard 17799
- Praxisorientierte Maßnahmensammlung

: ISO 27001 ist die zertifizierungsfähige Norm
- enthält die sogenannten „Clauses“
  Anforderungen an das Managementsystem

- risikoorientierte technische und organisatorische Anforderungen des Annex A
  (redundante Kurzform der 27002)

Überblick über die ISO27001:2013

Bisherige Version von 2005 / in deutsch von 2008

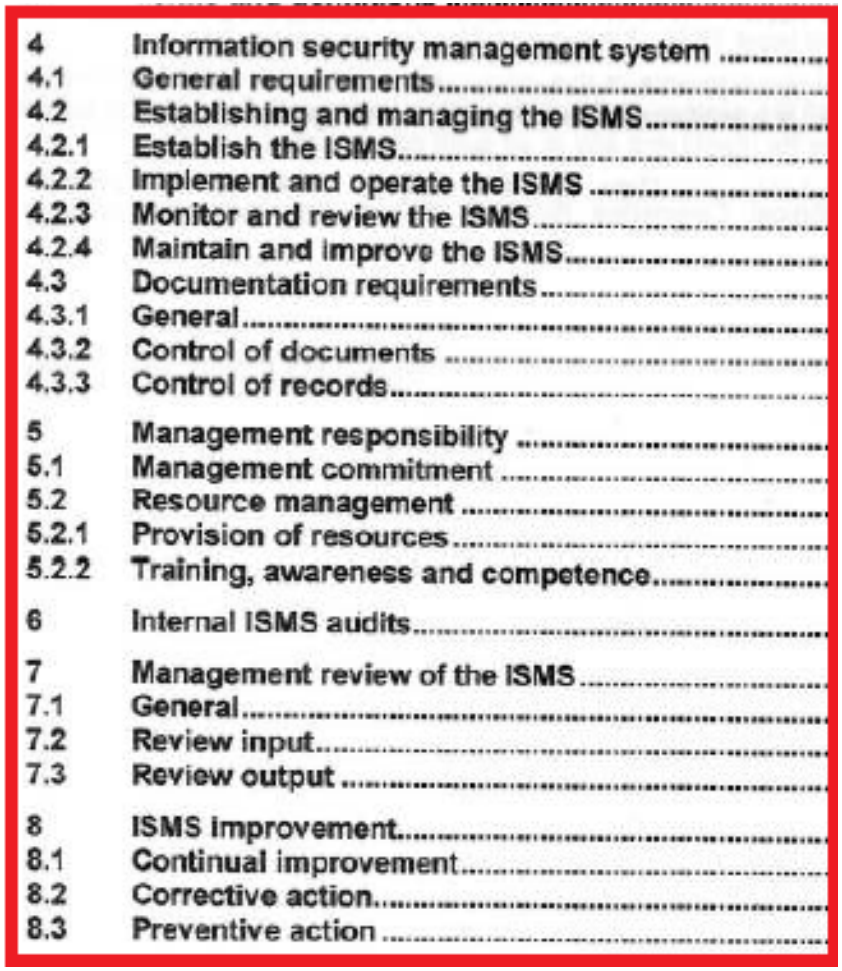
: 4 Managementsystem

: 5 Verantwortungen u. Pflichten des Managements

: 6 Interne Revision

: 7 Review des Systems

: 8 Steuerung des Systems



4	Information security management system
4.1	General requirements
4.2	Establishing and managing the ISMS
4.2.1	Establish the ISMS
4.2.2	Implement and operate the ISMS
4.2.3	Monitor and review the ISMS
4.2.4	Maintain and improve the ISMS
4.3	Documentation requirements
4.3.1	General
4.3.2	Control of documents
4.3.3	Control of records
5	Management responsibility
5.1	Management commitment
5.2	Resource management
5.2.1	Provision of resources
5.2.2	Training, awareness and competence
6	Internal ISMS audits
7	Management review of the ISMS
7.1	General
7.2	Review input
7.3	Review output
8	ISMS improvement
8.1	Continual improvement
8.2	Corrective action
8.3	Preventive action

ISACA Fachgruppe Informationssicherheit:
ISO Directiven

: Veröffentlichung eines
grundsätzlich neuen Ansatzes für ISO Normen

IEC

ISO/IEC DIR IEC SUP

Edition 7.0 2012-05

ISO/IEC Directives Supplement

ISO

ISO/IEC
Directives, Part 1

Consolidated ISO Supplement —
Procedures specific to ISO

High level structure, identical core text and common terms and core definitions for use in Management Systems Standards 131

Quelle: http://www.iso.org/sites/directives/directives.html

Überblick über die ISO27001:2013

Neuer Ansatz in den ISO Normen

Compliance mit
ISO Directives Annex SL für Managementsysteme

Ziel: Vereinfachung integrierter Managementsysteme

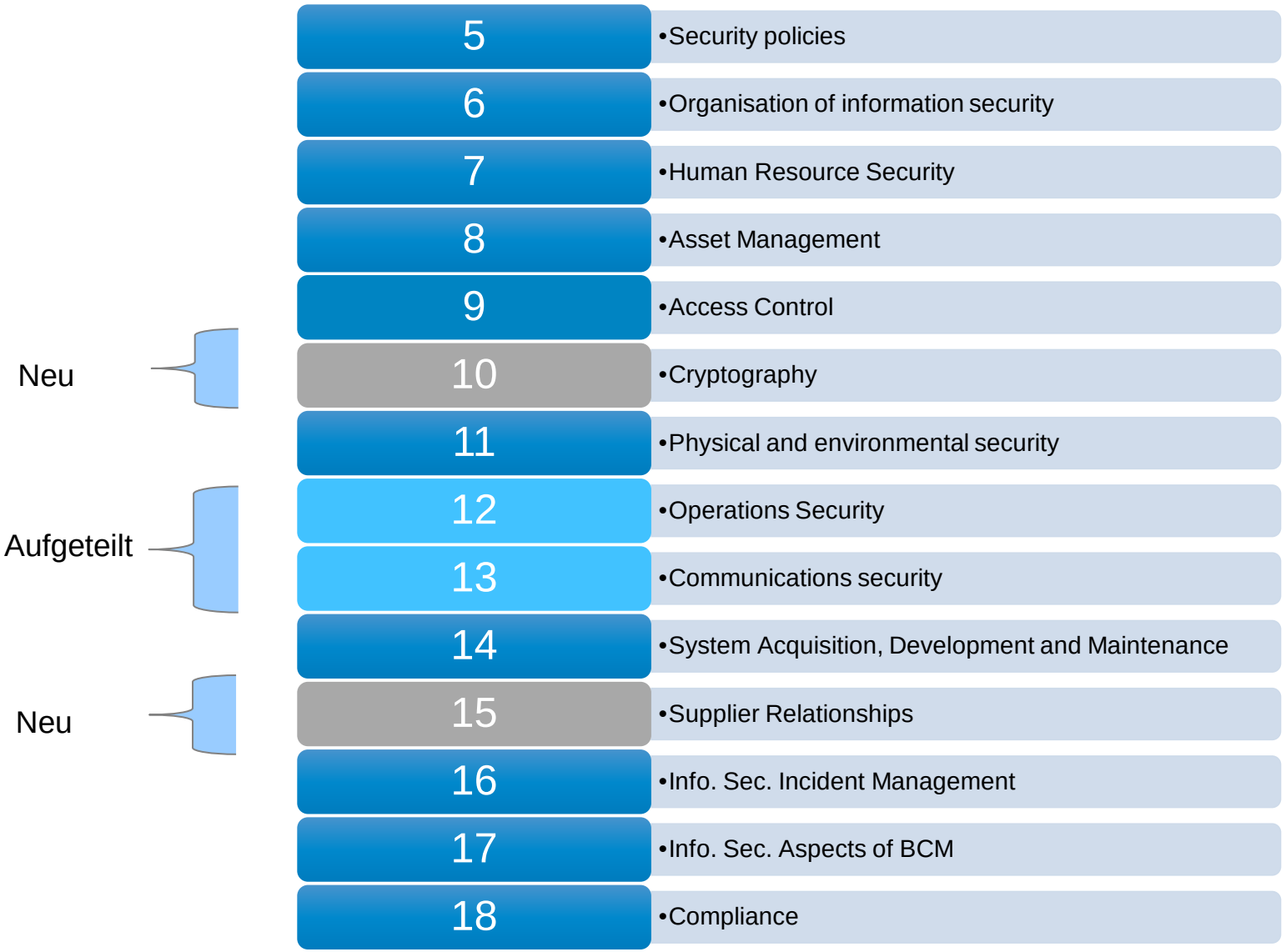
Überblick über die ISO27001:2013

Struktur ISO 27001:2013

5	• Leadership
6	• Planning
7	• Support
8	• Operation
9	• Performance evaluation
10	• Improvement

Struktur ISO 27001:2013

Struktur des Annex A und der ISO 27002



Überblick über die ISO27001:2013

Weiterentwicklung der ISO 27002

: Erneut eigenständig anwendbar

: Klarere Formulierungen dadurch einfachere Implementierung

: Reduktion von Redundanzen

: Aktualisierung und Verschlankung
- ca. 3.000 technische Änderungen

Überblick über die ISO27001:2013

Aktuelle Änderungen in der ISO 27002:2013

ISACA EXPERTS TOGETHER Germany Chapter

ISO 27002

Mobile Devices and Teleworking

- 6.2.1 A policy and supporting security measures should be adopted to protect against the risks introduced by using mobile devices
- Implementation guidance (exerpt):

  „Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas...“

Überblick über die ISO27001:2013

Aktuelle Änderungen in der ISO 27002:2013

ISACA EXPERTS TOGETHER Germany Chapter

27002

Management of technical vulnerabilities

- 12.6 Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization‘s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
- Implementation guidance (exerpt): „… once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken…“

Überblick über die ISO27001:2013

Aktuelle Änderungen in der ISO 27002:2013

27002

Secure Development Policy

- 14.2.1 Rules for the development of software and systems should be established and applied to developments within the organization
- Implementation guidance (exerpt): „… Secure programming techniques should be used both for new developments…“

Überblick über die ISO27001:2013

Aktuelle Änderungen in der ISO 27002:2013

27002

Technical compliance review

- 18.2.3 Information systems should be regularly reviewed for compliance with organization's information security policies and standards.
- Implementation guidance (exerpt): „… Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose…"

Transitions- und Implementierungsleitfaden ISO/IEC 27001:2013

Ziel

praxisorientierte Empfehlungen und Hinweise für Firmen
zum Betrieb eines Informationssicherheitsmanagementsystem (ISMS)
nach der ISO/IEC-Norm 27001:2013

Zielgruppen

: Firmen ohne etabliertes ISMS
  - Aufzeigen von themenbezogen wesentliche Erfolgsfaktoren für die Realisierung eines ISMS nach der ISO/IEC 27001:2013

: Für Firmen mit einem funktionsfähigen ISMS ISO/IEC 27001:2005
mit Zertifizierung oder ohne formale Zertifizierung
  - Hinweise für den Übergang zur ISO/IEC 27001:2013
    Anforderungen der neuen Norm an die Dokumentation.

ISACA Fachgruppe Informationssicherheit:
Transitions- und Implementierungsleitfaden

: Context of the Organization

: Leadership and Commitment

: IS Objectives

: IS Policy

: Roles, Responsibilities and Competencies

: Risk Management

: Documentation

: Improvement

: Communication

: Awareness

: Internal Audit

: Performance Monitoring & KPI

: Supplier Relationship

ISACA Fachgruppe Informationssicherheit:
Transitions- und Implementierungsleitfaden

: Sicht der Autoren relevant und sinnvoll,
über den Inhalt der ISO/IEC 27001:2013 und ISO/IEC 27002:2013

: Verweise auf hilfreiche Normen der ISO/IEC 270xx-Familie sowie weitere relevante ISO-Normen und Industriestandards. Fokus dieser Normen werden dargelegt.

: Es werden konkrete Beispiele anhand typischer Fragestellungen aufgeführt, deren anonymisierte Quellen aus der Praxis stammen.

: Die einzelnen Kapitel sind jeweils identisch in folgende Abschnitte gegliedert:

A. Wesentliche Erfolgsfaktoren aus der Praxis

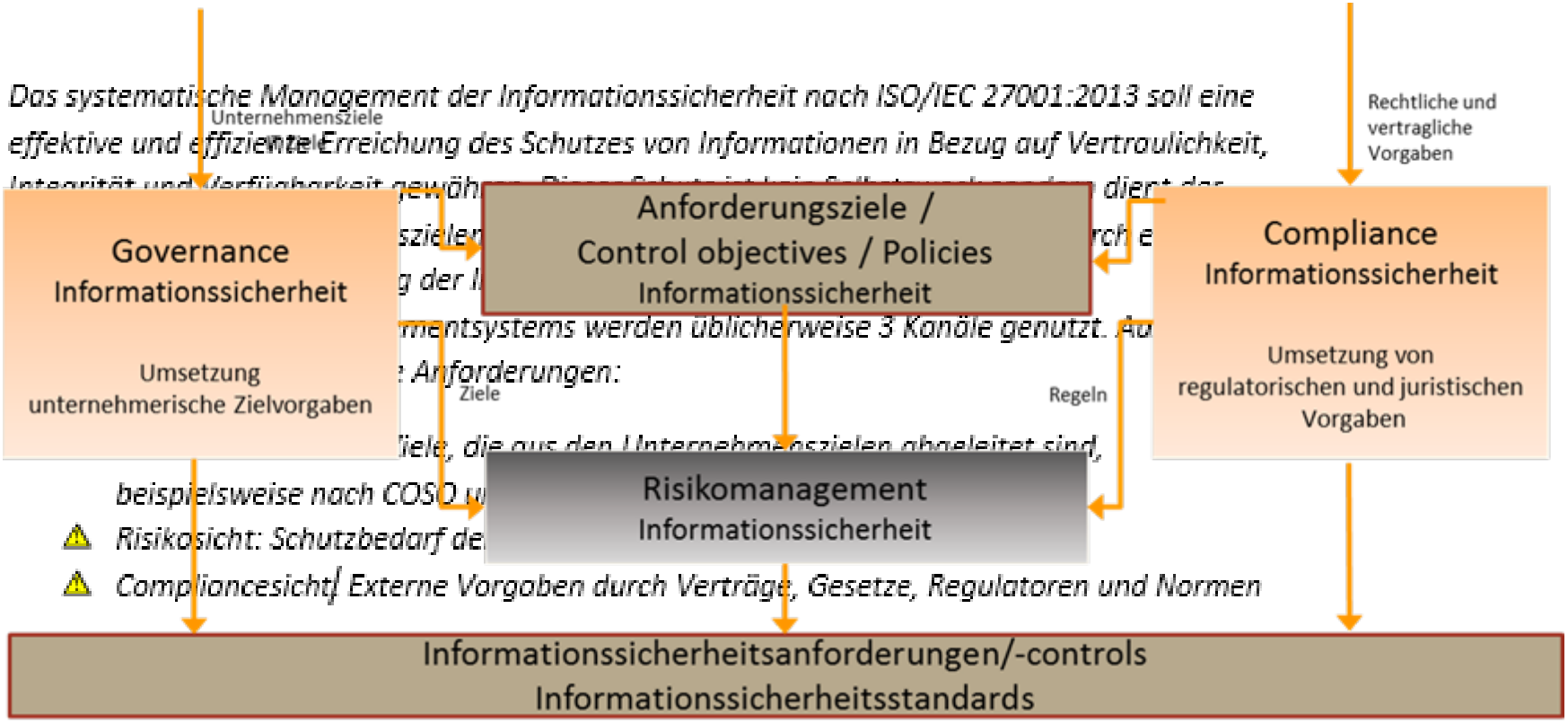
B. Anforderungen an die Dokumentation

C. Änderungen und Vorteile gegenüber ISO/IEC 27001:2005

D. Referenzen

Beispiel: Performance Monitoring & KPI

Wesentliche Erfolgsfaktoren aus der Praxis



Beispiel: Performance Monitoring & KPI

Anforderungen an die Dokumentation

Zusammenfassung zum Thema Dokumentation unterteilt nach „Aus der Praxis" und „normativ".

Normative Dokumentationspflicht:

- Die Organisation muss angemessen dokumentierte Informationen als Nachweise für die Überwachung und den gemessenen Ergebnissen aufbewahren.

Dokumentationen aus der Praxis:

- Dokumentation der Messstruktur für alle KPIs.
  - Mess- und welche Berechnungsmethoden, die zur Messung, Analyse und Bewertung herangezogen werden
    So können reproduzierbare Ergebnisse erzeugt werden
  - Beschreibung des Messobjektes, welches gemessen und bewertet wurde.
    z.B. Security Prozess und Maßnahme
  - Zeitpunkt und Frequenz der Messung
  - Verantwortlicher für die Messung
  - Zeitpunkt und Frequenz der Analyse und Bewertung
  - Verantwortlicher für die Analyse
- Ergebnisse der Messungen und die daraus abgeleiteten Managementberichte zur Eskalation.

Beispiel: Performance Monitoring & KPI

Änderungen und Vorteile gegenüber ISO/IEC 27001:2005

Während in der vorherigen Version des ISO27001 Standards die Effektivitätsmessung von Sicherheitsmaßnahmen als ein Unterpunkt des Management Reviews war und die in der ISO27004:2009 nur als Empfehlung galten, sind nun klare Anforderungen aus der ISO 27004:2009 in die zertifizierungsfähige ISO 27001 übergegangen.

Dadurch werden die im vorherigen Kapitel genannten Dokumentationsanforderungen verpflichtend für die Zertifizierung.

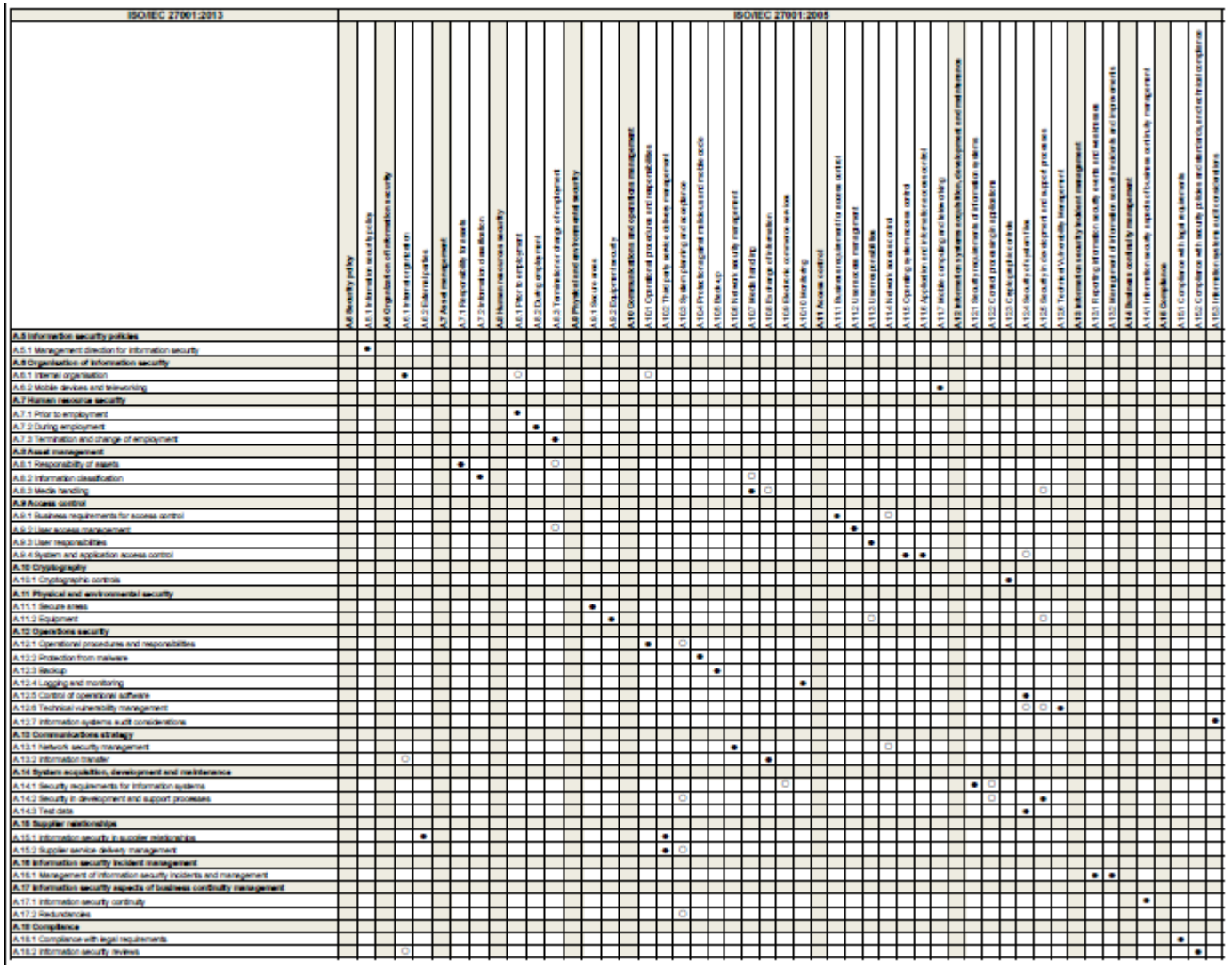
Referenzen

Kapitel, ISO/IEC 27001:2013 – 9.1

Kapitel, ISO/IEC 27004:2009 – 5,6,7,8,9,10 Annex A

ISACA Fachgruppe Informationssicherheit:
Transitions- und Implementierungsleitfaden

ISACA EXPERTS TOGETHER Germany Chapter



Es war mir ein Vergnügen!

Holger Schrader
Principal Consultant der CARMAO GmbH

Stellvertretender Leiter
der Fachgruppe Informationssicherheit
ISACA Germany Chapter