

HERZLICH WILLKOMMEN



Holger Schrader

Principal Consultant der CARMAO GmbH

**Stellvertretender Leiter
der Fachgruppe Informationssicherheit
ISACA Germany Chapter**

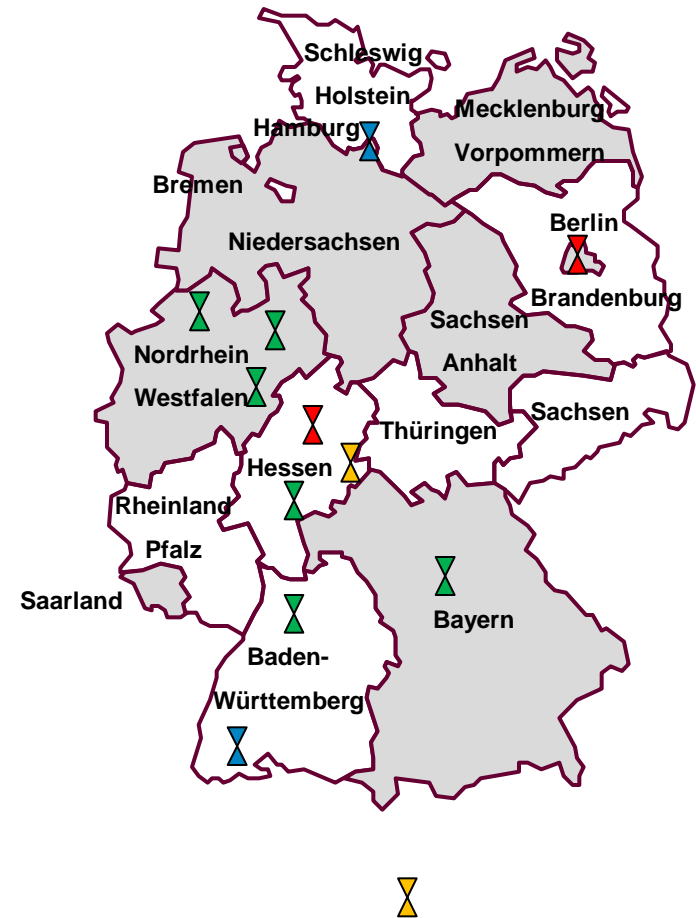
... seit 1998 tätig in den Themen

- IT Sicherheit
- Informationssicherheit
- Risikomanagement tätig

CISM, CRISC, Cyber Security Practitioner
und
Blutspender

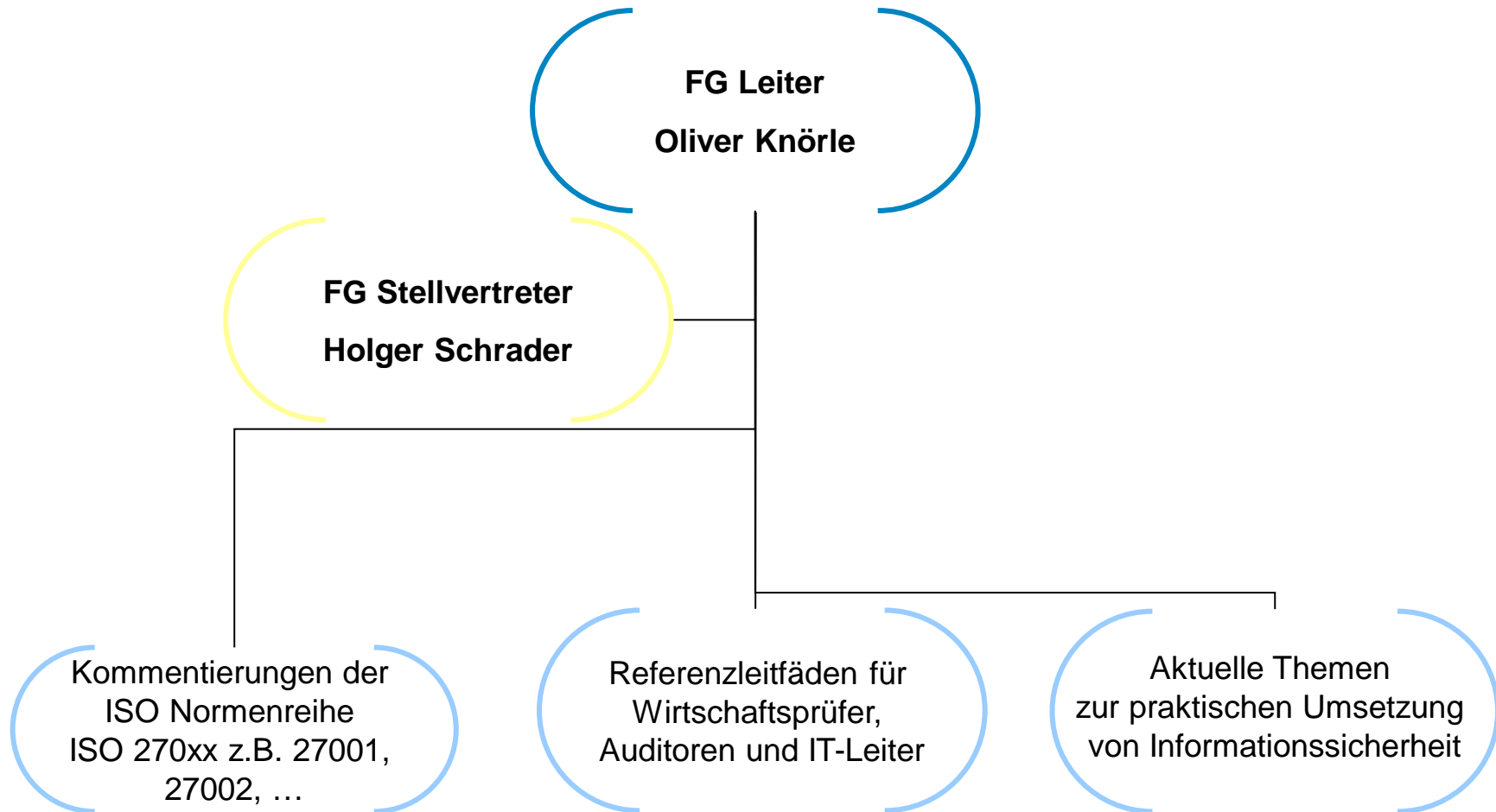
12 Fachthemen, die Sie mitbestimmen können

- : 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 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 270XX 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

27000	• Terms and Definitions	27006	• Req. For Certification Bodies
27001	• Requirements	27007	• Guidelines to Auditing
27002	• Code of Practice	27008	• Guidelines for Auditors on Controls
27003	• Implementation Guidance	27010	• Inter sector inter org. comm.
27004	• Measurements	27011	• Sector Telecommunication
27005	• IS Risk Management	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)

bsi.



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

- : Veröffentlichung eines grundsätzlich neuen Ansatzes für ISO Normen



ISO/IEC DIR IEC SUP

Edition 7.0 2012-05

ISO/IEC Directives Supplement



**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>

Compliance mit ISO Directives Annex SL für Managementsysteme

Ziel: Vereinfachung
integrierter
Managementsysteme

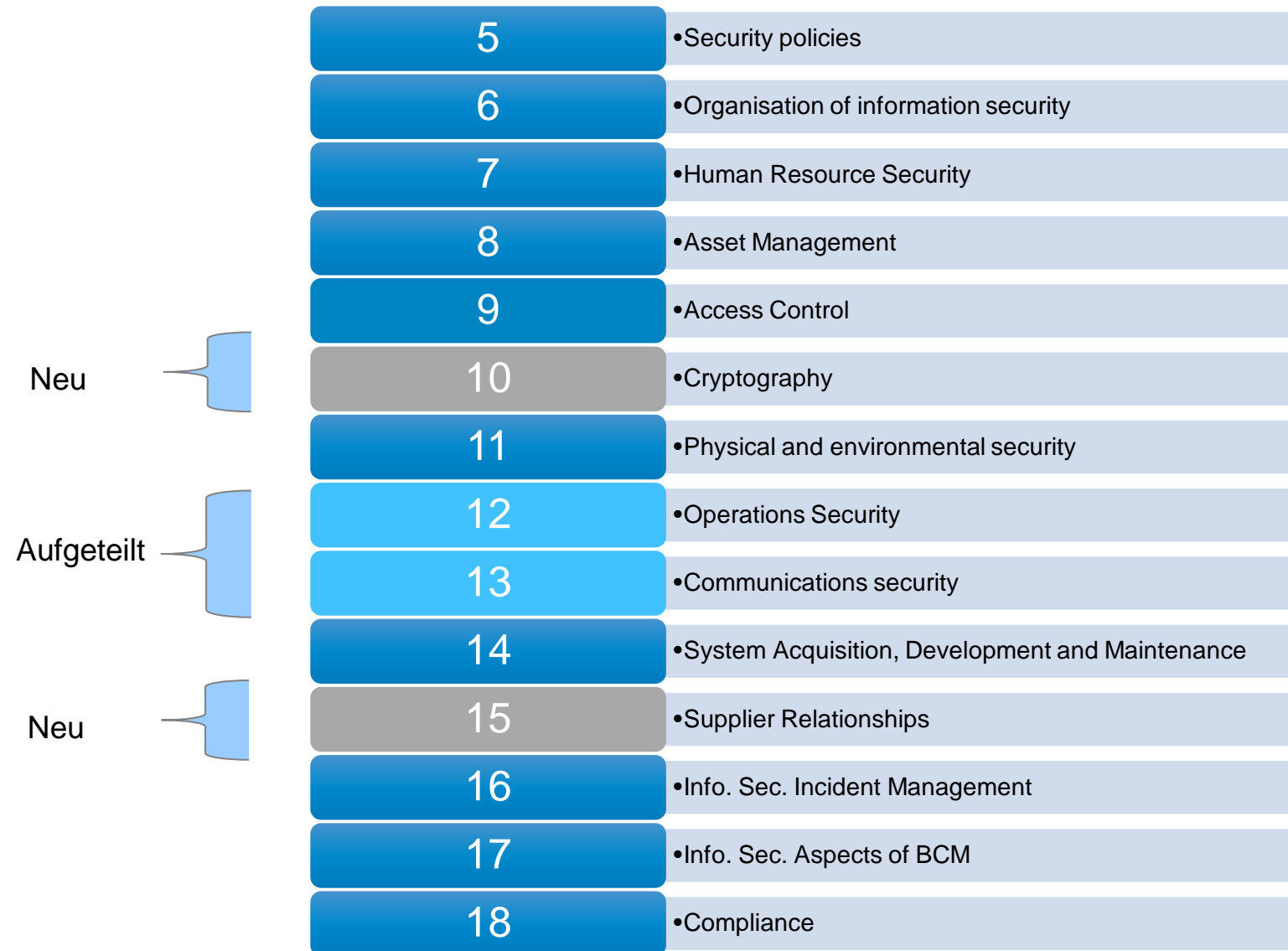
Überblick über die ISO27001:2013

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 Verschlankeung
 - ca. 3.000 technische Änderungen



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

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 (excerpt):
„... once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken...“

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 (excerpt):
„... Secure programming techniques should be used both for new developments...“

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 (excerpt):
„... 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 themenbezogenen 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

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

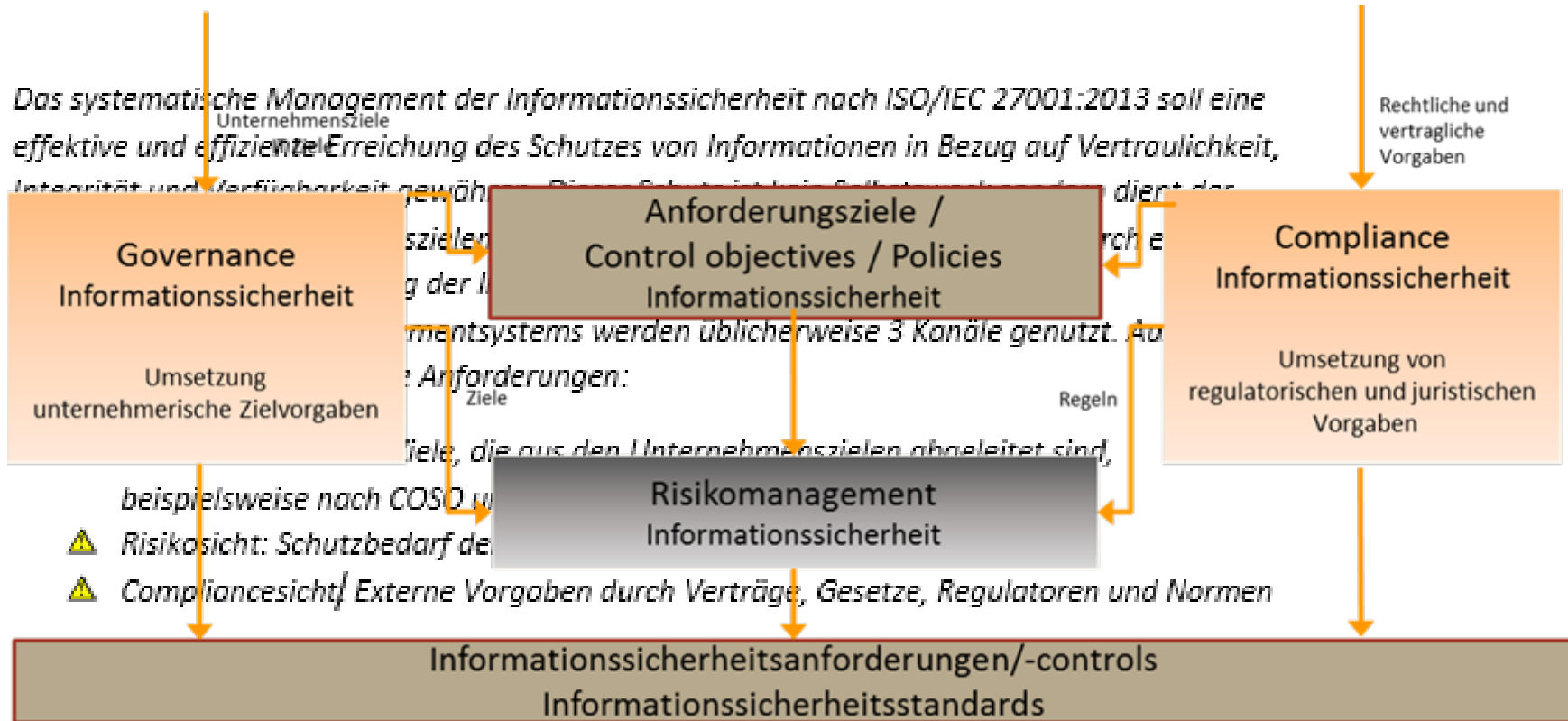
- : Verweise auf hilfreiche Normen der ISO/IEC 270xx-Familie sowie weitere relevante ISO-Normen und Industriestandards. Fokus dieser Normen werden dargelegt.

- : 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

ISO/IEC 27001:2013	ISO/IEC 27001:2005
	<ul style="list-style-type: none"> A6 Security policy A6.1 Internet security policy A6.2 Organisation of information security A6.3 Internal organization A6.4 Internal roles A7 Asset management A7.1 Responsibility to users A7.2 Internet classification A7.3 Internet classification A7.4 Internet classification A7.5 Internet classification A7.6 Internet classification A7.7 Internet classification A7.8 Internet classification A7.9 Internet classification A7.10 Internet classification A7.11 Internet classification A7.12 Internet classification A7.13 Internet classification A7.14 Internet classification A7.15 Internet classification A7.16 Internet classification A7.17 Internet classification A7.18 Internet classification A7.19 Internet classification A7.20 Internet classification A7.21 Internet classification A7.22 Internet classification A7.23 Internet classification A7.24 Internet classification A7.25 Internet classification A7.26 Internet classification A7.27 Internet classification A7.28 Internet classification A7.29 Internet classification A7.30 Internet classification A7.31 Internet classification A7.32 Internet classification A7.33 Internet classification A7.34 Internet classification A7.35 Internet classification A7.36 Internet classification A7.37 Internet classification A7.38 Internet classification A7.39 Internet classification A7.40 Internet classification A7.41 Internet classification A7.42 Internet classification A7.43 Internet classification A7.44 Internet classification A7.45 Internet classification A7.46 Internet classification A7.47 Internet classification A7.48 Internet classification A7.49 Internet classification A7.50 Internet classification A7.51 Internet classification A7.52 Internet classification A7.53 Internet classification A7.54 Internet classification A7.55 Internet classification A7.56 Internet classification A7.57 Internet classification A7.58 Internet classification A7.59 Internet classification A7.60 Internet classification A7.61 Internet classification A7.62 Internet classification A7.63 Internet classification A7.64 Internet classification A7.65 Internet classification A7.66 Internet classification A7.67 Internet classification A7.68 Internet classification A7.69 Internet classification A7.70 Internet classification A7.71 Internet classification A7.72 Internet classification A7.73 Internet classification A7.74 Internet classification A7.75 Internet classification A7.76 Internet classification A7.77 Internet classification A7.78 Internet classification A7.79 Internet classification A7.80 Internet classification A7.81 Internet classification A7.82 Internet classification A7.83 Internet classification A7.84 Internet classification A7.85 Internet classification A7.86 Internet classification A7.87 Internet classification A7.88 Internet classification A7.89 Internet classification A7.90 Internet classification A7.91 Internet classification A7.92 Internet classification A7.93 Internet classification A7.94 Internet classification A7.95 Internet classification A7.96 Internet classification A7.97 Internet classification A7.98 Internet classification A7.99 Internet classification A7.100 Internet classification
A.5 Information security policies	
A.5.1 Management direction for information security	<input checked="" type="checkbox"/>
A.6 Organisation of information security	
A.6.1 Internal organization	<input checked="" type="checkbox"/>
A.6.2 Mobile devices and teleworking	<input type="checkbox"/>
A.7 Human resource security	
A.7.1 Staff to employment	<input checked="" type="checkbox"/>
A.7.2 Staff employment	<input checked="" type="checkbox"/>
A.7.3 Termination and change of employment	<input checked="" type="checkbox"/>
A.8 Asset management	
A.8.1 Responsibility of assets	<input checked="" type="checkbox"/>
A.8.2 Information classification	<input checked="" type="checkbox"/>
A.8.3 Media handling	<input checked="" type="checkbox"/>
A.9 Access control	
A.9.1 Business requirements for access control	<input checked="" type="checkbox"/>
A.9.2 User access management	<input checked="" type="checkbox"/>
A.9.3 User responsibilities	<input checked="" type="checkbox"/>
A.9.4 System and application access control	<input checked="" type="checkbox"/>
A.10 Cryptographic	
A.10.1 Cryptographic controls	<input checked="" type="checkbox"/>
A.11 Physical and environmental security	
A.11.1 Secure areas	<input checked="" type="checkbox"/>
A.11.2 Equipment	<input checked="" type="checkbox"/>
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	<input checked="" type="checkbox"/>
A.12.2 Protection from malware	<input checked="" type="checkbox"/>
A.12.3 Security	<input checked="" type="checkbox"/>
A.12.4 Configuration and monitoring	<input checked="" type="checkbox"/>
A.12.5 Control of operational software	<input checked="" type="checkbox"/>
A.12.6 Technical vulnerability management	<input checked="" type="checkbox"/>
A.12.7 Information systems asset considerations	<input checked="" type="checkbox"/>
A.13 Communications strategy	
A.13.1 Network security management	<input checked="" type="checkbox"/>
A.13.2 Information transfer	<input checked="" type="checkbox"/>
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements for information systems	<input checked="" type="checkbox"/>
A.14.2 Security in development and support processes	<input checked="" type="checkbox"/>
A.14.3 Test data	<input checked="" type="checkbox"/>
A.15 Supplier relationships	
A.15.1 Information security in supplier relationships	<input checked="" type="checkbox"/>
A.15.2 Supplier service delivery management	<input checked="" type="checkbox"/>
A.16 Information security incident management	
A.16.1 Management of information security incidents and management	<input checked="" type="checkbox"/>
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	<input checked="" type="checkbox"/>
A.17.2 Redundancies	<input checked="" type="checkbox"/>
A.18 Compliance	
A.18.1 Compliance with legal requirements	<input checked="" type="checkbox"/>
A.18.2 Information security reviews	<input checked="" type="checkbox"/>

Es war mir ein Vergnügen!



Holger Schrader

Principal Consultant der CARMAO GmbH

**Stellvertretender Leiter
der Fachgruppe Informationssicherheit
ISACA Germany Chapter**