managementsysteme by migosens

EINFÜHRUNG EINES **INFORMATIONS-SICHERHEITS-MANAGEMENT-**SYSTEMS

Fachtagung Datenschutz im Gesundheitswesen 2023

Heiko Gossen, migosens

Persönliche Vorstellung

managementsysteme by migosens

- Lead Auditor ISO 27001 i.A. der TÜV Rheinland Cert GmbH
- Datenschutzauditor (TÜVCert)
- Ext. Datenschutzbeauftragter verschiedener Unternehmen
- Network Security Engineer
- Vorsitzender des Bitkom AK Datenschutzes

HEIKO GOSSEN
Geschäftsführer

migosens GmbH
Wiesenstraße 35
45473 Mülheim an der Ruhr
Tel. 0208 / 99395110
heiko.gossen@migosens.de

https://www.linkedin.com/in/heiko-gossen-2a5a9a1b7/

https://www.migosens.de

Unser Serviceportfolio gliedert sich in vier Bereiche

managementsysteme by migosens

migosens

datenschutz

Strategische und operative Beratung

Audits (intern/extern)

Datenschutzbeauftragter

branchenübergreifende Datenschutzkonzepte

Projektbegleitung

managementssysteme*

Beratung

Audits (intern/extern)

Informationssicherheits- und Qualitätsmanagementbeauftragter

Einführung von Managementsystemen für Informationssicherheit, Datenschutz, Qualität und Business Continuity

worksmart

Führung und Zusammenarbeit

Organisationsentwicklung

Arbeitsumfeld gestalten

akademie

Datenschutzbeauftragten-Ausbildung

Projekte und Prozesse

Informationssicherheit

Integrierte Managementsysteme

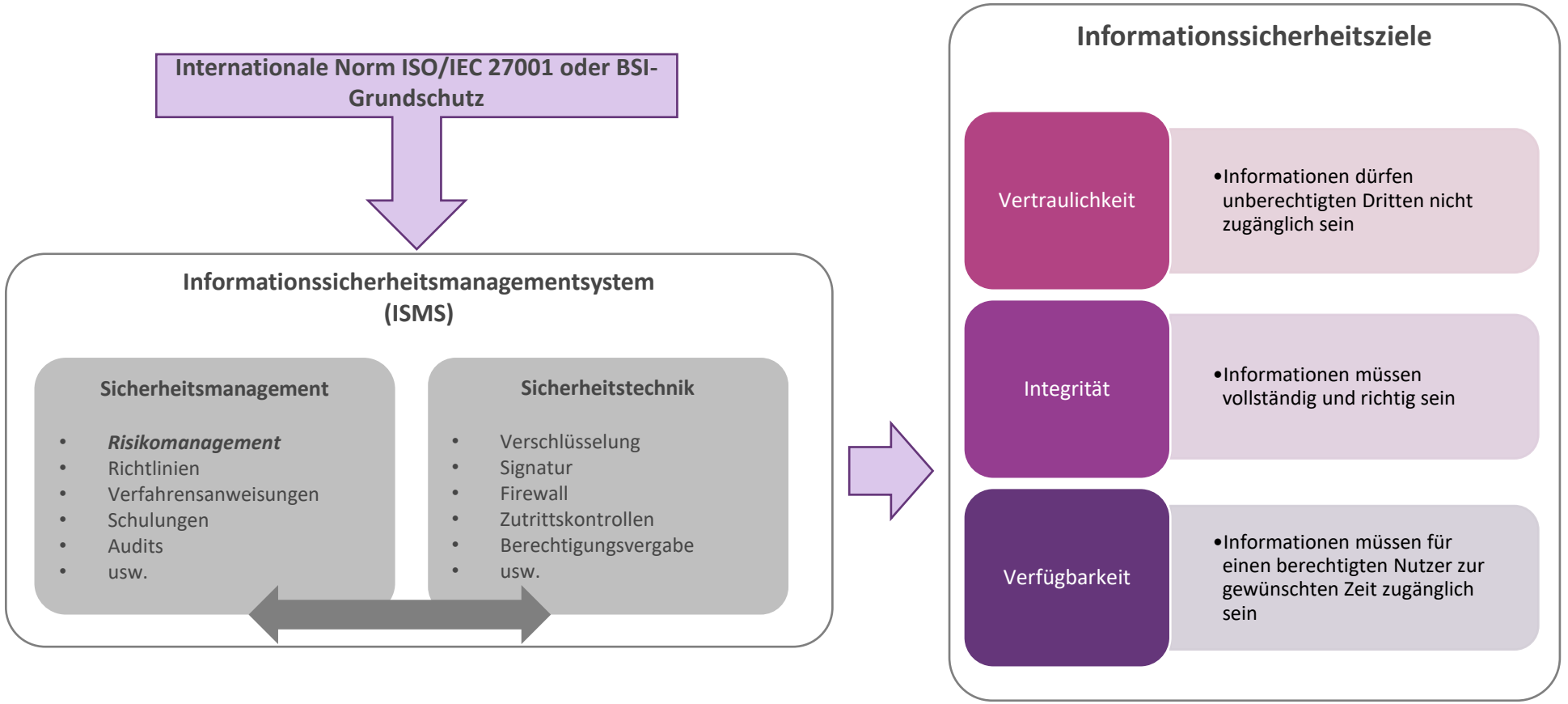
ERFAHRUNG. WISSEN. BERATUNG.

* ein Angebot der migosens management GmbH

Agenda

managementsysteme by migosens

Informationssicherheit muss gesteuert werden!



Vorteile einer ISO 27001 Zertifizierung

managementsysteme by migosens

Wettbewerbs-vorteile

Wettbewerbs-vorteile durch einen **internationalen Standard**

Risiko-Identifikation

Systematische Identifizierung der **IT-Risiken** und möglicher **Schäden**

Audits

Reduzierung von **Audits** durch Kunden

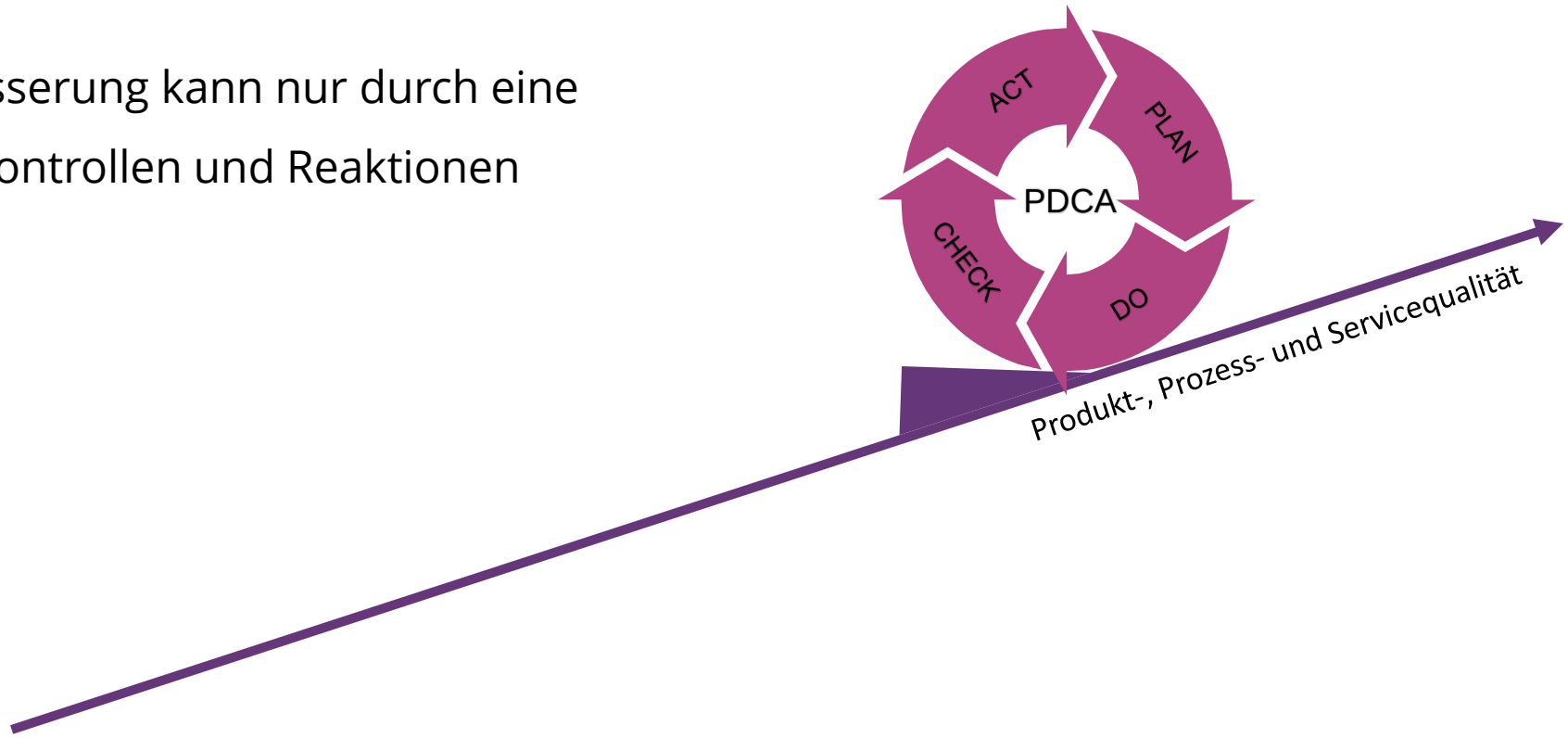
Bewusstsein

Erhöhtes **Bewusstsein** für **Informations-sicherheit** im Unternehmen

Allgemeine Definition eines Managementsystems

Grundgedanke eines Managementsystems

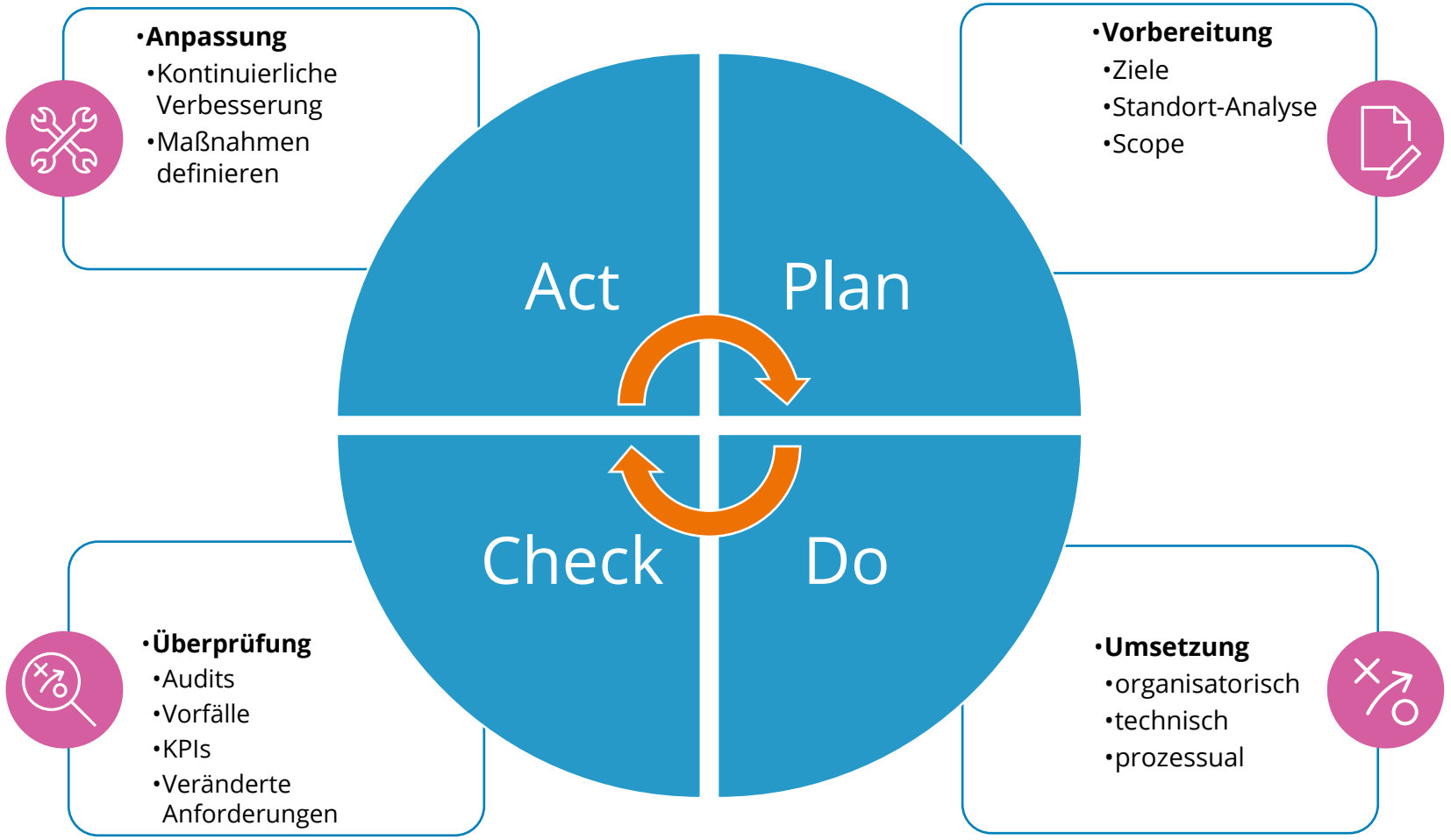
- Der Deming-Kreis war lange Zeit expliziter Bestandteil der ISO 9001 und ISO 27001
- Eine kontinuierliche Verbesserung kann nur durch eine adäquate Steuerung von Kontrollen und Reaktionen sichergestellt werden.



Managementsysteme allgemein | Der PDCA-Zyklus

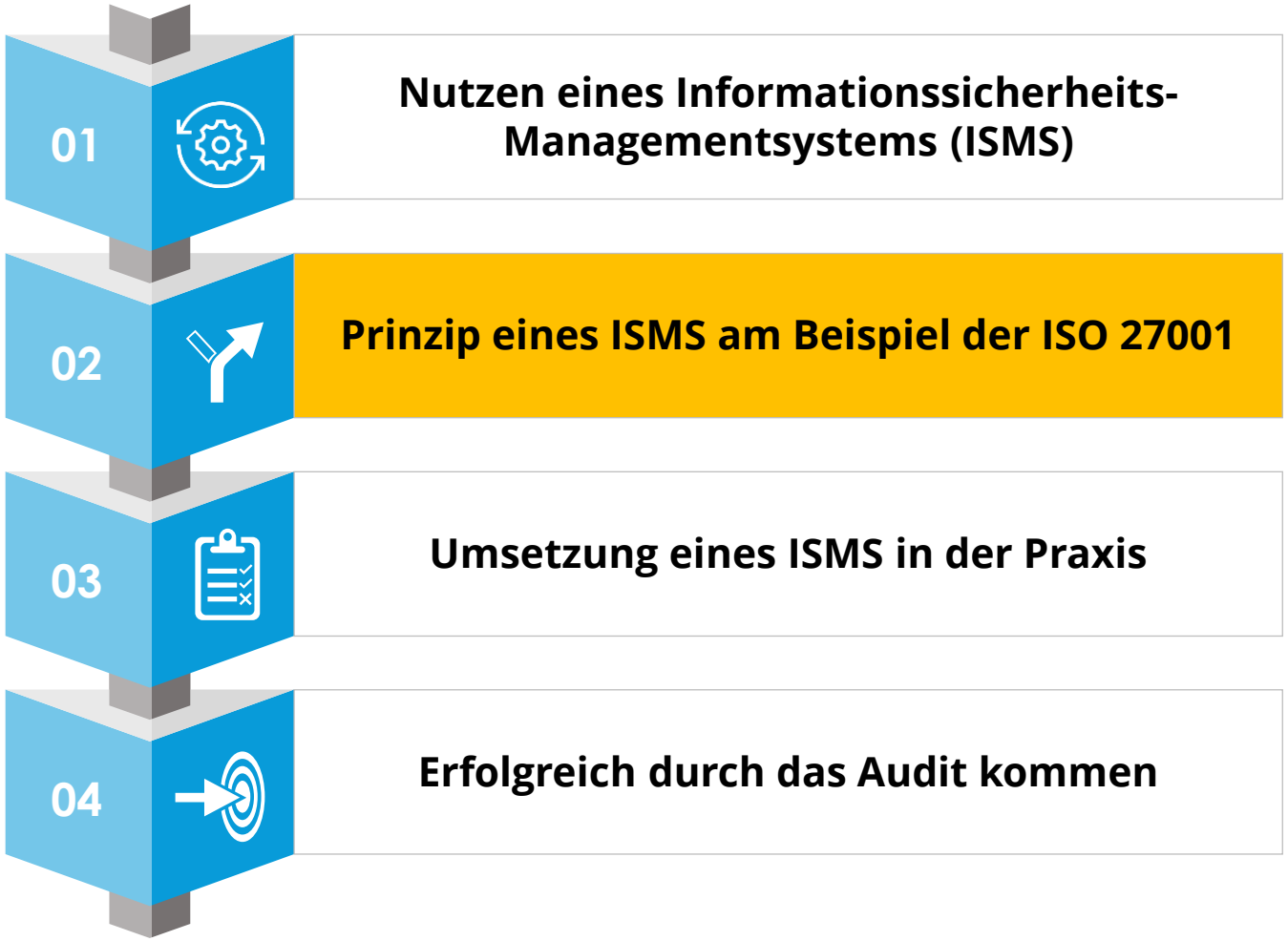
managementsysteme by migosens

- Qualität (ISO 9001)
- Umwelt (ISO 14001)
- IT Service (ISO 20001)
- BCM (ISO 22301)
- Informationssicherheit (ISO 27001)
- Risikomanagement (ISO 31000)
- u.v.a.



Agenda

managementsysteme by migosens



Die ISO/IEC 27001 und ISO/IEC 27002

managementsysteme by migosens


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

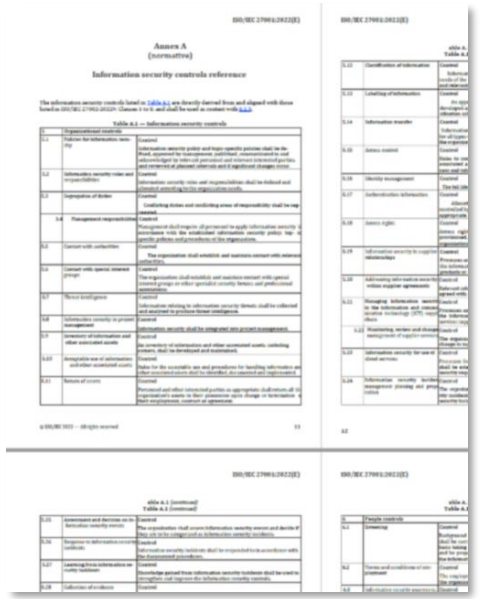
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

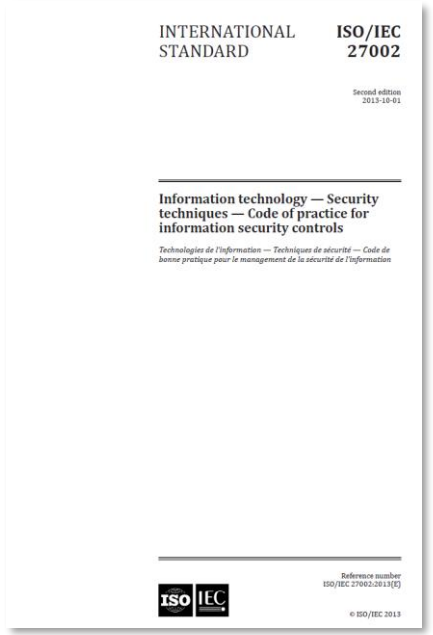
Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022


Information security, cybersecurity and privacy protection — Information security management systems — Requirements


Annex A
(normative)

Information security controls reference


INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

© ISO/IEC 2013

Normativ

Best Practice

Übersicht der ISO 27000 – Normenreihe (Auszug)

managementsysteme by migosens

Überblick & Begriffe	27000			
Anforderungen	ISMS 27001	Datenschutzmgmt. 27701	Akkreditierung Zert-Stellen 27006	Struktur Sektor-Leitlinien 27009
Leitlinien	Anleitung ISO 27001 Anh. A 27002	Vorgehen bei ISO 27001 27003	ISMS-Bewertung 27004	IS-Risikomanagement 27005
	Audits (ergänzt ISO 19011) 27007	Auditbewertungen TR 27008	Integration ISO 20000-1 27013	IS-Governance 27014
	Betriebswirtschaftliche Bewertung TR 27016	Kompetenz 27021		
Sektorspezifische Leitlinien	übergreifend 27010	Telekommunikation 27011	Cloud-Dienstleister allgemein 27017	Cloud-Auftragsver-arbeiter 27018
	Energieversorger 27019	Gesundheit 27799		

Managementsysteme allgemein | High Level Structure (HLS)

managementsysteme by migosens

- Qualität (ISO 9001)
- Umwelt (ISO 14001)
- IT Service (ISO 20001)
- BCM (ISO 22301)
- Informationssicherheit (ISO 27001)
- Risikomanagement (ISO 31000)
- u.v.a.

4 Kontext der Organisation	Plan
5 Führung	
6 Planung	
7 Unterstützung	Do
8 Betrieb	
9 Leistung und Evaluierung	Check
10 Verbesserung	Act

4 Kontext der Organisation

managementsysteme by migosens

4
Kontext der Organisation

5
Führung

6
Planung

7
Unterstützung

8
Betrieb

9
Leistung und Evaluierung

10
Verbesserung

- Geltungsbereich des ISMS festlegen
- Beschreibung der Organisation
- Regulatorische Anforderungen identifizieren
- Erwartungen der Interessierten verstehen

Plan

Do

Check

Act

5 Führung

managementsysteme by migosens

4
Kontext der Organisation

5
Führung

6
Planung

7
Unterstützung

8
Betrieb

9
Leistung und Evaluierung

10
Verbesserung

- Commitment des Managements
- Leitlinie
- Festlegung von Rollen und Verantwortlichkeiten

Plan

Do

Check

Act

6 Planung

managementsysteme by migosens

4
Kontext der Organisation

5
Führung

6
Planung

7
Unterstützung

8
Betrieb

9
Leistung und Evaluierung

10
Verbesserung

- Durchführung Risk Assessment
- Risikobehandlung
- Ziele und Planung zur Umsetzung

Plan

Do

Check

Act

7 Unterstützung

managementsysteme by migosens

4 Kontext der Organisation

5 Führung

6 Planung

7 Unterstützung

8 Betrieb

9 Leistung und Evaluierung

10 Verbesserung

Plan

Do

- Festlegung und Klärung von Ressourcen, Kompetenzen
- Sensibilisierung der Beteiligten
- Kommunikation
- Dokumentation
  - Form, Umfang
  - Tools
  - Pflege
  - Lenkung

Check

Act

8 Betrieb

managementsysteme by migosens

4 Kontext der Organisation

5 Führung

6 Planung

7 Unterstützung

8 Betrieb

9 Leistung und Evaluierung

10 Verbesserung

Plan

Do

- Laufender Betrieb
  - Einbindung in die operativen Prozesse
  - Beratung von Projekten
  - Bewertung von Veränderungen
  - Vorfälle
  - …
- regelmäßige Überprüfung der Risikobewertungen und -behandlung

Check

Act

9 Leistung und Evaluierung

managementsysteme by migosens

4 Kontext der Organisation

5 Führung

6 Planung

7 Unterstützung

8 Betrieb

9 Leistung und Evaluierung

10 Verbesserung

Plan

Do

Check

- Monitoring, Analyse, Bewertung von Kennzahlen
- Interne Audits (inkl. Auditprogramm)
- Formale Berichterstattung und Abstimmung mit dem obersten Management

Act

10 Verbesserung

managementsysteme by migosens

4 Kontext der Organisation

5 Führung

6 Planung

7 Unterstützung

8 Betrieb

9 Leistung und Evaluierung

10 Verbesserung

Plan

Do

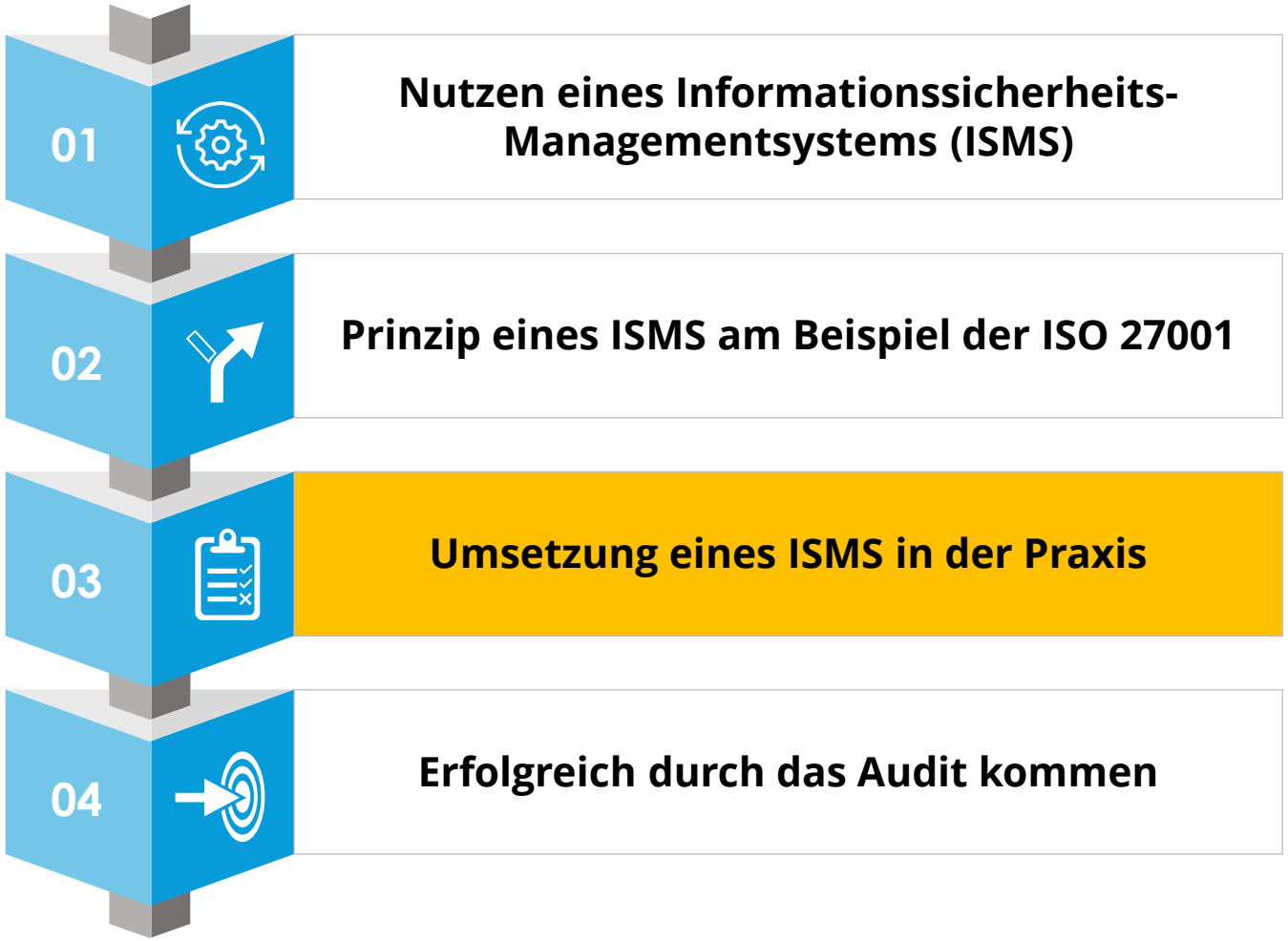
Check

Act

- Identifizierung von Verbesserungspotentialen
  - aus Vorfällen
  - aus internen Audits
  - aus Kundenaudits
- Kontinuierliche Verbesserung

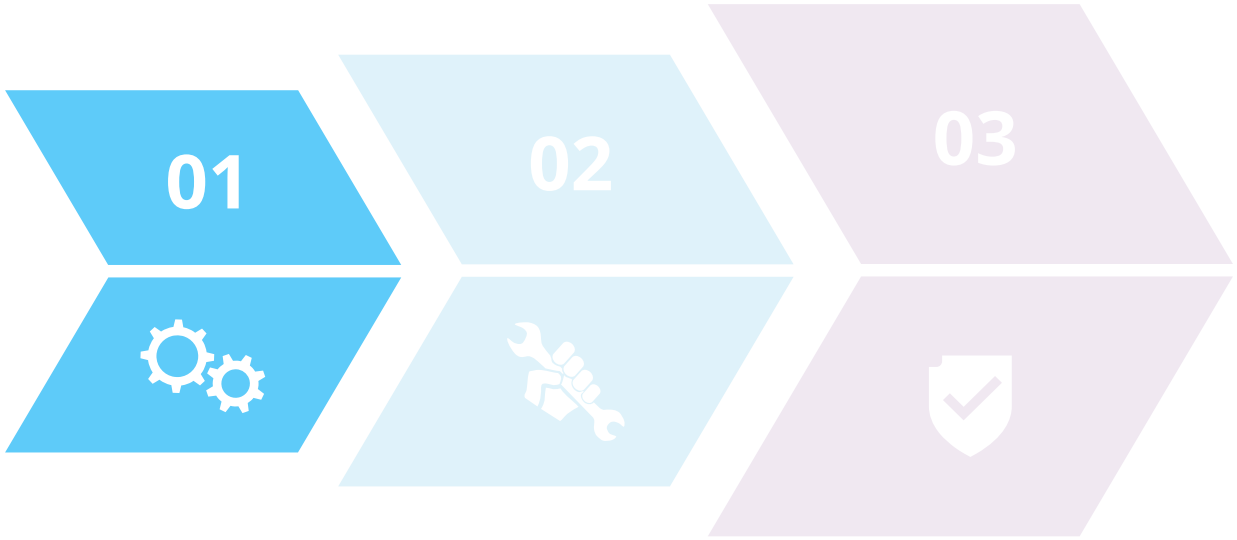
Agenda

managementsysteme by migosens



Implementierung eines ISMS in 3 Phasen

managementsysteme by migosens



1 Vorbereitung

Bestandsaufnahme, Ermittlung des Gestaltungsbereichs, Projektplanung, Maßnahmenplan

2 Aufbau des ISMS

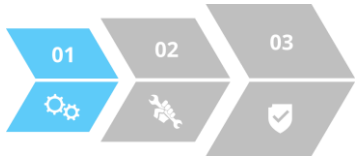
Assetmanagement, Risikomanagement, Dokumentationsstruktur, Awareness

3 Herstellung der Zertifizierungsreife

Maßnahmenbehandlung, Operative Integration, Bewertung, Auditbegleitung

Gute Vorbereitung ist für eine zielgerichtete Implementierung eine wichtige Grundlage

managementsysteme by migosens



Vorbereitung

Bestandsaufnahme

- **Bestimmung** der **Anforderungen**
- **Prüfung** von **Schnittstellen**
- Status Quo **erfassen**
- **Gaps** inkl. notwendiger Maßnahmen **identifizieren**
- Vorbereitung einer **Management-Entscheidung**

Ermittlung des Geltungsbereichs

- **Business Impact Analysis**: Ermittlung der Assets für den zu zertifizierenden Geschäftsprozess
- **Festlegung der Ziele und des Geltungsbereiches** technisch, rechtlich, organisatorisch
- Identifizierung von **Schnittstellen**

Projektplanung

- **Faktenbasierte Aufwandsbestimmung** auf Basis der Prüfergebnisse
- **Erstellung eines Zeitplanes** für die Implementierung
- **Zeitliche Budgetierung** (Ressourcenfestlegung) der einzelnen Projektschritte

Maßnahmenplan

- **Erstellung und Abstimmung** eines **Maßnahmenplans** mit den Maßnahmen aus der Bestandsaufnahme
- **Festlegung** der **Verantwortlichkeiten** und **Umsetzungszielen**
- **Permanentes Controlling** des Maßnahmenplanes und Unterstützung bei der **Abarbeitung der Maßnahmen**

Planung

managementsysteme by migosens

Warum ist eine Kalkulation wichtig?	• Vermeidung von Überlastung oder Unterbesetzung im Projektteam • Sicherstellung einer erfolgreichen Implementierung
Interne Ressourcen	• Definition von internen Ressourcen (z.B. Mitarbeiter, Zeit, Budget) • Welche Abteilungen sind betroffen? (IT, Compliance, Datenschutz etc.) • Wieviel Zeit wird benötigt? (Projektplanung)
Externe Ressourcen	• Definition von externen Ressourcen (z.B. Berater, Auditoren) • Wieviel Budget wird benötigt?
Faktoren zur Berechnung der benötigten Ressourcen	• Größe des Unternehmens (Anzahl der Mitarbeiter, Standorte etc.) • Komplexität des IT-Umfelds (Systeme, Anwendungen etc.) • Erfahrung im Bereich Informationssicherheit

Eine sorgfältige Kalkulation kann entscheidend für eine erfolgreiche Implementierung eines ISMS nach ISO 27001 sein!

Verantwortlichkeiten

Diese Verantwortlichkeiten sollten in einer klaren Organisationsstruktur festgelegt sein, um sicherzustellen, dass alle Beteiligten ihre Aufgaben effektiv erfüllen können.

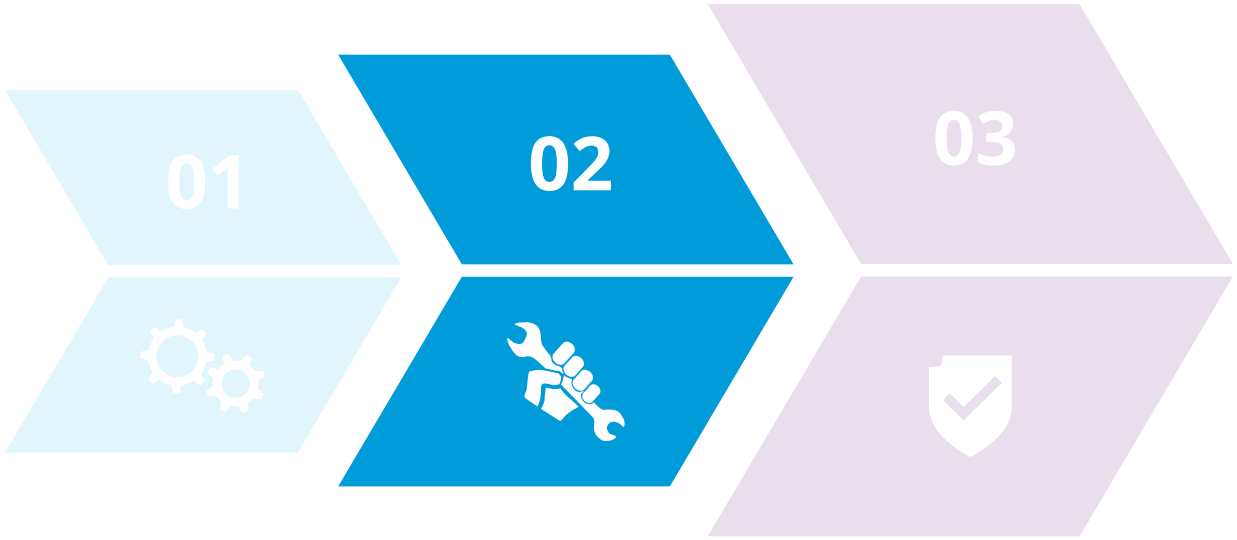
Innerhalb von Richtlinien und Prozessen werden konkrete Aufgaben und Verantwortlichkeiten definiert.

Der „Chief Information Security Officer” (CISO)

managementsysteme by migosens

Mögliche Aufgaben und Verantwortlichkeiten:	Entwicklung, Implementierung und Überwachung von Strategien zur Gewährleistung der IKT-Sicherheit im gesamten Unternehmen
	Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele
	Ausarbeitung, Anpassung von Sicherheitsrichtlinien und IT-Sicherheitszielen, inkl. Definition von KPIs
	Identifizierung von Bedrohungen und Schwachstellen in den IT-Systemen des Unternehmens sowie Planung und Durchführung von Maßnahmen zur Risikominimierung
	Überwachung von Compliance-Anforderungen wie Datenschutzgesetzen oder branchenspezifischen Vorschriften
	Schulung von Mitarbeitern in Bezug auf IT-Sicherheitsbewusstsein und Durchführung von Sicherheitsaudits
	Zusammenarbeit mit externen Partnern wie Regulierungsbehörden, Strafverfolgungsbehörden oder externen Beratern bei Bedarf

Implementierung eines ISMS in 3 Phasen



1 **Vorbereitung**

Bestandsaufnahme, Ermittlung des Gestaltungsbereichs, Projektplanung, Maßnahmenplan

2 **Aufbau des ISMS**

Assetmanagement, Risikomanagement, Dokumentationsstruktur, Awareness

3 **Herstellung der Zertifizierungsreife**

Maßnahmenbehandlung, Operative Integration, Bewertung, Auditbegleitung

Gute Vorbereitung ist für eine zielgerichtete Implementierung eine wichtige Grundlage

managementsysteme by migosens

Aufbau des ISMS

Assetmanagement

- Erstellung und Abstimmung eines **Prozesses zum Assetmanagement**
- **Erfassen** sämtlicher relevanten **Assets** und **Festlegung der Verantwortlichkeiten**
- **Kritikalitätsbetrachtung** der einzelnen Assetgruppen

Dokumentationsstruktur

- **Konzeption der ISMS-Dokumentation** sowie Abbildung der „High-Level-Structure“
- Nutzung vorhandener Strukturen des **Wissensmanagements**
- **Erstellung** der grundlegenden **ISMS-Dokumente**

Risikomanagement

- Etablierung einer schlanken **Methodik** zur Risikobewertung- und Behandlung
- **Durchführung von Workshops** zum Risikomanagement mit den Fachbereichen
- **Formulierung der initialen Maßnahmen** zur Risikobehandlung auf Basis der Bestandsaufnahme

Awareness

- Erstellung und Abstimmung geeigneter **Awarenessmaßnahmen und Schulungen**
- **Durchführung** von Awareness-Maßnahmen bei allen Mitarbeitern
- Aufstellung eines **Awareness- und Schulungskonzeptes** für die weitere Zukunft

Pflichtdokumente ISO/IEC 27001:2022

managementsysteme by migosens

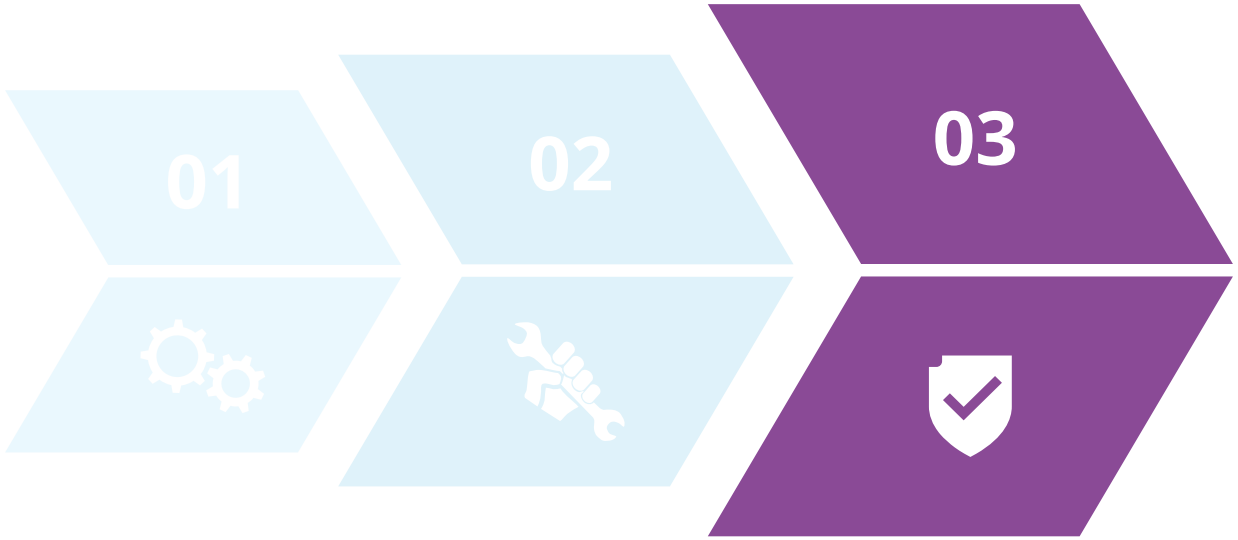
Norm-anforderung	Pflichtdokument
4.3	ISMS scope
5.1 & 5.2	Information security policy
6.1.2	Information security risk assessment procedure
6.1.3 (d)	Statement of Applicability
6.1.3	Information security risk treatment procedure
6.2	Information security objectives
7.2	Personnel records
8.1	ISMS operational information
8.2	Risk assessment reports
8.3	Risk Treatment Plan

Norm-anforderung	Pflichtdokument
9.1	Security metrics
9.2.2	ISMS internal audit programme and audit reports
9.3.3	ISMS management review reports
10.1	Records of nonconformities and corrective actions
A.5.1	Policies for information security
A.5.9	Invetory of information and other associated assets
A.5.13	Procedures for information labelling
A.5.19	Processes and procedures for information security in supplier relationships

Norm-anforderung	Pflichtdokument
A.5.21	Processes and procedures to manage information security risks with ICT products and services supply chain
A.5.24	Security incident management processes, roles and responsibilities
A.5.31	Documented legal, statutory, regulatory and contractual requirements
A.5.37	Documented operating procedures
A.6.2	Terms and conditions of employment
A.6.6	Confidentiality or non-disclosure agreements
A.8.27	Secure system architecture and engineering principles

Implementierung eines ISMS in 3 Phasen

managementsysteme by migosens



1 **Vorbereitung**

Bestandsaufnahme, Ermittlung des Gestaltungsbereichs, Projektplanung, Maßnahmenplan

2 **Aufbau des ISMS**

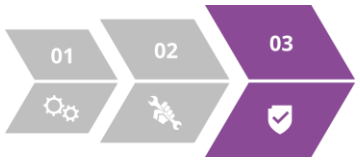
Assetmanagement, Risikomanagement, Dokumentationsstruktur, Awareness

3 **Herstellung der Zertifizierungsreife**

Maßnahmenbehandlung, Operative Integration, Bewertung, Auditbegleitung

Gute Vorbereitung ist für eine zielgerichtete Implementierung eine wichtige Grundlage

managementsysteme by migosens



Herstellung der Zertifizierungsreife

Maßnahmenbehandlung

- Risikobasierte **Priorisierung** der Maßnahmen
- **Begleitung** der Maßnahmen-verantwortlichen bei der **Umsetzung**
- **Regelmäßiges Controlling** der Maßnahmen und **Optimierung** des Reifegrades

Bewertung

- **Definition und Auswertung** von **Kennzahlen** zur Messung
- **Erstellung eines internen Auditprogrammes** und **Durchführung** von internen Audits
- Erstellung und gemeinsame Durchführung der ersten **Managementbewertung**

Operative Integration

- **Harmonisierung des ISMS mit operativen Prozessen** und IT-Administration
- **Unterstützung der Fachbereiche** bei Umsetzung von Maßnahmen
- Vollständige Erstellung der **ISMS-Dokumentation** nach Normanforderung

Auditbegleitung

- **Abstimmungen** mit dem ausgewählten Zertifizierer und Terminfindung
- **Briefing des Auditteams** und **Vorbereiten der Mitarbeiter** auf das Zertifizierungsaudit
- **Begleitung und Hilfestellung** bei der **Durchführung** des Zertifizierungsaudits

managementsysteme by migosens

A5 Organisatorische Maßnahmen

- Bedrohungsanalyse
- Informationssicherheit im Projekt Management
- Klassifizierung und Kennzeichnung von Informationen
- Zugangskontrolle
- Identitätsmanagement
- Informationssicherheit bei Lieferanten Beziehungen
- Umgang mit der Informationssicherheit im Rahmen von Lieferantenvereinbarungen
- Informationssicherheit bei der Nutzung von Cloud-Diensten
- Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen
- Bewertung und Entscheidung über Informationssicherheitsereignissen
- Reaktion auf und Lernen aus Informationssicherheitsvorfälle
- Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
- Rechte an geistigem Eigentum
- Privatsphäre und Schutz von personenbezogenen Daten (PII)

Maßnahmen der Erklärung zur Anwendbarkeit umsetzen (Auszug)

managementsysteme by migosens

A6 Personelle Maßnahmen

- Überprüfung des Hintergrunds
- Bedingungen und Konditionen für die Beschäftigung
- Bewusstsein für Informationssicherheit, Bildung und Ausbildung
- Disziplinarverfahren
- Zuständigkeiten nach der Kündigung oder Wechsel des Arbeitsplatzes
- Remote-Arbeit
- Meldung von Informationssicherheitsvorfällen

A7 Physische Maßnahmen

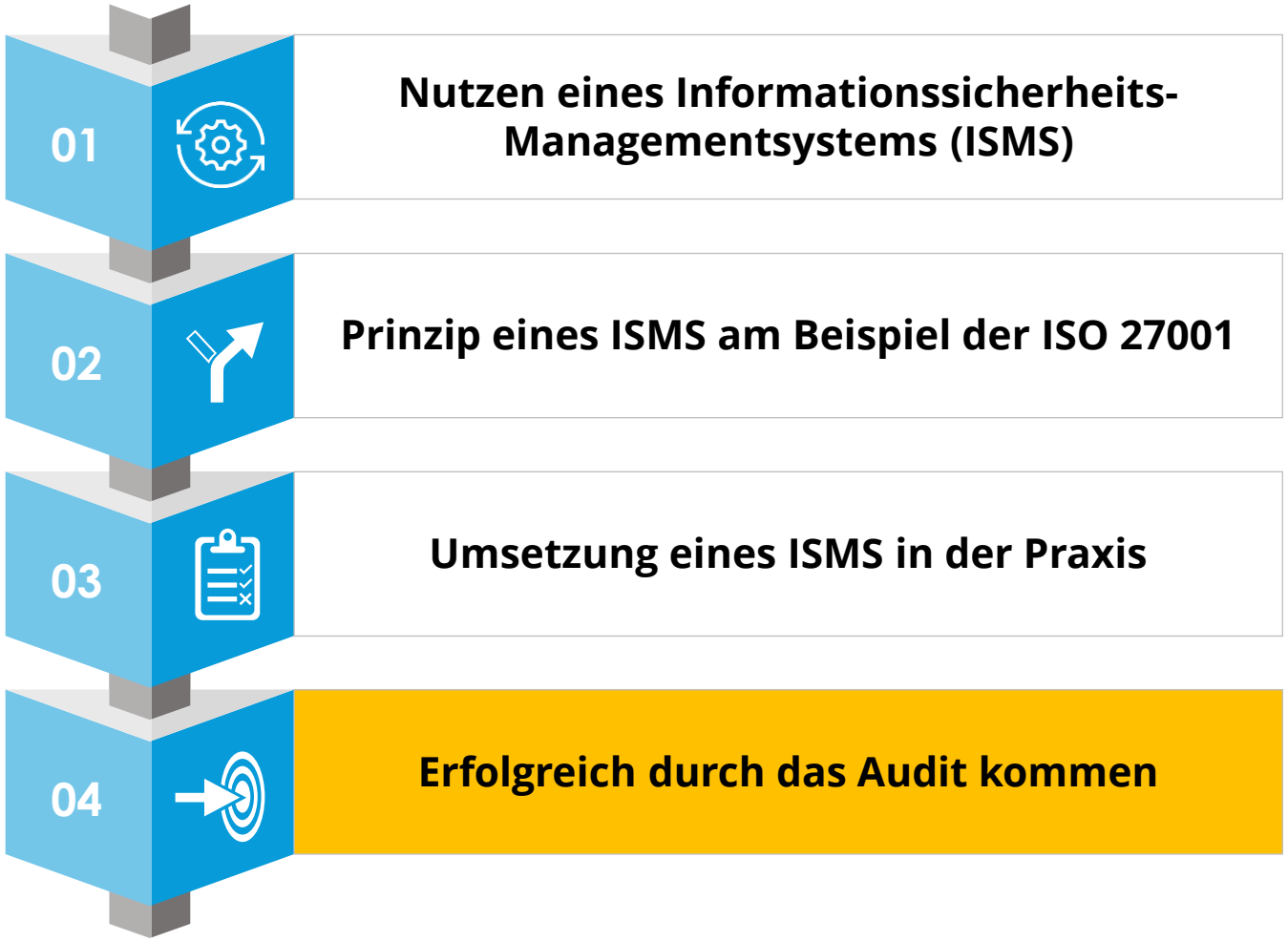
- Physische Sicherheitsabgrenzungen
- Physischer Zutrittskontrolle
- Sicherheitsüberwachung
- Clear Desk & Clear Screen
- Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen
- Speichermedien
- Sicherheit der Verkabelung

A8 Technologische Maßnahmen

- Privilegierte Zugriffsrechte
- Zugang zum Quellcode
- Schutz vor Schadsoftware
- Verwaltung der technischen Schwachstellen
- Maskierung von Daten
- Protokollierung
- Installation der Software auf dem Betriebssystem
- Web-Filterung
- Einsatz von Kryptographie

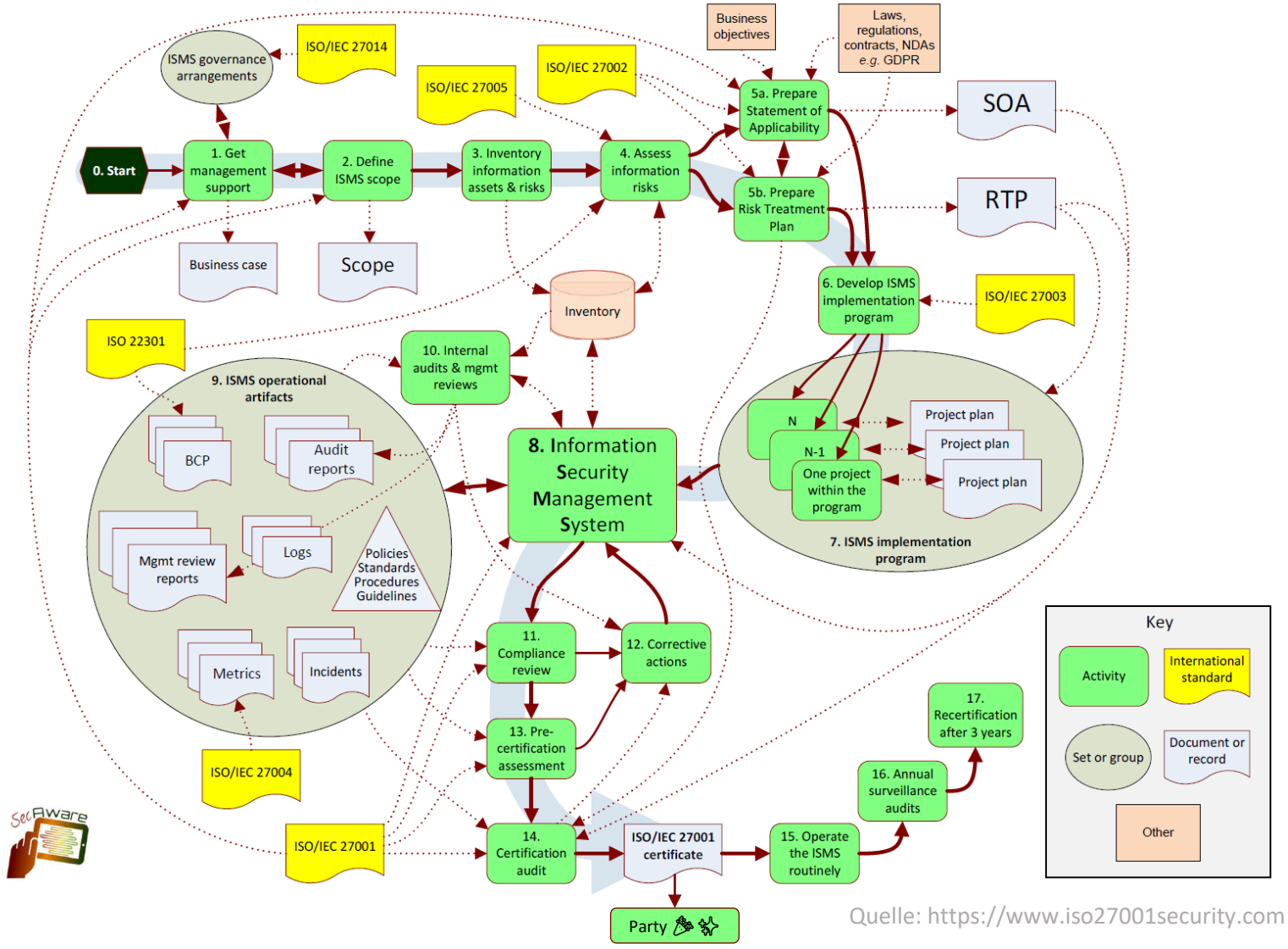
Agenda

managementsysteme by migosens



Ablauf einer ISO 27001-Implementierung

managementsysteme by migosens



Quelle: https://www.iso27001security.com

Kontakt und weitere Informationsangebote

managementsysteme by migosens

migosens

migosens GmbH
Wiesenstr. 35
45473 Mülheim an der Ruhr

Tel. 0208 / 99395110

datenschutzberatung@migosens.de

@DS_TALK

datenschutztalk_podcast

linkedin.com/company/migosensgmbh/

Allgemeine Informationen

ISO27001Security
https://www.iso27001security.com

Der Datenschutz Talk Podcast
https://www.migosens.de/podcast/

migosens
YouTube Channel
https://www.youtube.com/channel/UCyJ2BKkK5qNnNZuTaAi1lkQ

managementsysteme by migosens

Darf ich noch Fragen beantworten?

Empfehlung des Hauses

SCAN ME

Spotify

iTunes

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT
UND
VIEL FREUDE BEI DEN FOLGENDEN VORTRÄGEN!