ANMATHO AG
IT-Services & Solutions

Informationssicherheit und die Einführung eines ISMS nach ISO 27001

Agenda

- Hintergrund
- Darstellung & Funktionsweise der ISO 27001
- Dokumentenstruktur & Rollen der ISO 27001
- Bedeutung der Security Awareness in der ISO 27001

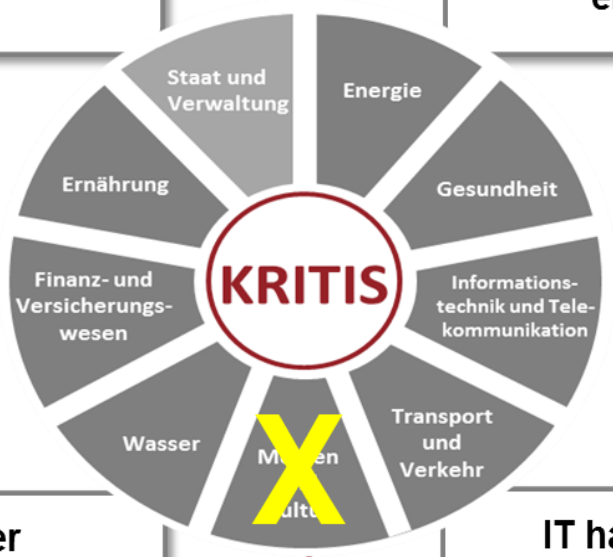
HINTERGRUND

ANMATHO AG
IT-Services & Solutions

Was ist eigentlich KRITIS?

Deutschland will die sichersten IT-Systeme & digitalen Infrastrukturen weltweit (Digitale Agenda)

Deutlich erhöhte Bedrohungslage



Vermeidung erheblicher Störungen der öffentl. Sicherheit

Verbesserung der IT-Sicherheit notwendig

Vermeidung nachhaltiger Versorgungsengpässe

IT hat hohe Bedeutung für das Funktionieren des Gemeinwesens

ANMATHO AG
IT-Services & Solutions

Das IT-Sicherheitsgesetz und dessen Anforderungen

Anforderungen des IT-SiG

Technische & organisatorische Maßnahmen
zum Schutz der maßgeblichen

- IT-Systeme
- Komponenten
- Prozesse

Aufstellung & Nachweis

(alle 2 Jahre)

- Sicherheits- & Notfallkonzepte
- Regelmäßige Prüfungen & Sicherheitsaudit
- Zertifizierung **(ggf.)**

24/7-Kontaktstelle zum BSI

(binnen 6 Monaten)

Meldepflicht für Störfälle

- I.d.R. anonym
- nur bei Ausfall oder Beeinträchtigung der Kritischen Infrastruktur namentlich

Vorschlag

von geeigneten branchen-spezifischen Sicherheitsstandards

(z.B. IT-SiKat)

Stand der Technik

!

Kommerzielle Websitebetreiber:
Erhöhte Anforderung an Sicherheit der Kundendaten

ANMATHO AG
IT-Services & Solutions

Bestimmung der KRITIS-Unternehmen durch Rechtsverordnung

§ 10 Abs. 1 IT-SiG:

Das Bundesinnenministerium bestimmt in einer Rechtsverordnung, welche Einrichtungen, Anlagen oder Teile aus den Sektoren als Kritische Infrastrukturen gelten.

Kritische Dienstleistung

Bedeutender Versorgungsgrad

Kriterium 1: Qualität

Kriterium 2: Quantität

Maßstab: Branchenspezifischer Schwellenwert

KRITIS-Unternehmen

Darstellung & Funktionsweise der ISO 27001

Definition ISMS

„Ein **Information Security Management System (ISMS)** ist eine

- Aufstellung von **Verfahren und Regeln** innerhalb eines Unternehmens,

welche dazu dienen, die **Informationssicherheit**

dauerhaft

- zu definieren,
- zu steuern,
- zu kontrollieren,
- aufrechtzuerhalten
- und fortlaufend zu verbessern.“

Begriffsbestimmung

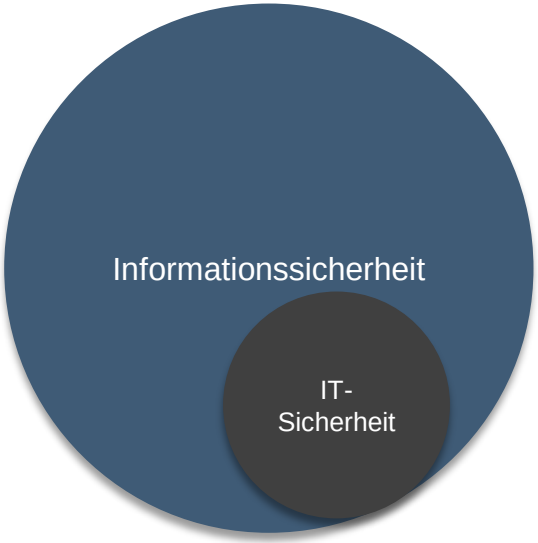
Die Begriffe IT-Sicherheit und Informationssicherheit werden oft synonym verwendet, jedoch sagen sie etwas unterschiedliches aus:

IT-Sicherheit:

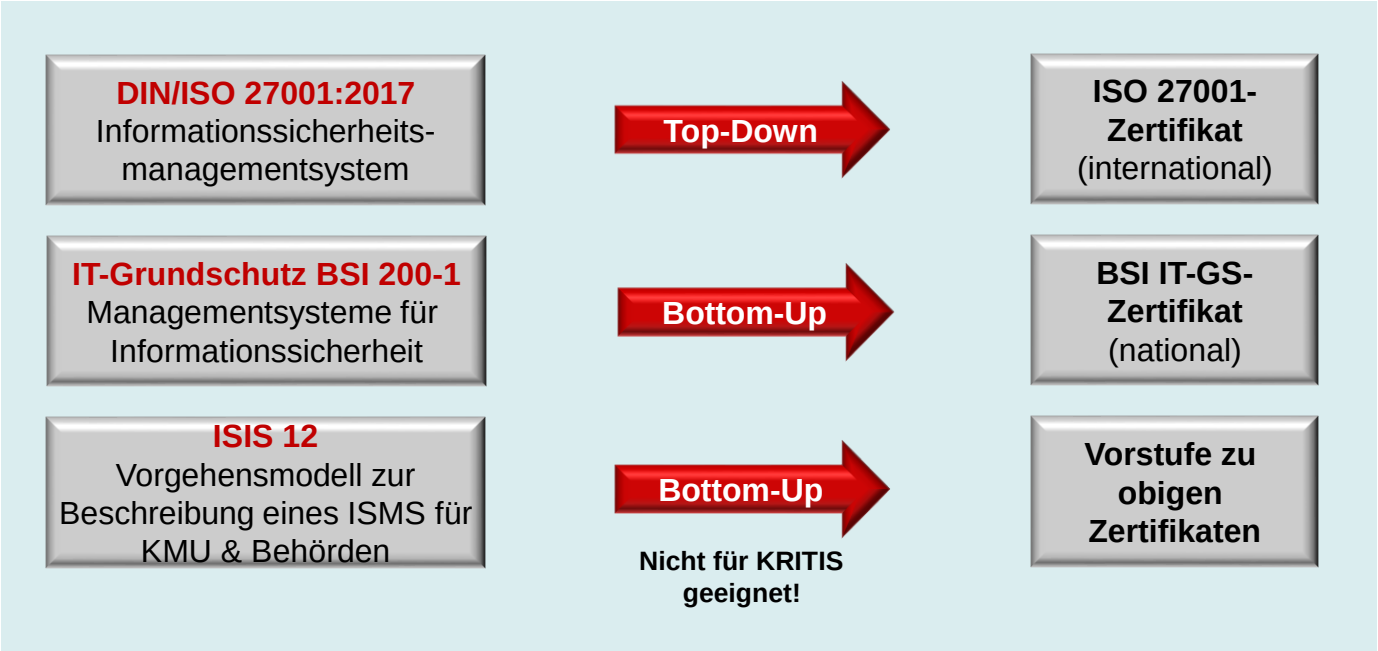
Die IT-Sicherheit beinhaltet die Sicherheit der technischen Komponenten.

Informationssicherheit:

Die Informationssicherheit beinhaltet den Schutz aller sensibler Unternehmensinformationen, darunter fällt auch die IT-Sicherheit. Somit ist die IT-Sicherheit ein Teil der Informationssicherheit und nicht synonym zu verwenden.

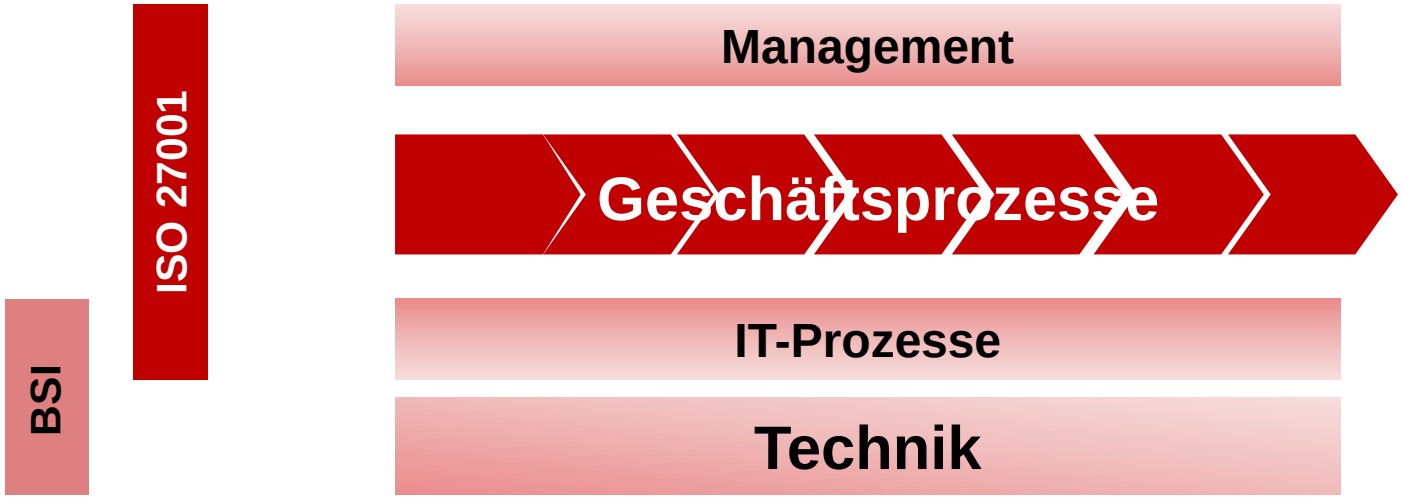


Verschiedene Standards und Zertifizierungsmöglichkeiten



ANMATHO AG
IT-Services & Solutions

Wo setzt die ISO 27001 an?



Die ISO 2700X-Reihe (Auszug)

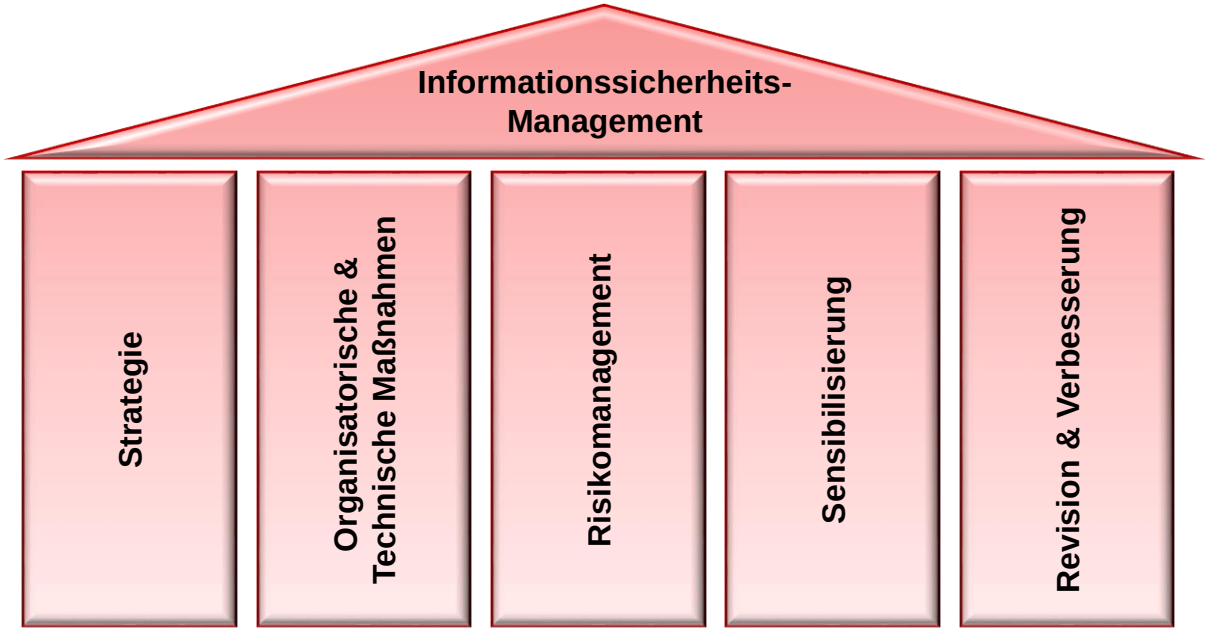
Norm	Bezeichnung
ISO 27001	Information security management systems requirements specification
ISO 27002	Code of practice for information security management
ISO 27003	Guidance in implementing an ISMS
ISO 27004	Measures and measurement for the assessment of the effectiveness
ISO 27005	Information security risk management
ISO 27006	Requirements for …. audit and certification of information security management systems

Sektorenspezifische Standards der ISO 2700X-Reihe

Norm	Bezeichnung
ISO 27010	Information security management for inter-sector & inter-organisational communications
ISO 27011	ISM guidelines for telecommunications organisations based on ISO/IEC 27002
ISO 27015	ISMS for **financial sector**
ISO 27017	Code of practice for information security controls for cloud computing services based od ISO/IEC 27002
ISO 27018	Code of practice for PII protection in public clouds acting as PII processors
ISO/IEC TR 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the **energy utility industry**

ANMATHO AG
IT-Services & Solutions

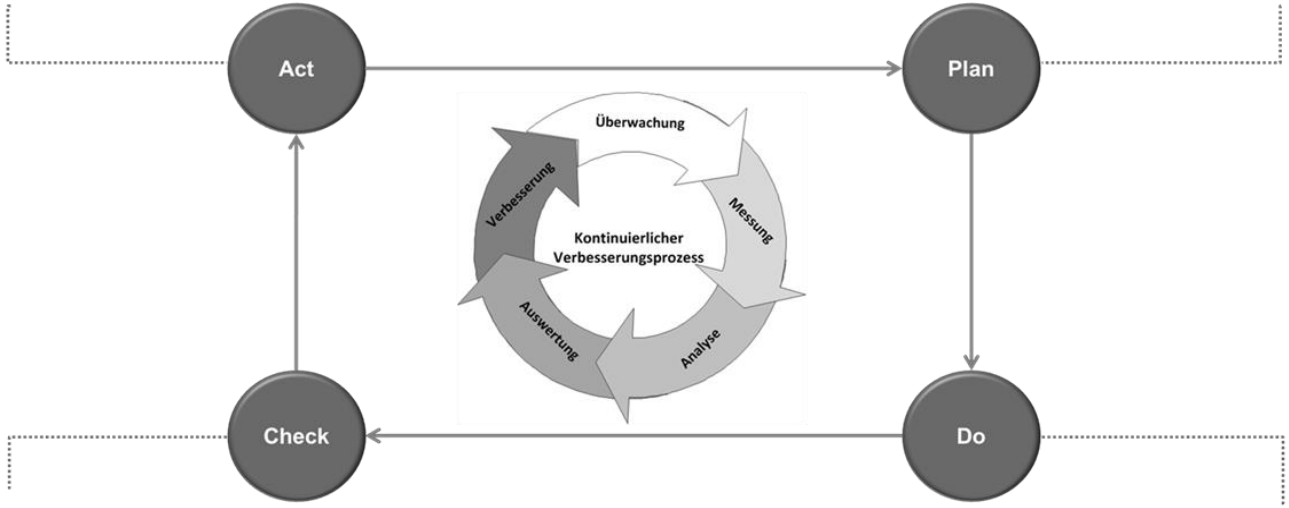
ISMS nach ISO 27001 – Ein ganzheitlicher Lösungsansatz



PDCA und KVO als Regelprozess der ISO 27001

- Prozesse reflektieren
- Korrektur- und Folgemaßnahmen anstoßen
- Verbesserungsmaßnahmen ableiten
- Zertifikat

- Relevante Prozesse identifizieren
- Anforderungen definieren
- Risikomanagement betreiben
- Ziele und Maßnahmen ableiten



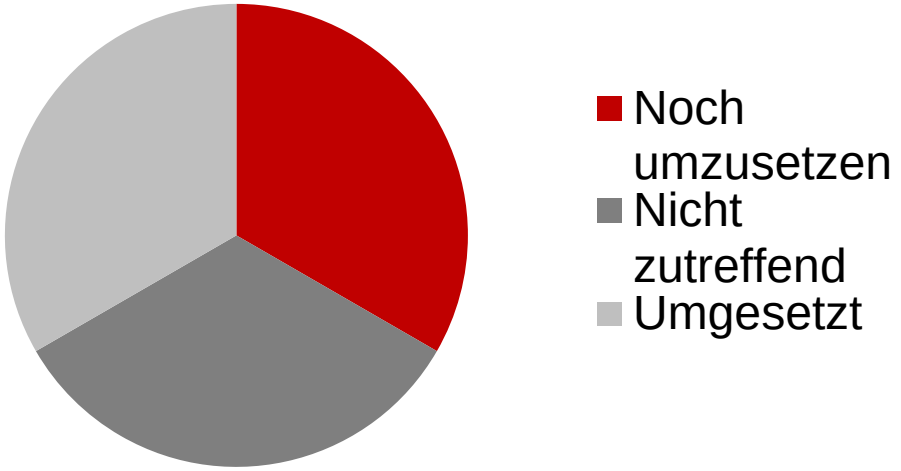
- Prozesse überwachen und bewerten (interne Audits)
- Zielerreichung prüfen (Revision)
- Managementbewertung

- Implementierung und Aufnahme der geplanten Prozesse und Maßnahmen

Die Controls der ISO 27001

Controls:

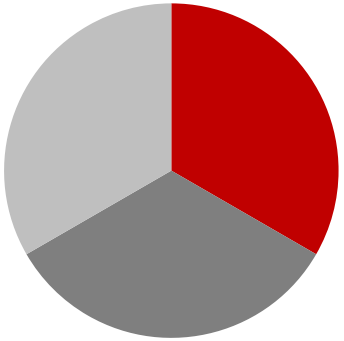
114 ISO 27001:2017



ANMATHO AG
IT-Services & Solutions

Anhang A der ISO 27001

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



Die ISO 27001 spezifiziert also die Anforderungen für…

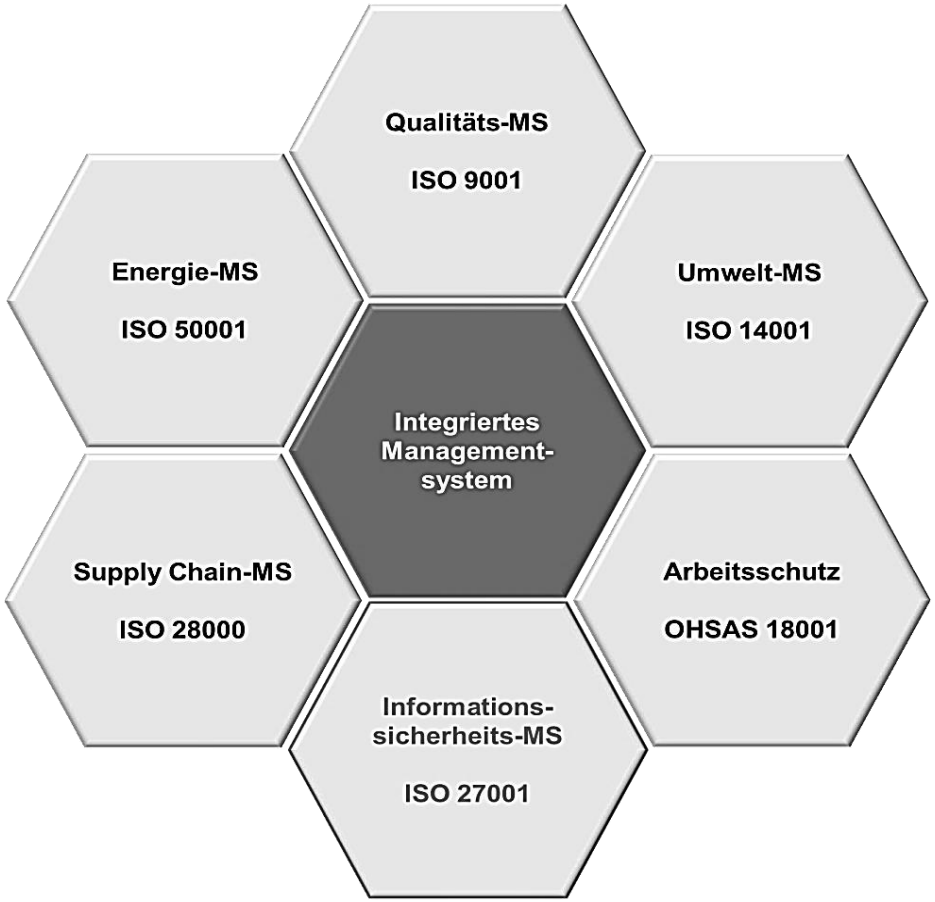
- die Herstellung,
- die Einführung,
- den Betrieb,
- die Überwachung,
- den kontinuierlichen Verbesserungsprozess (KVP)

eines ISMS.

- Die ISO 27001 kann auf **jede Organisationsform und Größe** angewendet werden.

ANMATHO AG
IT-Services & Solutions

Integriertes Managementsystem



Vorteile eines ISMS nach ISO 27001 (1/2)

- Internationales Grundverständnis für Informationssicherheit und -management
- Akzeptanz bei Kunden und Lieferanten (globale Geltung)
- International anerkannte Zertifizierung
- „Ganzheitlicher“ Ansatz – Verantwortung liegt beim Management
- Bezieht Geschäftsstrategie und -ziele mit ein
- Folgt den Geschäftsprozessen
- Bezieht die Maßnahmenebene mit ein
- Sinnvolle Anwendung auch ohne Zertifizierung möglich
- Unternehmensrisiken werden erkannt und verstanden
- Die Aufmerksamkeit richtet sich auf Informationsressourcen, die das größte Risiko inne haben.

Vorteile eines ISMS nach ISO 27001 (2/2)

- "Owner" kennen das akzeptable Risikoniveau und sind motiviert ihre Risiken zu minimieren.
- Nachweis der Informationssicherheit gegenüber Dritten (Gesetzgeber, Lieferanten und Kunden) →Wettbewerbsvorteil
- Sicherheit wird integraler Bestandteil der Geschäftsprozesse
- Sicherheit im Unternehmen wird messbar
- Allgemein erhöhtes Sicherheitsbewusstsein im Unternehmen
- Erleichterte Einhaltung gesetzlicher Bestimmungen, z.B. BDSG (neu)/DS-GVO
- Nahtloses Einpassen von ISO 27001 in andere Managementsysteme, wie z.B. ISO 9001

Dokumentenstruktur & Rollen der ISO 27001

ANMATHO AG
IT-Services & Solutions

Dokumentation und Nachweisbarkeit „Accountability“

- Dokumentation des **aktuellen Zustands** und **Fortschritts** von festgelegten Prozessen
- Dokumentation von **verabschiedeten Richtlinien** und deren **Verbreitung**
- Dokumentation von **Gesamt- und Einzelkonzepten**
- Dokumentation von **Maßnahmen**

Dokumentation und Nachweisbarkeit „Accountability“

- Pflichtdokumente des ISMS müssen grundsätzlich immer erstellt werden!
- Form und Inhalte sind z.T. vorgeschrieben

➢ **Achten Sie auf einen geeigneten Revisionszyklus Ihrer Dokumente!**

- Dokumentation ist ein Qualitätsmerkmal
- Dokumentation trägt zur Risikominimierung bzw. Schadensbegrenzung im Störfall bei:

  Z.B. bei Wiederanlauf von Systemen: deutlich schneller, wenn Verfahren dokumentiert sowie aktuell ist und geübt wird

  Ein Protokoll mit Auswertung der Wiederanlaufübungen dient z.B. als Nachweis für den Auditor und den Wirtschaftsprüfer.

Dokumentenstruktur in der Sicherheitspyramide

Die Informationssicherheitsleitlinie

- … ist ein **strategisches Dokument** der Geschäftsleitung.
- … ist ein **verbindliches Dokument** für alle Mitarbeiter des Unternehmens.
- … drückt die **Entscheidung** der Unternehmensleitung zur IS aus.
- … gibt den groben **Rahmen** vor.

Die Informations-Richtlinien

- …**ergänzen** die **Leitlinie** und sind **verbindlich.**
- …müssen die **Ziele** der Leitlinie beachten.
- …legen **organisatorische** und **technische Anforderungen** fest.

Beispiele für Richtlinien:

- Richtlinie zur Zugangsteuerung
- Richtlinie zur Klassifizierung von Informationen
- Richtlinie zur Handhabung von Informationssicherheitsvorfällen

ANMATHO AG
IT-Services & Solutions

Anweisungen und Dokumentation

Arbeitsanweisungen sind konkrete	**Anweisungen, Arbeitsabläufe, Zielvorgaben, How to´s**	wie z.B. :	**Feinkonzepte, Systemhandbücher, Notfallpläne**

- Sie enthalten eindeutige, konkrete, im Voraus definierte Handlungsanweisungen für entsprechende Adressatenkreise (Administratoren, Notfallbeauftragte etc.):

Hierzu zählen Anweisungen z.B.

- wie IT-Systeme konfiguriert werden müssen,
- welche Sicherheitsmaßnahmen im Notfall eingeleitet werden müssen.

ANMATHO AG
IT-Services & Solutions

Pflichtdokumentation

Folgende Dokumente sind zwangsläufig gemäß ISO 27001 zu erstellen (1/4)

Thema	Inhalt
ISMS Leitlinie	Informationssicherheitsstrategie
Risikobewertungsmethode	Methode zur Risikobewertung, die zu nachvollziehbaren und rückverfolgbaren Ergebnissen führt
Anwendbarkeitserklärung	Aussage zu den Maßnahmenzielen aus dem Anhang - angewendet ja/nein und Begründung dazu
Risikobehandlungsplan	Lenkung der Maßnahmen, um die Risiken adäquat zu behandeln
Wirksamkeitsbewertung der Maßnahmenziele	Definition, wie Maßnahmenziele auf ihre Wirksamkeit hin bewertet werden sollen

Pflichtdokumentation

Folgende Dokumente sind zwangsläufig gemäß ISO 27001 zu erstellen (2/4)

Thema	Inhalt
Lenkung von Dokumenten	Wie werden Dokumente freigegeben und gelenkt?
Lenkung von Aufzeichnungen	Wie werden Aufzeichnungen gelenkt und aufbewahrt?
Anwendungsbereich und Grenzen	Beschreibung und Definition des Scope

Pflichtdokumentation

Folgende Dokumente sind zwangsläufig gemäß ISO 27001 zu erstellen (3/4)

Thema	Inhalt
Bericht über Risikobewertung	Kompletter Durchlauf des Risk Assessments inkl. der Auswertung der Ergebnisse
Bewertung der ISMS-Wirksamkeit	Bewertung der Wirksamkeit der implementierten Maßnahmen
Bewertung der Methode zur Risikobewertung und des Restrisikos/akzeptierten Risikos	
Aufzeichnungen über Ausbildung, Training, Kompetenz, Erfahrung, Qualifikationen	

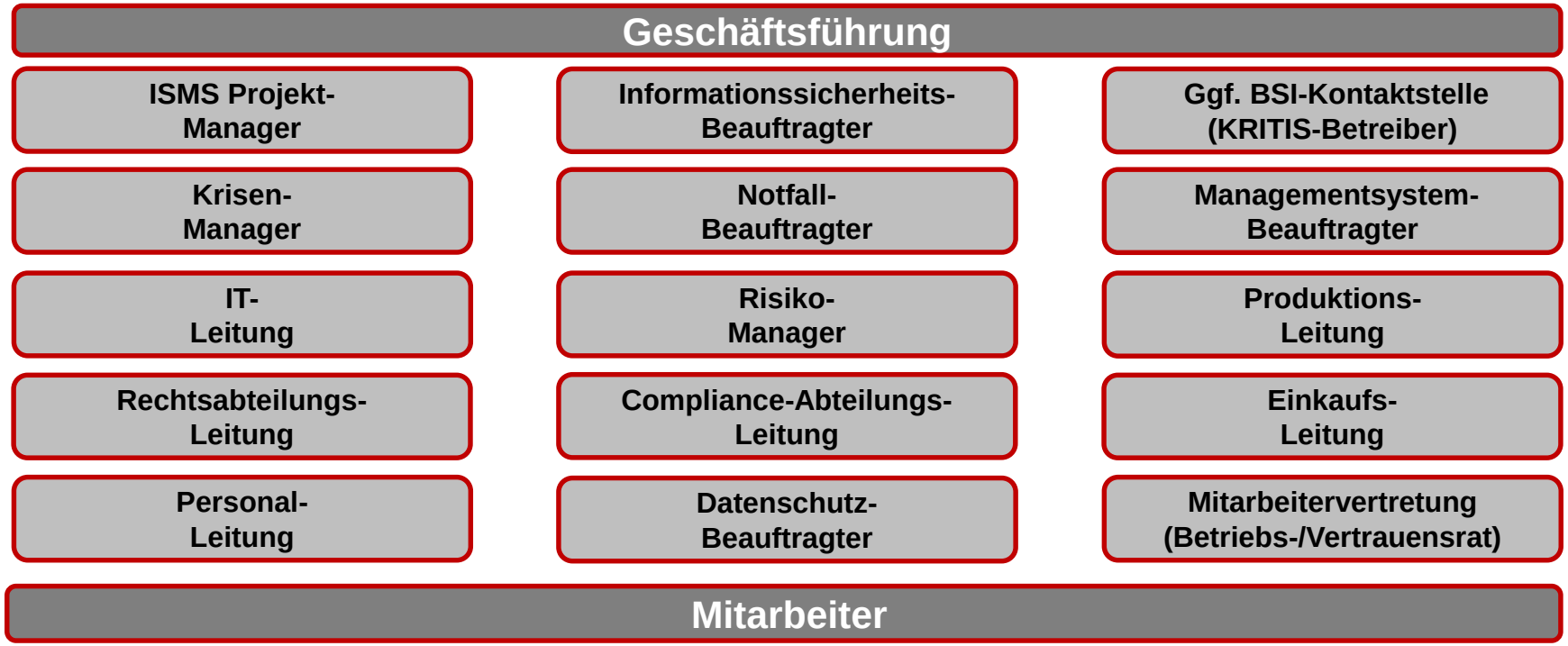
Pflichtdokumentation

Folgende Dokumente sind zwangsläufig gemäß ISO 27001 zu erstellen (4/4)

Thema	Inhalt
Interne ISMS Audits	Aufzeichnung über geplante, durchgeführte und bewertete interne ISMS Audits
Managementbewertung	Aufzeichnung über geplante, durchgeführte und bewertete Managementbewertungen

ANMATHO AG
IT-Services & Solutions

Überblick: Rollen in der Informationssicherheitsorganisation



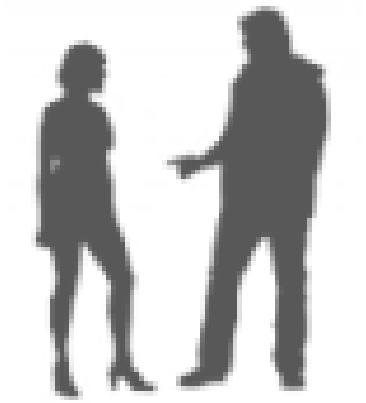
Bedeutung der Security Awareness in der ISO 27001

ANMATHO AG
IT-Services & Solutions

Sicherheitslücken sind oft hausgemacht

- Unvollständige Dokumentation
- Ungenehmigte techn. Maßnahmen
- Inkonsistentes & inkonsequentes Recovery
- Social Engineering

Faktor Mensch



Risiko & Erfolg

- Fehlende Prozesse für Alltag & Notfall
- Unkontrollierter Datenaustausch
- Zusammenarbeit
- Priorisierung & Überlastung

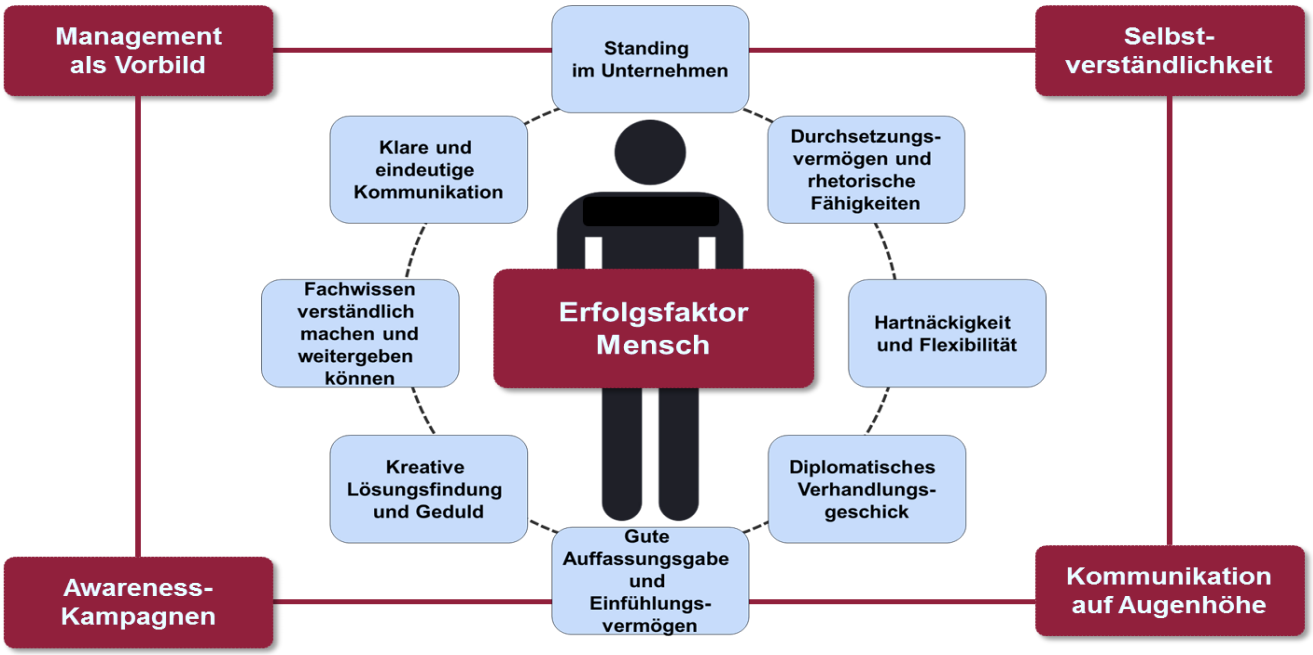
Sicherheitslücken sind oft hausgemacht

- Kritische Geschäftsprozesse werden von **Menschen** gesteuert.
- Vertrauliche Daten werden von Menschen verarbeitet.
- Die IT ist „nur“ ein Hilfsmittel zur Aufgabenerledigung.

Sicherheit hängt vor allem von menschlichen Handlungen ab!

- An dieser Stelle liegt zumeist das Problem!
- Mitarbeiter sind **mit Sicherheitsmaßnahmen oft überfordert**.
- Fehlendes Bewusstsein & Wissen
- Fehlende Einsicht, fehlende Bereitschaft mitzuwirken.
- Achtlosigkeit aufgrund von Unwissenheit

Der Schlüssel zum Erfolg: Unternehmenskultur & Kommunikation



Lösungsansätze

- **Etablierung und kontinuierliche Aufrechterhaltung des Sicherheitsbewusstseins** bei jedem einzelnen Mitarbeiter.
- Allen Mitarbeitern ist die Auswirkung der Beeinträchtigung der **Sicherheitsschutzziele** Vertraulichkeit, Verfügbarkeit, Integrität **bewusst zu machen**.
- Alle Mitarbeiter sind zur **Mitwirkung** durch Aufmerksamkeit, Mitdenken und Melden zu bewegen.
- **Maßnahmen sind stetig** an technische und organisatorische Weiterentwicklungen und Bedrohungen **anzupassen**.
- Mitarbeiter sind **zu befähigen**.
- Das ausschließliche **Aussprechen von Verboten hilft nur bedingt.**

Ist etwas unklar geblieben?

Vielen Dank für Ihre Aufmerksamkeit

Ihr Ansprechpartner

Dipl.-Kfm.
Christian Westerkamp, LL.M.

Mitglied der Geschäftsleitung

E-Mail: christian.westerkamp@anmatho.de
Mobil: +49 160 970 40 900

ANMATHO AG
IT-Services & Solutions

Winterhuder Weg 8
22085 Hamburg

Tel.: +49 40 229 47 19-0
E-Mail: info@anmatho.de
URL: www.anmatho.de