Fachliche Vorbereitung für eine grundlegende Zertifizierungsreife

Know-how to go – ISMS-Zertifizierung

HiSolutions AG

Kerstin Holzbaur

Kerstin Holzbaur

Senior Consultant

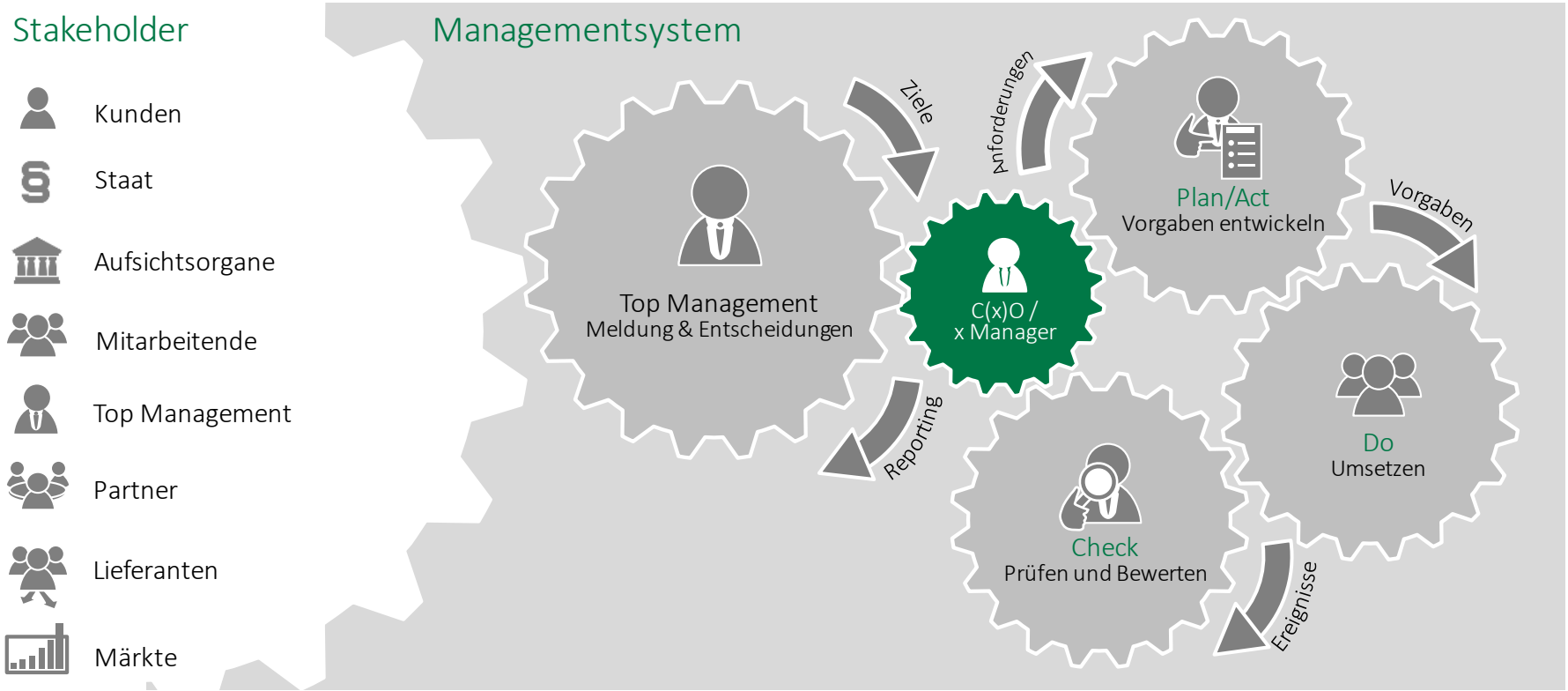
- Senior Consultant bei HiSolutions
- Einführung und Weiterentwicklung von Informationssicherheitsmanagement-Systemen
- Zertifizierte Lead Auditorin für Managementsysteme nach ISO 27001 nativ
- Informationssicherheit nach VDA ISA und TISAX-Assessments

Agenda

- Wie ist ein ISMS aufgebaut?
- Was sind zentrale Schritte zur Umsetzung eines ISMS?
- Was sind mögliche Herausforderungen?

Wie ist ein ISMS aufgebaut?

Der allgemeine Aufbau eines Managementsystems richtet sich nach internen und externen Anforderungen

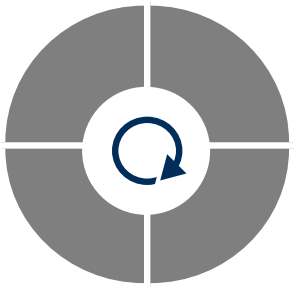


Elemente für ein anforderungsgerechtes und risikoorientiertes ISMS

Ein ISMS besteht aus vier wesentlichen Elementen:

Aufbauorganisation

Dokumentation

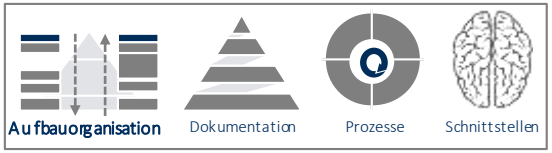


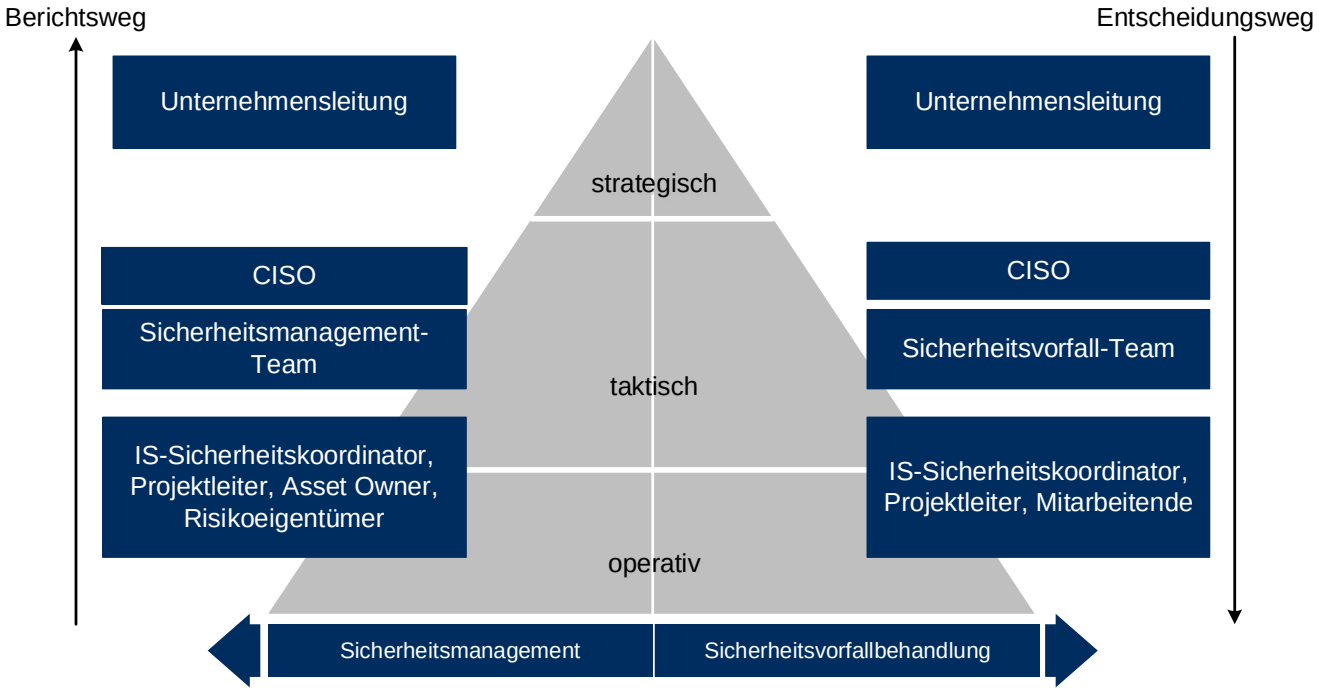
Prozesse

Schnittstellen

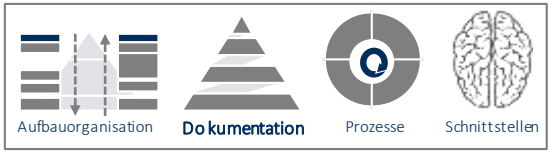
Assetmanagement und IS-Risiko- und Chancenmanagement sind elementare Prozesse des ISMS

Mögliche Aufbau- und Ablauforganisation





Möglicher Aufbau der ISMS-Dokumentation



Leitline
erläutert Ziele und Zweck

Rahmenwerke
geben Aufbau und Inhalt vor

Richtlinien
erläutern Methoden und Verfahren

Hilfsmittel & Templates
unterstützen in der Umsetzung

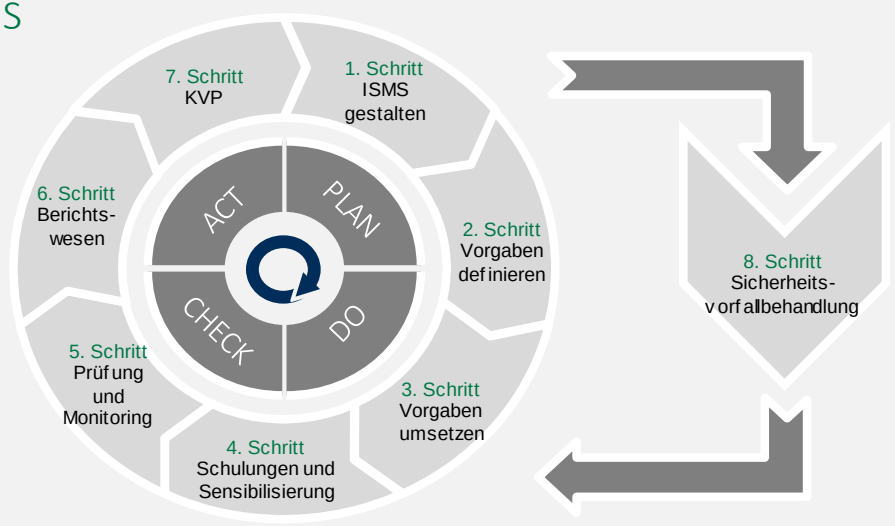
Die Dokumentation muss nicht immer einer klassischen Richtlinienstruktur entsprechen

Etablierung der ISMS-Prozesse

ISMS-Anforderungen

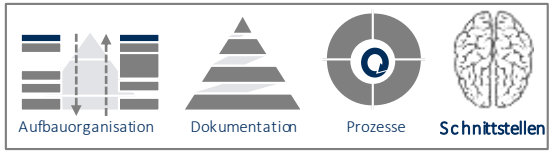
- Gesetzliche Vorgaben
- Externe Vorgaben
- Konzernanforderungen
- Unternehmensziele
- Interne Anforderungen

ISMS



Assetmanagement und IS-Risiko- und Chancenmanagement sind elementare Prozesse des ISMS

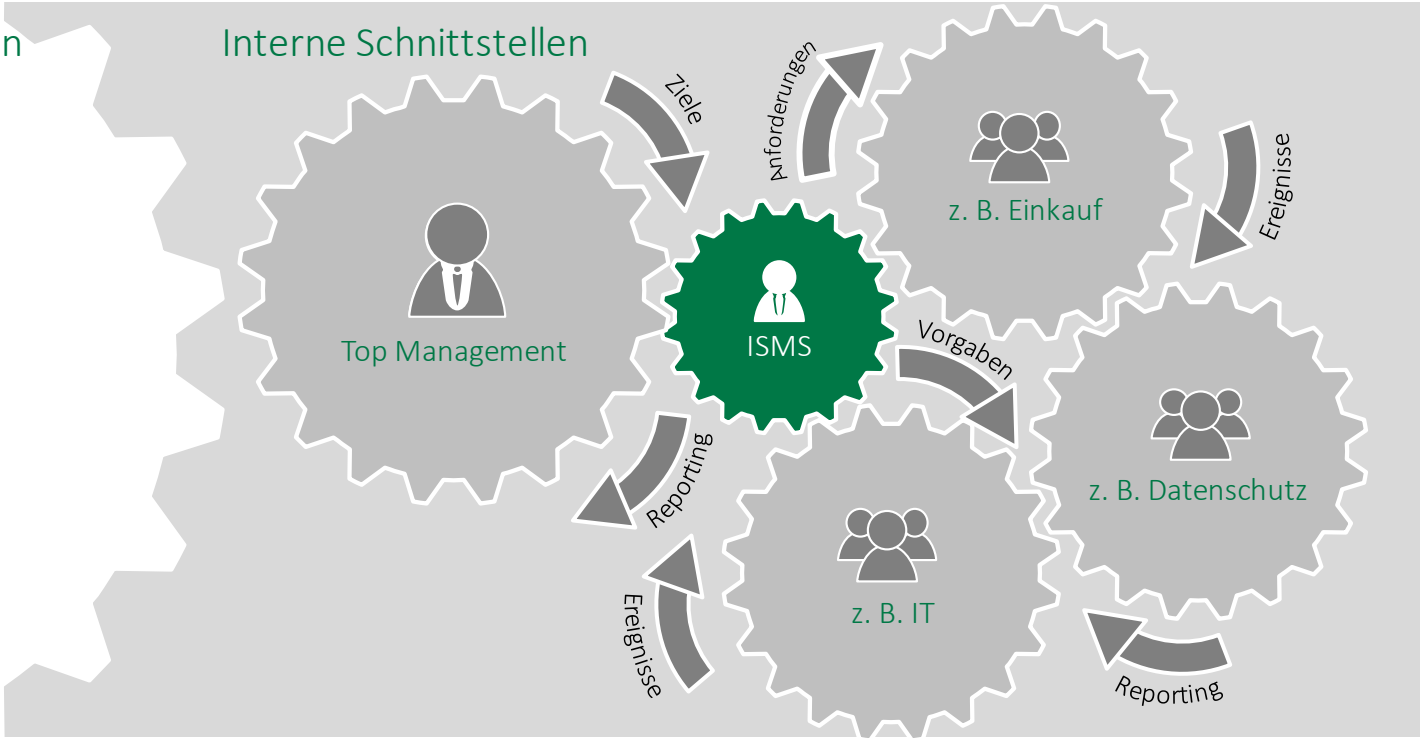
Betrachtung der Schnittstellen



Externe Schnittstellen

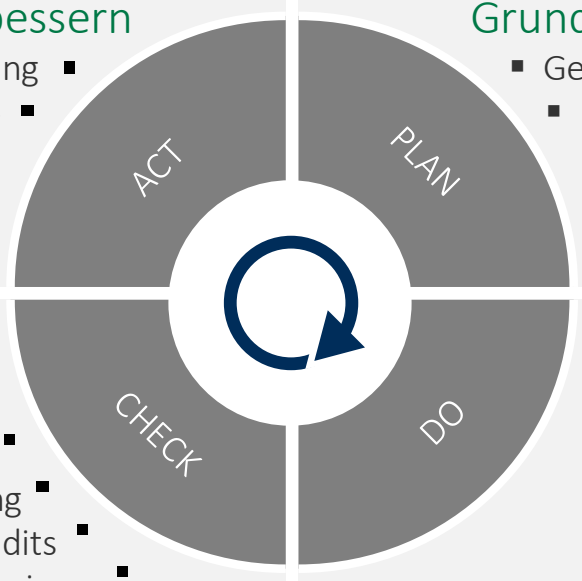
- Kunden
- Staat
- Aufsichtsorgane
- Partner
- Lieferanten
- Märkte

Interne Schnittstellen



Was sind zentrale Schritte zur Umsetzung eines ISMS?

Der gesamte PDCA-Zyklus muss durchlaufen werden



Grundlagen schaffen

- Geltungsbereich, Ziele und Zweck
- Interested Parties
- Top-Management-Unterstützung
- Ressourcen
- Awareness & Kommunikation

Umsetzen & Betreiben

- Schutzbedarfsanalysen
- Information Security Risk Management
- Mindestvorgaben an die Informationssicherheit (2nd Line)
- Sicherheitsvorgaben (1st Line)

Überwachen & Überprüfen

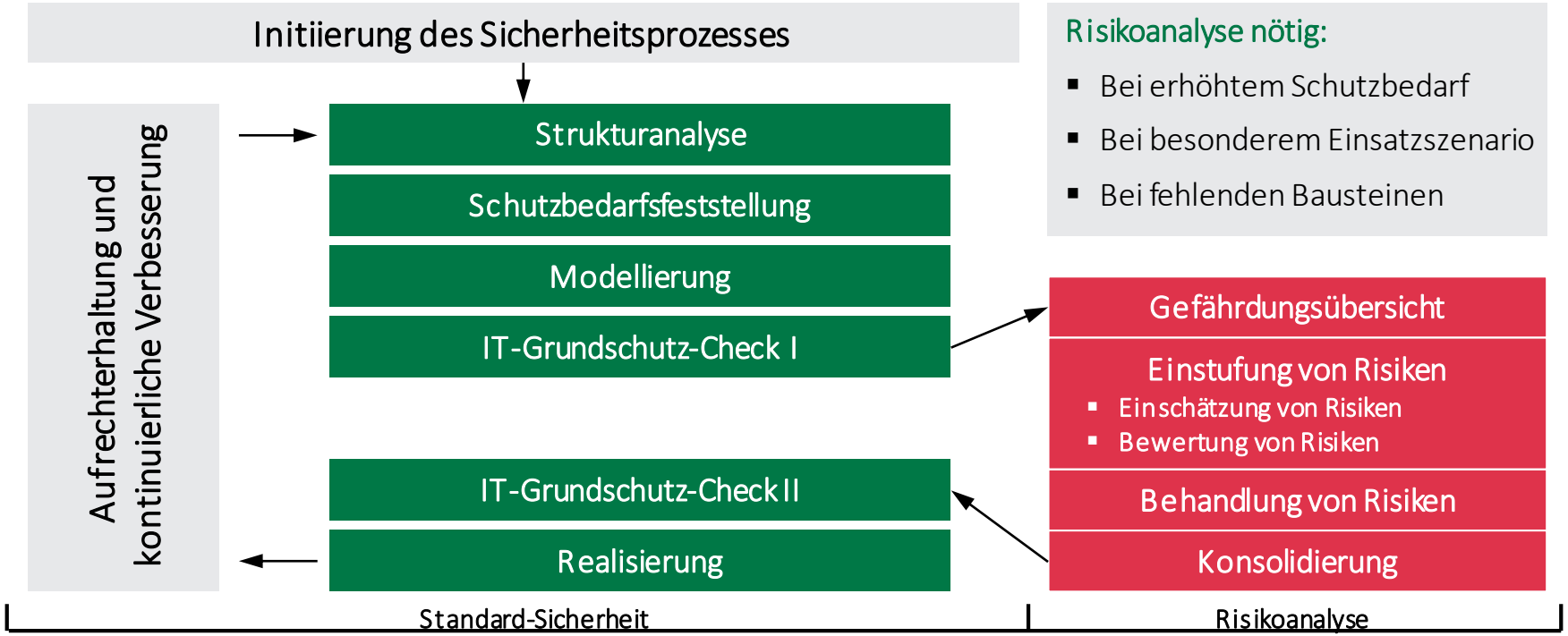
- Leistungsüberwachung
- Messung
- Bewertung
- Interne Audits
- Management Reviews

Aufrechterhalten & Verbessern

- Konformitätsprüfung
- Korrektur- und Verbesserungs-maßnahmen
- Kontinuierlicher Verbesserungs-prozess

Mögliches Vorgehen in der Implementierung (ISO 27001)

Vorgehensweise gemäß BSI-Standard 200-2



Risikoanalyse nötig:

- Bei erhöhtem Schutzbedarf
- Bei besonderem Einsatzszenario
- Bei fehlenden Bausteinen

Was sind mögliche Herausforderungen?

Stolpersteine bei der Implementierung

Ressource Informationssicherheitsbeauftragter
Gerade KMU tun sich schwer, einen Informationssicherheitsbeauftragten (ISB) zu benennen. Der ISB ist oft sehr überlastet.

Ressourcenknappheit innerhalb der IT-Abteilung
Die IT-Abteilung ist meist viel zu klein und findet in den Augen der Geschäftsführung kaum Beachtung.

„Inselwissen“ der langjährigen Mitarbeitenden
Mängel bestehen beim Wissensaustausch und der Dokumentation der Prozesse, Anwendungen und IT-Systeme. Es fehlt eine zentrale Übersicht.

Fehlende Akzeptanz für das ISMS
Es fehlen Maßnahmen zur Sensibilisierung und Schulung der Mitarbeitenden und der obersten Leitung, wodurch kein nachhaltiges Verhältnis zum Thema aufgebaut wird.

Ungeregelte Beschaffung von Produkten & Dienstleistungen
Es fehlt häufig der Beschaffungsprozess, der eine Abstimmung im Sinne der Informationssicherheit oder Systemarchitektur vorsieht.

Unübersichtliche Dokumentation
ISMS-Dokumente enthalten widersprüchliche und überflüssige Inhalte, wodurch die notwendige Aussagekraft verloren geht.

Unklarheiten bei der Verantwortung der Führung
Die Leitung ist sich ihrer Verantwortung im ISMS nicht bewusst. Sie muss aktiv in die Planung und Operationalisierung eines ISMS einbezogen werden.

Unrealistische Projektzeiten und -ziele
Oft sind Projektziele und Umsetzungszeiten zu optimistisch geplant. Dies kann sich negativ auf das Engagement und die Motivation der Mitarbeitenden auswirken.

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com