secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vortrag:

Datenschutzmanagement nach der ISO/IEC 27701

verinice.XP

Berlin, 27. Februar 2020

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

Über uns

- gegründet 1. Juli 1982
- Gäufelden bei Stuttgart
- IT-Sicherheit seit 1988
- heute reiner IT-Sicherheitsdienstleister
- aktuell ca. 27 Mitarbeitende
- inhabergeführt
- herstellerunabhängig

secuvera

- BSI-zert. IT-Sicherheitsdienstleister
- Geschäftsbereiche
  - Sicherheitsberatung (BSI-Grundschutz / ISO 27001)
  - Penetrationstests / Webanwendungsprüfungen
  - BSI-Prüfstelle für Common Criteria
- akkreditiertes Prüflabor für IEC 62443 beim TÜV Nord

secuvera

Ann-Kathrin Udvary

- seit 2019 bei der secuvera
- Trainee
- Studium der Wirtschaftsinformatik
- Schwerpunkte
  - Informationssicherheits- und Datenschutzmanagement

secuvera

Björn Lemberg

- seit 2012 bei der secuvera
- leitender Sicherheitsberater ISMS
- Verantwortungsbereiche
  - ISO 27000er
  - VDA-ISA & ENX/TISAX
  - Datenschutz
- CISSP, 27001 Auditor, DSB
- intern: bDSB

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

Management-systeme

- Abgestimmte
  - Prozesse
  - Schritte
  - Verantwortlichkeiten

zur

- Erreichung festgelegter Ziele
- kontinuierlichen Verbesserung

secuvera

DS-GVO & MS

- Art. 5 DS-GVO
  - Rechenschaftspflicht
- Art. 32 DS-GVO
  - Verfahren zur
    - regelmäßigen Überprüfung,
    - Bewertung und
    - Evaluierung

    der Wirksamkeit der technischen und organisatorischen Maßnahmen

secuvera

Anforderungen

- Verzeichnis der Verarbeitungstätigkeiten
- Grundsätze der Verarbeitung
  - Rechtmäßigkeit & Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - *Vertraulichkeit, Integrität & Verfügbarkeit*
- Betroffenenrechte
- Datenschutzfolgeabschätzung
- Rechenschaftspflicht

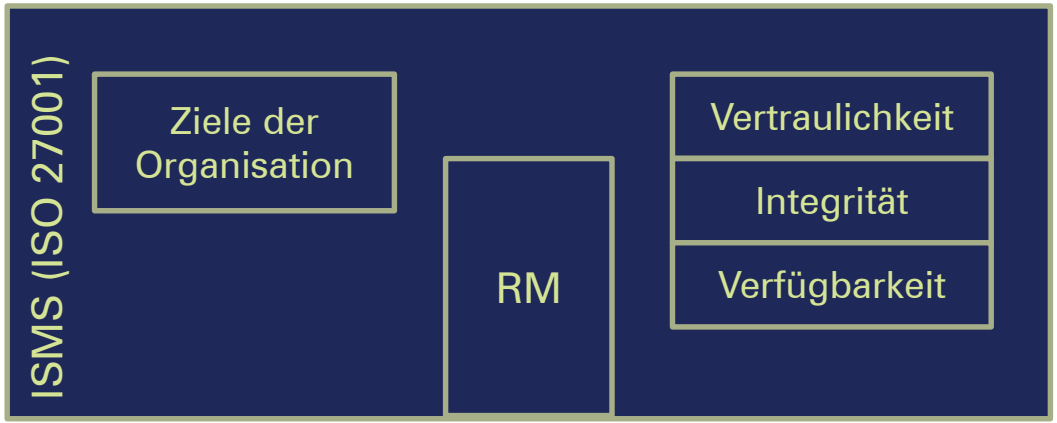
secuvera

Perspektiv-wechsel

- Datenschutz
  - personenbezogene Daten
  - DSFA als risikobasierter Ansatz
  - *Ziel:* Schutz der Rechte und Freiheiten Betroffener
- Informationssicherheit
  - Informationen allgemein
  - RM zur Gewährleistung der Angemessenheit
  - *Ziel:* Schutz der Organisation

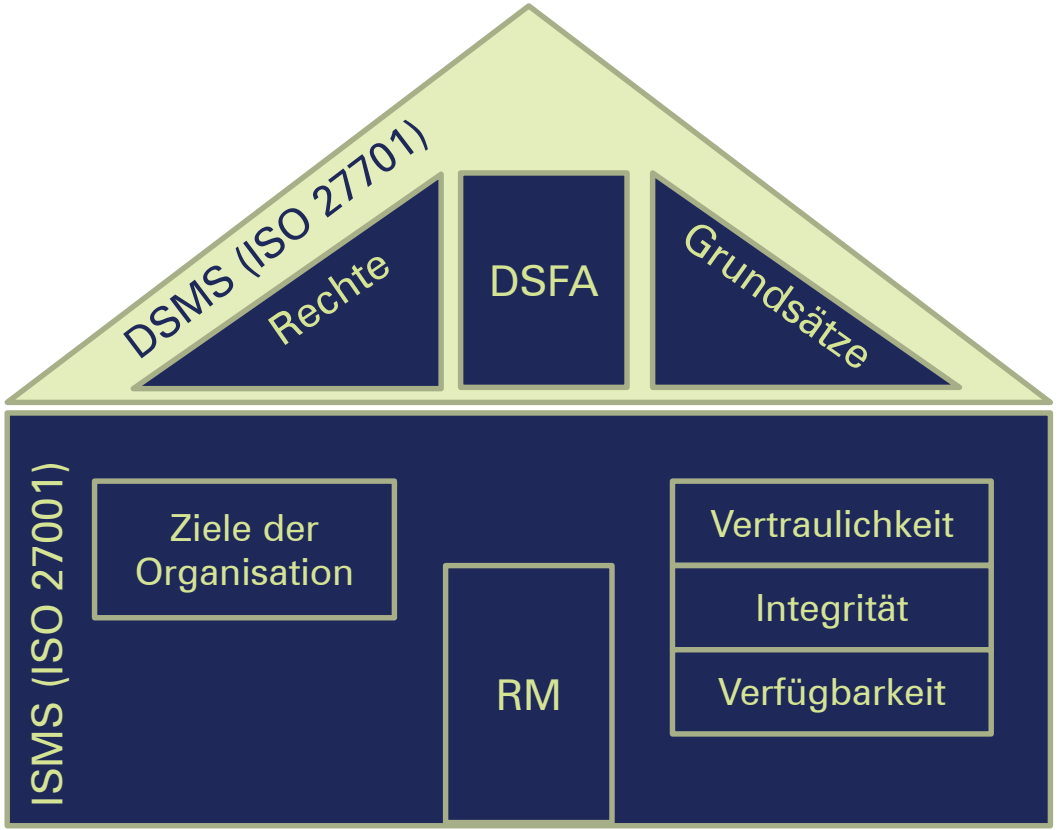
secuvera

Erweiterung des ISMS



secuvera

Erweiterung des ISMS



secuvera

ISO 27701

- Erweiterung zur ISO 27001 und ISO 27002 für das Datenschutzmanagement
- Anforderungen und Leitfaden
- Gültige Fassung seit August 2019
- Entwurfsfassung als ISO 27552

secuvera

High Level Structure

1. Anwendungsbereich
2. Normative Verweise
3. Begriffe
4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung

secuvera

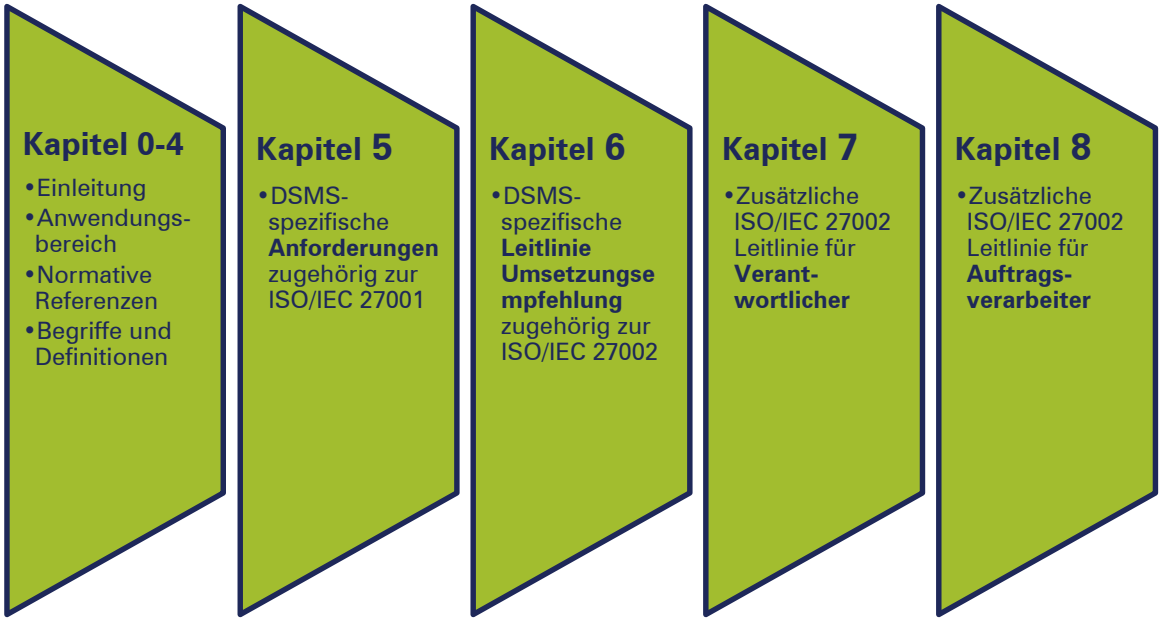
Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

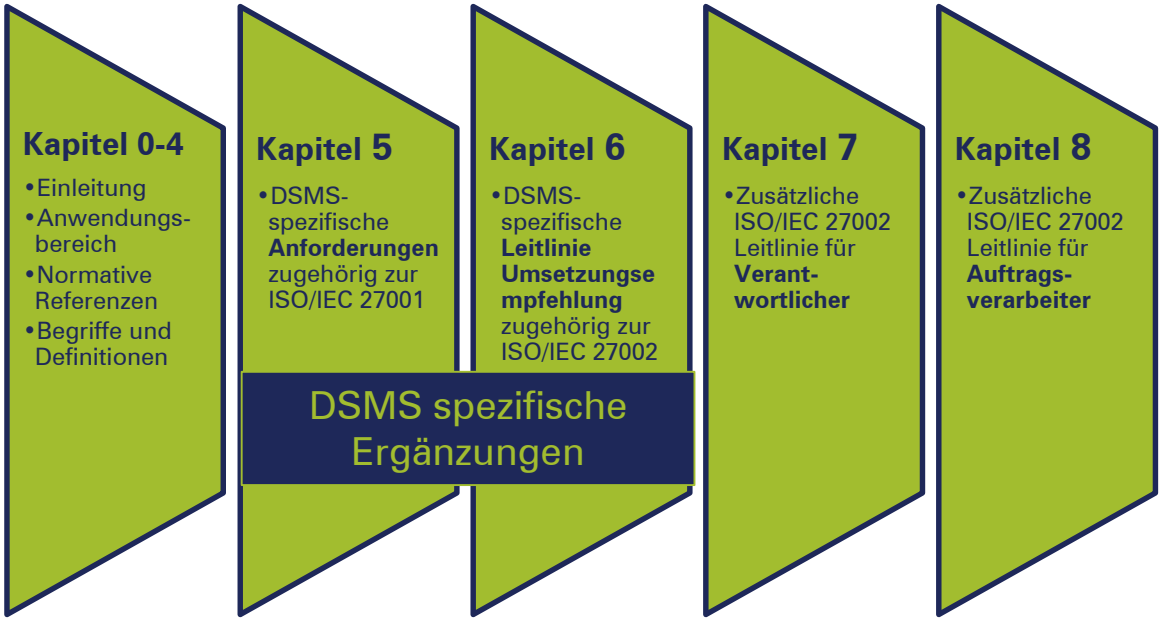
ISO 27701

Struktur / Inhalt



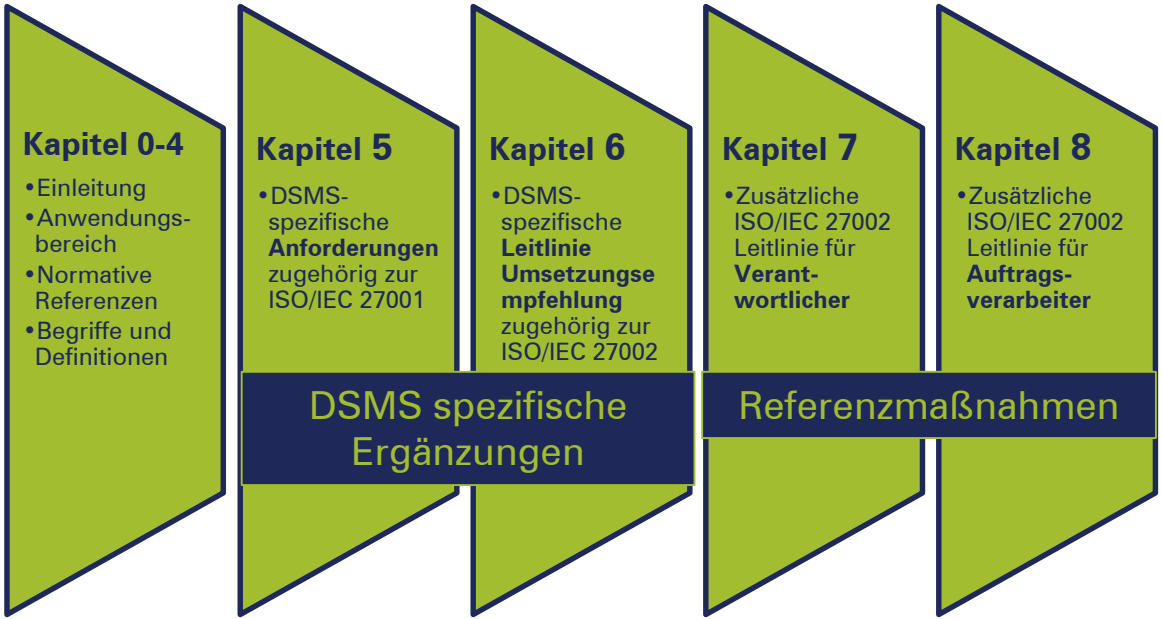
secuvera

ISO 27701 Struktur / Inhalt



secuvera

ISO 27701 Struktur / Inhalt



secuvera

ISO 27701

Struktur / Inhalt

secuvera

ISO 27701

Struktur / Inhalt

secuvera

ISO 27701

Struktur / Inhalt

secuvera

Kontext der Organisation

- Rolle der Organisation
  - Verantwortlicher
  - Auftragsverarbeiter
- Interessierte Parteien, insbesondere
  - betroffene Personen
  - interne interessierte Parteien
  - Aufsichtsbehörden

- Geltungsbereich
  - Unternehmensbereiche und deren Systeme in denen personenbezogene Daten verarbeitet werden
- Schnittstellen
  - Schnittstellen mit Bezug zur Verarbeitung von personenbezogenen Daten aufnehmen

➢ Geschäftsprozesse und Unterstützungsprozesse im VdV

secuvera

Politik

- Datenschutzleitlinie
  - definiert übergreifend Vorgaben des Datenschutzes
  - Bekenntnis zum Datenschutz
  - Zielsetzung in Bezug auf Datenschutz
    - Stellenwert in der Organisation
    - Grundlegende Leitsätze

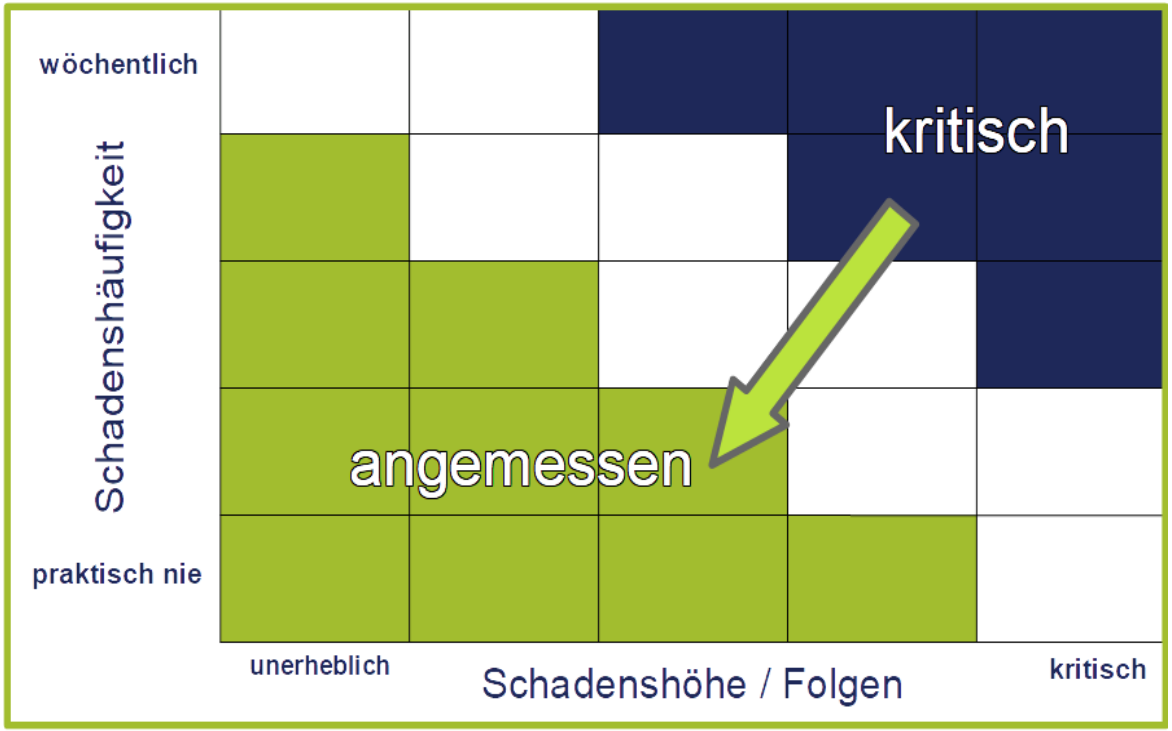
secuvera

Risiko-management

- Risiken für die betroffene Person bei der Verarbeitung personenbezogener Daten
  - Auswirkungen für die betroffene Person betrachten
  - keine zwingende Betrachtung daraus folgender Unternehmensrisiken
- Abdeckung durch DSFA

secuvera

Matrix



secuvera

Bewertung

- Wirksamkeit überprüfen
  - Bewertung der Leistung
  - Bericht an das Management
  - Managementbewertung
- Interne Audits durchführen
  - Aufdecken von Nichtkonformitäten
  - Identifikation von Verbesserungspotenzial

secuvera

Verbesserung

- Behandlung von Nichtkonformitäten
  - Bewertung
  - Ursachenbestimmung
- Entsprechende Korrekturmaßnahmen
  - dokumentieren
  - umsetzen
  - überprüfen

➢ Kontinuierliche Verbesserung

secuvera

Maßnahmen

- Referenzmaßnahmen
  - Anhang A für Verantwortlicher
    - 31 Maßnahmen
  - Anhang B für Auftragsverarbeiter
    - 18 Maßnahmen
- Umsetzungsempfehlungen
  - Kapitel 7 für Verantwortlicher
  - Kapitel 8 für Auftragsverarbeiter

secuvera

Maßnahmenziele	**Verantwortlicher** Anhang A | Kapitel 7	**Auftragsverarbeiter** Anhang B | Kapitel 8
Voraussetzungen für die Datenerhebung & Verarbeitung	A.7.2	A.8.2
Verpflichtungen gegenüber der betroffenen Person	A.7.3	A.8.3
Privacy by Design & Privacy by Default	A.7.4	A.8.4
Mitbenutzung, Übermittlung und Transfer	A.7.5	A.8.5

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

Zertifizierung nach Art. 42

- Art. 42 DS-GVO erwähnt explizit die Möglichkeit eines Zertifikats

  „Zertifizierungsverfahren […], die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.“

- Anforderungen an Zertifizierungsstellen in Art. 43 DS-GVO aufgeführt

➢ **Derzeit** keine Zertifizierung im Sinne eines DS-GVO Zertifikats möglich

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

Resümee

- Anwendung bewährter MS-Prozesse für
  - Steuerung
  - Nachweis
  - Kontinuierliche Verbesserung

  zur Erreichung von Datenschutzzielen
- Ganzheitlicher Ansatz
- Fundierte Maßnahmen
- Berücksichtigung der Ergebnisse des ISMS

secuvera

Inhalt

- Über uns
- Datenschutzmanagement
- DSMS nach der ISO 27701
- Art. 42 DS-GVO
- Resümee
- Diskussion

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank für die Aufmerksamkeit!

Bei Fragen und Anregungen sprechen Sie uns gerne an

Ihre Ansprechpartner:

Björn Lemberg
blemberg@secuvera.de
+49 7032 9758 19

Ann-Kathrin Udvary
audvary@secuvera.de
+49 7032 9758 48