entplexit
make IT simple

Datenschutz – Rechtliche Auswirkungen der Digitalisierung im Mittelstand

Oliver Greiner

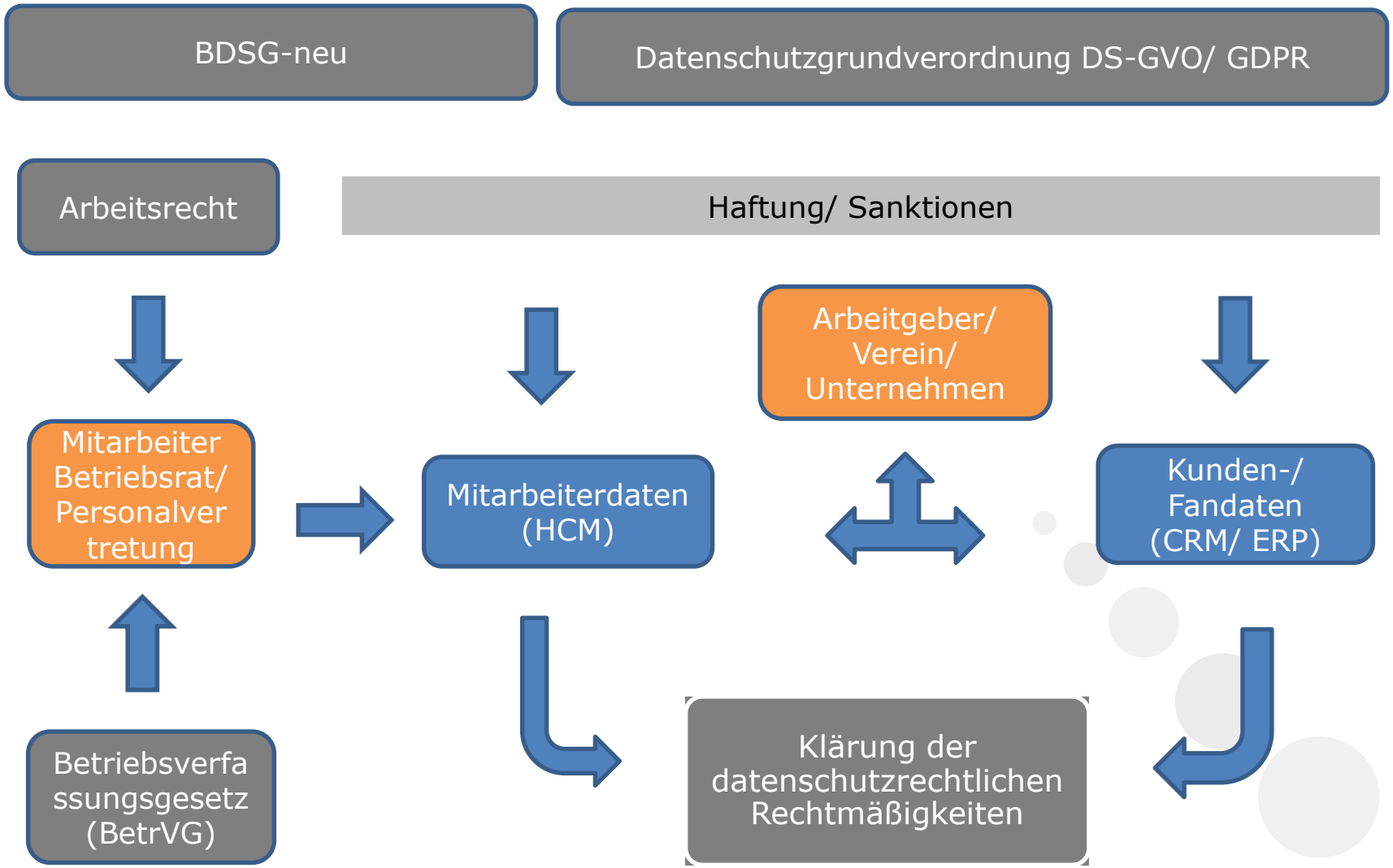
Datenschutzbeauftragter &
Datenschutzauditor

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Überblick aus der Praxis

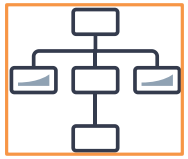
1. Kurze Einführung DSGVO – BDSG (neu)
2. Praktische Aufgaben des Datenschutzbeauftragten
3. Verzeichnis der Verarbeitungstätigkeiten (VVT)
4. Technische und organisatorische Maßnahmen aus der Praxis
5. Datenschutzfolgeabschätzung (DSFA)
6. Auftragsverarbeitung in der Praxis
7. Auditierung und Zertifikate – ISO27001/ BSI Grundschutz

Überblick der Gesetzgebung Innenverhältnis/ Außenverhältnis (Kunde/ Mitarbeiter)



2. Aufgaben des Datenschutzbeauftragten

Welche Verantwortlichkeiten benötige ich für den Datenschutz?



- Verantwortlichkeiten müssen definiert sein
- Datenschutz muss von der Geschäftsführung unterstützt werden!

GL

IT

DSB

HR

Legal

Marketing

Drei interne Hauptaufgaben im Unternehmen

1. Unterrichtung und Beratung - Art. 38 Abs. 1 Buchst. b verlangt die Überwachung der Einhaltung der DSGVO
   a. **Überwachung der Einhaltung von Vorgaben**
      a. Überwachung
      b. Sensibilisierung und Schulung der Mitarbeiter
      c. Datenschutzfolgeabschätzung (DSFA) - Art. 39 Abs. 1 Buchst. c DSGVO
      d. Prüfung Auftragsverarbeitung
2. Verhältnis zur Aufsichtsbehörde
   a. Zusammenarbeit und Kommunikation mit der Aufsichtsbehörde - 39 Abs. 1 Buchst. d DSGVO
   b. Meldung bei der Aufsichtsbehörde
   c. Meldung von Datenschutzverletzungen an die Aufsichtsbehörde
3. Ansprechpartner für Betroffene
   a. Adressierung der Betroffenenrechte
   b. Kontaktdaten des Datenschutzbeauftragten müssen bekannt sein

In der Praxis – Beispiele an Aufgaben

- Erstellung und/ oder Bearbeitung Verzeichnis der Verarbeitungstätigkeiten (VVT)
- Prüfung Auftragsverarbeitungsvertrag (AVV)
- Schulung Mitarbeiter
- Erstellung diverser Muster (Verpflichtungserklärung etc.)
- Erstellung in Zusammenarbeit mit den Fachbereich und Prüfung der technischen und organisatorischen Maßnahmen
- Durchführung von Audits
- Bearbeitung von Auskunftsersuchen
- Bearbeitung von Löschersuchen
- Bearbeitung von Datenschutzvorfällen

In der Praxis – Verzeichnis der Verarbeitungstätigkeiten (VVT)

Welcher Inhalt muss in ein VVT nach Art. 30 DSGVO?

- Name des Verfahren
- Als Auftragsverarbeiter (j / n)
- Datum der Erfassung
- Kontaktdaten der verantwortlichen Stelle -> Unternehmen
- Beschreibung der Verarbeitung / Zweck
- Betroffene Personengruppen
- Betroffene Daten
- Empfänger der Daten, ggfls. Empfänger der Daten in einem Drittland
- Beschreibung der Absicherung der Datenübermittlung in das Drittland/ Zertifikate
- Löschfrist -> Verweis auf das Löschkonzept

In der Praxis – Verzeichnis der Verarbeitungstätigkeiten (VVT)

Was sollte vermieden werden?

- Ein Verfahren pro System oder Abteilung erstellen!
- Eine zu granulare Übersicht erstellen!
- Nicht mehr als 10 VVT erstellen!

TIPP:
Erstellen Sie ein Verfahren pro Hauptprozess bei der Verarbeitung!

- Personaldatenverarbeitung
- Bewerbermanagement
- Kundenverwaltung mit Rechtsbeziehung
- Kundenbeziehung ohne Rechtsbeziehung (z.B. Newsletter)
- Lieferantenverwaltung

Technische und organisatorische Maßnahmen - TOM´s

Alt: §9 BDSG
Neu: Art. 32 DSGVO & §64 BDSG (neu)

Was ändert sich? -> nicht so viel

Zukünftig spricht man von „geeigneten“technischen und organisatorischen Maßnahmen.

<u>NACHWEISPFLICHT</u>
Nach Art. 5 Abs. 2 der EU-Datenschutzgrundverordnung besteht eine *Rechenschaftspflicht*. die verantwortliche Stelle wird also Nachweise erbringen müssen, dass die Sicherheit der Verarbeitung gewährleistet wird.

TOM´s im Detail nach §64 BDSG

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte **(Zugangskontrolle),**
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern **(Datenträgerkontrolle),**
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten **(Speicherkontrolle),**
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte **(Benutzerkontrolle),**
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben **(Zugriffskontrolle),**

TOM´s im Detail nach §64 BDSG

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können **(Übertragungskontrolle),**
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind **(Eingabekontrolle),**
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden **(Transportkontrolle),**
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können **(Wiederherstellbarkeit),**
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden **(Zuverlässigkeit),**

TOM´s im Detail nach §64 BDSG

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Durchgehen anhand eines Beispiels – TOM´s

5. Datenschutzfolgeabschätzung (DSFA)

Datenschutzfolgeabschätzung – DSFA - **Art. 35 DSGVO**

Wann muss ich eine DSFA machen?

1. …. Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge,…..

2. Speziell bei:
    1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen – Profiling/ Scoring
    2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1
    3. oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

5. Datenschutzfolgeabschätzung (DSFA)

Datenschutzfolgeabschätzung – DSFA - **Art. 35 DSGVO**

Was beinhaltet eine DSFA?

- systematische Beschreibung der geplanten Verarbeitungsvorgänge
- Zwecke der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren

- Checkliste DSFA
- Muster DSFA

6. Auftragsverarbeitung in der Praxis

Auftragsverarbeitung nach Art. 28 DSGVO

Welche Dokumente benötige ich bei einer Auftragsverarbeitung?
- TOM´s
- Übersicht der Subunternehmer beim Auftragnehmer
- AV-Vertrag wäre gut

Tipp:
- Verweisen Sie im AV-Vertrag auf eine Liste der weiteren Auftragnehmer.
- Achten Sie auf die Formulierungen bezüglich der Haftung und auf die Kontrollrechte des Auftraggebers.

7. Auditierung und Zertifikate

Auditierung und Zertifikate – ISO27001/ BSI Grundschutz

Art. 42 DSGVO Zertifizierung

…Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird…..

7. Auditierung und Zertifikate

Übersicht ist zu finden unter:

https://stiftungdatenschutz.org/zertifizierung/zertifikate-uebersicht/ &

https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Zertifizierungsuebersicht/SDS-Zertifizierungsuebersicht_02_2017.pdf

Es Bedarf einer Akkreditierung der Zertifizierungsstelle im Sinne von § 39 BDSG.

- Althammer & Kill GmbH & Co. KG
- datenschutz cert GmbH
- ePrivacy GmbH
- interev GmbH
- Institut für organische Informationssysteme INOIS (entplexit)
- ISiCO Datenschutz GmbH

7. Auditierung und Zertifikate

Aktuell gibt es kein abgestimmtes Vorgehen was und wie geprüft wird.

Welche Prüfmöglichkeiten gibt es aktuell und was ist zu empfehlen?

ISO 27001 (nativ)
Dieser Standard ist eher prozessorientiert, da hier die Prozesse der Informationssicherheit betrachtet werden. Ein wichtiger Bestandteil des ISMS ist eine Risikoanalyse zur Identifikation von Risiken und deren Behandlung. Zudem muss sich das Unternehmen zu den ca. 150 allgemein gefassten Maßnahmen der ISO Norm erklären. Dabei bietet die Norm keine konkreten Handlungsempfehlungen, so dass das Unternehmen bei der Umsetzung der Maßnahmen zwar relativ frei ist, die Details aber selbst erarbeiten muss (eine Orientierung an ISO 27002 oder BSI IT-Grundschutz kann dabei behilflich sein). Zu beachten ist, dass es eine ISO 27000ff Normenreihe gibt, wobei Grundlage einer Zertifizierung immer **nur** ISO 27001 ist. Die übrigen Standards wie z.B. ISO 27018 für Cloud Computing bieten u.a. eine Hilfestellung an. Unternehmen können diesem Standard entsprechen, nicht aber danach zertifiziert werden.

ISMS - Informationssicherheits-Managementsystem (ISMS)

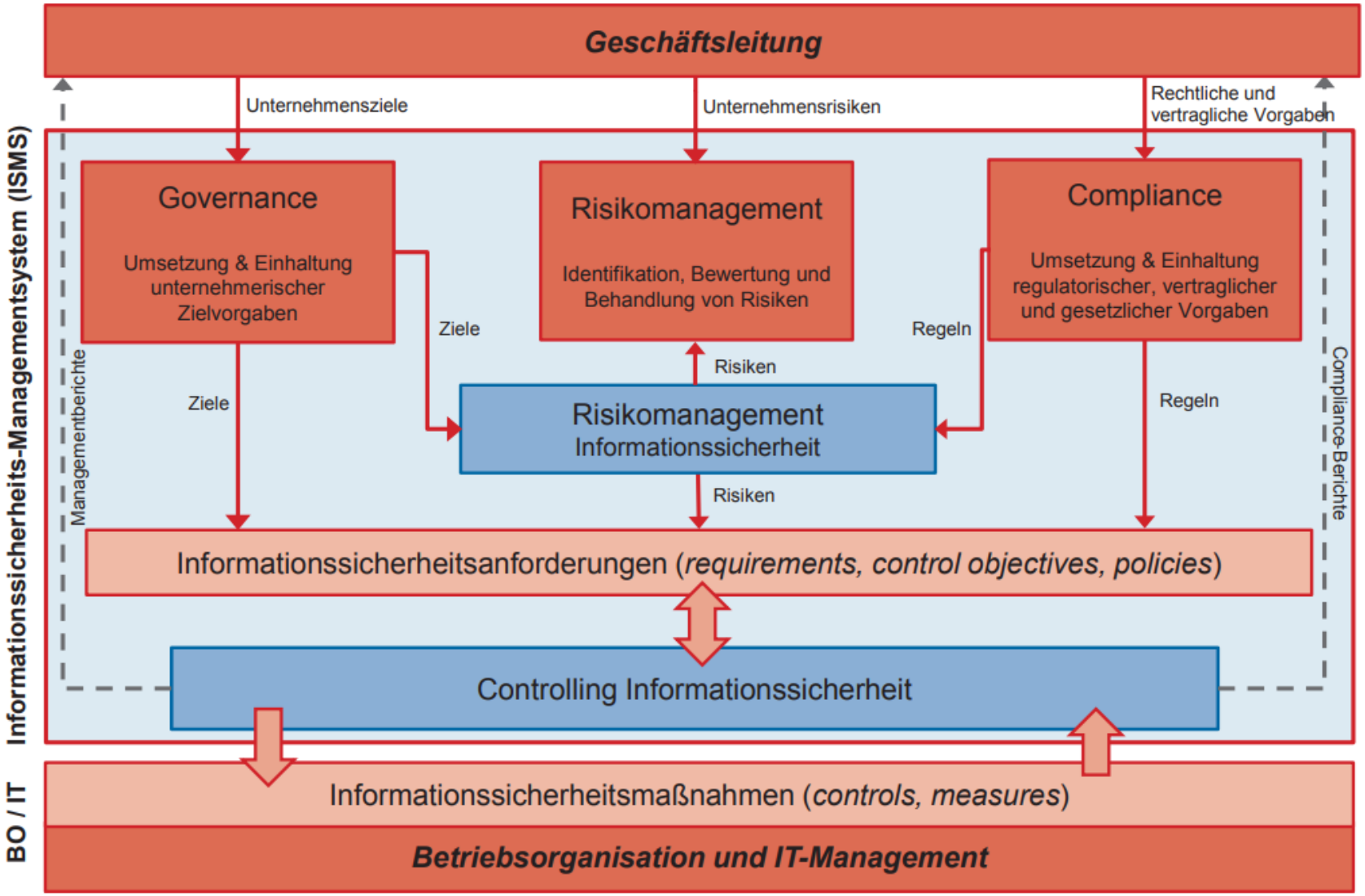
7. Auditierung und Zertifikate

ISO 27001 auf der Basis von IT-Grundschutz
Dieser Standard ist eher maßnahmenorientiert. Das BSI nimmt den Unternehmen die Arbeit ab und bewertet typische Gefährdungen selbst, so dass eine umfassende Risikoanalyse entfallen kann. Um diesen umfassenden Grundschutz zu realisieren, muss das Unternehmen jedoch eine Vielzahl von konkreten Maßnahmen tatsächlich umsetzen, was sehr aufwendig sein kann. Eine Risikoanalyse ist dann nur bei Systemen mit höheren Schutzbedarf durchzuführen, was an hier wiederum Arbeit erspart. Der Grundschutz wird zurzeit vom BSI modernisiert.

Leitfaden für eine

https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_i_gesamt_web.pdf

7. Auditierung und Zertifikate

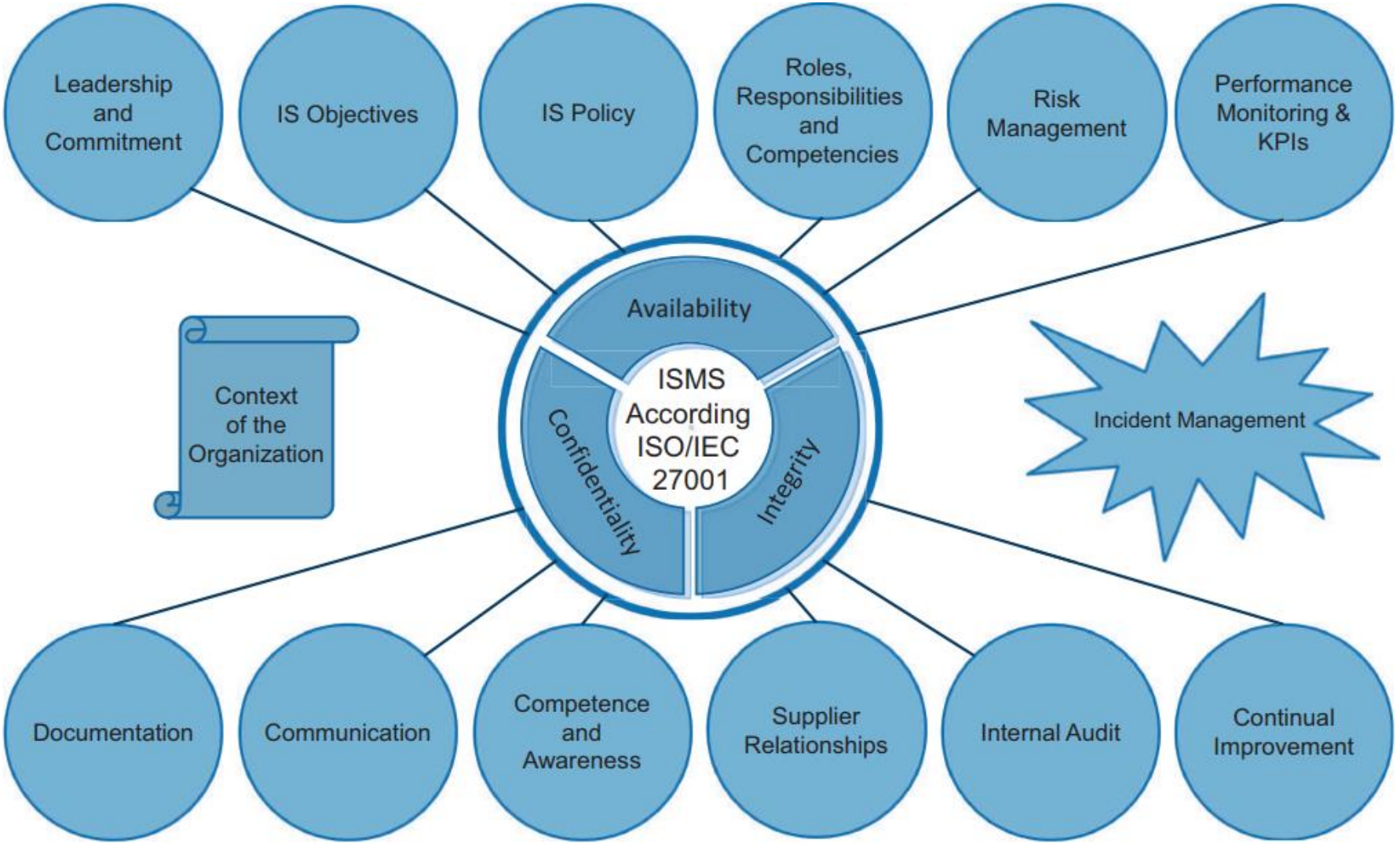


7. Auditierung und Zertifikate

Themenbereiche einer ISO27001 Zertifizierung

1. Context of the Organization
2. Leadership and Commitment
3. IS Objectives
4. IS Policy
5. Roles, Responsibilities and Competencies
6. Risk Management
7. Performance Monitoring & KPIs
8. Documentation
9. Communication
10. Compentence and Awareness
11. Supplier Relationships
12. Internal Audit
13. Incident Management
14. Continual Improvement

7. Auditierung und Zertifikate



7. Auditierung und Zertifikate

Fazit:

Empfehlung ist, dass eine Zertifizierung nach ISO27001 angestrebt wird, jedoch maßnahmenorientiert, nach BSI Grundschutz.

Aktuell ist es zu früh, um eine rechtskonforme Zertifizierung zu empfehlen.

Probleme:

Beide Normen, sowohl BSI-Grundschutz und ISO27001 sind zu älter.

BSI Grundschutz wird aktuell aktualisiert.

ISO27001 ist zu umfangreich für ein mittelständisches Unternehmen.

Kontaktdaten

Vielen Dank für Ihre Aufmerksamkeit!

Oliver Greiner

entplexit GmbH
Kölner Straße 12
65760 Eschborn

Tel: +49 6196 97344 00
datenschutz@entplexit.com