SEC4YOU

Advanced IT-Audit Services

Datenschutzgrundverordnung

Technische und organisatorische Maßnahmen gemäß Artikel 32

Manfred Scholz / 18.1.2018 V1.1

Einführung

- **Was** ist zu tun?
- **Wie** ist es zu tun?
- **Wo** ist es zu tun?
- **Wer** muss es tun?

Einführung

Betrachtung der Anforderungen der DSGVO
aus fachlicher Sicht

Begriffsdefinitionen

Personenbezogene Daten

Alle Informationen, die sich auf eine
identifizierte oder **identifizierbare** natürliche Person
beziehen (betroffene Person)

(Artikel 4 Abs. 1)

Begriffsdefinitionen

Besondere Kategorien personenbezogener Daten

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- das Sexualleben oder die sexuelle Orientierung
- Gesundheitsdaten
- **genetische und biometrische Daten**

(Artikel 9 Abs. 1)

Begriffsdefinitionen

Der Verantwortliche

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
die allein oder gemeinsam mit anderen
über die Zwecke und Mittel der Verarbeitung entscheidet.

(Artikel 4 Abs. 7)

Begriffsdefinitionen

Der Auftragsverarbeiter

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
die personenbezogene Daten
im **Auftrag des Verantwortlichen** verarbeitet.

(Artikel 4 Abs. 8)

Anforderungen an den Verantwortlichen (Art. 24 Abs. 1)

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen um, um sicherzustellen** und den **Nachweis dafür erbringen** zu können, **dass die Verarbeitung gemäß dieser Verordnung erfolgt**.

Datenschutz by Design (Art. 25 Abs. 1)

… **trifft der Verantwortliche** sowohl **zum Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** - wie z. B. Pseudonymisierung - trifft, die dafür ausgelegt sind, die **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die notwendigen **Garantien** in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Datenschutz by Default (Art. 25 Abs. 2)

Der **Verantwortliche** trifft **geeignete technische und organisatorische Maßnahmen**, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Sicherheit der Verarbeitung (Art. 32 Abs. 1)

Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und Schwere des **Risikos** für die **Rechte und Freiheiten natürlicher Personen** treffen der **Verantwortliche** und der **Auftragsverarbeiter** **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Sicherheit der Verarbeitung

a) die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten** und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;

d) ein Verfahren zur **regelmäßigen Überprüfung** Bewertung und Evaluierung der **Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(Artikel 32 Abs. 1)

Ausgangssituation

Definitionen

IT-Kontrollen (Controls)

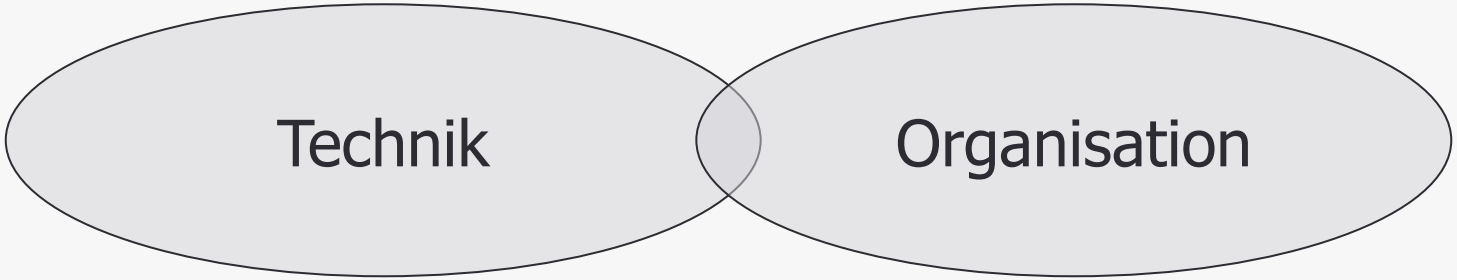
- Maßnahmen (z.B. Richtlinie, Zutrittsschutz, Firewall, etc.)
- Das Risiko soll vermindert bzw. beherrscht werden
- Verhinderung, Erkennung oder Korrektur
- Geschäftsziel wird mit höherer Wahrscheinlichkeit erreicht

Definitionen

Kontrollziel (Control Objective)

- Definiertes Ziel einer IT-Kontrolle
- Wird durch **wirksame** Kontrollen erreicht

IT-Kontrollen



Kombination aus

technischen und organisatorischen Maßnahmen (TOM‘s)

Anwendungsunabhängige Kontrollen (General Controls)

Eigenschaften

- High Level Controls
- Erstrecken sich über das gesamte Unternehmen
- Nicht an eine Applikation gebunden

Beispiele

- IT-Strategie
- Organisation
- Risikomanagement
- Benutzerverwaltung
- Systementwicklung
- **Changemanagement**
- Notfallplanung
- Physischer Sicherheit
- Schulung/Ausbildung

Anwendungsabhängige Kontrollen (Application Controls)

Eigenschaften

- Stellen sicher das nur vollständige, genaue und gültige Daten verarbeitet werden
- Ergebnisse entsprechen den Erwartungen
- Daten werden angemessen gewartet
- Doppelte Transaktionen werden erkannt

Beispiele

- Passwörter
- Prüfsummen
- **Einfache Eingabemasken**
- Signaturen
- Fehlerkorrektur Prozeduren
- Transaktionsprotokoll
- Versionsverwaltung
- Fortlaufende Nummerierung

Effektivität von IT-Kontrollen

Design Effektivität

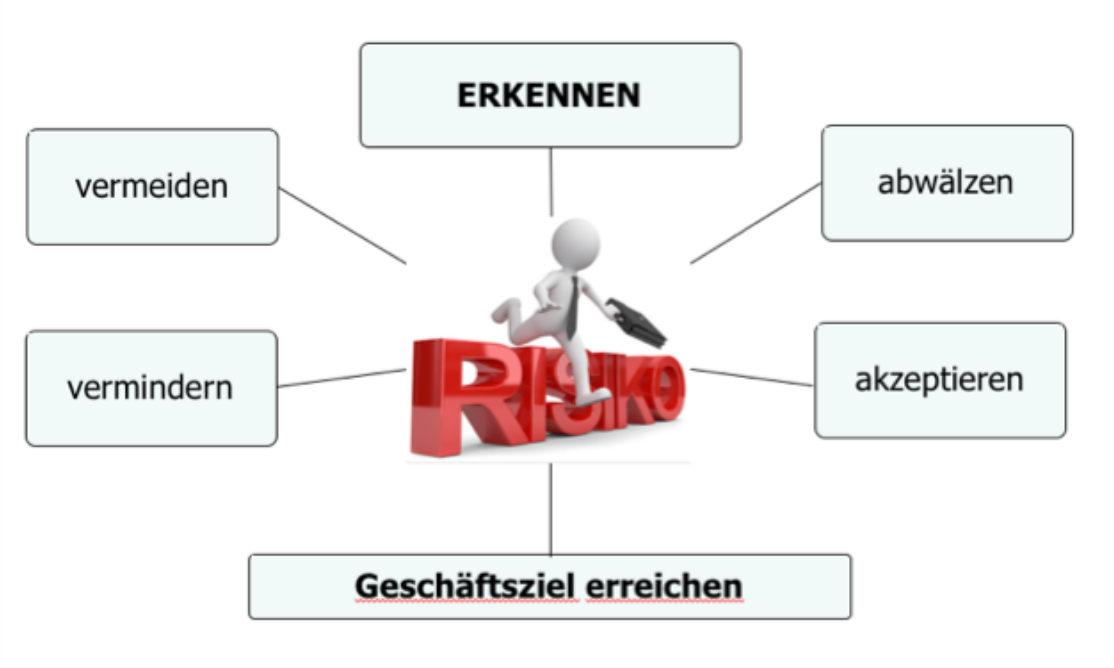
Eine IT-Kontrolle ist **grundsätzlich geeignet** die ihr zugrundeliegenden Risiken zu beherrschen.

+

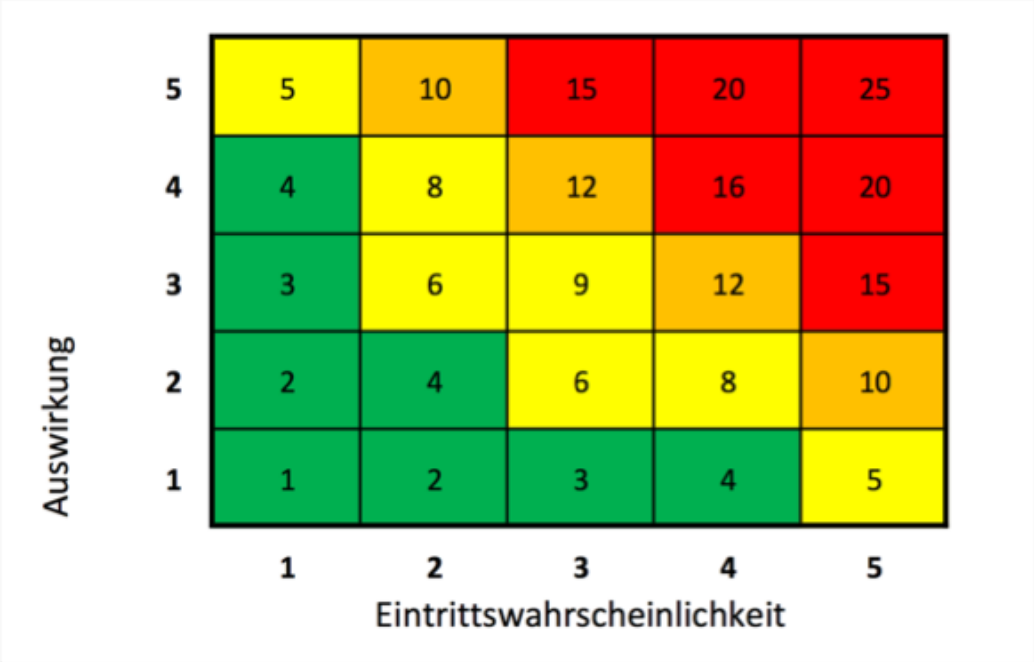
Operative Wirksamkeit

Die IT-Kontrolle **ist wie vorgesehen implementiert** bzw. wird in der täglichen Praxis **tatsächlich angewendet**.

Risikomanagement



Risikomanagement



Sicherheit der Verarbeitung

Sicherheitsrisiken müssen auf ein **akzeptables** Maß reduziert werden!

Einsatz von Normen und Standards als Lösungsansatz

… gelten als Stand der Technik!

Normen und Standards

Gemeinsame Regeln führen zu vergleichbaren Ergebnissen

Herausforderungen bei der Auswahl

Grundschutzkataloge (BSI)

ISO/IEC 20000

IT-SEC

ITIL

COBIT

Six Sigma

ISAE 3402

Österreichische Sicherheitshandbuch

ISO TR 13335

ISO/IEC 27001

Allianz für Cybersicherheit

NIST

ISO 27033

OWASP

ÖNORM S2109

ÖNORM A7700

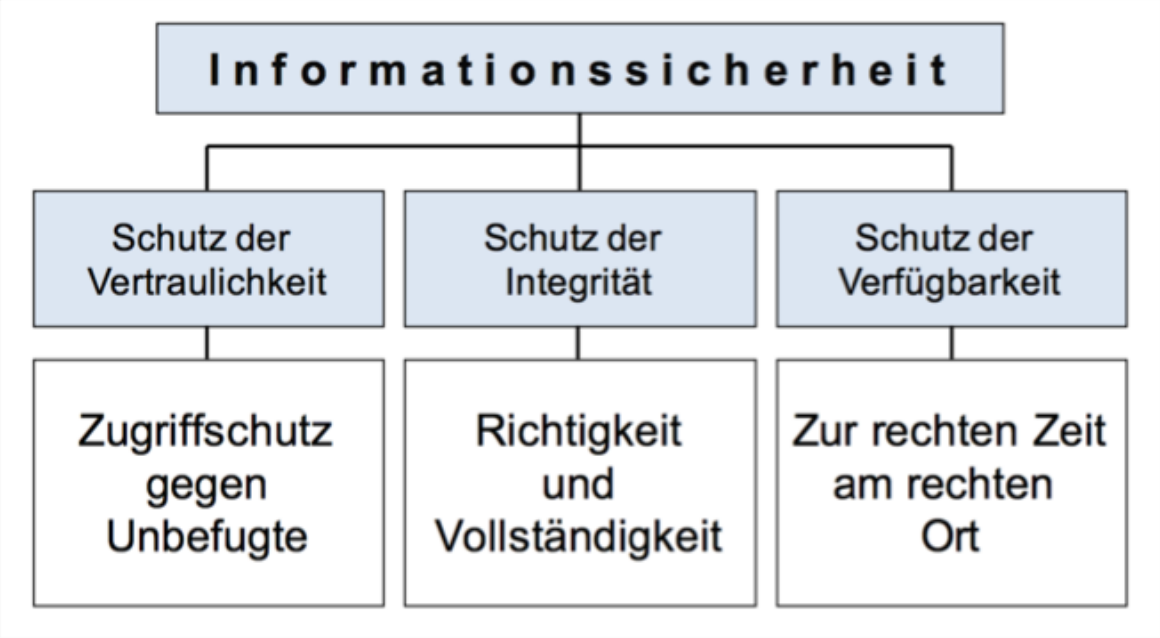
Eurocloud Star Audit

Zertifizierungen

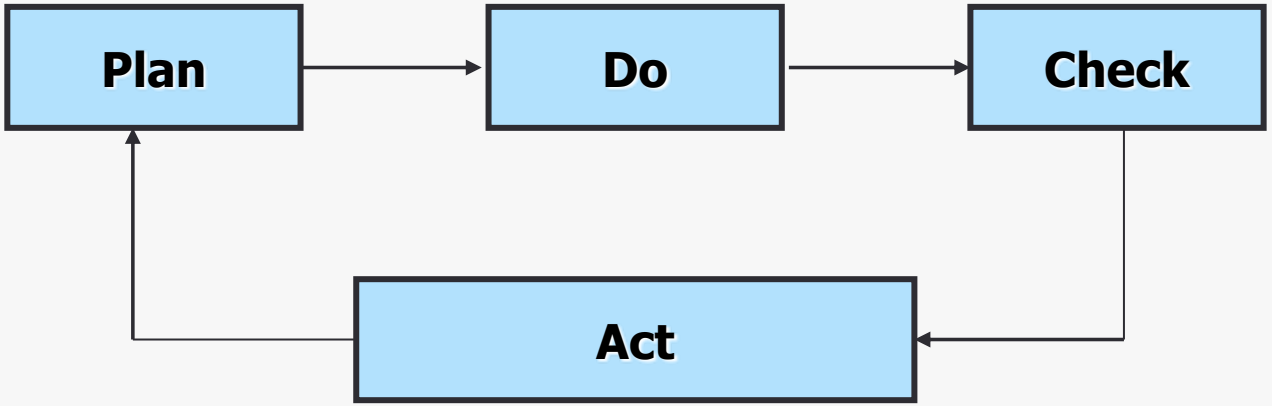
Zertifizierung

Information Security Management Systeme (ISMS)

ISMS nach ISO 27001



ISMS nach ISO 27001



Einführung eines KVP-Prozesses

ISO 27001 (Kapitel 4-10)

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Einsatz
9. Leistungsauswertung
10. Verbesserung

ISO 27001 (Anhang A)

A.5 Sicherheitsleitlinien

A.6 Organisation der Informationssicherheit

A.7 Sicherheit des Personals

A.8 Wertemanagement

A.9 Zugriffskontrolle

A.10 Kryptographie

A.11 Schutz vor physischen Zugang und Umwelteinflüssen

ISO 27001 (Anhang A)

A.12 Betriebssicherheit

A.13 Sicherheit der Kommunikation

A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen

A.15 Lieferantenbeziehungen

A.16 Management von Informationssicherheitsvorfällen

A.17 Informationssicherheitsaspekte des BCM

A.18 Richtlinienkonformität

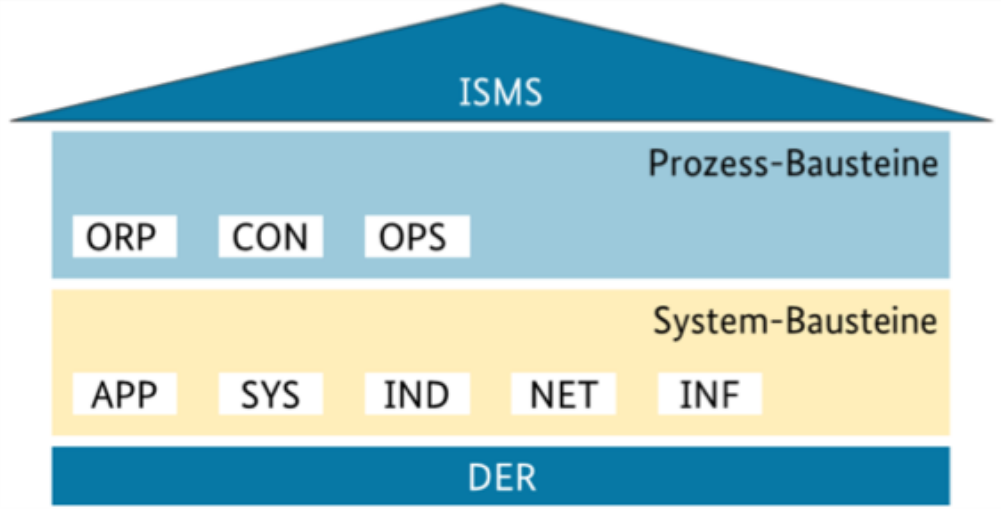
… definiert 114 Maßnahmen (Kontrollen)

IT-Grundschutzkataloge (BSI)

- Bundesamt für Sicherheit in der Informationstechnik
- Vorwiegend im Deutschen Sprachraum
- Sammlung von Maßnahmen (Bausteinen)
- Durchführung von Risikoanalysen
- Zertifizierbar (27001 ++)

https://www.bsi.bund.de

IT-Grundschutz Kompendium



Schichtenmodell des IT-Grundschutzes (BSI)

BSI-Standards (200)

In 3 Schritten zur Informationssicherheit

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Leitfaden_Basisabsicherung/Leitfaden_Basisabsicherung_node.html

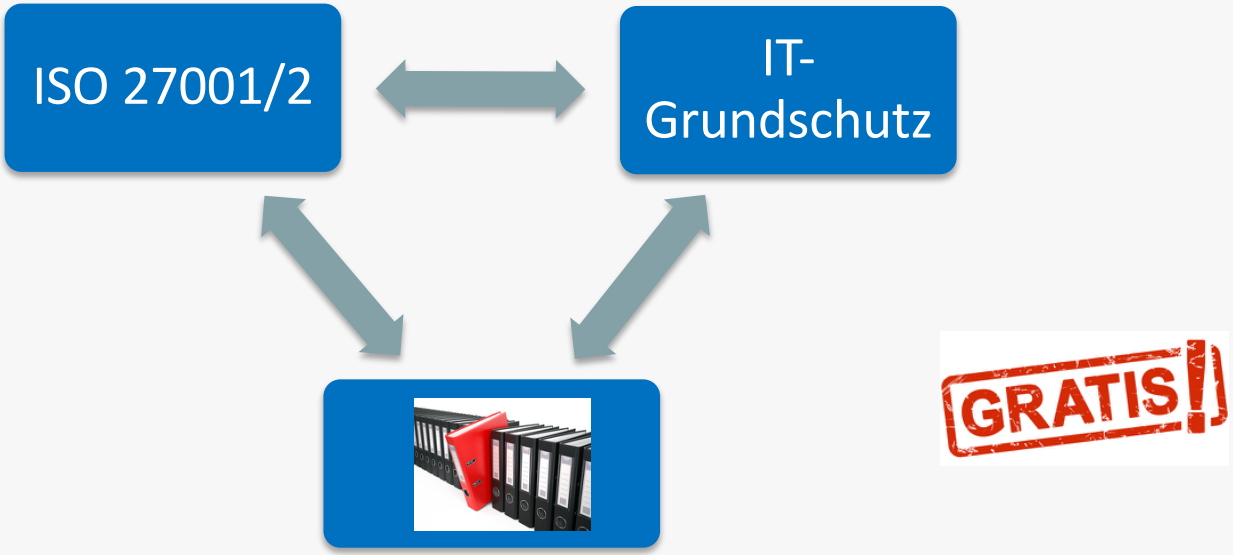
BSI-Standards (200)

- 200-1: Managementsysteme für Informationssicherheit
- 200-2: IT-Grundschutz-Vorgehensweise
- 200-3: Risikomanagement

Österreichische Sicherheitshandbuch

https://www.sicherheitshandbuch.gv.at

Österreichische Sicherheitshandbuch



Risikomanagement

Management von Risiken ist auch der Mut zur Lücke !

Seminartipp

Datenschutzgrundverordnung (DSGVO) (CPE 7)

Kurstermin	CPE	Veranstaltungsort
22.01.2018	7	Akademie Interne Revision GmbH | Anfahrt

Seminarthema:

Nach vielen Jahren intensiver Verhandlungen haben sich die Mitgliedsstaaten der EU auf eine Reform des Datenschutzes in Europa geeinigt. Die DSGVO ist am 24.05.2016 in Kraft getreten und ist ab 25.05.2018 anzuwenden. In Fachkreisen wird diese Verordnung als Meilenstein für einen einheitlichen Standard für die Verarbeitung personenbezogener Daten in Europa gefeiert. Aufgrund der zahlreichen Öffnungsklauseln, die nationale Anpassungen ermöglichen, erntete diese aber auch starke Kritik. Letztendlich bleibt abzuwarten welchen Handlungsspielraum der Europäische Gerichtshof den Mitgliedsstaaten tatsächlich gewährt, oder ob der Grundgedanke der Öffnungsklauseln "Präzisierung" sehr eng ausgelegt wird.

http://www.internerevision.at/seminare/it-revision/seminar/datenschutzgrundverordnung-dsgvo-210/

Vorankündigung

DSGVO Workshop „Was & Wie“

Der richtige Umgang mit externen und internen Dienstleistern im Sinne der DSGVO - Artikel 28

23. Februar 2018

Star Inn Hotel Wien Schönbrunn, Linke Wienzeile 224, 1150 Wien

Finale

Manfred.Scholz@sec4you.com
https://sec4you.com
XING, LinkedIn
Tel.: +43 1 2531 797-10