Wie gelangt man zu einer erfolgreichen ISO 27001-Zertifizierung?

Vortrag für die Mitglieder des

Spitzenverband Digitale Gesundheitsversorgung

Dr. Michael Monka

11. Januar 2022

Dr. Michael Monka

Mittelstandsberater &
ISO 27001-Lead-Auditor / KRITIS-Auditor

www.vialevo.de
monka@vialevo.de

Siebengebirgsstrasse 200
53229 Bonn

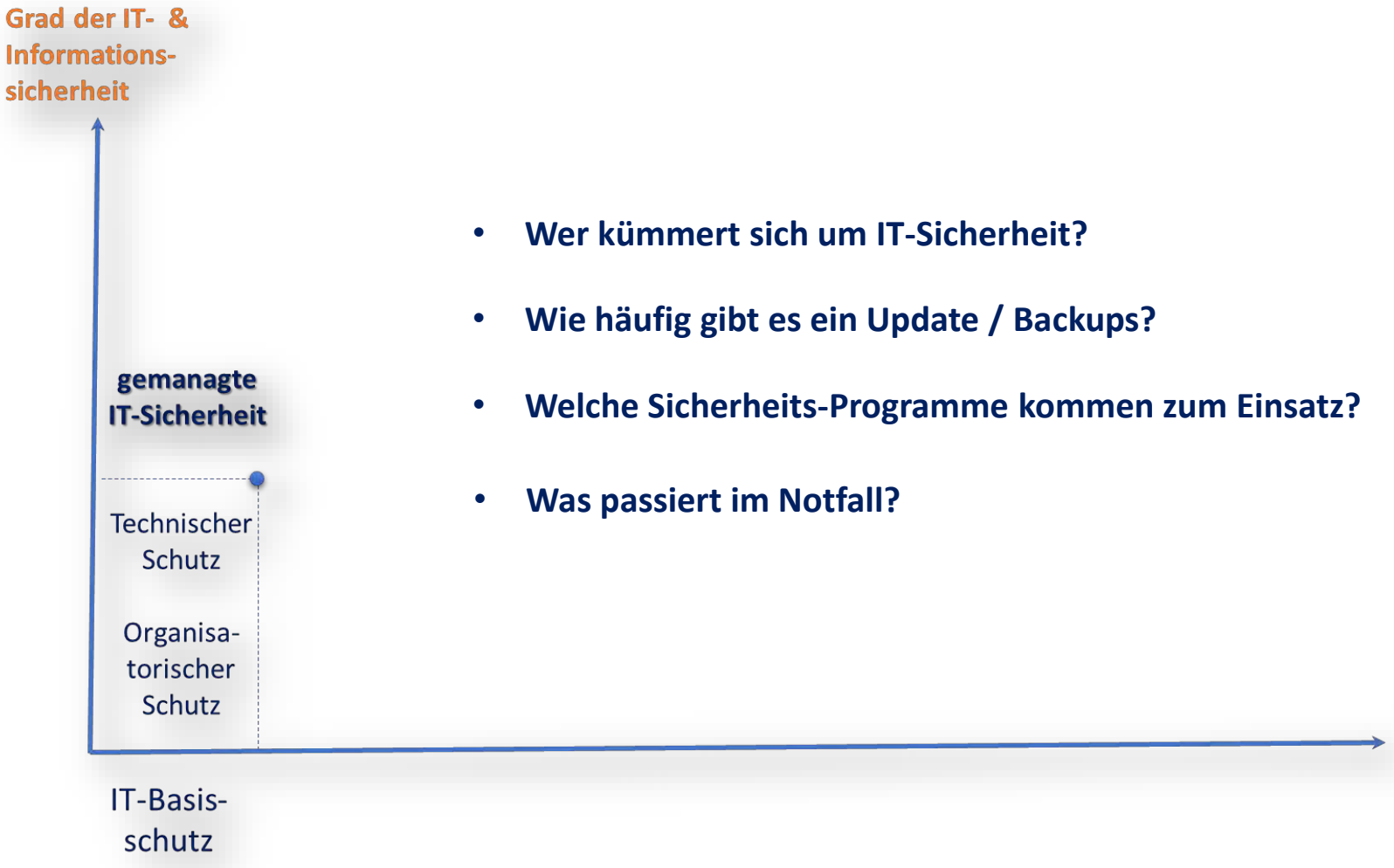
Berufliche Erfahrungen

- Wissenschaftlicher Mitarbeiter im WIdO
- Herausgeber Krankenhaus-Report
- Leiter „Integrierte Versorgung im Rheinland“

Seit 1995 beratend tätig
➲ mittelständischen Unternehmen

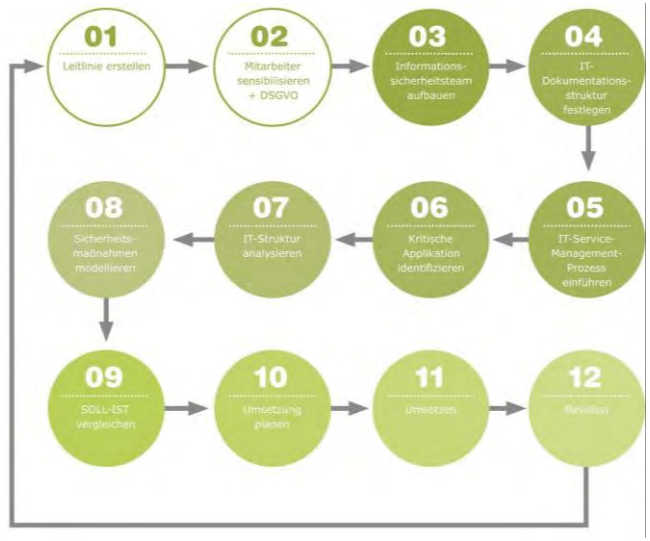
Beratungsfelder

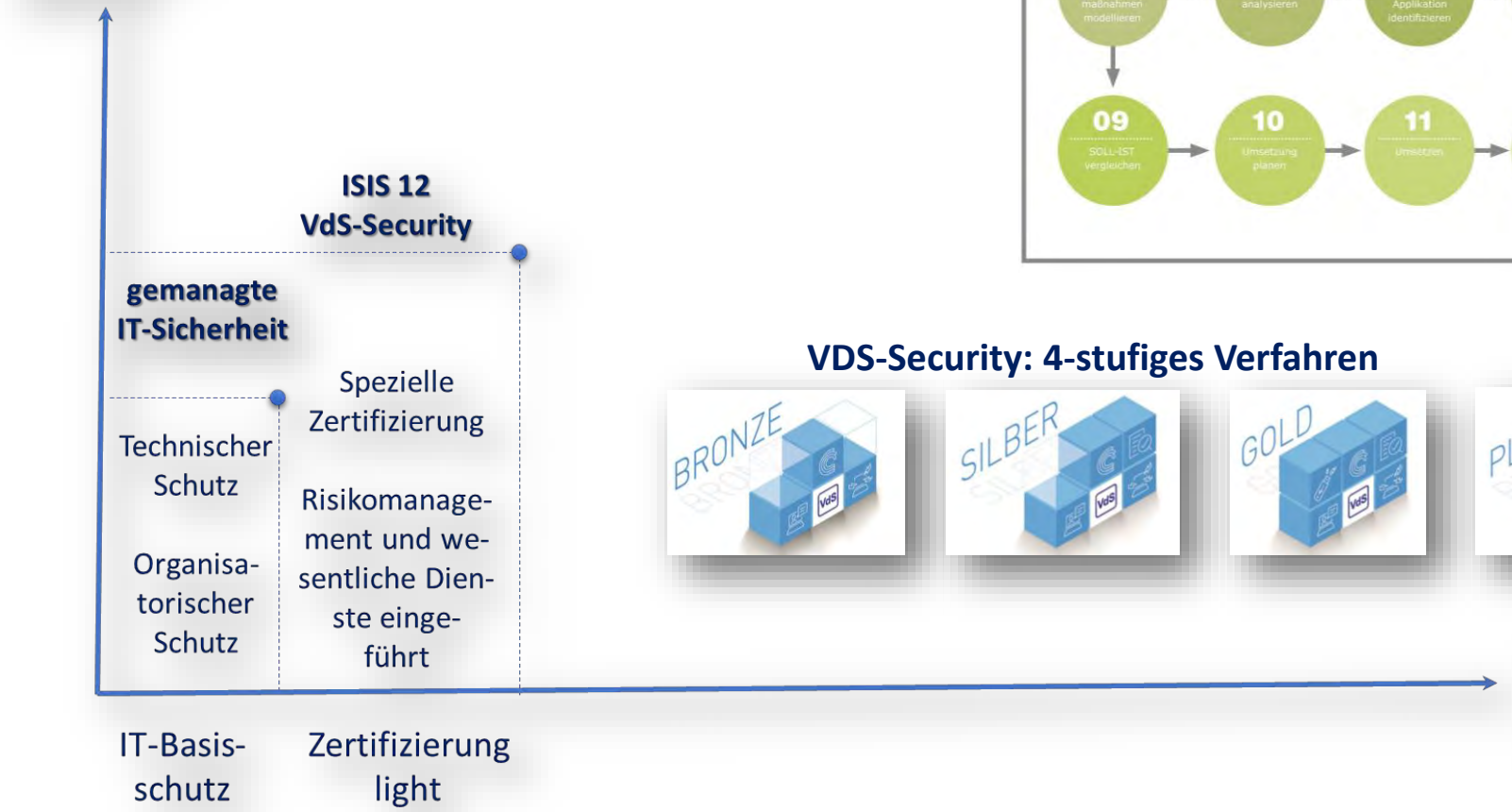
Einordnung: Das Verhältnis zwischen Aufwand und Nutzen bei der IT-Sicherheit



- **Wer kümmert sich um IT-Sicherheit?**
- **Wie häufig gibt es ein Update / Backups?**
- **Welche Sicherheits-Programme kommen zum Einsatz?**
- **Was passiert im Notfall?**

ISIS 12: 12-stufiges Verfahren





VDS-Security: 4-stufiges Verfahren

Grad der IT- & Informations-sicherheit

ISO/IEC 27001
IT-Grundschutz nach BSI

ISIS 12
VdS-Security

gemanagte IT-Sicherheit

Alle sicherheitsbezogenen Prozesse sind definiert. ISMS wird kontinuierlich optimiert. IT-Sicherheit ist messbar

Gerüstet für die Anforderungen zu kritischen Infrastrukturen (KRITIS) sowie Ausschreibungen, die eine zertifizierte IT- und Informationssicherheit verlangen

Spezielle Zertifizierung

Technischer Schutz

Risikomanage-ment und we-sentliche Dien-ste einge-führt

Organisa-torischer Schutz

Abhängig vom Scope (Anwendungsbereich)

Aufwand an Zeit und Ressourcen

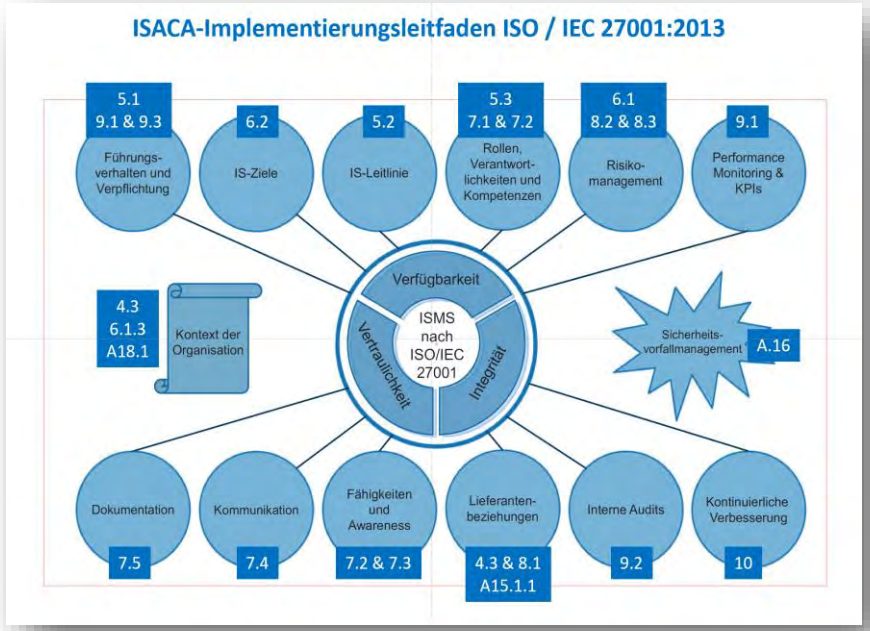
IT-Basis-schutz

Zertifizierung light

Nationale und internationale Zertifizierung

Nützliche Links vorab ...

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Downloadserver/IT-Grundschutz-Kataloge/IT-Grundschutz-Kataloge-15-EL.html



https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf

Ein empfehlenswertes Buch vorab ...

Die ISO 27001 in der Originalfassung als eBook

Eine kommentierte Fassung als Paper- und eBook

Auf die neueste Ausgabe achten!

Was ist das Ziel der ISO 27001-Norm?

ISO 27001 ist eine **internationale** Norm, die von der Internationalen Organisation für Standardisierung (ISO) veröffentlicht wurde. Sie beschreibt, wie **Informationssicherheit** in einem Unternehmen gewährleistet werden kann.

ISO 27001 kann in **jeder Art von Organisation** umgesetzt werden – kommerziell oder gemeinnützig, privat oder staatlich, klein oder groß. Der Standard wurde von weltweit führenden Experten für Informationssicherheit verfasst und stellt die Methodologie für Informationssicherheit in einem Unternehmen zur Verfügung.

Der Standard ermöglicht auch die Zertifizierung eines Unternehmens, wobei eine **unabhängige Zertifizierungsstelle** bescheinigt, dass das Unternehmen Informationssicherheit in Übereinstimmung mit ISO 27001 umgesetzt hat.

Wie ist die ISO 27001 grundsätzlich aufgebaut?

ISMS (Kapitel 4 – 10):
INFORMATION SECURITY MANAGEMENT SYSTEM

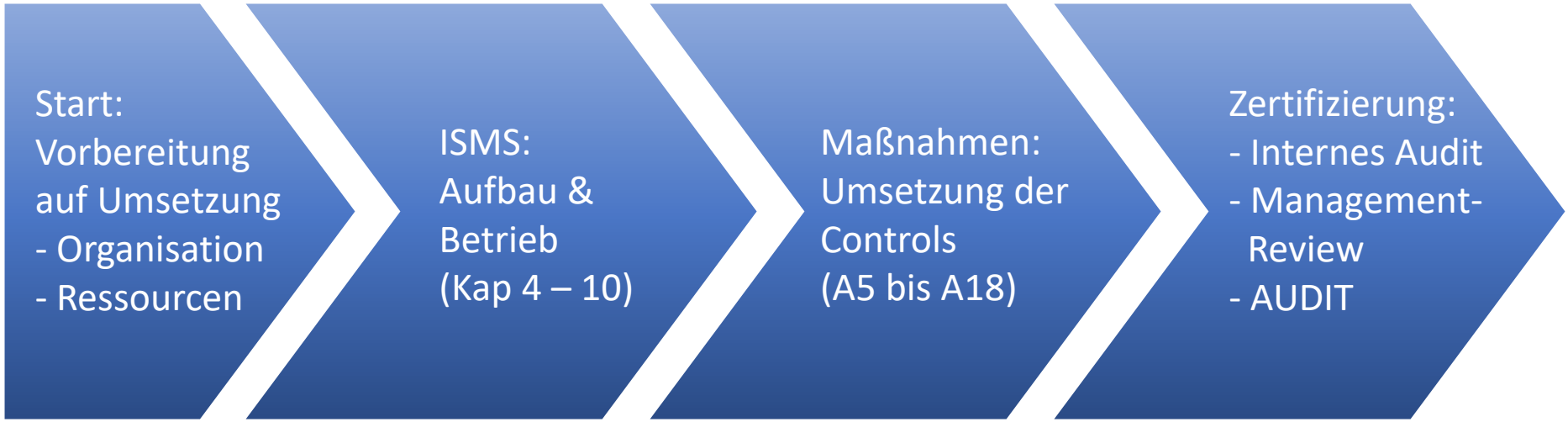
INFORMATIONSWERTE
- Vertraulichkeit
- Integrität
- Verfügbarkeit

RISIKEN
- Verwundbarkeit
- Bedrohungen und Szenarien
- Wahrscheinlichkeit

RISIKOMANAGEMENT
- Vermeiden
- Reduzieren
- Akzeptieren

Maßnahmen zur Informationssicherheit
(Maßnahmen A5 – A18)

Ablauf einer ISO 27001-Implementierung: 5 wesentliche Schritte



Was bedeutet das zeitlich?

Heute:
11. Januar 2022

Ca. 2 - 3 Monate*

Ca. 1 – 2 Monate*

Ca. 1/2 Monat*

Ca. 3-4 Monate*

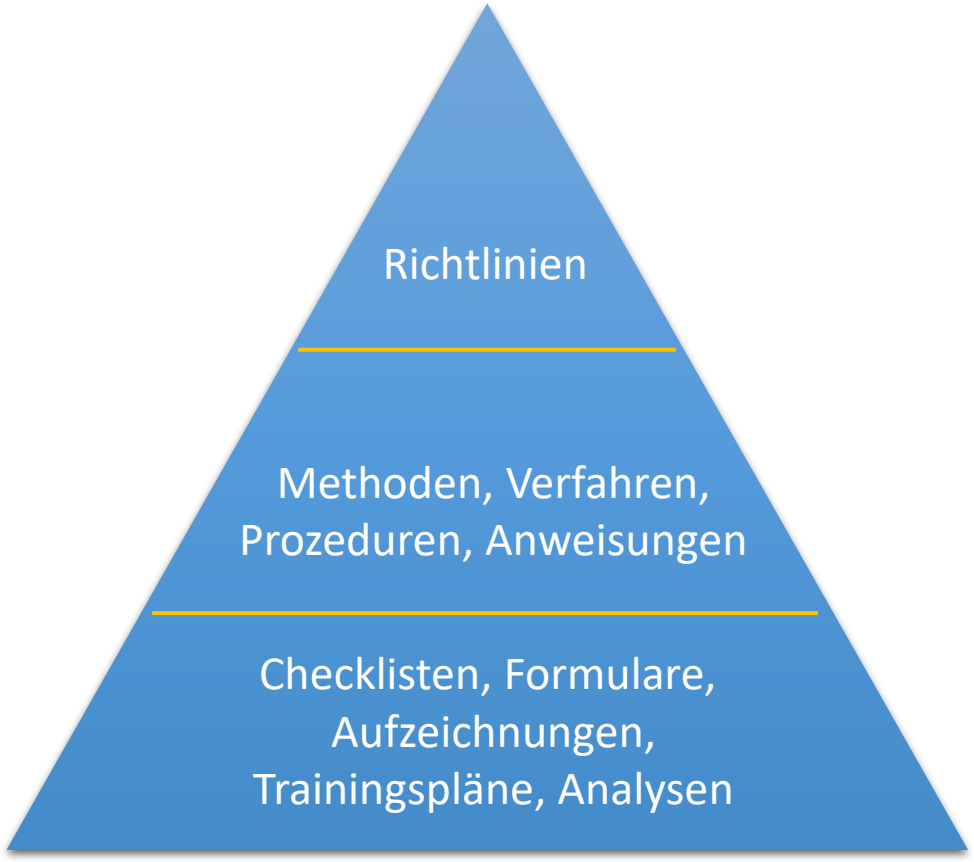
Zertifizierung
Monat? Jahr?

* Erfahrungswerte, bezogen auf eine Person zu 100%

Die Rolle des Informations-Sicherheitsbeauftragten (ISB)

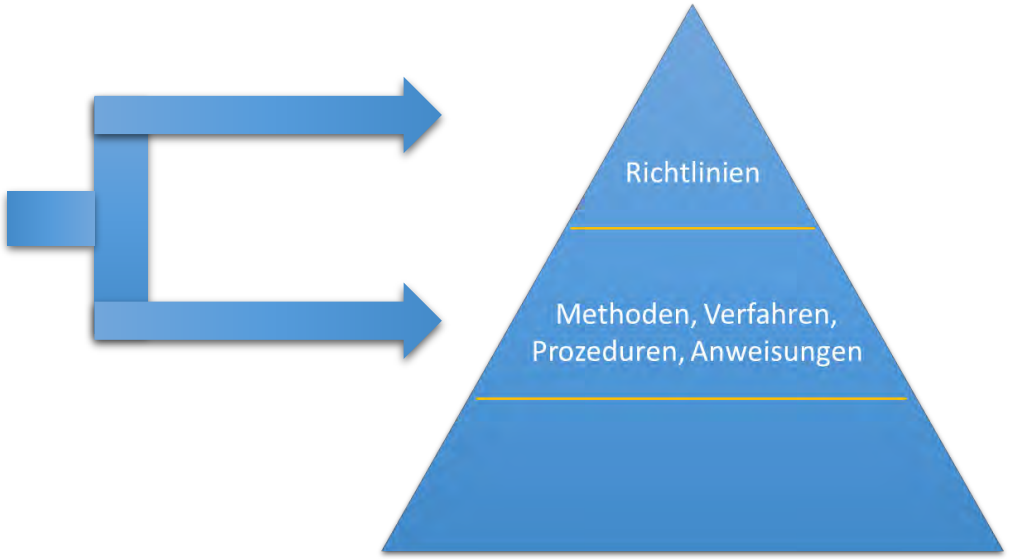
- Umsetzung der ISO 27001
- Ausarbeitung von Sicherheitskonzepten
- Sichtung und Umsetzung von aktuellen Vorschriften
- Schulung der Mitarbeiter
- Beratung der Geschäftsführung
- Planung der Internen Audits
- Zusammenarbeit mit dem Datenschutzbeauftragten
- Koordinator bei Notfällen
- Ansprechpartner bei Fragen und Problemen

Zentral: Die Dokumentationsebenen der ISO 27001



Die ISO 27001 Dokumentation: Diese Texte sind ein „Muss“!

Kapitel	Dokument
4.2	04-Kontext Organisation_20_A08-1-1_**Verfahren_zur_Identifikation_der_Anforderungen**_V1.0.docx
4.2	04-Kontext Organisation_20_A08-1-1_**Liste_ gesetzlicher_amtlicher_vertraglicher_Anforderungen-Anhang**_V1.0.docx
4.3	04-Kontext Organisation_30_**ISMS-Anwendungsbereich**_V1.0.docx
5.2	05-Führung_20_**Informationssicherheitspolitik** _V1.0.docx
6.1.2	06-Planung_10__**Methodik zur Risikoeinschätzung und Risikobehandlung**_V1.0.docx
6.1.2	06-Planung_10_Anhang_1_**Verzeichnis der Risikoeinsschaetzung_und_Behandlung**_V1.0.xlsx
6.1.2	06-Planung_10_08-2_Anhang_2_**Bericht_ zur_Risikoeinschaetzung_und_Risikobehandlung**_V1.0.docx
6.1.3	06-Planung_10_**SOA_Erklaerung_zur_Anwendbarkeit** _V1.1.docx
6.1.3	06-Planung_10_**SOA_Anhang_1_Plan_zur_Risiko-behandlung**_V1.0.xlsx
7.2	07-Unterstuetzung_20_**Plan_fuer_Training_und_ Awareness**_V1.0.docx
7.5	07-Unterstuetzung_50_**Verfahren_zur_Lenkung_von_ Dokumenten_und_Aufzeichnungen**_V1.0.docx
9.2	09-Bewertung_20__**Verfahren_fuer_interne_Audits** _V1.0.docx
10.1	10-Verbesserung_10_**Verfahren_zu_Korrekturmassnahmen**_V1.0.docx
A6.2	A06-IS-Richtlinien_20_**Bring-your-own-device**_V1.0.docx
A8.1	A08-Werte_10_Anhang_1_**Inventar-der-Werte**_V1.0.xlsx
A8.2	A08-Werte_20_**Sicherheitspolitik**_V1.0.docx
A8.3	A08-Werte_30_**Klassifizierung-von-Informationen**_V1.0.docx
A9.1	A09-Zugangssteuerung_10_**Zugangssteuerungs-Richtlinie**_V1.0.docx
A9.2	A09-Zugangssteuerung_20_**Passwort-Richtlinie**_V1.0.docx
A10.1	A10-Kryptographie_10_**Richtlinie-des-Einsatzes-von-Verschluesselung**_V1.0.docx
A11.2	A11-umgebungsbezogene-Sicherheit_20_A08-3_**Richtlinie-zur-Entsorung-und-Vernichtung**_V1.0.docx
A11.2	A11-umgebungsbezogene-Sicherheit_20_**Richtlinie-aufgeräumter-Arbeitsplatz**_V1.0.docx
A11.3	A11-umgebungsbezogene-Sicherheit_30_**Arbeit-In-sicheren-Bereichen**_V1.0.docx
A12.2	A12-Betriebssicherheit_20_**Richtlinie-Aenderungsmanagement**_V1.0.docx
A12.3	A12-Betriebssicherheit_30_**Backup-Richtlinie**_V1.0.docx
A13.1	A13-Kommunikation_10_**Netzwerksicherheits-Management**_V1.0.docx
A14.1	A14-Systementwicklung_10__**Richtlinie-Entwicklungssicherheit**_V1.0.docx
A14.1	A14-Systementwicklung_10_Anhang-1_**Spezifikation-Sicherheitsanforderungen**_V1.0.docx
A15.1	A15-Lieferantenbeziehungen_10__**Sicherheitspolitik-fuer-Lieferanten**_V1.0.docx
A15.2	A15-Lieferantenbeziehungen_20_**Vereinbarung-Datenverarbeitung-Lieferanten-A**_V1.0.docx
A15.3	A15-Lieferantenbeziehungen_30_**Vereinbarung-Datenverarbeitung-Lieferanten-B**_V1.0.docx
A15.5	A15-Lieferantenbeziehungen_50_**Sicherheitsabschnitte-fuer-Lieferanten-und-Partner**_V1.0.docx
A16.1	A16-Informationssicherheitsvorfaelle_10_**Verfahren-zum-Vorfallsmanagement**_V1.0.docx
A16.1	A16-Informationssicherheitsvorfaelle_10_**Verfahren-zum-Vorfallsmanagement**_Anlage_Verzeichnis_Vorfälle_V1.0.docx
A17.1	2019-02-02_A17-BCM_10_**Notfallwiederherstellungsplan**_V1.0.docx



Worum geht es bei einem ISMS?

Eine Vorbemerkung: Warum ist der Nachweis des ISMS so wichtig?

In der Zertifizierung bekommen Auditoren häufig „relativ gut beschriebene Texte“ (Richtlinien) vorgestellt.

Ob die Inhalte entsprechend gelebt werden, können sie daraus nicht erkennen oder ableiten.

Stellen sie sich daher frühzeitig darauf ein, „den Nachweis zu führen“, dass das ISMS auch „gelebt“ wird.

Was ist ein ISMS? Welche Anforderungen hat es? – Scope

Der **Anwendungsbereich** (Scope) eines ISMS ist meist die **gesamte Organisation**. Es ist aber legitim, das ISMS beschränkt auf **bestimmte** Standorte, Geschäftsprozesse, Abteilungen etc. zu beschränken.

Die internen **Scope-Einflussfaktoren** stehen im Zusammenhang damit, wie eine Organisation ihre **Ziele** erreichen will: Hier spielen die **Aufbau- und Ablauforganisation**, die Unternehmens**kultur**, die Unternehmens**strategie** aber auch jeder weitere **interne** Faktor, der ein ISMS beeinflussen kann, wichtige eine Rolle.

Wichtige **Aufgaben** eines ISMS sind:

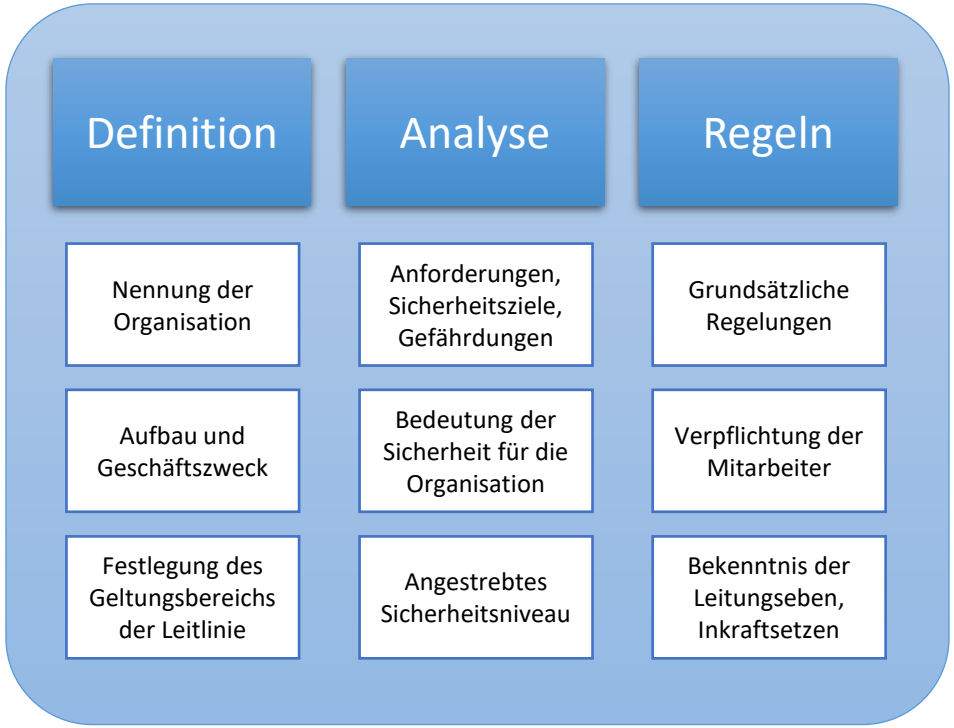
- Die Formulierung des Scope
- Die Formulierung von (Sicherheits-)**Zielen**
- Die Bestimmung der **Assets**
- Die Risiko**beurteilung**
- Die Risiko**behandlung**
- Die kontinuierliche **Verbesserung**

Zur Bestimmung eines konkreten Scopes können die folgenden **Fragestellungen** eine gute Hilfestellung leisten:

- Welche (Teil-)Organisation oder **Organisationseinheit** soll vom ISMS abgedeckt werden?
- Was sind die (informationsverarbeitenden) **Prozesse** und die zugehörigen Datenflüsse?
- Welche Anforderungen stellen **Dritte** an die Organisation (besonders auch rechtlicher Natur)?
- Welche Dritte sind zu **berücksichtigen** (Kunden, Mitarbeiter, Lieferanten, Aufsichtsbehörden, ...)?
- Welche (impliziten) **Erwartungen** stellen Dritte an die Organisation?

Was ist ein ISMS? Welche Anforderungen hat es? - Leitlinie

Der Aufbau einer Leitlinie sollte folgende **Form** haben:



in der Leitlinie sollte das etablierte ISMS samt seiner Rollen und Verantwortlichkeiten in ausreichender **Kürze** beschrieben werden:

- Die IS-Leitlinie muss von der **höchsten Leitungsebene** (Topmanagement) verabschiedet sein und den zuständigen Aufsichtsgremien zur Verfügung gestellt werden.
- Die IS-Leitlinie muss als **dokumentierte Information** verfügbar sein und einer nachvollziehbaren Dokumentenlenkung unterliegen.
- Die IS-Leitlinie **kann** einen Verweis auf die **Unternehmensziele** und IT-Ziele beinhalten.
- Im Rahmen der **Mitarbeitersensibilisierung** ist sicherzustellen, dass **alle** betroffenen Mitarbeiter innerhalb des Geltungsbereichs die IS-Leitlinie **kennen**.
- Die IS-Leitlinie sollte nicht mit weitergehenden Dokumentationen und Umsetzungsvorgaben **vermischt** werden.

Was ist ein ISMS? Welche Anforderungen hat es? - Assets

Unter Asset wird alles verstanden, was für eine Organisation einen **Wert** darstellt (Grundstücke, Gebäude, Maschinen und Anlagen, Geschäftsprozesse etc.) sowie **Information** Assets, wie Daten, Systeme, Anwendungen, IT Services – aber auch **Soft Assets** wie das **Image** oder die Kreditwürdigkeit.

Eine Anforderung der Norm ist, dass **alle für die Organisation relevanten** Assets erfasst bzw. inventarisiert werden – z.B. in Form einer **Tabelle** oder **Datenbank**. Dabei werden weitere Daten erfasst, wie z.B. Speicher-, Lager- oder Standort sowie eine Klassifizierung des Wertes und der **Asset Owner**. Dieser ist für das Asset **verantwortlich**.

Was ist ein ISMS? Welche Anforderungen hat es? - Risikobeurteilung

In der Informationssicherheit wird der mögliche **Eintritt von Sicherheitsereignissen** als Risiko angesehen. Ein Risiko wird in der Regel als eine Kombination aus **Eintrittswahrscheinlichkeit** und **Schadenhöhe** definiert.

Auswirkungen auf die Sicherheit (**Sicherheits-ereignisse**) liegen immer dann vor, wenn Sicherheitsziele einer Organisation beeinträchtigt werden.
Ein **Sicherheitsvorfall** ist ein Ereignis, bei dem eine hohe Wahrscheinlichkeit für die Auswirkungen auf die Sicherheit besteht.
Ein **(Sicherheits-)Notfall** ist ein Sicherheitsvorfall mit gravierenden oder sogar katastrophalen Auswirkungen auf die Sicherheit.
Bei der **Risikoidentifizierung** geht es um die Ermittlung von einzelnen Risiken. Diese muss im Zusammenspiel mit den Verantwortlichen für die Werte geschehen.
In der **Risikoanalyse** wird für jedes Risiko die Schadenhöhe und die Eintrittshäufigkeit abgeschätzt.
Bei der **Risikobewertung** geht es um die Feststellung, welche Auswirkungen ein Risiko auf die Organisation hat.

In der Norm wird Risikobeurteilung als Zusammenfassung aus **Risikoidentifizierung**, **Risikoanalyse** und **Risikobewertung** betrachtet

Was ist ein ISMS? Welche Anforderungen hat es? - Risikobehandlung

Zur Behandlung ermittelter Risiken dienen nach Vorgaben der Norm **Optionen** und **Sicherheitsmaßnahmen**

Sicherheitsmaßnahmen können aus sehr **unterschiedlichen Bereichen** kommen: rechtliche, organisatorische, personelle, infrastrukturelle und IT-Maßnahmen.

Typische Optionen zur Risikobehandlung sind:

- **Risikoakzeptanz** – man übernimmt einfach das Risiko ohne weitere Maßnahmen.
- **Risikoverlagerung** – z.B. durch Verlagerung an einen sicheren Ort, etwa einem qualifizierten Dienstleister, oder durch Versicherung der möglichen Schäden.
- **Risikoreduktion** – durch Einsatz geeigneter Sicherheitsmaßnahmen
- **Risikobeseitigung** – z.B. durch Änderung des fraglichen Geschäftsprozesses und der unterstützenden IT

Was ist ein ISMS? Welche Anforderungen hat es? – Kontinuierliche Verbesserung

die **Grundprinzipien** des PDCA-Zyklus (Nachdenken, Umsetzen, Erfolgskontrolle und Verbesserung) finden sind in Reinform in der Gliederung wieder: Die Kapitel *vier bis sieben* des Standards sind der **Plan-Phase** zuzuordnen, das Kapitel *acht* der **Do-Phase**, das Kapitel *neun* der **Check-Phase** und schlussendlich das Kapitel *zehn* der **Act-Phase**.

PLAN:

- Etablierung von Maßnahmen**zielen** und **Verantwortlichkeiten** für deren Erreichung
- Etablierung der Sicherheits**maßnahmen** zur Erreichung der Maßnahmenziele und der operativen Prozessverantwortlichen für diese Maßnahmen
- Definition der Leistungs**indikatoren**, die eine Leistungsmessung gegen die Maßnahmenziele erlauben
- Definition des **Prozesses** zur Messung der Leistung inklusive der Messpunkte, Berechnungsmethode des Indikators und der Norm- u. Toleranzbereiche
- Definition der **Korrekturmaßnahmen**, um die Sicherheitsmaßnahme im Normbereich zu regeln

DO:

- Kontinuierliche **Messung** der Maßnahmenzielerreichung mit Lieferung an das Security Controlling innerhalb d. ISMS
- Einleitung von Korrekturen bei festgestellten Mängeln oder Nichtkonformitäten

CHECK:

- **Überwachen** der einzelnen Sicherheitsmaßnahmen-Indikatoren und Vergleichen der einzelnen Leistungsfähigkeiten mit den Maßnahmenzielen
- Aufsicht über die eingeleiteten **Gegenmaßnahmen** und deren Verantwortliche, wenn eine Sicherheitsmaßnahme den Normbereich der Effektivität verlassen hat.
- Erstellen von Sicherheitsberichten mit **Key-Performance**-Indikatoren für das Management, basierend auf den Maßnahmenzielen und Sicherheitszielen.

ACT:

- Treffen von notwendigen **Managemententscheidungen**, um die Effektivität von Sicherheitsmaßnahmen oder ganzen Maßnahmenzielen wiederherzustellen.
- Die getroffenen Entscheidungen werden mit Begründungen angemessen **dokumentiert**

Was ist das Ziel der ISO 27001-Maßnahmen?

Im normativen **Anhang A** Referenzmaßnahmenziele und -maßnahmen beschreibt ISO/IEC 27001 eine sehr umfangreiche Reihe von Maßnahmen, deren Umsetzung zur Reduzierung der Risiken für die Informationssicherheit beiträgt.

Die ISO/IEC 27000-Normenreihe fasst die Maßnahmen in 14 Kategorien zusammen. In jeder Kategorie wird mindestens ein Maßnahmenziel definiert, und pro Maßnahmenziel existieren eine oder, was die Regel ist, mehrere Maßnahmen.

Beispiel: A8.1 - **Maßnahmen:** Verantwortlichkeit für Werte

Was ist bei der Umsetzung zu beachten?

Hier geht es darum, die Werte des Unternehmens zu identifizieren, zu kennen und Verantwortlichkeiten für ihren Schutz zu schaffen.

Typische Fragen im Audit:

Sind alle Werte der Organisation identifiziert und mit ihren Kenndaten in ein Verzeichnis eingetragen?

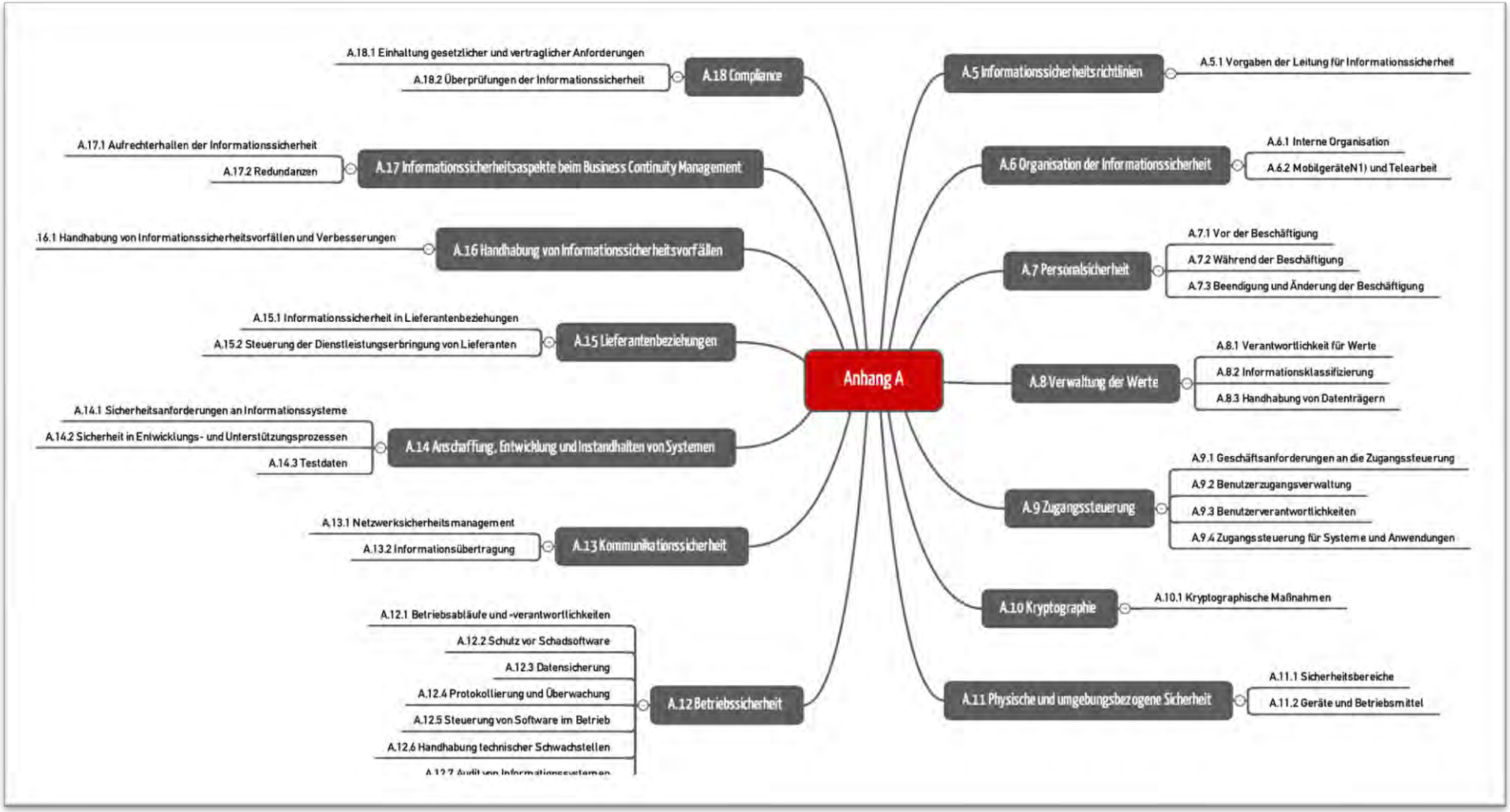
Ist jedem Informationswert ein Zuständiger bzw. Eigentümer (kann Person, Rolle oder Organisationseinheit sein) zugeordnet?

Sind Zugriffs, Nutzungs- und Zutritts-Beschränkungen schriftlich festgelegt?

Alle organisationseigenen Werte und die damit zusammenhängende Risikoanalyse werden im Rahmen des Sicherheitsmanagements durch folgende Controls beschrieben:

- **A8.1.1:** Bei der Inventarisierung sind alle entsprechenden Werte der Organisation zu identifizieren und mit ihren Kenndaten in ein Inventarverzeichnis (Tabelle, Datenbank, Spreadsheet, Webpage etc.) einzutragen
- **A8.1.2:** Jeder Informationswert muss einem Zuständigen bzw. Eigentümer (Owner) zugewiesen sein, der dafür gegenüber der Organisationsleitung verantwortlich ist.
- **A8.1.3:** Für jeden Informationswert wird es Regeln für den ordnungsgemäßen bzw. zulässigen Gebrauch geben. Das heißt: Nicht alles ist erlaubt – es bestehen je nach Typ des Assets z. B. Zugriffs-, Zugangs- und Zutrittsbeschränkungen.
- Ein unzulässiger Gebrauch von Daten liegt z.B. dann vor, wenn diese an Unbefugte gelangen; in sensiblen Kontexten muss deshalb dem Schutz vor unerwünschtem Datenabfluss besondere Priorität eingeräumt werden
- **A8.1.4:** Diese Maßnahme zeigt einen oft vernachlässigten Punkt, nämlich die Rückgabe der Informationswerte der Organisation: dies können „physische oder logische Schlüssel“, „Kryptomittel und Kryptogeräte“, „Authentisierungsmittel (wie Tokens, Chipkarten)“ – aber auch vertrauliche bzw. wichtige Unterlagen/Informationen sein.

Mindmap der Maßnahmen



Zertifizierungsablauf zur ISO 27001

Unterstützung bei der Umsetzung der ISO 27001: Dokumentation / Tools

Kapitel	Dokument
4.2	04-Kontext Organisation_20_A08-1-1_**Verfahren_zur_Identifikation_der_Anforderungen**_V1.0.docx
4.2	04-Kontext Organisation_20_A08-1-1_**Liste_ gesetzlicher_amtlicher_vertraglicher_Anforderungen-Anhang**_V1.0.docx
4.3	04-Kontext Organisation_30_**ISMS-Anwendungsbereich**_V1.0.docx
5.2	05-Führung_20_**Informationssicherheitspolitik** _V1.0.docx
6.1.2	06-Planung_10__**Methodik zur Risikoeinschätzung und Risikobehandlung**_V1.0.docx
6.1.2	06-Planung_10_Anhang_1_**Verzeichnis der Risikoeinsschaetzung_und_Behandlung**_V1.0.xlsx
6.1.2	06-Planung_10_08-2_Anhang_2_**Bericht_ zur_Risikoeinschaetzung_und_Risikobehandlung**_V1.0.docx
6.1.3	06-Planung_10_**SOA_Erklaerung_zur_Anwendbarkeit** _V1.1.docx
6.1.3	06-Planung_10_**SOA_Anhang_1_Plan_zur_Risiko-behandlung**_V1.0.xlsx
7.2	07-Unterstuetzung_20_**Plan_fuer_Training_und_ Awareness**_V1.0.docx
7.5	07-Unterstuetzung_50_**Verfahren_zur_Lenkung_von_ Dokumenten_und_Aufzeichnungen**_V1.0.docx
9.2	09-Bewertung_20__**Verfahren_fuer_interne_Audits** _V1.0.docx
10.1	10-Verbesserung_10_**Verfahren_zu_Korrekturmassnahmen**_V1.0.docx
A6.2	A06-IS-Richtlinien_20_**Bring-your-own-device**_V1.0.docx
A8.1	A08-Werte_10_Anhang_1_**Inventar-der-Werte**_V1.0.xlsx
A8.2	A08-Werte_20_**Sicherheitspolitik**_V1.0.docx
A8.3	A08-Werte_30_**Klassifizierung-von-Informationen**_V1.0.docx
A9.1	A09-Zugangssteuerung_10_**Zugangssteuerungs-Richtlinie**_V1.0.docx
A9.2	A09-Zugangssteuerung_20_**Passwort-Richtlinie**_V1.0.docx
A10.1	A10-Kryptographie_10_**Richtlinie-des-Einsatzes-von-Verschluesselung**_V1.0.docx
A11.2	A11-umgebungsbezogene-Sicherheit_20_A08-3_**Richtlinie-zur-Entsorung-und-Vernichtung**_V1.0.docx
A11.2	A11-umgebungsbezogene-Sicherheit_20_**Richtlinie-aufgeräumter-Arbeitsplatz**_V1.0.docx
A11.3	A11-umgebungsbezogene-Sicherheit_30_**Arbeit-in-sicheren-Bereichen**_V1.0.docx
A12.2	A12-Betriebssicherheit_20_**Richtlinie-Aenderungsmanagement**_V1.0.docx
A12.3	A12-Betriebssicherheit_30_**Backup-Richtlinie**_V1.0.docx
A13.1	A13-Kommunikation_10_**Netzwerksicherheits-Management**_V1.0.docx
A14.1	A14-Systementwicklung_10__**Richtlinie-Entwicklungssicherheit**_V1.0.docx
A14.1	A14-Systementwicklung_10_Anhang-1_**Spezifikation-Sicherheitsanforderungen**_V1.0.docx
A15.1	A15-Lieferantenbeziehungen_10__**Sicherheitspolitik-fuer-Lieferanten**_V1.0.docx
A15.2	A15-Lieferantenbeziehungen_20_**Vereinbarung-Datenverarbeitung-Lieferanten-A**_V1.0.docx
A15.3	A15-Lieferantenbeziehungen_30_**Vereinbarung-Datenverarbeitung-Lieferanten-B**_V1.0.docx
A15.5	A15-Lieferantenbeziehungen_50_**Sicherheitsabschnitte-fuer-Lieferanten-und-Partner**_V1.0.docx
A16.1	A16-Informationssicherheitsvorfaelle_10_**Verfahren-zum-Vorfallsmanagement**_V1.0.docx
A16.1	A16-Informationssicherheitsvorfaelle_10_**Verfahren-zum-Vorfallsmanagement**_Anlage_Verzeichnis_Vorfälle_V1.0.docx
A17.1	2019-02-02_A17-BCM_10_**Notfallwiederherstellungsplan**_V1.0.docx

Unterstützende Umsetzungs-Tools, wie z.B.

- Step-by-Step-ISMS-Umsetzungsleitfaden
- Projekt- und Umsetzungsdokumentations-Vorlage
- Anleitung und Vorlage einer ISMS-Risikoanalyse
- Kennzahlen-Pool für das ISMS und alle Controlls in Anhang A
- Präsentationen für Trainings- und Awareness-Schulungen
- Audit-Checklist

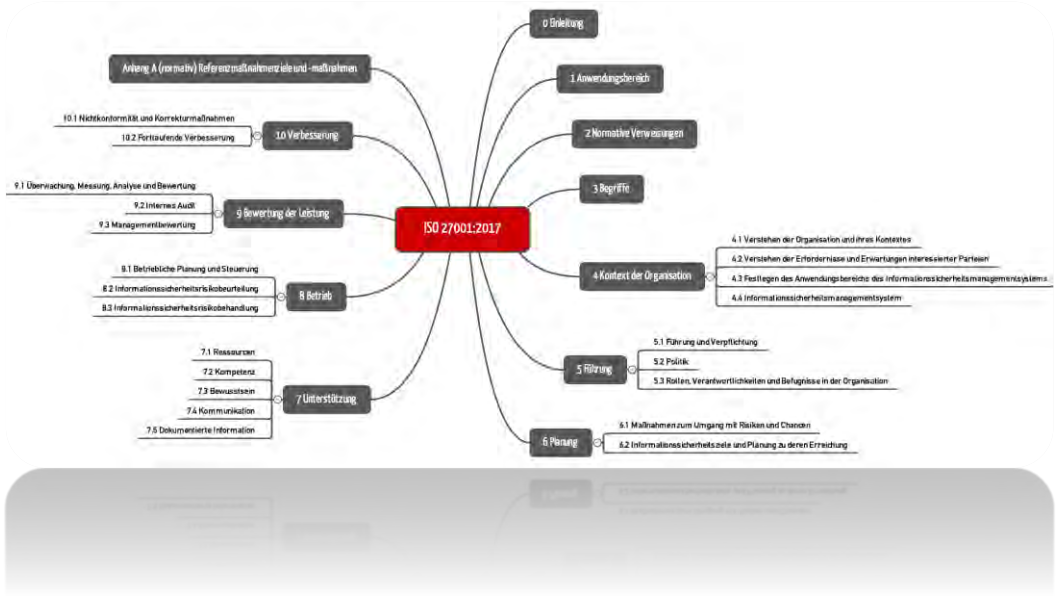
Dokumentation (Mustervorlagen)

z.B. https://advisera.com/store/standard/iso-27001-iso-22301/

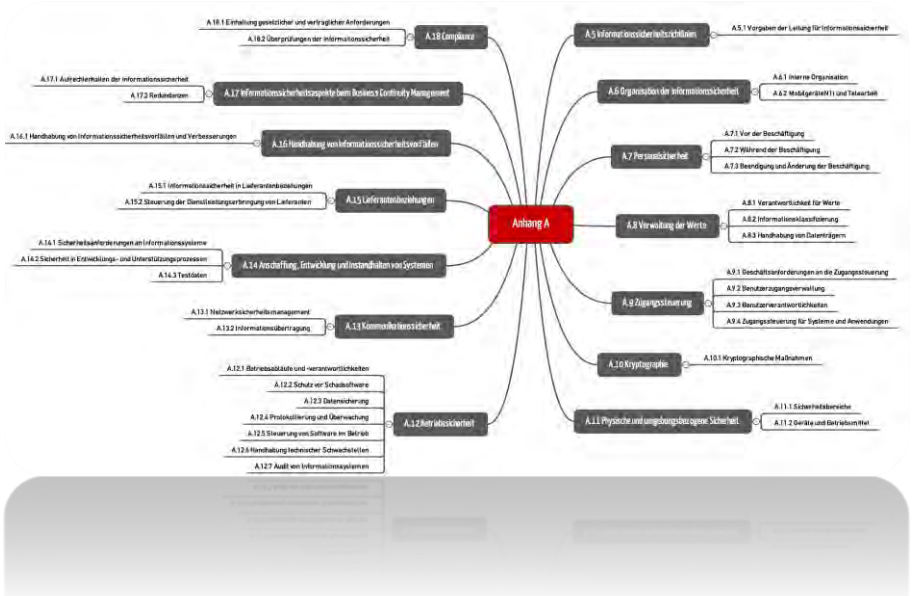
Implementierungs-Tools

https://www.vialevo.de/isms-implementierung/

Unterstützung bei der Umsetzung der ISO 27001: Umsetzungs-Workshops



Tag 1: ISMS



Tag 2: Maßnahmen

https://www.vialevo.de/iso-27001-beratung/

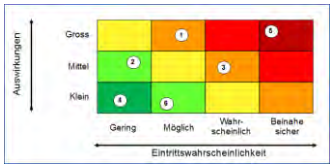
Unterstützung bei der Umsetzung der ISO 27001: Mentoring

Status-Analyse

Projektplan

Dokumentation

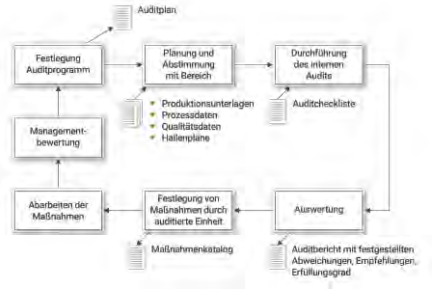
Risikoanalyse



Aufbau ISMS

Umsetzung der Maßnahmen

Internes Audit



https://www.vialevo.de/

Vielen Dank!

Haben Sie weitere Fragen?

Copyright