verinice.XP

Die Anwenderkonferenz für Informationssicherheit

Version 1.0 | Februar 2023 | Sven Perscheid

ISO27001:2022/ISO27005:2022 The next Generation of ISMS

cassini

KIX

neam

SerNet

1. Änderung des Namens

- ISO 27001:2013/17
  Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme
- ISO 27001:2022
  Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen

Der Datenschutz ist als neues Ziel hinzugekommen. Auch wenn die Blickrichtung nicht mit IS-Sicherheit gleichzusetzen ist, so trägt sie der kooperativen Erreichung beider Ziele Rechnung

2. Kapitel 4-10

- In den Kapitel 4-10 haben sich mehrere geringfügigen Änderungen ergeben.
- Dabei liegt das Augenmerk auf 4.2, 6.2, 6.3 und 8.1, wo zusätzliche neue Inhalte hinzugefügt wurden.
- An der Zielrichtung hat sich aber nichts geändert. Weitere Aktualisierungen umfassen geringfügige Änderungen in der Terminologie und die Umstrukturierung von Sätzen und Beschreibungen.
- Titel und Reihenfolge bleiben gleich

3. Risikokontrollmaßnahmen

- Die Zahl der Risikokontrollmaßnahmen wurde von von 114 auf 93 reduziert.
- Die Aufteilung in der ISO 27001:2022 erfolgt nun in 4 statt wie bisher in 14 Kapiteln:

  Organisatorische Maßnahmen (37 Maßnahmen)

  Personenbezogene Maßnahmen (8 Maßnahmen)

  Physische Maßnahmen(14 Maßnahmen)

  Technologische Maßnahmen (34 Maßnahmen)

4. Neue Risikokontrollmaßnahmen

- 5.7 Bedrohungsintelligenz
- 5.23 Informationssicherheit für die Nutzung von Cloud-Diensten
- 5.30 IKT-Bereitschaft für Business Continuity
- 7.4 Physische Sicherheitsüberwachung
- 8.9 Konfigurationsmanagement
- 8.10 Löschung von Informationen
- 8.11 Datenmaskierung
- 8.12 Verhinderung von Datenlecks
- 8.16 Überwachung von Aktivitäten
- 8.23 Webfilterung
- 8.28 Sicheres Coding

5. Neuer Kontrolltyp: Maßnahmenart

Dies wird zur besseren Einordnung in der ISO27002:2022 Kapitel 4.2 erläutert.

- **Maßnahmenart**
  Die Maßnahmenart ist ein Attribut für die Sicht der Maßnahmen unter dem Gesichtspunkt, wann und wie die Maßnahme das Risiko in Bezug auf das Auftreten eines Informationssicherheitsvorfalls verändert.
- Attributwerte bestehen aus
  Präventiv
  (die Maßnahme, die das Auftreten eines Informationssicherheitsvorfalls verhindern soll),
  Detektiv
  (die Maßnahme wirkt, wenn ein Informationssicherheitsvorfall auftritt) und
  Korrektiv
  (die Maßnahme wirkt, nachdem ein Informationssicherheitsvorfall auftritt).

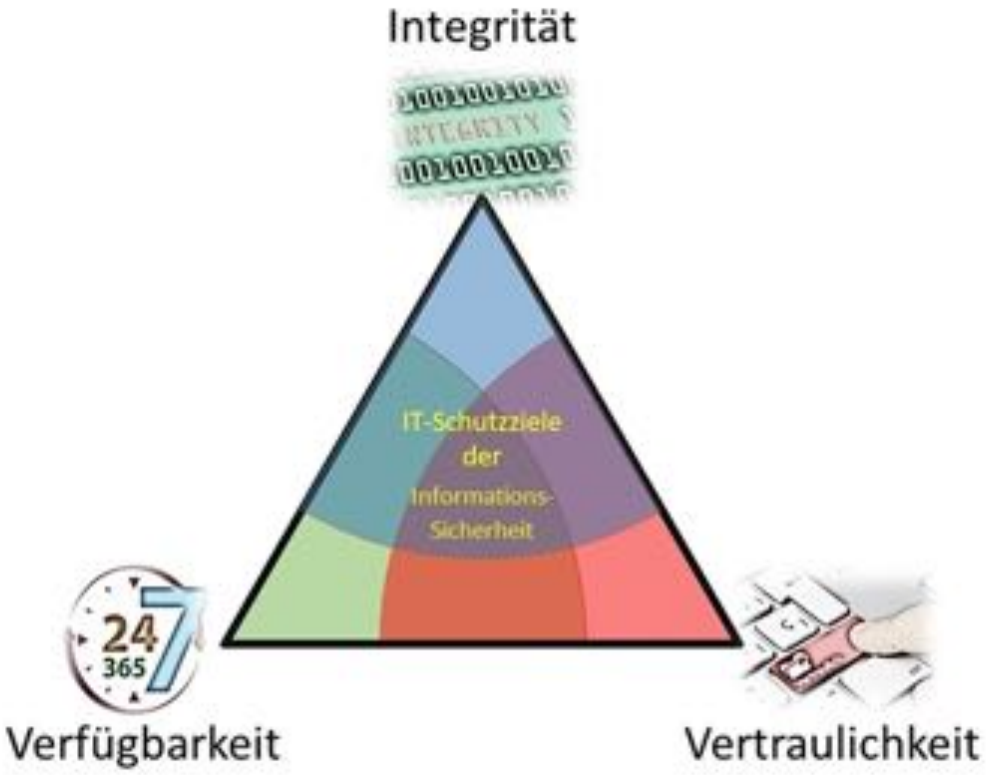
Neuer Kontrolltyp: Informationssicherheitseigenschaften

Dies wird zur besseren Einordnung in der ISO27002:2022 Kapitel 4.2 erläutert

- **Informationssicherheitseigenschaften**

  Die Informationssicherheitseigenschaften sind ein Attribut, mit dem Maßnahmen unter dem Gesichtspunkt betrachtet werden können, welches Merkmal der Informationen durch die Maßnahme geschützt werden soll.

- Die Attributwerte bestehen aus **Vertraulichkeit, Integrität und Verfügbarkeit**.



Neuer Kontrolltyp: Konzepte zur Cybersicherheit

Dies wird zur besseren Einordnung in der ISO27002:2022 Kapitel 4.2 erläutert.

- **Konzepte zur Cybersicherheit**

  Das Attribut „Cybersicherheitskonzepte“ dient dazu, Maßnahmen aus der Perspektive der Zuordnung von Maßnahmen zu Cybersicherheitskonzepten zu betrachten, die in dem in ISO/IEC TS 27110 beschriebenen Cybersicherheitsrahmenwerk definiert sind.

- Die Attributwerte bestehen aus:
  Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

Neuer Kontrolltyp: Betriebsfähigkeit

Dies wird zur besseren Einordnung in der ISO27002:2022 Kapitel 4.2 erläutert.

- **Betriebsfähigkeit**

  Das Attribut „Betriebsfähigkeit“ dient dazu, die Maßnahmen aus der Perspektive der Informationssicherheitsfähigkeiten zu betrachten.

- Die Attributwerte umfassen
  Governance, Asset_Management, Informationsschutz, Sicherheit der Humanressourcen, physische Sicherheit, System- und Netzwerksicherheit, Anwendungssicherheit, sichere Konfiguration, Identitäts- und Zugangsverwaltung, Bedrohungs- und Schwachstellenmanagement, Kontinuität, Sicherheit der Lieferantenbeziehungen, Recht und Compliance, Informationssicherheits-Ereignis-Management und Vertrauenswürdigkeit
  in Bezug auf die Informationssicherheit.

Neuer Kontrolltyp: Sicherheitsdomänen

Dies wird zur besseren Einordnung in der ISO27002:2022 Kapitel 4.2 erläutert.

- **Sicherheitsdomänen**
  Sicherheitsdomänen ist ein Attribut, mit dem Maßnahmen aus der Perspektive von vier Informationssicherheitsdomänen betrachtet werden können:

- „Governance und Ökosystem“ umfasst
  „Governance und Risikomanagement für die Sicherheit von Informationssystemen“ und „Cybersicherheitsmanagement im Ökosystem“ (einschließlich interner und externer interessierter Parteien)

- „Schutz“ umfasst
  „IT-Sicherheitsarchitektur“, „IT-Sicherheitsverwaltung“, „Identitäts- und Zugangssverwaltung“, „IT-Sicherheitswartung“ und „physische und umgebungsbezogene Sicherheit“; „Verteidigung“ umfasst „Erkennung“ und „Management von Computersicherheitsvorfällen“

- „Resilienz“ umfasst
  „Betriebskontinuität“ und „Krisenmanagement“.
  Die Attributwerte bestehen aus Governance_und_Ökosystem, Schutz, Verteidigung und Resilienz.

6. Eigene Kontrolltypen

- Organisationen können sich dafür entscheiden, eines oder mehrere der im ISO 27001:2022 aufgeführten Attribute zu ignorieren.
- Sie können wahlweise auch eigene Attribute (mit den entsprechenden Attributwerten) anlegen, um ihre eigenen Organisationssichten zu erstellen.

Anmerkung:
Die Anpassungen sollten mit Bedacht vorgenommen werden, denn es soll im Unternehmen verstanden werden.

Zertifizierung und Fristen

- Die ISO 27001:2022 wurde am 25. Oktober 2022 veröffentlicht.
  Dabei ist die Übergangsfrist auf drei Jahre (36 Monate) festgelegt worden.
- Zertifizierungsbereitschaft nach ISO/IEC 27001:2022:
  voraussichtlich ab Februar - April 2023
- Letzter Termin für Erst-/Rezertifizierungsaudits nach der früheren ISO 27001:2013:
  18 Monate nach Veröffentlichung der neuen ISO/IEC 27001:2022
- Umstellung aller bestehenden Zertifikate auf die neue ISO/IEC 27001:2022:
  3 Jahre, bezogen auf letzten Tag des Ausgabemonats von ISO/IEC 27001:2022 (Oktober 2025)

ISO 27005:2022

ISO 27005:2022

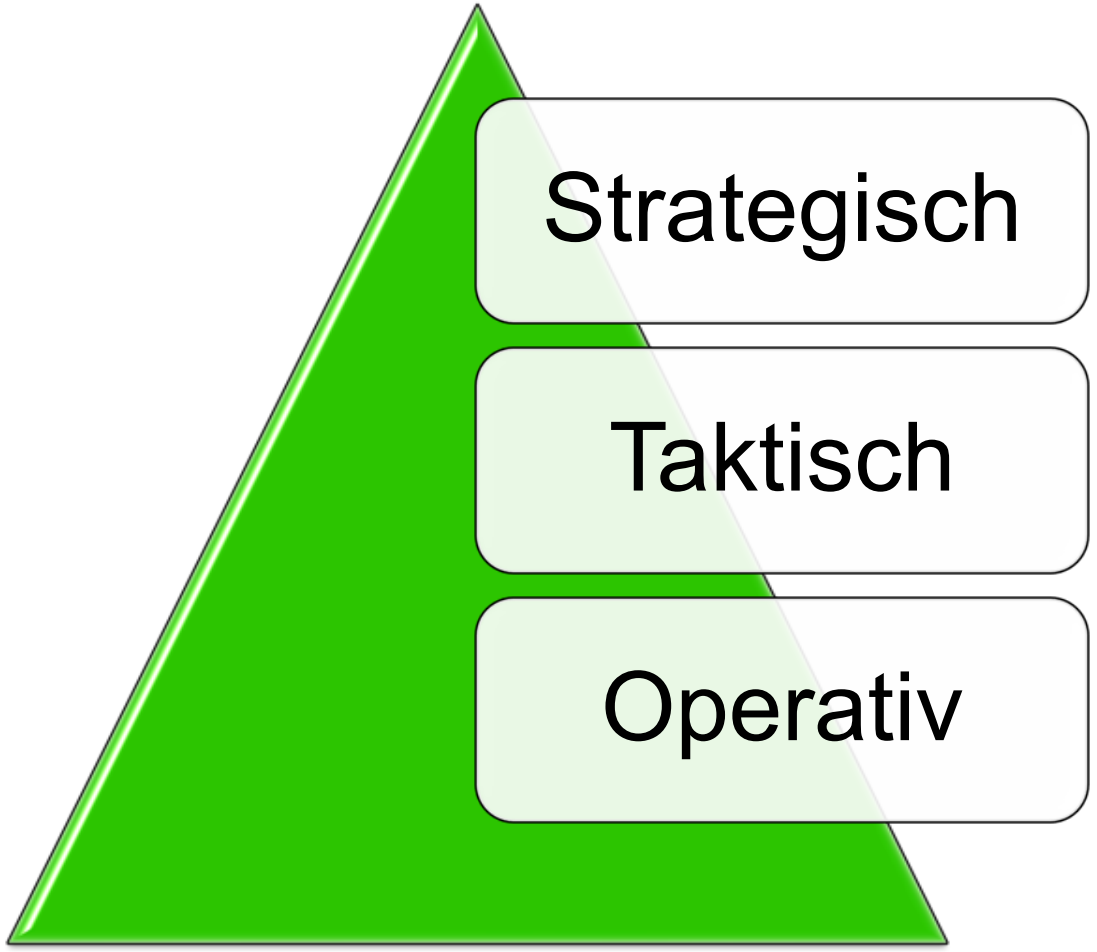
Aufbau

- Kapitel 1-4 sind inhaltlich gleich
- Anstatt 12 Kapitel sind es nun 10 Kapitel
- NEU: Zur Erläuterung von Kapitel 7&8 gibt es nun Kapitel 9 „Operation“
- NEU: In Kapitel 8 „Risk Treatment“ ist nun das alte Kapitel 10 „Risk Acceptance“ eingeflossen
- NEU: In Kapitel 10 „Leveraging related ISMS processes“ sind die alten Kapitel 11 „ Information security risk communication and consultation“ und Kapitel 12 „Information security risk monitoring and review“ aufgegangen.
- NEU: Nur noch ein ANNEX-A, statt Annex A-E

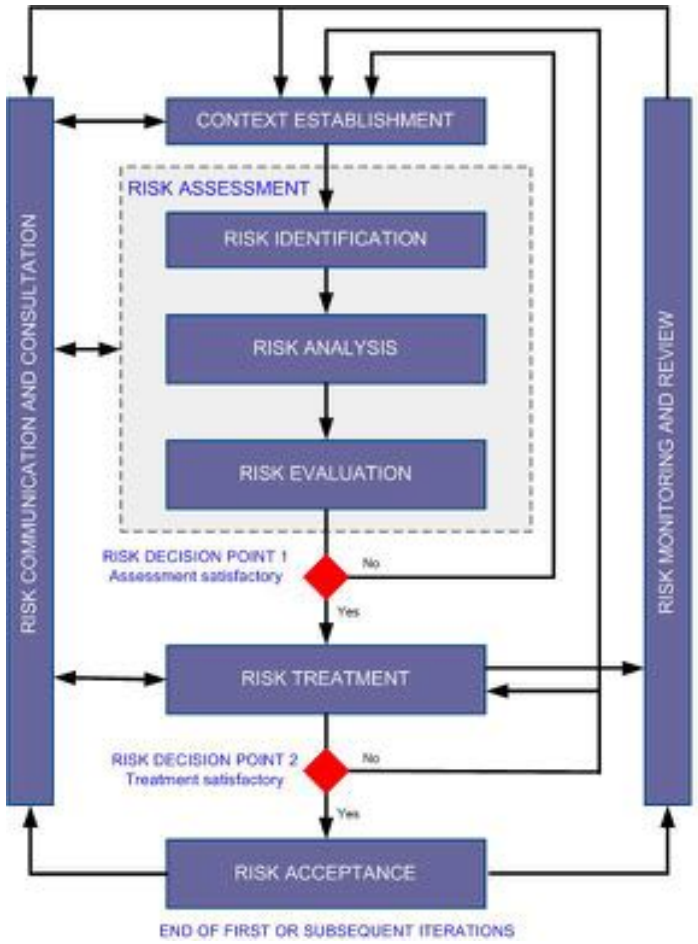
Risikolevel

- Strategische Risiken sind vom Umfeld und der strategischen Ausrichtung bestimmt
- Taktische Risiken umfassen aktuelle Unternehmenssituation mit aktuellen Gegebenheiten
- Operative Risiken sind die aktuellen Vorkommnisse und damit verbundenen Verfahren

- **Der Risikoeigentümer ist nun explizit eingeführt satt nur allgemein als „Stakeholder“**

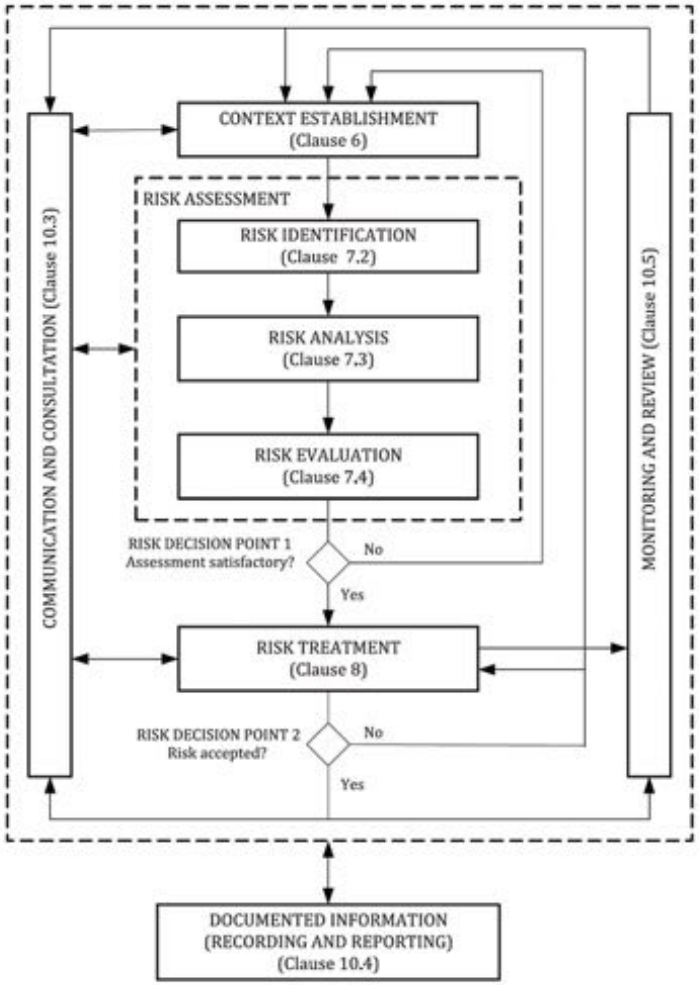


Risikoprozess alt/neu



Quelle: ISO27005/2011

- Risikoakzeptanz nun Bestandteil der Risikobehandlung
- Dokumentation der Risikobewertung kam neu dazu
- Enge Verzahnung mit ISO 27001
- Event und Asset-basierender Ansatz



Quelle: ISO27005/2022

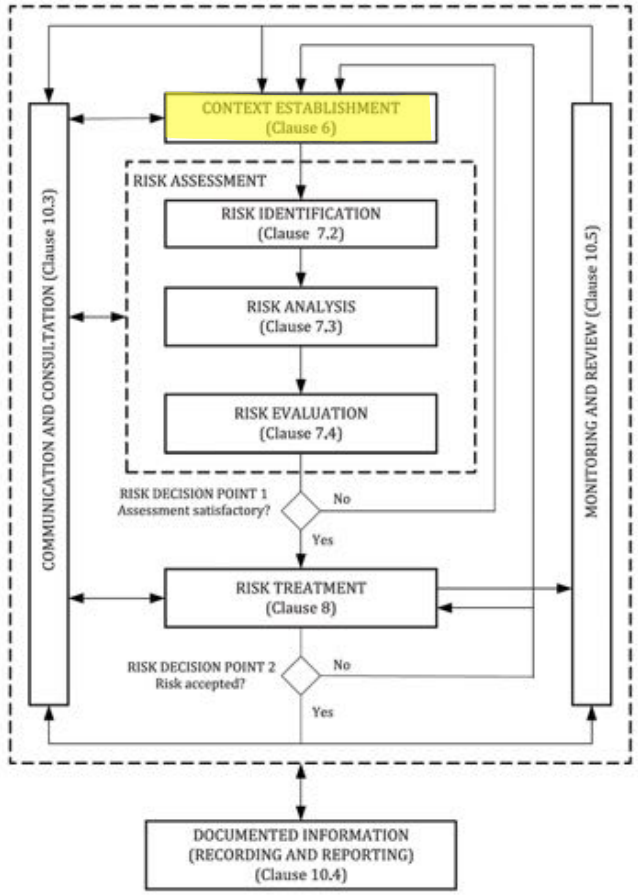
Festlegung des Kontextes

- Umfeld der Organisation
- Anforderungen der Stakeholder

Wahl der Methode:

- Kohärenz : Bewertungen derselben Risiken, die wiederholt von einem oder verschiedenen Personen durchgeführt werden, sollen zu den gleichen Ergebnissen kommen
- Vergleichbarkeit: Einheitliche Bewertungskriterien
- Gültigkeit: Realitätsnahe Bewertungen

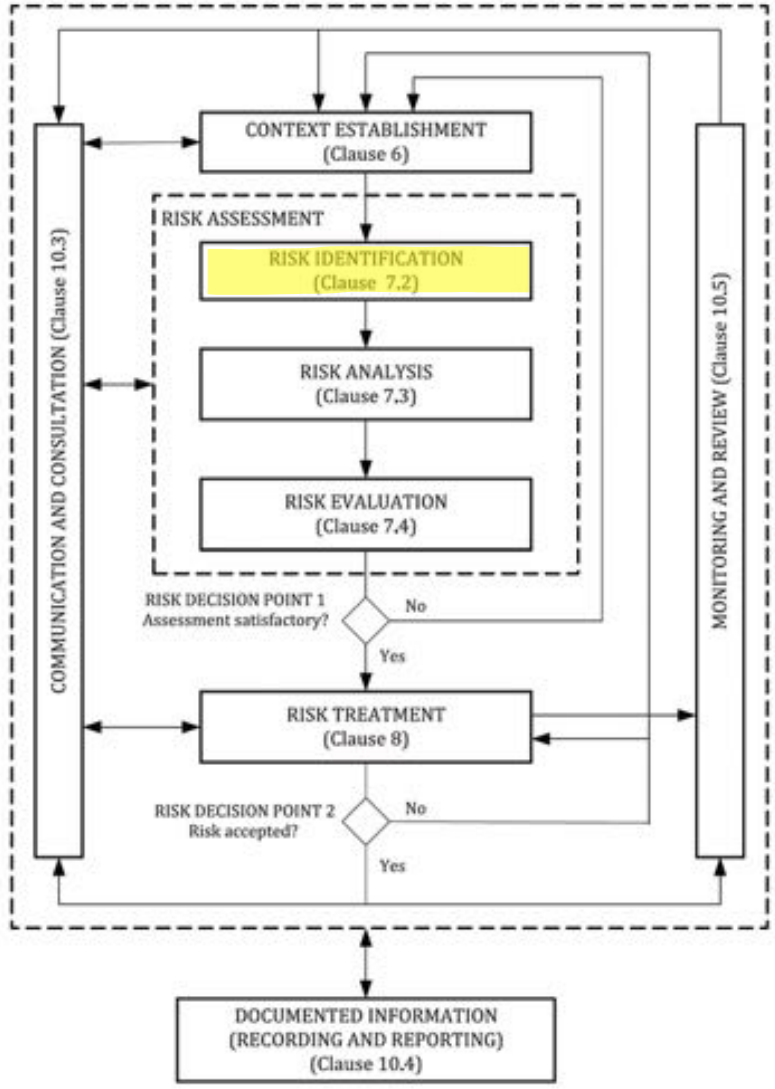
Erläuterungen zu Bewertungskriterien



Quelle: ISO27005/2022

Risiko Identifikation

- Event-basierender Ansatz
  - Ereignisse und daraus resultierende Folgen
  - Ohne Assets
- Asset basierender Ansatz
  - Klassischer Ansatz von Schwachstellen und Bedrohungen zu Assets
- Umfangreiche Neustrukturierung des Annex-A

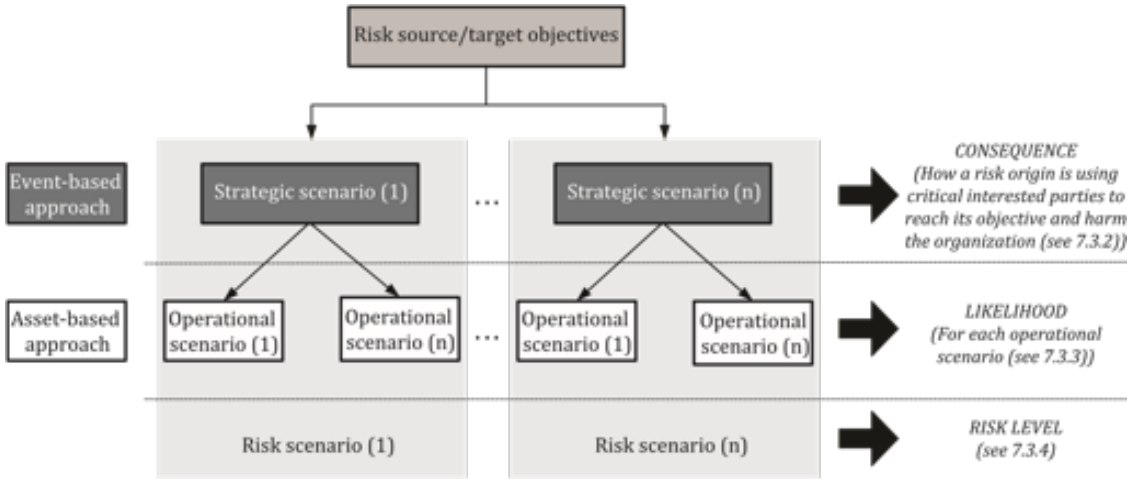


Quelle: ISO27005/2022

Klare Strukturen bei Bedrohungen und Schwachstellen

ANNEX-A

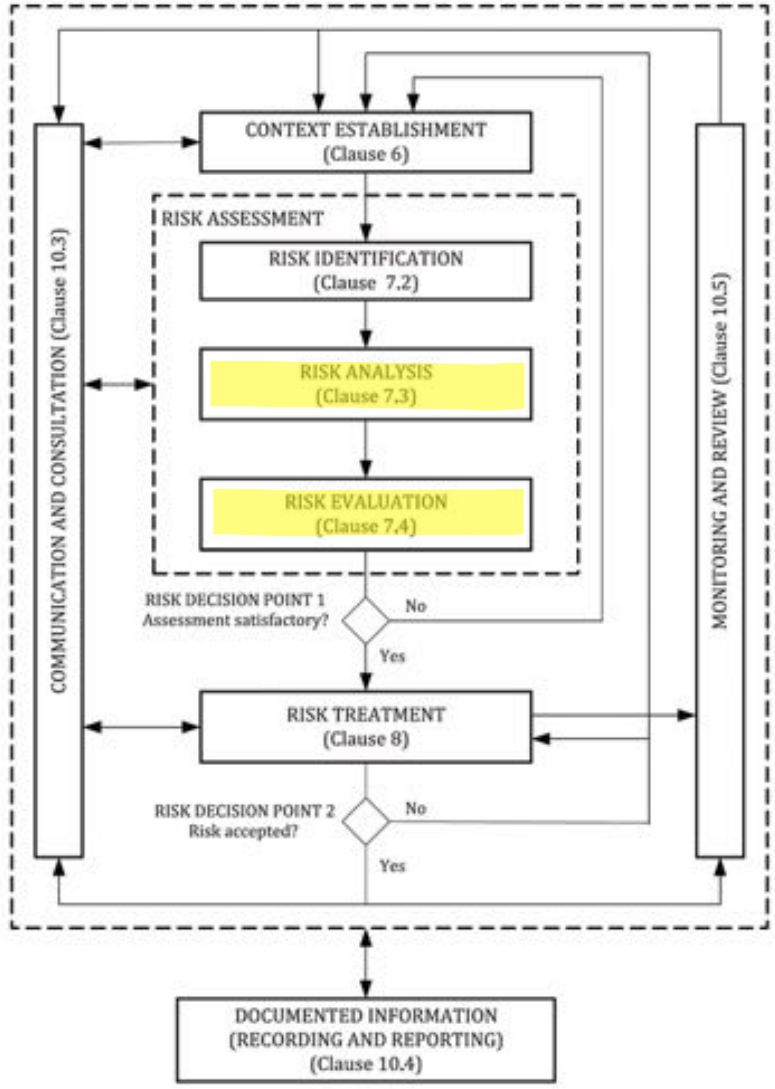
- Der Annex –A enthält eine aktualisierte Liste von Bedrohungen und Schwachstellen.
  Z.B. auch Pandemie hinzugekommen, oder schädliche Strahlung
- Jede Kategorie ist mit einer eindeutigen Nummer versehen, z.B. TP01 (**T**hreat **P**hysical 01)
  oder VS01 (**V**ulnerability **S**oftware **01**)
- Verknüpfung von Event- und Asset-bassierenden Szenrios



Quelle: ISO27005/2022

Risiko Analyse

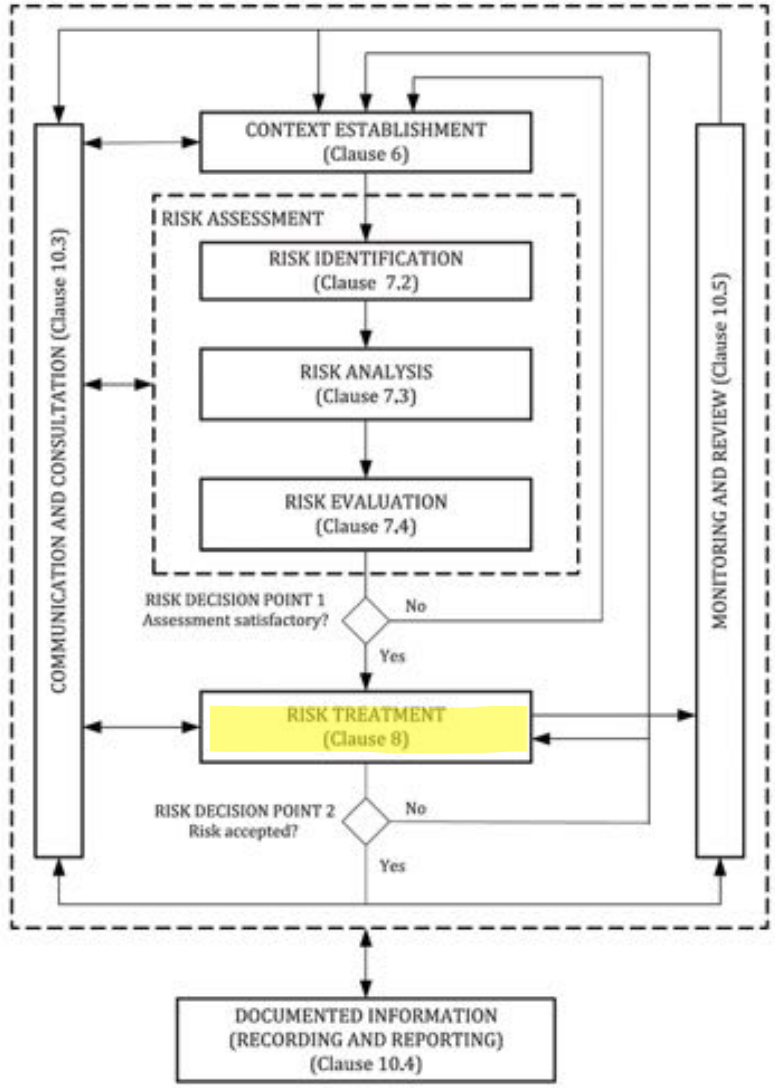
- Eintrittswahrscheinlichkeit und Auswirkungen werden in Kapitel 7 beispielhaft erläutert.
- Hier erhält man eine gute Hilfestellung für den quantitativen und qualitativen Risikoansatz.
- Auch wird die Bedeutung der Wahrscheinlichkeitsrechnung und einer praktischen Herangehensweise erläutert.



Quelle: ISO27005/2022

Risiko Treatment

- Risk-Acceptance nun integriert
- In Kapitel 8 erfolgt eine Handlungsanleitung, wie in enger Anlehnung an die ISO 27001 Controls die nötigen Risikobehandlungsmaßnahmen abgeglichen und das „Statement of Applicability“ erstellt werden sollen.
- Dazu erfolgt die Erstellung eines Risikobehandlungsplans für Informationssicherheitsrisiken zur Ergänzung der Controls

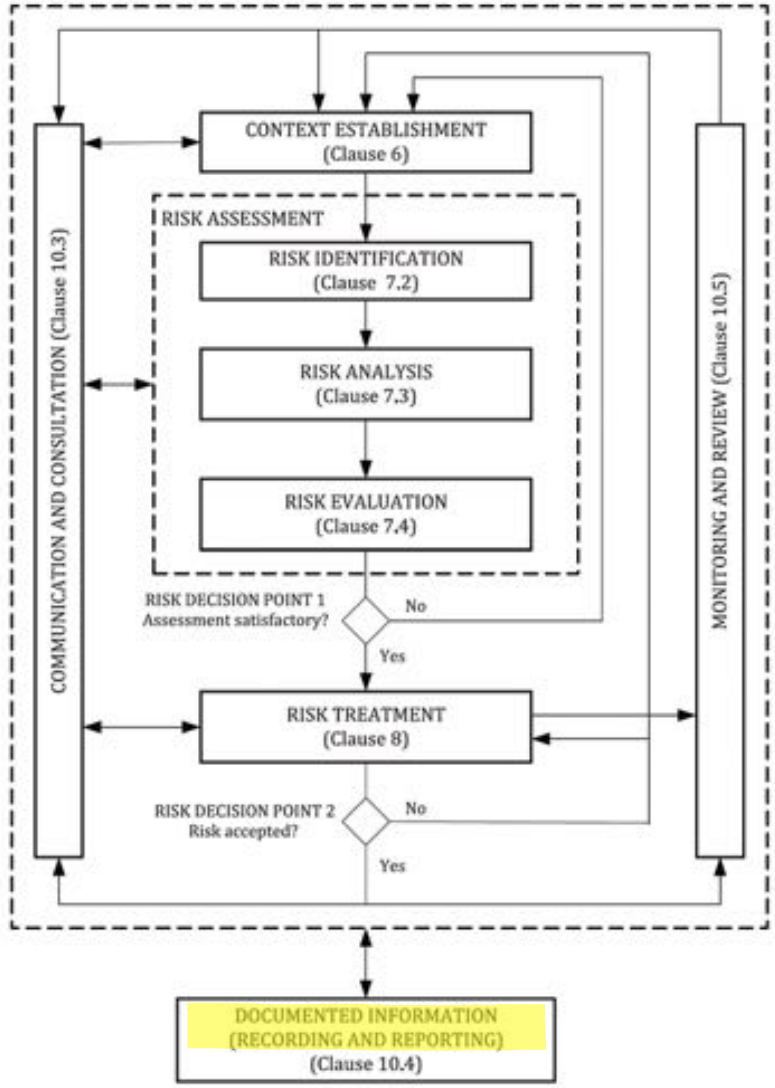


Quelle: ISO27005/2022

Kapitel 10

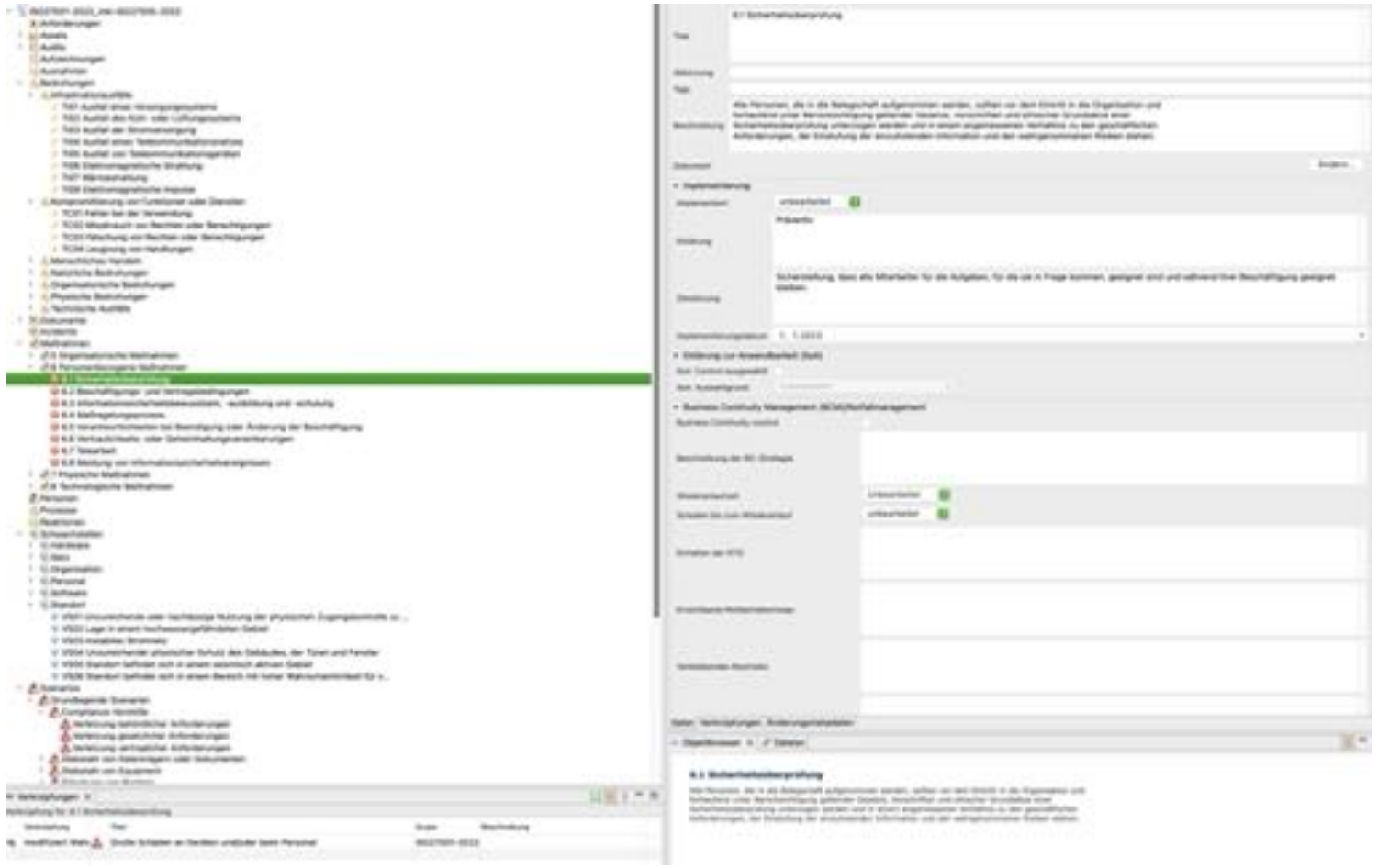
Kapitel 4-10 der ISO 27001 werden nochmal in den Kontext des Risikomanagements gehoben und erklärt.

- 4 Kontext: Identifikation externer und interner Risikoquellen
- 5 Führung: Bedeutung Riskowner, Verantwortung des Managements, Ressourcenbereitstellung und Kommunikation
- 6 Planung: Siehe Kontext
- 7 Unterstützung: Definition der Riskowner, Dokumentation der Methodik und Ergebnisse der Risikoerhebung und Behandlung
- 8 Betrieb: Umsetzung
- 9 Bewertung der Leistung: Audits, Monitoring und Beurteilung
- 10 Verbesserung: Management Review, ggf. Anpassungen der Methodik und Risikobehandlung



Quelle: ISO27005/2022

Umsetzung Verinice



Fragen?

Vielen Dank für Ihre Aufmerksamkeit

Sven Perscheid

Senior Consultant

sven.perscheid@cassini.de

T +49 (0) 151 11 44 01 63