Business Continuity

Szenario – Integration in die ISO 22301

19.09.2024, Impulsvortrag

IHK Südlicher Oberrhein

SDCON

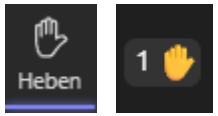
Orga und Agenda

IHK Südlicher Oberrhein

SDCON

Wie gehen wir heute miteinander um?

Kamera und Mikro standardmäßig deaktivieren !
Tippen mit offenem Mikro stört die anderen, die Kamera beeinträchtigt u.U. die Bandbreite bei vielen Teilnehmern…



Diskussion erwünscht !
Einfach Hand heben, die Moderatoren passen hoffentlich auf…

Chatten !
Einfach Dinge in den Chat schreiben, die Moderatoren passen hoffentlich auf …

Zielsetzungen Vortragsreihe

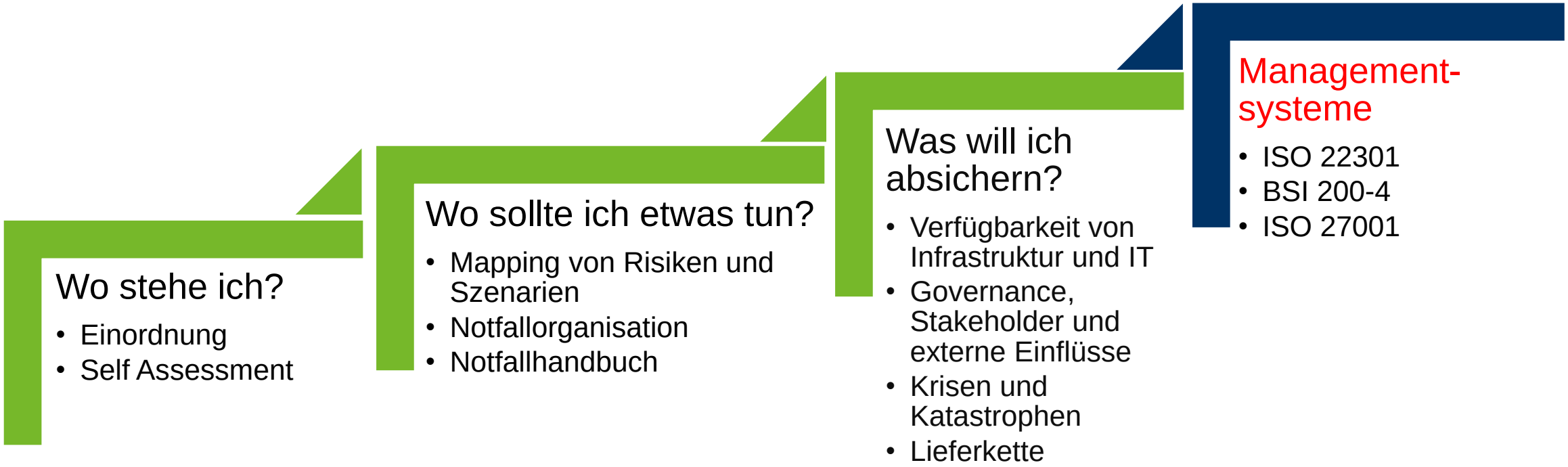
Überblick geben:
Was nützt Continuity Management?

Orientierung geben:
Was kann ich tun?
Wieviel sollte ich tun?

Tools an die Hand geben:
Nützliche Hilfsmittel, einfaches Notfall-Handbuch, Tools für ein Managementsystem

Verankerung in der Organisation:
Organigramm , Prozesse, Verfahrensanweisungen, Dokumente

Vortragsreihe



Agenda für heute

- **Normen und Standards**
  - ISO 22301: Struktur, Inhalte, Tools
  - ISO 27001: Struktur, Inhalte, Tools
  - BSI 200-4: Struktur, Inhalte, Tools
- **Business Impact Analyse**
  - Grundlagen
  - Schritte, Kenngrößen, MTPD, Notbetriebsniveau, Auswertungen
  - Tool: BIA-Auswertungsbogen des BSI
- **Anpassung der BIA light**
- **Ausblick**

Wer ist SD-Con?

Kurzvorstellung

IHK Südlicher Oberrhein

SDCON

Wer sind wir und was tun wir?

- **Das Unternehmen**
  - 2009 gegründet, 7 Mitarbeiter
  - Büros in
    36325 Feldatal
    87600 Kaufbeuren
  - Ca. 130 aktive Kunden in D/A/CH, branchenübergreifend
- **Beratung, Coaching und Wissen für**
  - Integrierte Managementsysteme (IMS)
  - Methoden, Prozesse, Audits, Schulungen
  - Compliance-Management
  - CSR-/ESG-Management
  - Regelbasierte Organisation

Warum Business Continuity Management?

Was sind Ihre Erwartungen für heute?
Schreiben Sie es in den Chat !

ISO 22301 Business Continuity Management

Struktur, Inhalte und Maßnahmenliste

IHK Südlicher Oberrhein

SDCON

Worum geht es bei der ISO 22301?

- **Sicherheit und Resilienz - Business Continuity Management System - Anforderungen**
- **Diese Norm legt Anforderungen fest, um**
  - ein Managementsystem zu verwirklichen, aufrechtzuerhalten und zu verbessern
  - sich gegen Störungen zu schützen, die Wahrscheinlichkeit ihres Auftretens zu vermindern, sich auf diese vorzubereiten,
  - auf diese zu reagieren und sich von diesen zu erholen, wann immer sie auftreten
- **Diese Norm kann dazu genutzt werden,**
  - die Befähigung einer Organisation zur Erfüllung ihrer eigenen Erfordernisse und
  - Verpflichtungen in Bezug auf die Aufrechterhaltung der Betriebsfähigkeit zu bewerten.

Struktur der ISO 22301

- **Orientierung an der High Level Structure (HLS)**
- **Die HLS ist eine Struktur für Managementsysteme**
  - Kontext der Organisation
  - Führung
  - Planung
  - Unterstützung
  - Betrieb
  - Leistungsbewertung
  - Verbesserung

Abschnitt 4: Kontext der Organisation

- **Relevante externe und interne Themen müssen bestimmt werden, sofern sie relevant für die Geschäftsfortführung sind**
- **Unterabschnitte**
  - Verstehen der Organisation und ihres Kontextes
  - Verstehen der Erfordernisse und Erwartungen interessierter Parteien
  - Festlegung des Anwendungsbereichs des Business Continuity Management Systems
  - Business Continuity Management System

Kernforderungen	Das Normkapitel "Kontext der Organisation" beschreibt die Anforderungen an den Kontext, interessierte Parteien, Anwendungsbereich sowie Anforderungen an das BCM-System.
Best Practice	Normanforderungen sowie Best Practices finden Sie in den Unterkapiteln
Unterkapitel	4.1 Verstehen der Organisation und ihres Kontextes 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien 4.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems 4.4 Business Continuity Management System

Abschnitt 4: Kontext der Organisation

- **Wichtige Anforderungen und Dokumente**
  - Kontextanalyse (FB) mit Einflussfaktoren auf das Unternehmen
  - Analyse der interessierten Parteien (FB), ggf. mit Kommunikationsmatrix (FB)
  - Festlegung und Dokumentation von Anwendungsbereich (FB) und Grundsatzerklärung (FB), aber auch Abgrenzungen und Ausschlüsse (FB)
  - Erstellung einer Prozessliste (FB) inkl. Darstellung der Wechselwirkungen zwischen Prozessen
  - Hinweis/Einbindung des Prozesses „Kontinuierliche Verbesserung“ (FB)
  - Verpflichtung zum Aufbau, Verwirklichung, Aufrechterhaltung und fortlaufender Verbesserung des Systems

Abschnitt 5: Führung

- **Anforderungen an Führung, Verpflichtung der Führung, Politik, Rollen, Verantwortlichkeiten und Befugnisse werden definiert**
- **Unterabschnitte**
  - Führung und Verpflichtung
  - Politik
  - Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
- **Wichtige Anforderungen und Dokumente**
  - Grundsatzerklärung (FB) und Übernahme von Verpflichtung/Verantwortung (FB)
  - Politik/en (FB) und BCM-Ziele (FB)
  - Organigramm (FB), Beauftragte (FB), Notfallorganisation (FB)
  - Ressourcen- und Investitionsplan (FB)

Kernforderungen	Das Normkapitel "Führung" beschreibt die Anforderungen an Führung und Verpflichtung, Politik sowie Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.
Best Practice	Normanforderungen sowie Best Practices finden Sie in den Unterkapiteln.
Unterkapitel	5.1 Führung und Verpflichtung 5.2 Politik 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

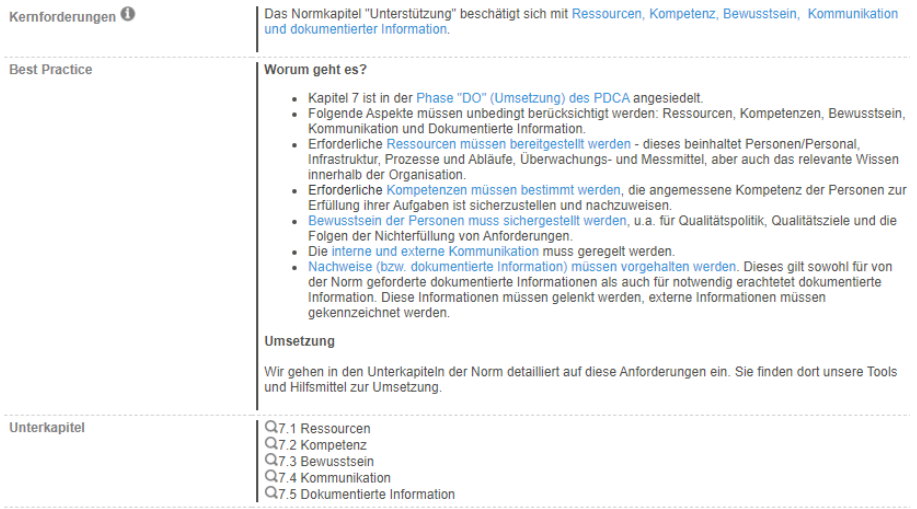
Abschnitt 6: Planung

- **Risiken und Chancen, Aufrechterhaltung der Betriebsfähigkeit, Änderungsmanagement**
- **Unterabschnitte**
  - Maßnahmen zum Umgang mit Risiken und Möglichkeiten
  - Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung zu deren Erreichung
  - Planung von Änderungen am BCMS
- **Wichtige Anforderungen und Dokumente**
  - Prozessliste (FB)
  - Bewertung von Risiken und Chancen (FB) in Bezug auf Prozesse, Interessierte Parteien (FB), Inventar (FB) und Kontext (FB)
  - BCMS-Ziele (FB) unter Berücksichtigung der Messbarkeit und mit Bezug auf Maßnahmen (FB) und Umsetzung
  - Prozess der kontinuierlichen Verbesserung (FB) mit Bezug auf Maßnahmen
  - Änderungsverfahren (FB) für Prozesse, Dokumente, Inventar, Organigramm usw. mit Bezug auf Maßnahmen

Kernforderungen	Das Normkapitel "Planung" beschäftigt sich mit Risiken und Möglichkeiten, Zielen zur Aufrechterhaltung der Betriebsfähigkeit sowie der Planung von Änderungen am BCMS.
Best Practice	Normanforderungen sowie Best Practices finden Sie in den Unterkapiteln
Unterkapitel	6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten 6.2 Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung zu deren Erreichung 6.3 Planung von Änderungen am BCMS

Abschnitt 7: Unterstützung

- **Bereitstellung angemessener Ressourcen, Aufrechterhaltung von Kompetenzen, Bewusstsein und Kommunikation**
- **Unterabschnitte**
  - Ressourcen:
    Infrastruktur, Gebäude, Anlagen, Software, Patente, Rechte, Lizenzen, Personen und Beauftragte, Prozesse, Wissen / Know-how
  - Kompetenz
  - Bewusstsein
  - Kommunikation
  - Dokumentierte Information



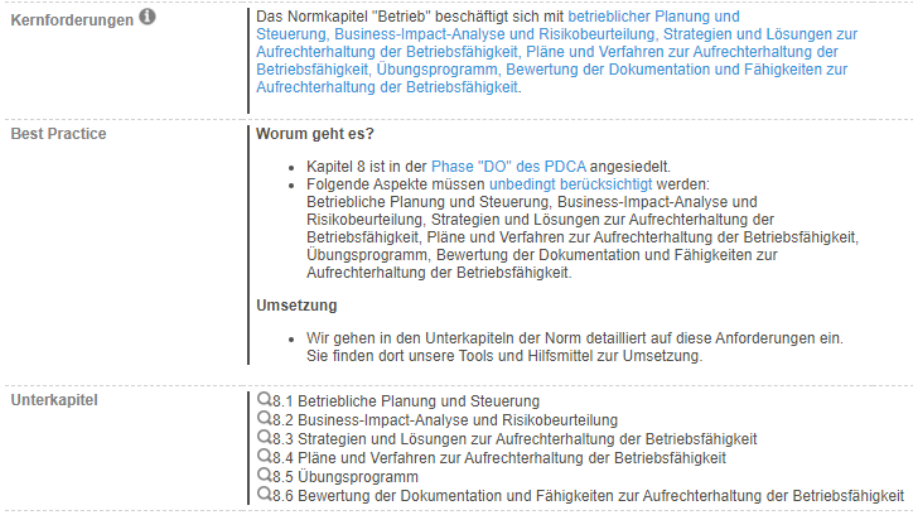
Kernforderungen	Das Normkapitel "Unterstützung" beschätigt sich mit Ressourcen, Kompetenz, Bewusstsein, Kommunikation und dokumentierter Information.
Best Practice	**Worum geht es?** • Kapitel 7 ist in der Phase "DO" (Umsetzung) des PDCA angesiedelt. • Folgende Aspekte müssen unbedingt berücksichtigt werden: Ressourcen, Kompetenzen, Bewusstsein, Kommunikation und Dokumentierte Information. • Erforderliche Ressourcen müssen bereitgestellt werden - dieses beinhaltet Personen/Personal, Infrastruktur, Prozesse und Abläufe, Überwachungs- und Messmittel, aber auch das relevante Wissen innerhalb der Organisation. • Erforderliche Kompetenzen müssen bestimmt werden, die angemessene Kompetenz der Personen zur Erfüllung ihrer Aufgaben ist sicherzustellen und nachzuweisen. • Bewusstsein der Personen muss sichergestellt werden, u.a. für Qualitätspolitik, Qualitätsziele und die Folgen der Nichterfüllung von Anforderungen. • Die interne und externe Kommunikation muss geregelt werden. • Nachweise (bzw. dokumentierte Information) müssen vorgehalten werden. Dieses gilt sowohl für von der Norm geforderte dokumentierte Informationen als auch für notwendig erachtetet dokumentierte Information. Diese Informationen müssen gelenkt werden, externe Informationen müssen gekennzeichnet werden. **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	7.1 Ressourcen 7.2 Kompetenz 7.3 Bewusstsein 7.4 Kommunikation 7.5 Dokumentierte Information

Abschnitt 7: Unterstützung

- **Wichtige Anforderungen und Dokumente**
  - Inventarisierung von Assets (FB) und Prozessen (FB) sowie Berücksichtigung der BCM-Bewertung und Überwachung
  - Instandhaltungs- und Wartungspläne (FB)
  - Investitions- und Budgetpläne (FB) zur Sicherstellung angemessener Ressourcen
  - Personalpläne (FB), Einarbeitungspläne (FB), Qualifikationsmatrix (FB), Schulungsplanung (FB) zur Sicherstellung der Qualifikation (FB) und angemessener Ressourcen und Kenntnisse
  - Kommunikationsmatrix (FB, ggf. in Verbindung mit den interessierten Parteien), Aushänge, News
  - Organigramm (FB) und Notfallorganisation (FB) mit –beauftragten (FB)
  - Regelungen zur Änderungsdokumentation (FB) mit Berechtigungen, ggf. Klassifizierung von Dokumenten, Ablage/Archivierung (physisch / elektronisch)

Abschnitt 8: Betrieb

- **Betriebliche Planung und Steuerung inkl. Business-Impact, Risiken, Aufrechterhaltung des Betriebs, Übungen**
- **Unterabschnitte**
  - Betriebliche Planung und Steuerung
  - Business-Impact-Analyse und Risikobeurteilung
  - Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit
  - Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit
  - Übungsprogramm
  - Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit



Kernforderungen	Das Normkapitel "Betrieb" beschäftigt sich mit betrieblicher Planung und Steuerung, Business-Impact-Analyse und Risikobeurteilung, Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit, Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit, Übungsprogramm, Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit.
Best Practice	**Worum geht es?** • Kapitel 8 ist in der Phase "DO" des PDCA angesiedelt. • Folgende Aspekte müssen unbedingt berücksichtigt werden: Betriebliche Planung und Steuerung, Business-Impact-Analyse und Risikobeurteilung, Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit, Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit, Übungsprogramm, Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit. **Umsetzung** • Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	8.1 Betriebliche Planung und Steuerung 8.2 Business-Impact-Analyse und Risikobeurteilung 8.3 Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit 8.4 Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit 8.5 Übungsprogramm 8.6 Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit

Abschnitt 8: Betrieb

- **Wichtige Anforderungen und Dokumente**
  - Unternehmensziele (FB) und Strategieplan (FB) auf Basis von Anforderungen, Priorisierung von Tätigkeiten, definierten Zeiträumen und festgelegten Kapazitäten
  - Business Impact Analyse (FB) als Grundlage für die Strategie
  - Festlegung von Anforderungen an Tätigkeiten hoher Priorität, Zeitrahmen und Kapazitäten sind festzulegen, Umfang und Art von Risiken
  - Festlegung des Ressourcenbedarfs (FB) zur Aufrechterhaltung der Betriebsfähigkeit.
    Zu berücksichtigen sind u.a. Personen, Informationen und Daten, materielle Infrastruktur, Ausrüstung und Verbrauchsmittel, ICT-Systeme, Transport und Logistik, Finanzen, Partner und Lieferanten
  - Umsetzungspläne (FB) zur Implementierung geplanter Lösungen zur Aufrechterhaltung der Betriebsfähigkeit
  - Reaktions-Struktur (FB) sowie Pläne und Verfahren (FB) für Warnungen und Kommunikation mit interessierten Parteien, zur Steuerung während Störungen und zur Aufrechterhaltung der Betriebsfähigkeit
  - Prozesse zur Wiederherstellung (FB) und Rückkehr (FB) zu den Geschäftstätigkeiten
  - Durchführung von Übungsprogrammen (FB) inkl. Änderungs- und Verbesserungsmanagement
  - Bewertung der Dokumentation: Eignung, Angemessenheit, Wirksamkeit, Aktualität

Abschnitt 9: Bewertung der Leistung

- **Phase CHECK des PDCA mit Überwachung, Messung, Analyse, Internes Audit, Management-bewertung**
- **Unterabschnitte**
  - Überwachung, Messung, Analyse und Bewertung
  - Internes Audit
  - Managementbewertung

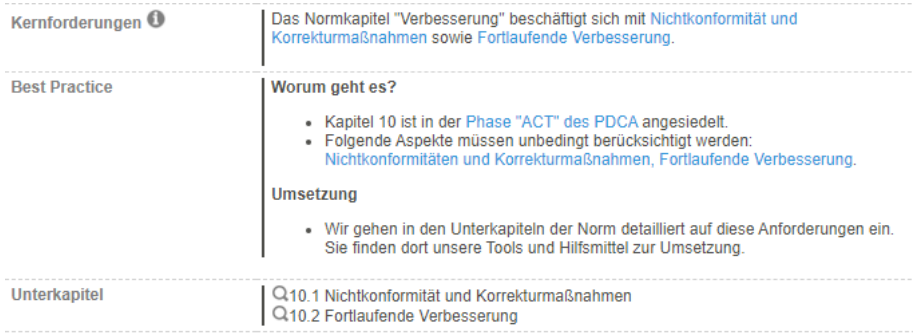
Kernforderungen	Das Normkapitel "Bewertung der Leistung" beschäftigt sich mit Überwachung, Messung, Analyse und Bewertung, Internes Audit, Managementbewertung
Best Practice	**Worum geht es?** • Abschnitt 9 ist in der Phase "CHECK" des PDCA angesiedelt. • Folgende Aspekte müssen unbedingt berücksichtigt werden: Festlegung der Überwachungsgegenstände mit Zeiträumen und Personen, Planung und Durchführung von internen Audits unter Berücksichtigung der Auditanforderungen, Durchführung von Managementbewertungen unter Berücksichtigung der erforderlichen Angaben, Maßnahmenmanagement. **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	9.1 Überwachung, Messung, Analyse und Bewertung 9.2 Internes Audit 9.3 Managementbewertung

Abschnitt 9: Bewertung der Leistung

- **Wichtige Anforderungen und Dokumente**
  - Festlegung, WAS überwacht und gemessen werden muss inkl. dazugehörige Methoden (WIE)
  - Festlegung von Zeiträumen (WANN) und durchführenden Personen (WER)
  - Festlegung eines Auditprogramms (FB) und von Verantwortlichkeiten (FB)
  - Durchführung von internen Audits inkl. Planung (FB) und Berichterstattung (FB), aber auch Berücksichtigung der Auditorenqualifikation (FB)
  - Durchführung einer regelmäßigen Managementbewertung (FB) unter Berücksichtigung der geforderten Inhalte sowie Bewertung in Bezug auf Verbesserungen und Effizienz
  - Verfolgung von Feststellungen und Korrekturmaßnahmen (FB)

Abschnitt 10: Verbesserung

- **Nichtkonformitäten, Korrekturmaßnahmen sowie Fortlaufende Verbesserung**
- **Unterabschnitte**
  - Nichtkonformität und Korrekturmaßnahmen
  - Fortlaufende Verbesserung
- **Wichtige Anforderungen und Dokumente**
  - Möglichkeiten zur Verbesserung (FB) bestimmen, Maßnahmen (FB) verwirklichen
  - Berücksichtigung von Analysen, Bewertungen, Management-Review (FB)
  - Reaktion auf Nichtkonformitäten (FB), ggf. Maßnahmen zur Überwachung und zur Korrektur (FB) ergreifen und mit den Folgen umgehen
  - Maßnahmen zur Beseitigung der Ursachen bewerten, erforderliche Maßnahmen einleiten, Wirksamkeit (FB) prüfen
  - Bei Bedarf das BCMS ändern



Kernforderungen	Das Normkapitel "Verbesserung" beschäftigt sich mit Nichtkonformität und Korrekturmaßnahmen sowie Fortlaufende Verbesserung.
Best Practice	**Worum geht es?** • Kapitel 10 ist in der Phase "ACT" des PDCA angesiedelt. • Folgende Aspekte müssen unbedingt berücksichtigt werden: Nichtkonformitäten und Korrekturmaßnahmen, Fortlaufende Verbesserung. **Umsetzung** • Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	10.1 Nichtkonformität und Korrekturmaßnahmen 10.2 Fortlaufende Verbesserung

BCM-Maßnahmenliste

https://service.sd-con.de/containerDocs/34B7EDEC

Audit-Checkliste ISO 22301

https://service.sd-con.de/containerDocs/2C280DFA

ISO 27001 Information Security Management

Struktur, Inhalte und Maßnahmenliste

IHK Südlicher Oberrhein

SDCON

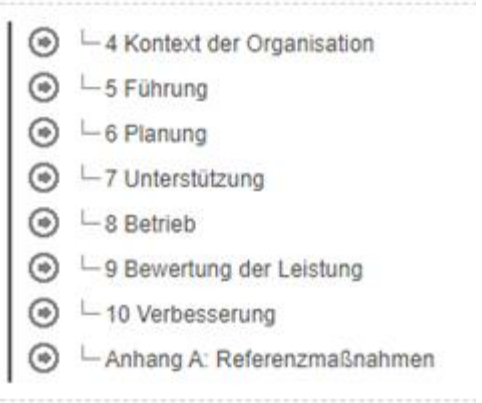
Worum geht es bei der ISO 27001?

- **Informationstechnik – Sicherheitsverfahren – Information Security Management System - Anforderungen**
- **Diese Norm legt Anforderungen fest, um**
  - ein Managementsystem zu verwirklichen, aufrechtzuerhalten und zu verbessern
  - Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation zu verwirklichen
  - die Beurteilung und Behandlung von Informationssicherheitsrisiken gemäß den Bedürfnissen der Organisation abzubilden

IHK Südlicher Oberrhein

Struktur der ISO 27001

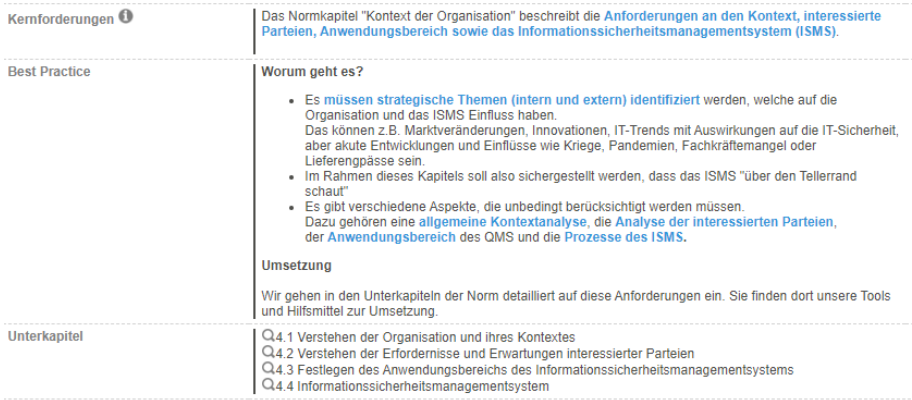
- **Orientierung an der High Level Structure (HLS)**
  - Kontext der Organisation
  - Führung
  - Planung
  - Unterstützung
  - Betrieb
  - Leistungsbewertung
  - Verbesserung
  - Anhang A: Referenzmaßnahmen



SDCON

Abschnitt 4: Kontext der Organisation

- **Relevante externe und interne Themen müssen bestimmt werden, sofern sie relevant für die Geschäftsfortführung sind**
- **Unterabschnitte**
  - Verstehen der Organisation und ihres Kontextes
  - Verstehen der Erfordernisse und Erwartungen interessierter Parteien
  - Festlegung des Anwendungsbereichs des Informationssicherheits-managementsystems
  - Informationssicherheitsmanagementsystem



Kernforderungen	Das Normkapitel "Kontext der Organisation" beschreibt die **Anforderungen an den Kontext, interessierte Parteien, Anwendungsbereich sowie das Informationssicherheitsmanagementsystem (ISMS)**.
Best Practice	**Worum geht es?** • Es **müssen strategische Themen (intern und extern) identifiziert** werden, welche auf die Organisation und das ISMS Einfluss haben. Das können z.B. Marktveränderungen, Innovationen, IT-Trends mit Auswirkungen auf die IT-Sicherheit, aber akute Entwicklungen und Einflüsse wie Kriege, Pandemien, Fachkräftemangel oder Lieferengpässe sein. • Im Rahmen dieses Kapitels soll also sichergestellt werden, dass das ISMS "über den Tellerrand schaut" • Es gibt verschiedene Aspekte, die unbedingt berücksichtigt werden müssen. Dazu gehören eine **allgemeine Kontextanalyse**, die **Analyse der interessierten Parteien**, der **Anwendungsbereich** des QMS und die **Prozesse des ISMS.** **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	4.1 Verstehen der Organisation und ihres Kontextes 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien 4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems 4.4 Informationssicherheitsmanagementsystem

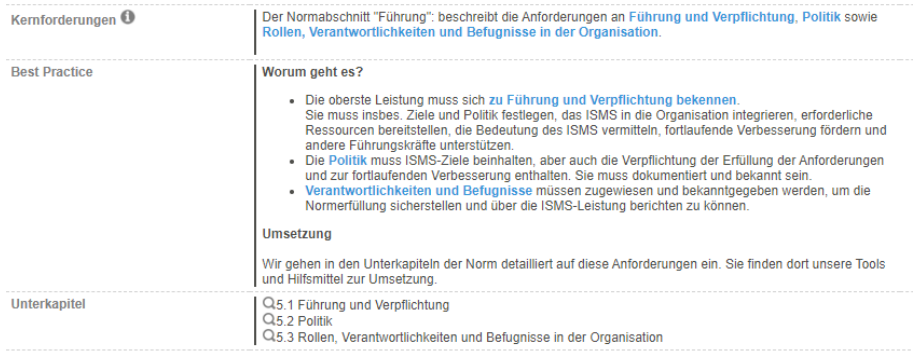
Abschnitt 4: Kontext der Organisation

- **Wichtige Anforderungen und Dokumente**
  - Kontextanalyse (FB) mit Einflussfaktoren auf das Unternehmen
  - Analyse der interessierten Parteien (FB), ggf. mit Kommunikationsmatrix (FB)
  - Festlegung und Dokumentation von Anwendungsbereich (FB) und Grundsatzerklärung (FB), aber auch Abgrenzungen und Ausschlüsse (FB)
  - Erstellung einer Prozessliste (FB) inkl. Darstellung der Wechselwirkungen zwischen Prozessen
  - Hinweis/Einbindung des Prozesses „Kontinuierliche Verbesserung“ (FB)
  - Verpflichtung zum Aufbau, Verwirklichung, Aufrechterhaltung und fortlaufender Verbesserung des Systems

Fast identisch zu ISO 22301 und anderen Normen

Abschnitt 5: Führung

- **Anforderungen an Führung, Verpflichtung der Führung, Politik, Rollen, Verantwortlichkeiten und Befugnisse werden definiert**
- **Unterabschnitte**
  - Führung und Verpflichtung
  - Politik
  - Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
- **Wichtige Anforderungen und Dokumente**
  - Grundsatzerklärung (FB) und Übernahme von Verpflichtung/Verantwortung (FB)
  - Politik/en (FB) und ISMS-Ziele (FB)
  - Ressourcen- und Investitionsplan (FB)
  - Organigramm (FB), Beauftragte (FB)

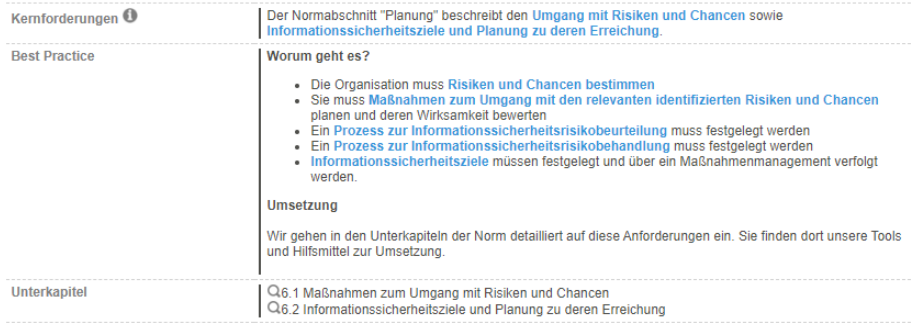


Kernforderungen	Der Normabschnitt "Führung": beschreibt die Anforderungen an **Führung und Verpflichtung**, **Politik** sowie **Rollen, Verantwortlichkeiten und Befugnisse in der Organisation**.
Best Practice	**Worum geht es?** • Die oberste Leistung muss sich **zu Führung und Verpflichtung bekennen**. Sie muss insbes. Ziele und Politik festlegen, das ISMS in die Organisation integrieren, erforderliche Ressourcen bereitstellen, die Bedeutung des ISMS vermitteln, fortlaufende Verbesserung fördern und andere Führungskräfte unterstützen. • Die **Politik** muss ISMS-Ziele beinhalten, aber auch die Verpflichtung der Erfüllung der Anforderungen und zur fortlaufenden Verbesserung enthalten. Sie muss dokumentiert und bekannt sein. • **Verantwortlichkeiten und Befugnisse** müssen zugewiesen und bekanntgegeben werden, um die Normerfüllung sicherstellen und über die ISMS-Leistung berichten zu können. **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	5.1 Führung und Verpflichtung 5.2 Politik 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Fast identisch zu ISO 22301 und anderen Normen

Abschnitt 6: Planung

- **Risiken und Chancen, ISMS-Ziele und Planung zur Erreichung dieser Ziele**
- **Unterabschnitte**
  - Maßnahmen zum Umgang mit Risiken und Chancen
  - Informationssicherheitsziele und Planung zu deren Erreichung
- **Wichtige Anforderungen und Dokumente**
  - Prozessliste (FB)
  - Bewertung von Risiken und Chancen (FB) in Bezug auf Prozesse, Interessierte Parteien (FB), Inventar (FB) und Kontext (FB)
  - Festlegung von Prozessen zur Informationssicherheitsrisikobeurteilung und Informationssicherheitsrisikobehandlung sowie Identifizierung, Analyse und Bewertung dieser Risiken und Festlegung von Maßnahmen
  - ISMS-Ziele (FB) unter Berücksichtigung von Risiken und mit Bezug zu Maßnahmen (FB)

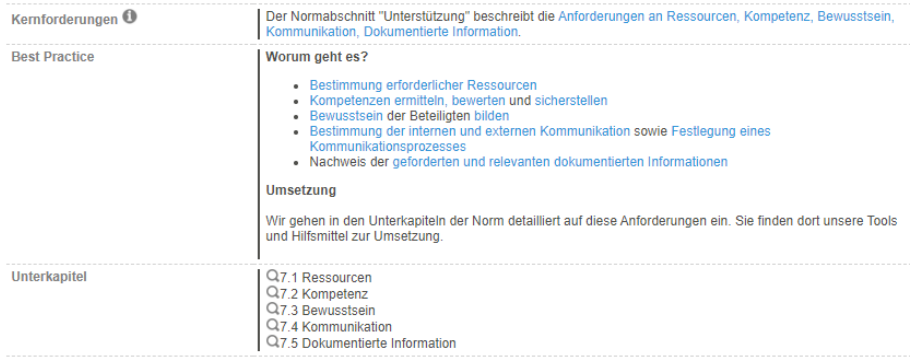


Kernforderungen	Der Normabschnitt "Planung" beschreibt den Umgang mit Risiken und Chancen sowie Informationssicherheitsziele und Planung zu deren Erreichung.
Best Practice	**Worum geht es?** • Die Organisation muss Risiken und Chancen bestimmen • Sie muss Maßnahmen zum Umgang mit den relevanten identifizierten Risiken und Chancen planen und deren Wirksamkeit bewerten • Ein Prozess zur Informationssicherheitsrisikobeurteilung muss festgelegt werden • Ein Prozess zur Informationssicherheitsrisikobehandlung muss festgelegt werden • Informationssicherheitsziele müssen festgelegt und über ein Maßnahmenmanagement verfolgt werden. **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	6.1 Maßnahmen zum Umgang mit Risiken und Chancen 6.2 Informationssicherheitsziele und Planung zu deren Erreichung

IHK Südlicher Oberrhein

Abschnitt 7: Unterstützung

- **Bereitstellung angemessener Ressourcen, Aufrechterhaltung von Kompetenzen, Bewusstsein und Kommunikation**
- **Unterabschnitte**
  - Ressourcen: Infrastruktur, Gebäude, Anlagen, Software, Patente, Rechte, Lizenzen, Personen und Beauftragte, Prozesse, Wissen / Know-how
  - Kompetenz
  - Bewusstsein
  - Kommunikation
  - Dokumentierte Information



Kernforderungen	Der Normabschnitt "Unterstützung" beschreibt die Anforderungen an Ressourcen, Kompetenz, Bewusstsein, Kommunikation, Dokumentierte Information.
Best Practice	**Worum geht es?** • Bestimmung erforderlicher Ressourcen • Kompetenzen ermitteln, bewerten und sicherstellen • Bewusstsein der Beteiligten bilden • Bestimmung der internen und externen Kommunikation sowie Festlegung eines Kommunikationsprozesses • Nachweis der geforderten und relevanten dokumentierten Informationen **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	7.1 Ressourcen 7.2 Kompetenz 7.3 Bewusstsein 7.4 Kommunikation 7.5 Dokumentierte Information

Fast identisch zu ISO 22301 und anderen Normen

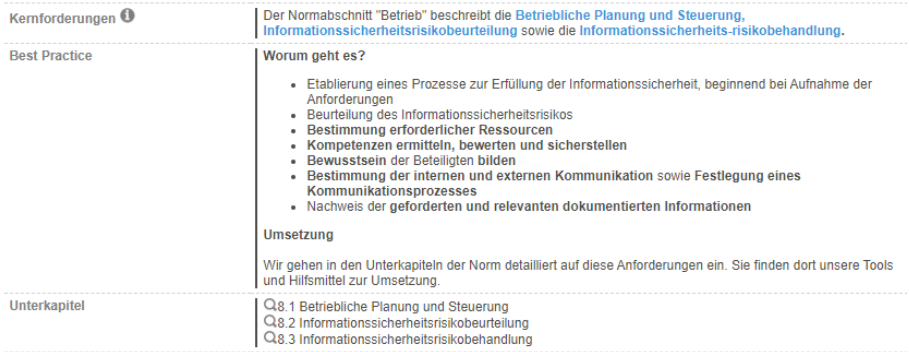
SDCON

Abschnitt 7: Unterstützung

- **Wichtige Anforderungen und Dokumente**
  - Inventarisierung von Assets (FB) und Prozessen (FB) sowie Berücksichtigung der ISM-Bewertung und Überwachung
  - Investitions- und Budgetpläne (FB) zur Sicherstellung angemessener Ressourcen
  - Personalpläne (FB), Einarbeitungspläne (FB), Qualifikationsmatrix (FB), Schulungsplanung (FB) zur Sicherstellung der Qualifikation (FB) und angemessener Ressourcen
  - Schulungen, Übungspläne (FB) zur Sicherstellung der Kenntnis über das ISMS
  - Kommunikationsmatrix (FB, ggf. in Verbindung mit den interessierten Parteien), Aushänge, News
  - Regelungen für angemessenen Schutz (z. B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität), Verteilung, Zugriff, Auffindung und Verwendung, Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit, Überwachung von Änderungen (z. B. Versionskontrolle), Aufbewahrung und Verfügung über den weiteren Verbleib.

Abschnitt 8: Betrieb

- **Betriebliche Planung und Steuerung inkl. Beurteilung des ISM-Risikos, Pläne zur Erreichung der Ziele, Änderungsmanagement, ausgegliederte Prozesse, ISM-Prozess und Risikobehandlung**
- **Unterabschnitte**
  - Betriebliche Planung und Steuerung
  - Informationssicherheitsrisikobeurteilung
  - Informationssicherheitsrisikobehandlung



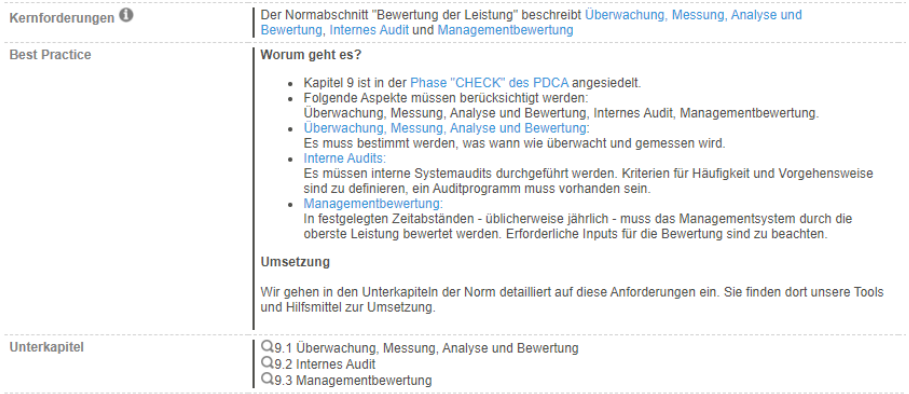
Kernforderungen	Der Normabschnitt "Betrieb" beschreibt die Betriebliche Planung und Steuerung, Informationssicherheitsrisikobeurteilung sowie die Informationssicherheits-risikobehandlung.
Best Practice	**Worum geht es?** • Etablierung eines Prozesse zur Erfüllung der Informationssicherheit, beginnend bei Aufnahme der Anforderungen • Beurteilung des Informationssicherheitsrisikos • **Bestimmung erforderlicher Ressourcen** • **Kompetenzen ermitteln, bewerten und sicherstellen** • **Bewusstsein** der Beteiligten **bilden** • **Bestimmung der internen und externen Kommunikation** sowie **Festlegung eines Kommunikationsprozesses** • Nachweis der **geforderten und relevanten dokumentierten Informationen** **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	8.1 Betriebliche Planung und Steuerung 8.2 Informationssicherheitsrisikobeurteilung 8.3 Informationssicherheitsrisikobehandlung

Abschnitt 8: Betrieb

- **Wichtige Anforderungen und Dokumente**
  - Prozessliste (FB) inkl. Kennzeichnung ausgegliederter Prozesse
  - Unternehmensziele (FB) auf Basis von Anforderungen mit Priorisierung
  - ISM-Umsetzungspläne (FB) inkl. Maßnahmenmanagement
  - ISM-Risikobeurteilungen (FB) mit Risikokatalogen
  - ISM-Risikobehandlung (FB) inkl. Maßnahmenmanagement und Kopplung zu Zielen

Abschnitt 9: Bewertung der Leistung

- **Phase CHECK des PDCA mit Überwachung, Messung, Analyse, Internes Audit, Management-bewertung**
- **Unterabschnitte**
  - Überwachung, Messung, Analyse und Bewertung
  - Internes Audit
  - Managementbewertung



Kernforderungen	Der Normabschnitt "Bewertung der Leistung" beschreibt Überwachung, Messung, Analyse und Bewertung, Internes Audit und Managementbewertung
Best Practice	**Worum geht es?** • Kapitel 9 ist in der Phase "CHECK" des PDCA angesiedelt. • Folgende Aspekte müssen berücksichtigt werden: Überwachung, Messung, Analyse und Bewertung, Internes Audit, Managementbewertung. • Überwachung, Messung, Analyse und Bewertung: Es muss bestimmt werden, was wann wie überwacht und gemessen wird. • Interne Audits: Es müssen interne Systemaudits durchgeführt werden. Kriterien für Häufigkeit und Vorgehensweise sind zu definieren, ein Auditprogramm muss vorhanden sein. • Managementbewertung: In festgelegten Zeitabständen - üblicherweise jährlich - muss das Managementsystem durch die oberste Leistung bewertet werden. Erforderliche Inputs für die Bewertung sind zu beachten. **Umsetzung** Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	9.1 Überwachung, Messung, Analyse und Bewertung 9.2 Internes Audit 9.3 Managementbewertung

Fast identisch zu ISO 22301 und anderen Normen

Abschnitt 9: Bewertung der Leistung

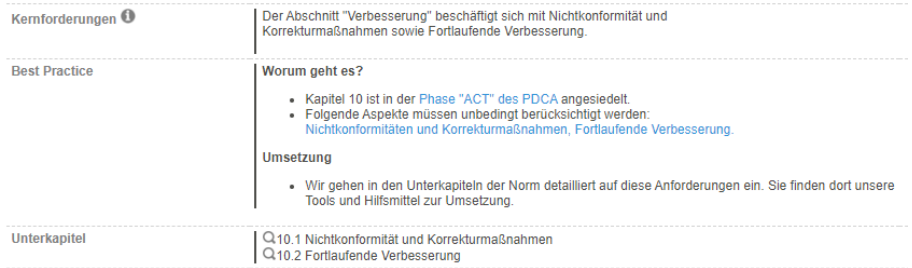
- **Wichtige Anforderungen und Dokumente**
  - Festlegung, WAS überwacht und gemessen werden muss inkl. dazugehörige Methoden (WIE)
  - Festlegung von Zeiträumen (WANN) und durchführenden Personen (WER)
  - Festlegung eines Auditprogramms (FB) und von Verantwortlichkeiten (FB)
  - Durchführung von internen Audits inkl. Planung (FB) und Berichterstattung (FB), aber auch Berücksichtigung der Auditorenqualifikation (FB)
  - Durchführung einer regelmäßigen Managementbewertung (FB) unter Berücksichtigung der geforderten Inhalte sowie Bewertung in Bezug auf Verbesserungen und Effizienz
  - Verfolgung von Feststellungen und Korrekturmaßnahmen (FB)

Fast identisch zu ISO 22301 und anderen Normen

IHK Südlicher Oberrhein

Abschnitt 10: Verbesserung

- **Nichtkonformitäten, Korrekturmaßnahmen sowie Fortlaufende Verbesserung**
- **Unterabschnitte**
  - Nichtkonformität und Korrekturmaßnahmen
  - Fortlaufende Verbesserung
- **Wichtige Anforderungen und Dokumente**
  - Möglichkeiten zur Verbesserung (FB) bestimmen, Maßnahmen (FB) verwirklichen
  - Berücksichtigung von Analysen, Bewertungen, Management-Review (FB)
  - Reaktion auf Nichtkonformitäten (FB), ggf. Maßnahmen zur Überwachung und zur Korrektur (FB) ergreifen und mit den Folgen umgehen
  - Maßnahmen zur Beseitigung der Ursachen bewerten, erforderliche Maßnahmen einleiten, Wirksamkeit (FB) prüfen
  - Bei Bedarf das ISMS ändern



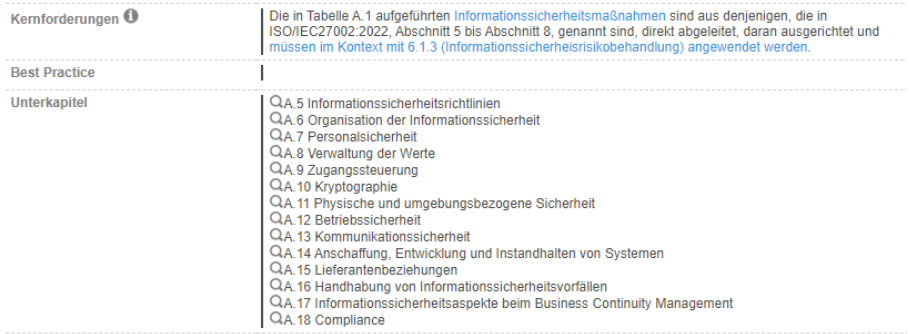
Kernforderungen	Der Abschnitt "Verbesserung" beschäftigt sich mit Nichtkonformität und Korrekturmaßnahmen sowie Fortlaufende Verbesserung.
Best Practice	**Worum geht es?** • Kapitel 10 ist in der Phase "ACT" des PDCA angesiedelt. • Folgende Aspekte müssen unbedingt berücksichtigt werden: Nichtkonformitäten und Korrekturmaßnahmen, Fortlaufende Verbesserung. **Umsetzung** • Wir gehen in den Unterkapiteln der Norm detailliert auf diese Anforderungen ein. Sie finden dort unsere Tools und Hilfsmittel zur Umsetzung.
Unterkapitel	10.1 Nichtkonformität und Korrekturmaßnahmen 10.2 Fortlaufende Verbesserung

Fast identisch zu ISO 22301 und anderen Normen

SDCON

Anhang A.1

- **Informationssicherheitsmaßnahmen im Kontext mit 6.1.3 (Informationssicherheisrisikobehandlung)**
- **Unterabschnitte**
  - A.5 Informationssicherheitsrichtlinien
  - A.6 Organisation der Informationssicherheit
  - A.7 Personalsicherheit
  - A.8 Verwaltung der Werte
  - A.9 Zugangssteuerung
  - A.10 Kryptographie
  - A.11 Physische und umgebungsbezogene Sicherheit
  - A.12 Betriebssicherheit
  - A.13 Kommunikationssicherheit
  - A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
  - A.15 Lieferantenbeziehungen
  - A.16 Handhabung von Informationssicherheitsvorfällen
  - A.17 Informationssicherheitsaspekte beim Business Continuity Management
  - A.18 Compliance



Kernforderungen	Die in Tabelle A.1 aufgeführten Informationssicherheitsmaßnahmen sind aus denjenigen, die in ISO/IEC27002:2022, Abschnitt 5 bis Abschnitt 8, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit 6.1.3 (Informationssicherheisrisikobehandlung) angewendet werden.
Best Practice	
Unterkapitel	A.5 Informationssicherheitsrichtlinien A.6 Organisation der Informationssicherheit A.7 Personalsicherheit A.8 Verwaltung der Werte A.9 Zugangssteuerung A.10 Kryptographie A.11 Physische und umgebungsbezogene Sicherheit A.12 Betriebssicherheit A.13 Kommunikationssicherheit A.14 Anschaffung, Entwicklung und Instandhalten von Systemen A.15 Lieferantenbeziehungen A.16 Handhabung von Informationssicherheitsvorfällen A.17 Informationssicherheitsaspekte beim Business Continuity Management A.18 Compliance

Assessment zur Bewertung der Umsetzung der ISO 27001

https://service.sd-con.de/containerDocs/4D8373A1

BSI 200-4 Business Continuity Management

Struktur, Inhalte und Maßnahmenliste

IHK Südlicher Oberrhein

SDCON

Worum geht es bei dem BSI-Standard 200-4?

- **Der BSI-Standard 200-4 Business Continuity Management beschreibt, mit welchen Methoden BCM in einer Institution generell initiiert, implementiert und gesteuert werden kann.**
- **Diese Norm legt Anforderungen fest, um**
  - ein BCMS schrittweise einzuführen. Der Standard bildet die Phasen der Einführung mitsamt Best Practices ab
  - Institutionen in die Lage zu versetzen, alle Arten von Notfällen erfolgreich sowie Krisen zumindest rudimentär zu bewältigen
- **Der Standard ist mit 312 Seiten sehr umfangreich (ISO 22301: 34 Seiten) und für größere Organisationen ausgelegt (z.B. Kapitel 5 BAO).**
- **Der Standard ist kostenfrei verfügbar und liefert einige Arbeitshilfen**

Struktur des BSI-Standards 200-4

- **Phasen-Struktur ohne Orientierung an ISO-Normen und HLS**
- **Inhalte**
  - Was ist Business Continuity Management?
  - Initiierung, Konzeption und Planung des BCMS
  - BAO (Besondere Aufbauorganisation)
  - Business-Impact-Analyse inkl. BIA-Vorfilter
  - Soll-Ist-Vergleich
  - BCM-Risikoanalyse
  - BC-Strategien und Geschäftsfortführungsplanung
  - Wiederanlauf, Wiederherstellung, Üben, Testen
  - Leistungsüberprüfung, Berichterstattung, Verbesserung
  - Anhang A: Anforderungskatalog

Anhang A: Anforderungskatalog

- **Excel-Liste mit 583 Zeilen voll Anforderungen mit Kurzbeschreibung, Kapitelbezug und Anforderungsstrenge (MUSS / SOLLTE)**
- **255 MUSS-Anforderungen**

107	106	5 - Aufbau und Befähigung der BAO	ALARM-001-b	Der Alarmierungs- und Eskalationsprozess SOLLTE vorhandene Prozesse zur Behandlung von Störungen und Sicherheitsvorfällen berücksichtigen.	5.2	SOLLTE
108	107	5 - Aufbau und Befähigung der BAO	ALARM-001-c	Die Institution SOLLTE vorab festlegen, wie und über welche Kanäle die Meldung von Schadensereignissen mit Notfallpotenzial erfolgen soll.	5.2	SOLLTE
109	108	5 - Aufbau und Befähigung der BAO	ALARM-001-d	Die Institution SOLLTE unterscheiden, ob Meldungen der Information oder der Alarmierung dienen und Kriterien für jede Art der Meldung festlegen.	5.2	SOLLTE
110	109	5 - Aufbau und Befähigung der BAO	ALARM-001-e	Für den Alarmierungs- und Eskalationsprozess MUSS technisch sichergestellt sein, dass die Kommunikations- und Alarmierungstechnik auch in einem Not- oder Krisenfall zur Verfügung steht.	5.2	MUSS
111	110	5 - Aufbau und Befähigung der BAO	ALARM-001-f	Für den Alarmierungs- und Eskalationsprozess SOLLTEN Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.	5.2.1	SOLLTE
112	111	5 - Aufbau und Befähigung der BAO	ALARM-001-g	Der Alarmierungs- und Eskalationsprozess MUSS sicherstellen, dass Meldungen an die zuständigen Meldestellen gelangen und nicht verloren gehen.	5.2.1	MUSS
113	112	5 - Aufbau und Befähigung der BAO	ALARM-001-h	Die identifizierten und festgelegten Meldewege MÜSSEN mit den beteiligten organisatorischen Schnittstellen abgestimmt werden, sodass diese bei Schadensereignissen mit Notfallpotenzial mit den definierten Wegen vertraut sind.	5.2.1	MUSS
114	113	5 - Aufbau und Befähigung der BAO	ALARM-001-i	Die im Notfallhandbuch dokumentierten Meldeverfahren SOLLTEN den gelebten Prozessen entsprechen	5.2.1	SOLLTE
115	114	5 - Aufbau und Befähigung der BAO	ALARM-001-j	Durch Schulungen und Sensibilisierung aller Mitarbeitenden und gegebenenfalls externen Zuarbeitenden MUSS sichergestellt werden, dass der Alarmierungs- und Eskalationsprozess bekannt ist und korrekt angewendet wird.	5.2.1	MUSS
116	115	5 - Aufbau und Befähigung der BAO	ALARM-001-k	Der definierte Eskalations- und Alarmierungsprozess SOLLTE visualisiert und im Notfallhandbuch dokumentiert werden.	5.2.3	SOLLTE
				Die Institution SOLLTE sicherstellen, dass Schadensereignisse und Störungen mit Notfallpotenzial in angemessener Zeit an eine zentrale Entscheidungsinstanz gemeldet werden und Reaktionszeiten		

BSI 200-4 Business Continuity Management

BSI-Standard 200-4

BSI-Seite

Hilfsmittel

https://www.bsi.bund.de/dok/200-4-hilfsmittel

Anforderungskatalog

Download

Business Impact Analyse

IHK Südlicher Oberrhein

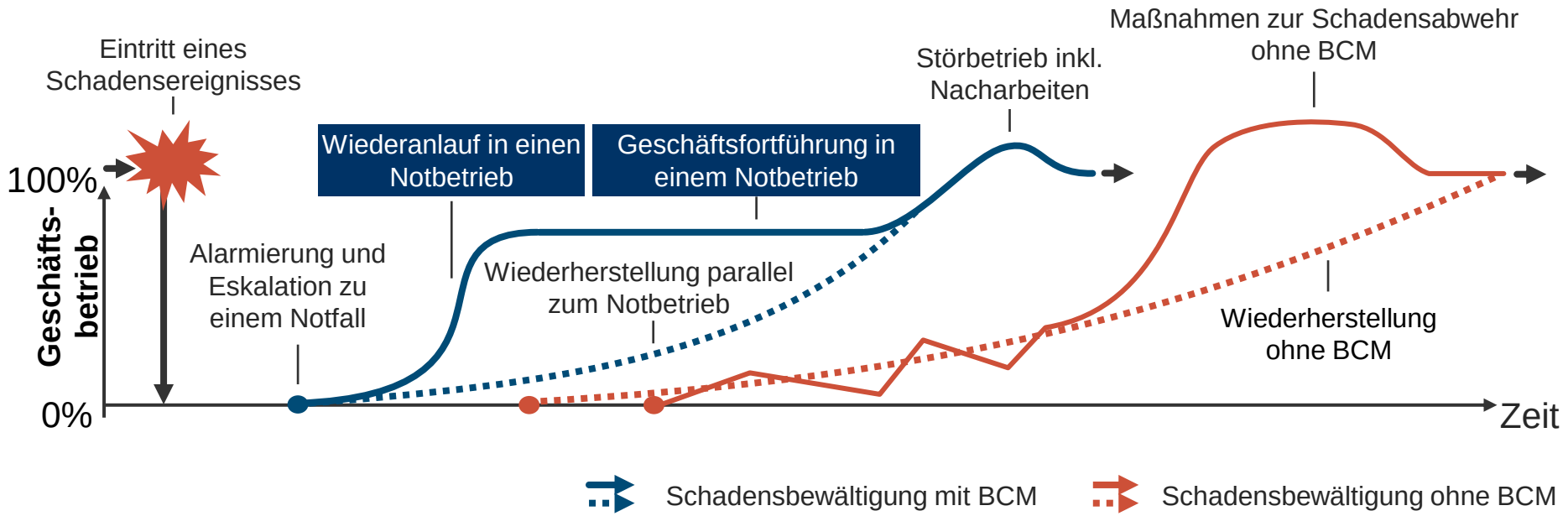
SDCON

Grundlagen

- **Definition und Zielsetzung**
  - Die Business Impact Analyse (BIA) ist ein systematischer Prozess, der dazu dient, die potenziellen Auswirkungen von Störungen oder Ausfällen auf die Geschäftsprozesse eines Unternehmens zu identifizieren und zu bewerten.
  - Ziel der BIA ist es, kritische Geschäftsprozesse und die damit verbundenen Ressourcen, Abhängigkeiten und Ausfallzeiten zu bestimmen, um geeignete Maßnahmen zur Schadensminimierung und Wiederherstellung zu planen.
- **Anforderung**
  - Abschätzung, welche Prozesse potenziell zeitkritisch sind
  - Bewertung der Schadensauswirkungen und die Überschreitung einer Toleranzgrenze
  - Ergreifen von Präventivmaßnahmen zur Gewährleistung eines Notbetriebs

Grundlagen

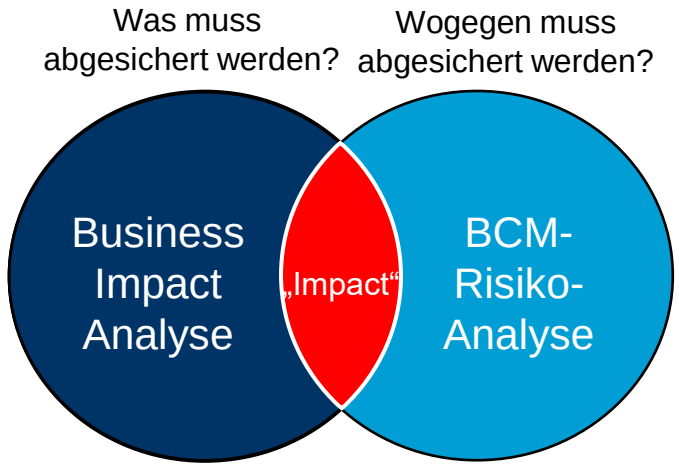
- **Ablauf der Bewältigung von Schadensereignissen**



Quelle: BSI 200-4 Hilfsmittel

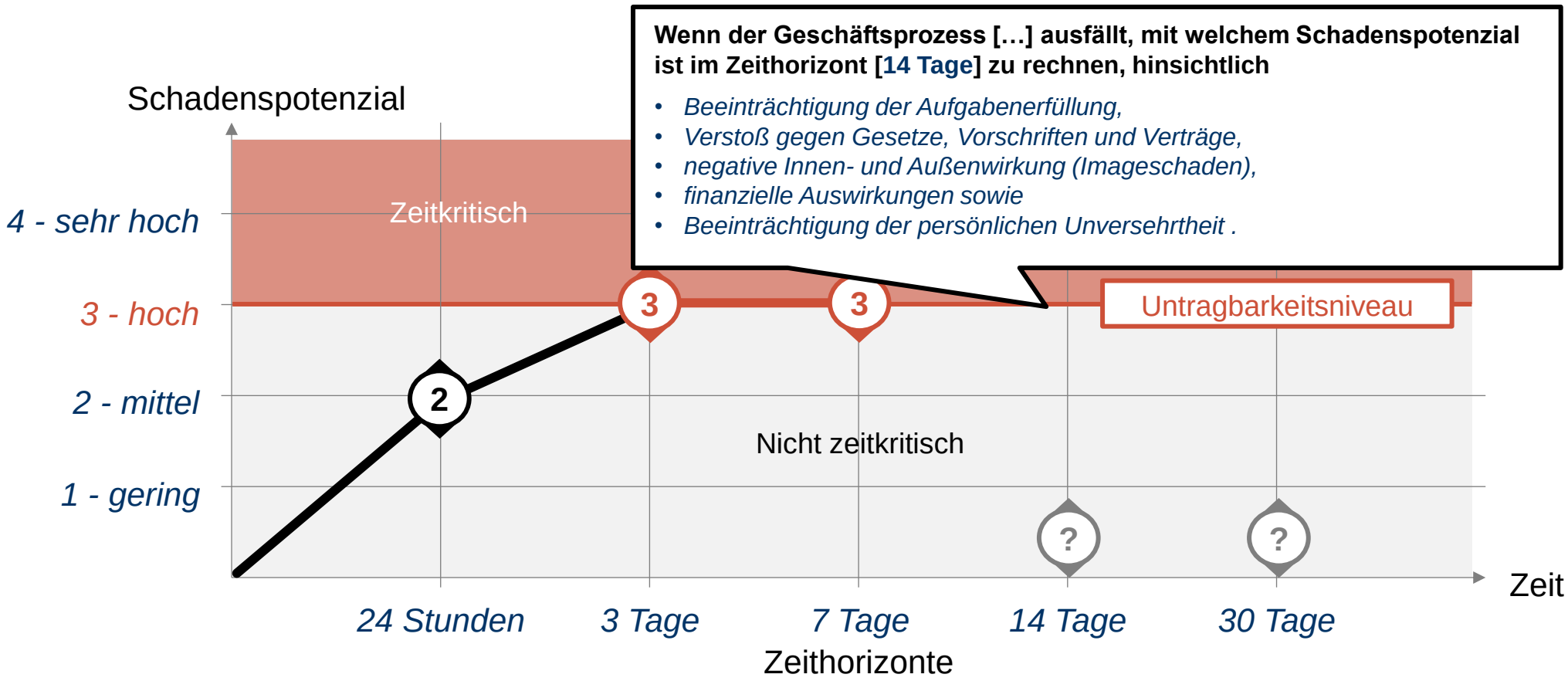
Grundlagen

- **Kernfrage: Sind bei einem Ausfall innerhalb von x Tagen zu hohe Schäden zu erwarten?**
- **Rahmenbedingungen zur Bewertung eines Business Impact**
  - Kritische Zeiträume „innerhalb von x Tagen“
  - Festlegung der Schadensarten / Risiken, z.B.
    - ✓ Beeinträchtigung der Aufgabenerfüllung
    - ✓ Verstoß gegen Gesetze
    - ✓ Imageschäden
    - ✓ Finanzielle Auswirkungen
    - ✓ Personenschäden
  - Festlegung des Schadenspotenzials:
    Wann hat eine Schadensart nicht tolerierbare Auswirkungen?



Quelle: BSI 200-4 Hilfsmittel

Business Impact Analyse



Quelle: BSI 200-4 Hilfsmittel

Business Impact Analyse

Schadens-kategorie	Allgemeine Beschreibung	Beeinträchtigung der Aufgabenerfüllung	Negative Innen- und Außenwirkung (Imageschaden)	Finanzielle Auswirkungen	Verstoß gegen Gesetze, Vorschriften und Verträge	Beeinträchtigung der persönlichen Unversehrtheit
3 - Hoch	*Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen.*	*Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.*	*Eine erhebliche, nachhaltige Ansehens- oder Vertrauens-beeinträchtigung ist intern und extern zu erwarten.*	*Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.*	*Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.*	*Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.*
4 - Sehr hoch	*Allgemeine Beschreibung: Ausfall führt zu existentiell bedrohlichen Auswirkungen.*	*Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden.*	*Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, ist zu erwarten.*	*Der finanzielle Schaden hat existenzbedrohende Ausmaße.*	*Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen.*	*Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.*

Quelle: BSI 200-4 Hilfsmittel

Grundlagen

- **Ergebnis**
  - Prozessliste mit Bewertung der kritischen Geschäftsprozesse
  - Festlegung der maximal tolerierbaren Ausfallzeit (Maximum Tolerable Period of Disruption MTPD)
  - Übersicht über zeitkritische Ressourcen und deren
    - ✓ geforderte Wiederanlaufzeit (Recovery Time Objective RTO)
    - ✓ Aktualität der Datenwiederherstellung (Recovery Point Objective RPO)
  - Übersicht über Prozessabhängigkeiten
  - Übersicht der möglichen “Single Points of Failure”

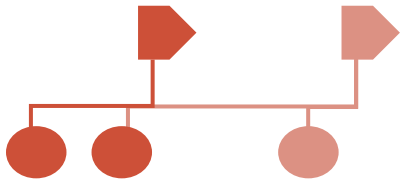
Grundlagen

- **WICHTIG:**
  - Bei der BIA geht es nicht darum, Ressourcen einzusparen oder die Wichtigkeit von Geschäftsprozessen zu diskutieren.
  - Es geht um die Gewährleistung eines Notbetriebs zur Sicherstellung des Überlebens einer Organisation.
  - Die BIA kann keinen vollständigen Überblick über Geschäftsprozesse geben. Sie ist unvollständig, weil sie sich auf kritische Prozesse und Ressourcen fokussiert

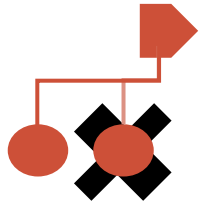
Schritte der BIA

1. Schadensbewertung und Identifikation der zeitkritischen Geschäftsprozesse

2. Identifizierung von Prozessabhängigkeiten



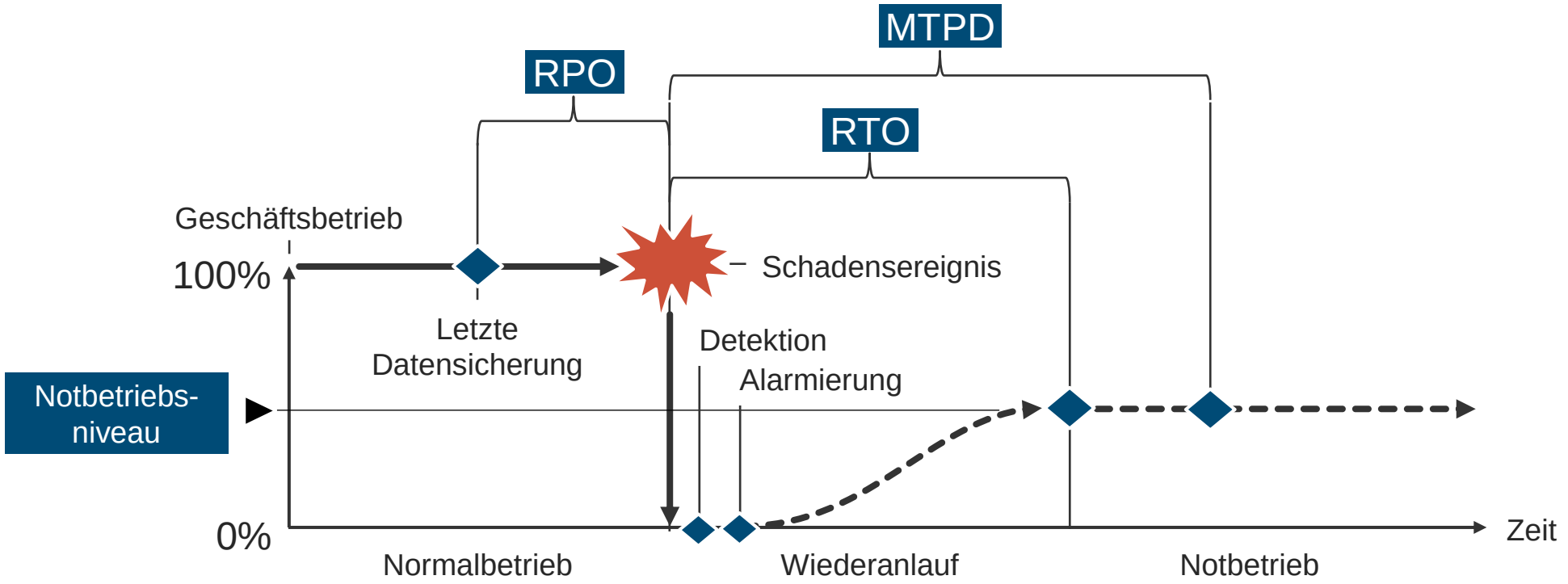
3. Identifizierung von Ressourcenabhängigkeiten



4. Identifizierung vorhandener Single Points of Failure

Quelle: BSI 200-4 Hilfsmittel

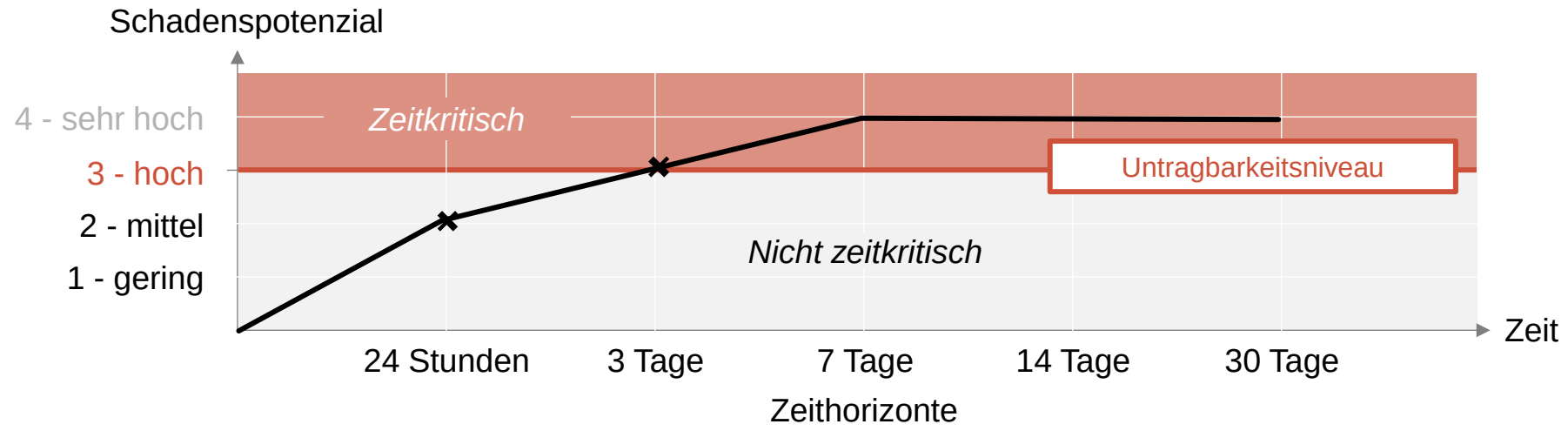
Kenngrößen der BIA



Quelle: BSI 200-4 Hilfsmittel

Ableitung der MTPD

Festgelegtes Untragbarkeitsniveau:



Schadensbewertung:

Geschäftsprozess	24 Std.	3 Tage	7 Tage	14 Tage	30 Tage
Prozess ABC	*2 mittel*	*3 hoch*	*4 - sehr hoch*	*4 - sehr hoch*	*4 - sehr hoch*

Quelle: BSI 200-4 Hilfsmittel

Festlegung des Notbetriebsniveaus

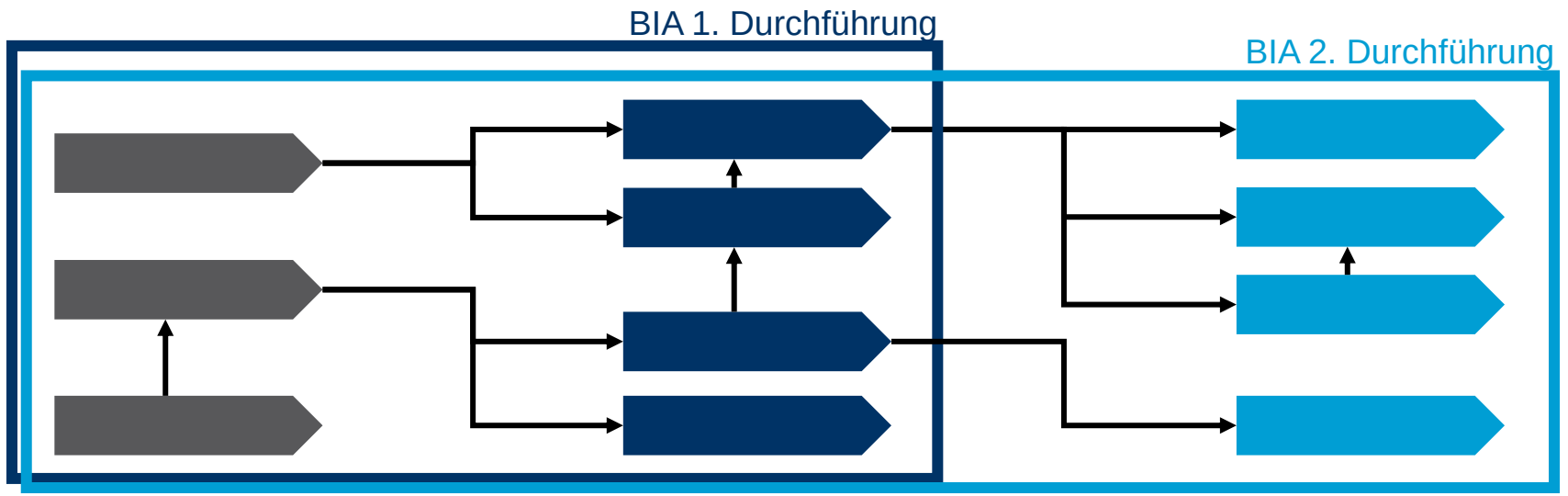
- **Welche Aktivitäten des Geschäftsprozesses müssen innerhalb des Notbetriebs aufrechterhalten werden ?**

Geschäftsprozess	MTPD	Notbetriebsniveau
Incident Management	*3 Tage*	*Der Fokus liegt auf der Bearbeitung von Major Incident-Tickets. Wenn der Notbetrieb nur wenige Tage andauert, können bei 50% Arbeitsvolumen die entstehenden Arbeitsrückstände leicht kompensiert werden. Da mit jedem weiteren Tag auf Notbetriebsniveau jedoch Tickets unbearbeitet bleiben, muss das Notbetriebsniveau schrittweise auf 80% Arbeitsvolumen gesteigert werden.*

Quelle: BSI 200-4 Hilfsmittel

Identifizierung von Prozessabhängigkeiten

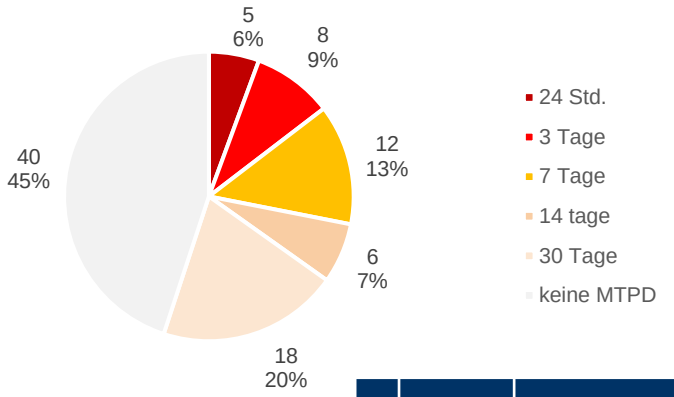
- **Ermittlung, z.B. über „Wechselwirkungen der Prozesse“**



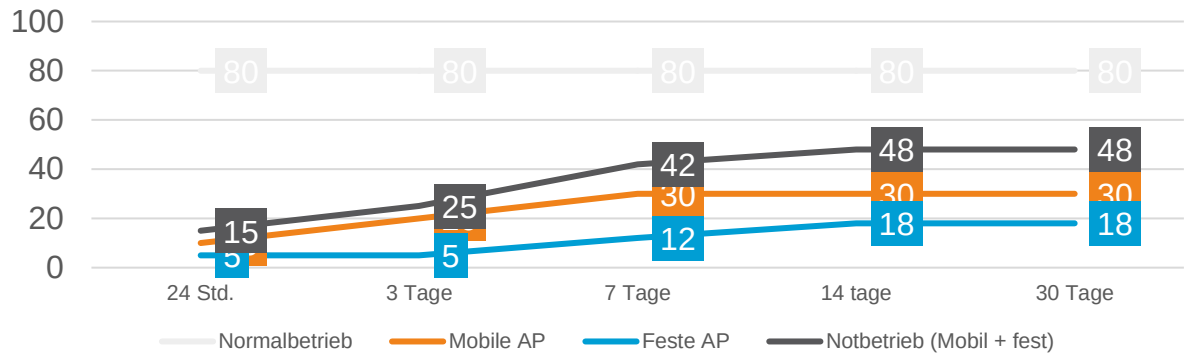
Quelle: BSI 200-4 Hilfsmittel

Auswertung

- **Verteilung der Geschäftsprozesse mit MTPD-Anforderungen**
- **Zeitkritische Geschäftsprozesse**
- **Anzahl der Arbeitsplätze im Normal- und Notbetrieb**



Nr.	Referat	Geschäftsprozess	MTPD
1	*BCM*	*Notfall managen*	24 Std.
2	*IT*	*Incident Management*	24 Std.
3	*IT*	*Berechtigungsmanagement*	24 Std.
4	*IT*	*Sicherstellung IT-Betrieb*	24 Std.
5	*[…]*	*[…]*	[…]
6	*IT*	*Sicherstellung IT-Betrieb*	3 Tage



AP = Arbeitsplätze

Quelle: BSI 200-4 Hilfsmittel

BIA-Auswertungsbogen als Testversion

https://www.bsi.bund.de/dok/200-4-hilfsmittel

Anpassung der „BIA light“

IHK Südlicher Oberrhein

SDCON

Wie kann die „BIA light“ verfeinert werden?

- **Ergänzung der Basistabellen um die Spalten**
  - Auswirkung auf Kontinuität der Geschäftsprozesse als gesonderte Spalte!
    Idealerweise lassen sich alle Inventare Prozessen zuordnen - im Beispiel wurden Inventare bewertet, was zu Bewertungsschwierigkeiten führen kann.
  - Filtern auf Kontinuitätsrelevanz
  - Kennwerte:
    - ✓ Wiederanlauf SOLL = RTO
    - ✓ Ergänzung um „Untragbare Zeit (MTPD)“
  - WICHTIG: hier vereinfachte Bewertung.
    Es müsste jeder Prozess für jeden Zeitraum gesondert bewertet werden
  - Erfüllung SOLL-Vorgabe auf Kontinuitätsrelevanz

Unternehmensbereich	Bezeichnung	Bezug zu BCM-Maßnahme	Auswirkung auf Kontinuität	Schadenauswirkung auf Betrieb	Wiederanlauf SOLL (RTO)	Untragbare Zeit (MTPD)	SOLL-Vorgabe erfüllt? (ja/nein)
Produktion	Absaugeinrichtungen	Betrieb aufrechterhalten	x	mittel	kurz (1 Tag)	3-6 Tage	Ja
Produktion	Abwasser-behandlungsanlage	Business Continuity verbessern	x	sehr hoch	sehr kurz (Stunden)	2 - 4 Std.	Nein
Produktion	Anlagen mit Kühlschmierstoffen	Unfälle vermeiden/abwickeln	x	mittel	kurz (1 Tag)	3-6 Tage	Ja
Produktion	Anlagen zur Beschichtung	Betrieb aufrechterhalten	x	sehr hoch	sehr kurz (Stunden)	2 - 4 Std.	Ja
Produktion	Anlagen zur Lackierung	Betrieb aufrechterhalten	x	gering	mittel (2-3 Tage)	3-6 Tage	Nein
Produktion	Anlagen zur Schmelze	Betrieb aufrechterhalten	x	sehr hoch	sehr kurz (Stunden)	4 - 24 Std.	Ja
Infrastruktur/Gebäude	Aufzüge (Personen- und Lastenaufzüge und Güterbeförderung)	Betrieb aufrechterhalten	x	gering	mittel (2-3 Tage)	3-6 Tage	Ja
Lager	Automatisches Lager	Betrieb aufrechterhalten	x	sehr hoch	sehr kurz (Stunden)	4 - 24 Std.	Nein

- **Auswertung auf**
  - Anzahl der Objekte mit RTO- und MTPD-Relevanz, gruppiert nach Einstufungen
  - Zuordnung von Mitarbeiterzahlen zu Not-/Normalbetrieb hängt von der gewählten Systemaik ab

Ausblick

IHK Südlicher Oberrhein

SDCON

Weitere Online-Briefings außerhalb der IHK-Reihe

- **Risikomanagement**
  - BSI 200-3
  - ISO 31000
- **NIS-2 Richtlinie (Cybersicherheit)**
- **KRITIS (Kritische Infrastrukturen = physische Sicherheit)**
- **TISAX (Trusted Information Security Assessment Exchange)**

Sie möchten über unseren News-Push informiert werden?

Mail an Thomas Schweppe
t.schweppe@sd-con.de