Folien:
Während des Audits

Norm-Textanalyse

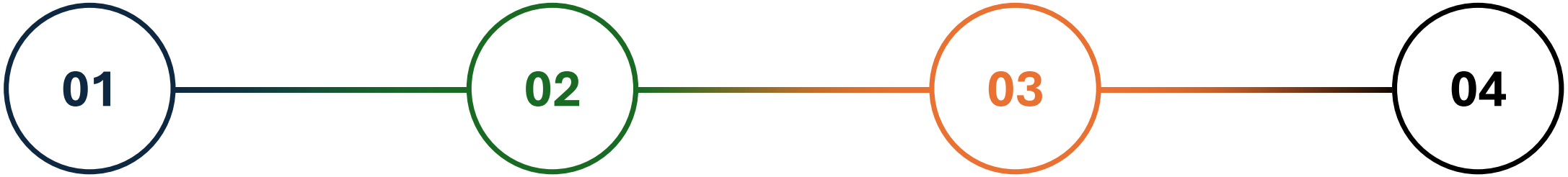
- als Fragetechnik im Prozess- und Systemaudit

Analyse der Anforderungen

- Norm
- Gesetze
- Interne Anforderungen
- Auditergebnisse
- Sicherheits-Umfeld

Auditfragen
Frageliste
Checkliste

Norm - Textanalyse



Textanayse

Abschnitt für Abschnitt vorhandene Anforderungen markieren

Anforderungen

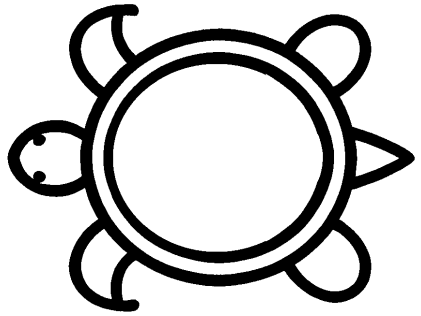
Ableitung von Kernfragen aus den Anforderungen

Vorgabedokumente

Ableitung von Kernfragen aus den Vorgabedokumenten

Auditfrageliste

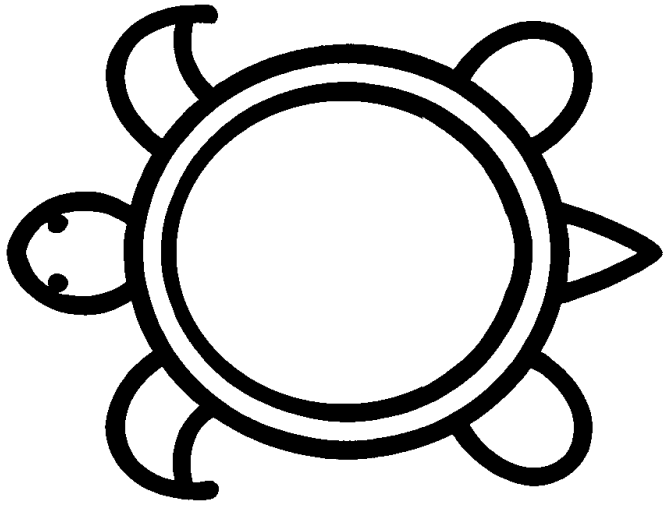
Formulierung von Auditfragen abgestimmt auf Abteilung, Branche, Personal etc.



Turtle-Methode

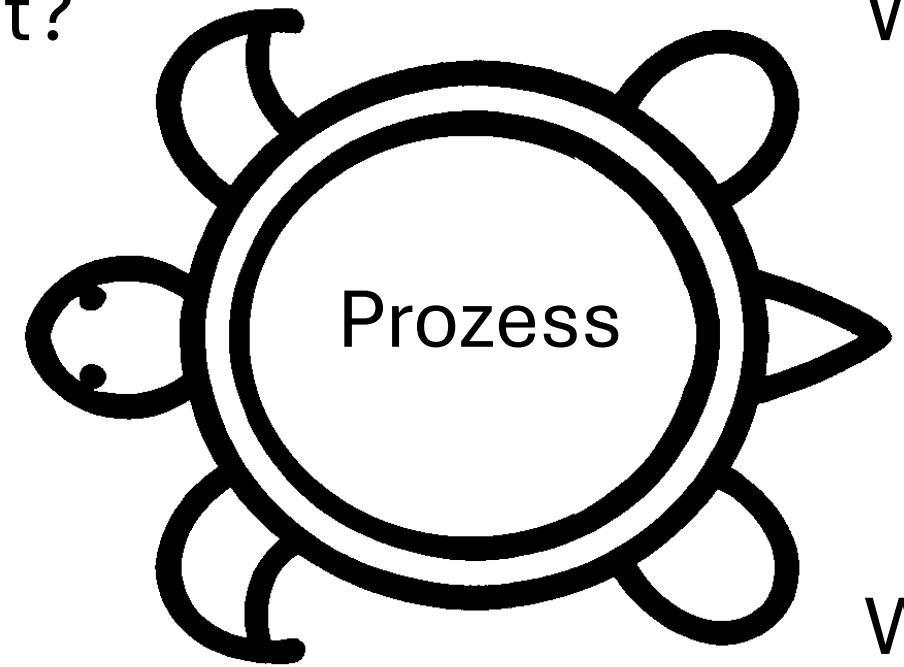
- als Fragetechnik im Prozess- und Systemaudit

Querschnittsfunktionen (Kapitel 6, 7, 9 und 10)

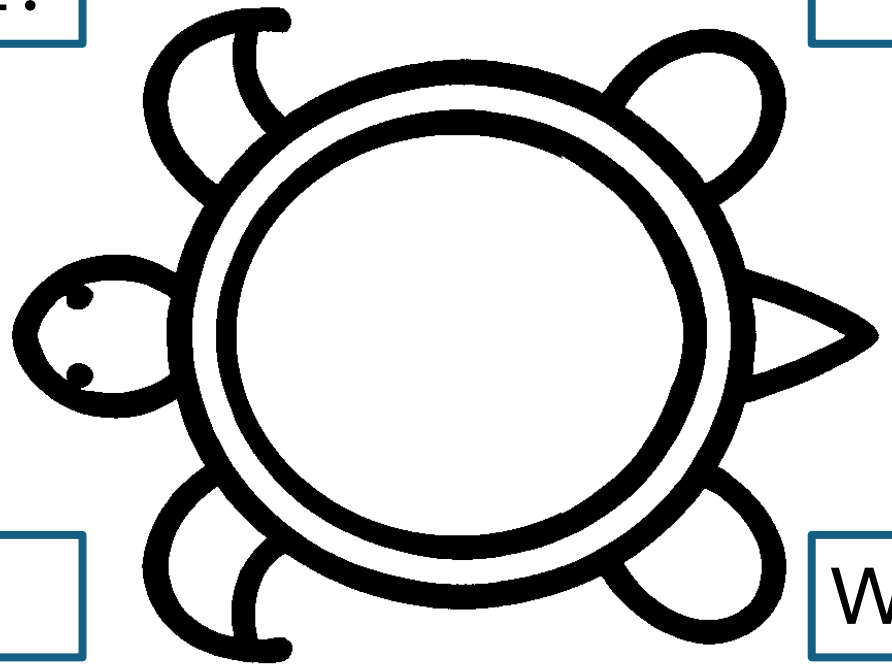


- Dokumentierte Information
- Risikomanagement
- Kommunikation
- Kompetenz und Awareness
- Interne Audits
- Nichtkonformitäten und Korrekturmaßnahmen

Querschnittsfunktionen (Kapitel 6, 7, 9 und 10)



Die 5 Stützfunktionen



Womit?

Wer?

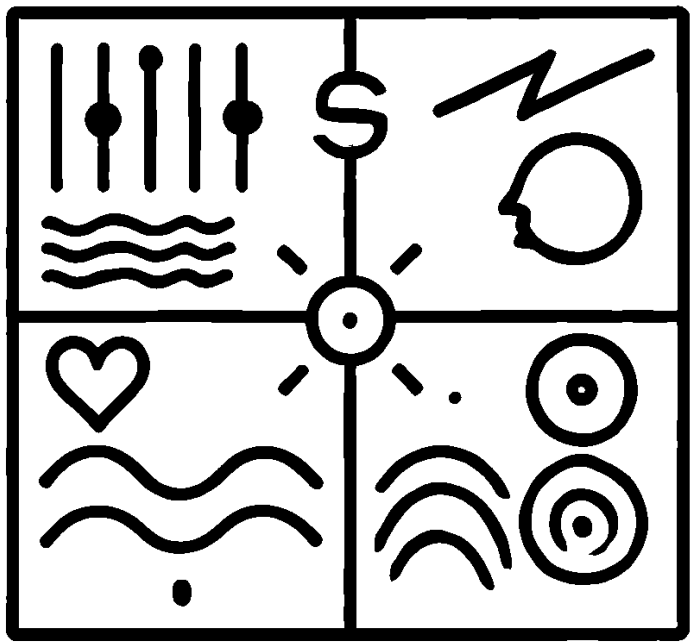
Wie?

Welche Kriterien?

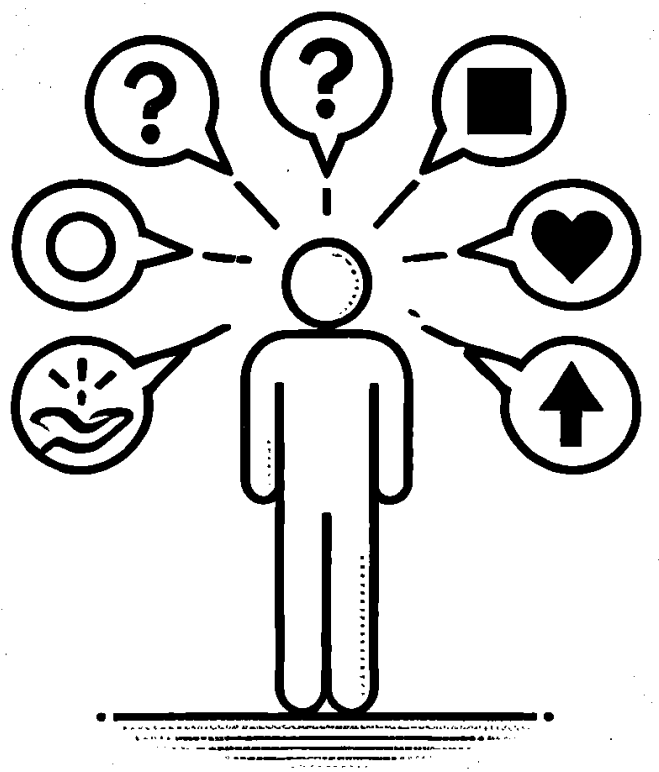
Welche Schnittstellen?

Kommunikation im Audit

- Ebenen der Kommunikatior
  - Sachebene
  - Beziehungsebene
- Arten der Kommunikation
  - Verbal
  - Paraverbal
  - Nonverbal

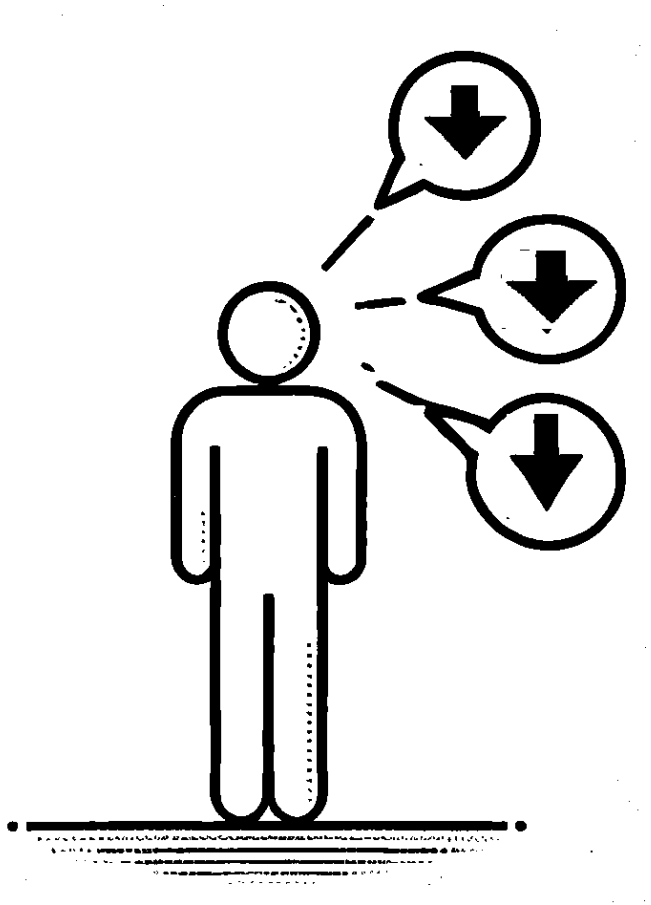


Fragetechniken



- Offene Fragen
- Geschlossene Fragen
- Alternativfragen
- Rhetorische Fragen
- Suggestivfragen

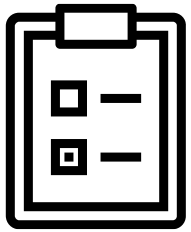
Interviewfragetechnik



- Zielorientiertes Fragen
- Einstiegsfrage
- Schrittweise Vertiefung der Auditfragen
- Freie vertiefende Folgefragen

Folien:
Nach dem Audit

Nach dem Audit



1

Maßnahmenplan

Planung der Behandlung von Nebenabweichungen und Nachaudit bei Hauptabweichungen

2

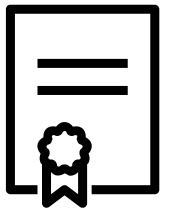
Vetoprüfung

Überprüfung durch eine unabhängige Stelle im Rahmen einer Zertifizierung

3

Auditbericht

Zusammenfassung und Aufbereitung der Ergebnisse im offiziellen Auditbericht

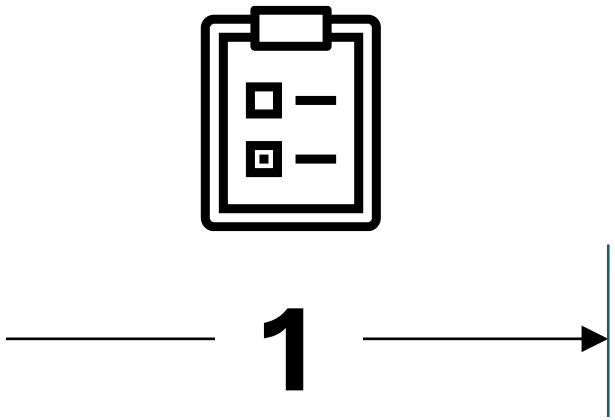


4

Zertifizierung

Ein Zertifizierungszyklus besteht aus Zertifizierungs und Überwachungsaudits

Nachbearbeitung



Maßnahmenplan

Planung der Behandlung von Nebenabweichungen und Nachaudit bei Hauptabweichungen

- Behandlungsplan / Nachaudit
  - Nichtkonformität
  - Ursache
  - Sofortmaßnahme
  - Ursachenbeseitigung
  - Priorität
  - Verantwortlich
  - Frist

Beispiel: Maßnahmenplan

Festgestellte Nichtkonformität	Ursache	Sofortmaßnahme	Ursachenbeseitigung	Priorität	Verantwortlich	Frist	Status
Es gibt keine formelle Richtlinie für den Umgang mit mobilen Endgeräten.	Fehlendes Bewusstsein für die Risiken der mobilen Endgeräte im Unternehmen.	Informelle Mitteilung an die Mitarbeiter, keine sensiblen Daten ohne Schutz auf mobilen Geräten zu speichern.	Entwicklung und Implementierung einer formellen Richtlinie für mobile Endgeräte, Schulung der Mitarbeiter, Einführung technischer Maßnahmen (z. B. Remote-Wipe).	Hoch	IT-Sicherheitsbeauftragter & Personalabteilung	30 Tage	Offen
Fehlende Verschlüsselung von sensiblen Daten auf tragbaren Datenträgern.	Fehlende Vorgabe und fehlende technische Infrastruktur zur Verschlüsselung.	Sofortige Anweisung, keine sensiblen Daten auf tragbaren Datenträgern zu speichern.	Einführung einer Verschlüsselungslösung für alle tragbaren Datenträger und Aktualisierung der ISMS-Dokumentation, stichprobenartige Kontrollen zur Überprüfung der Umsetzung.	Hoch	IT-Abteilung	60 Tage	Offen
Regelmäßige Sicherheitsupdates werden nicht dokumentiert.	Keine etablierten Prozesse für die Dokumentation von Updates.	Sofortige Erstellung eines einfachen Logbuchs, um Updates zu protokollieren.	Entwicklung eines standardisierten Prozesses zur Protokollierung und wöchentliche Überprüfung der Einhaltung.	Mittel	IT-Abteilung	21 Tage	Offen
Mitarbeiter haben keinen Zugang zu regelmäßigen Schulungen über aktuelle Sicherheitsbedrohungen.	Mangel an Weiterbildungsmöglichkeiten und Ressourcen.	Bereitstellung von kurzen, schriftlichen Sicherheitsrichtlinien für alle Mitarbeiter.	Einführung eines jährlichen Schulungsprogramms mit Pilotprojekten und Feedback-Runden zur kontinuierlichen Verbesserung.	Mittel	Personalabteilung	45 Tage	Offen
Physische Sicherheitsmaßnahmen im Serverraum sind unzureichend (fehlende Zutrittskontrollen).	Fehlende Investition in physische Sicherheitsmaßnahmen.	Sofortige Überwachung des Serverraums durch bestehendes Personal.	Installation eines elektronischen Zugangssystems und Einweisung der Mitarbeiter in die neuen Sicherheitsprotokolle.	Hoch	Facility Management	60 Tage	Offen

Festgestellte Nichtkonformität	Ursache	Sofortmaßnahme	Ursachenbeseitigung	Verantwortlich	Frist	Status
Es gibt keine formelle Richtlinie für den Umgang mit mobilen Endgeräten.	Fehlendes Bewusstsein für die Risiken der mobilen Endgeräte im Unternehmen.	Informelle Mitteilung an die Mitarbeiter, keine sensiblen Daten ohne Schutz auf mobilen Geräten zu speichern.	Entwicklung und Implementierung einer formellen Richtlinie für mobile Endgeräte, Schulung der Mitarbeiter, Einführung technischer Maßnahmen (z. B. Remote-Wipe).	IT-Sicherheitsbeauftragter & Personalabteilung	30 Tage	Offen
Fehlende Verschlüsselung von sensiblen Daten auf tragbaren Datenträgern.	Fehlende Vorgabe und fehlende technische Infrastruktur zur Verschlüsselung.	Sofortige Anweisung, keine sensiblen Daten auf tragbaren Datenträgern zu speichern.	Einführung einer Verschlüsselungslösung für alle tragbaren Datenträger und Aktualisierung der ISMS-Dokumentation, stichprobenartige Kontrollen zur Überprüfung der Umsetzung.	IT-Abteilung	14 Tage	Offen
Regelmäßige Sicherheitsupdates werden nicht dokumentiert.	Keine etablierten Prozesse für die Dokumentation von Updates.	Sofortige Erstellung eines einfachen Logbuchs, um Updates zu protokollieren.	Entwicklung eines standardisierten Prozesses zur Protokollierung und wöchentliche Überprüfung der Einhaltung.	IT-Abteilung	21 Tage	Offen
Mitarbeiter haben keinen Zugang zu regelmäßigen Schulungen über aktuelle Sicherheitsbedrohungen.	Mangel an Weiterbildungsmöglichkeiten und Ressourcen.	Bereitstellung von kurzen, schriftlichen Sicherheitsrichtlinien für alle Mitarbeiter.	Einführung eines jährlichen Schulungsprogramms mit Pilotprojekten und Feedback-Runden zur kontinuierlichen Verbesserung.	Personalabteilung	45 Tage	Offen
Physische Sicherheitsmaßnahmen im Serverraum sind unzureichend (fehlende Zutrittskontrollen).	Fehlende Investition in physische Sicherheitsmaßnahmen.	Sofortige Überwachung des Serverraums durch bestehendes Personal.	Installation eines elektronischen Zugangssystems und Einweisung der Mitarbeiter in die neuen Sicherheitsprotokolle.	Facility Management	60 Tage	Offen

Überprüfung

2

Vetoprüfung

Überprüfung durch eine unabhängige Stelle im Rahmen einer Zertifizierung

- Qualitätskontrollprozess der Zertifizierungsstelle
- Anforderungen der ISO 17021
- Zweck der zusätzlichen Prüfung
- Struktur und Ablauf
- Mögliche Rückweisungen
- Bedeutung und Freigabe

Dokumentation

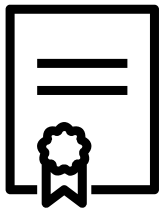
3

Auditbericht

Zusammenfassung und Aufbereitung der Ergebnisse im offiziellen Auditbericht

- Dokumentation der Auditergebnisse
- Grundlage für Zertifizierungsentscheidungen
- Geltungsbereich und Ziele
- Festgestellte Stärken und Schwächen
- Empfehlung zur Zertifikatserteilung
- Anhänge

Nachweisdokument: Zertifikat



4

Zertifizierung

Ein Zertifizierungszyklus besteht aus Zertifizierungs und Überwachungsaudits

- Zertifikatserteilung
- Zertifizierungszyklus
- Zertifikatsinhalt
- Zertifikatsübergabe
- certipedia.com