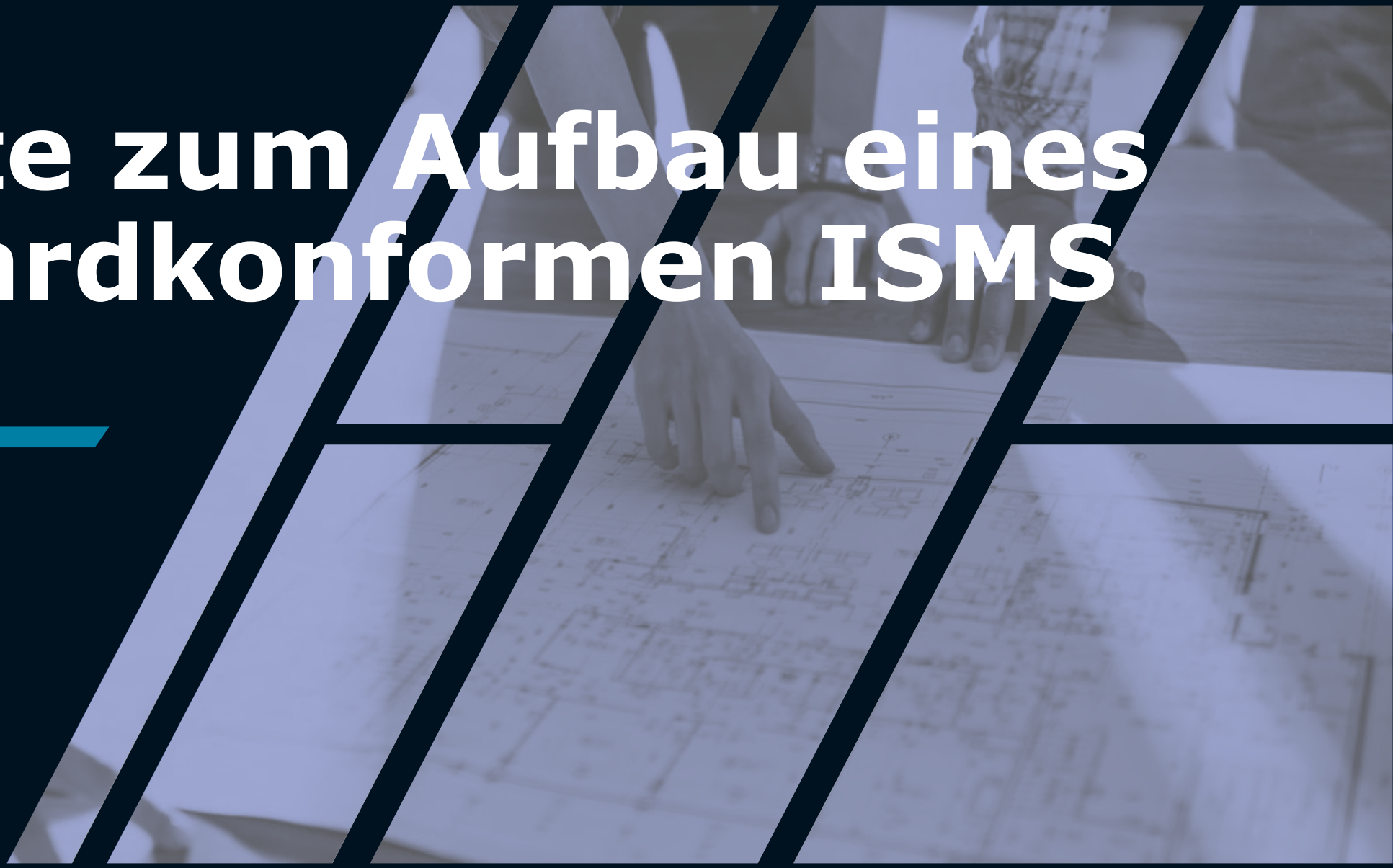
Schritte zum Aufbau eines Standardkonformen ISMS



Stean

25.09.2020

Agenda

- Kurzeinführung ISMS
- Im Vorfeld
- PDCA-Zyklus
- Kritische Erfolgsfaktoren

Kurzeinführung ISMS

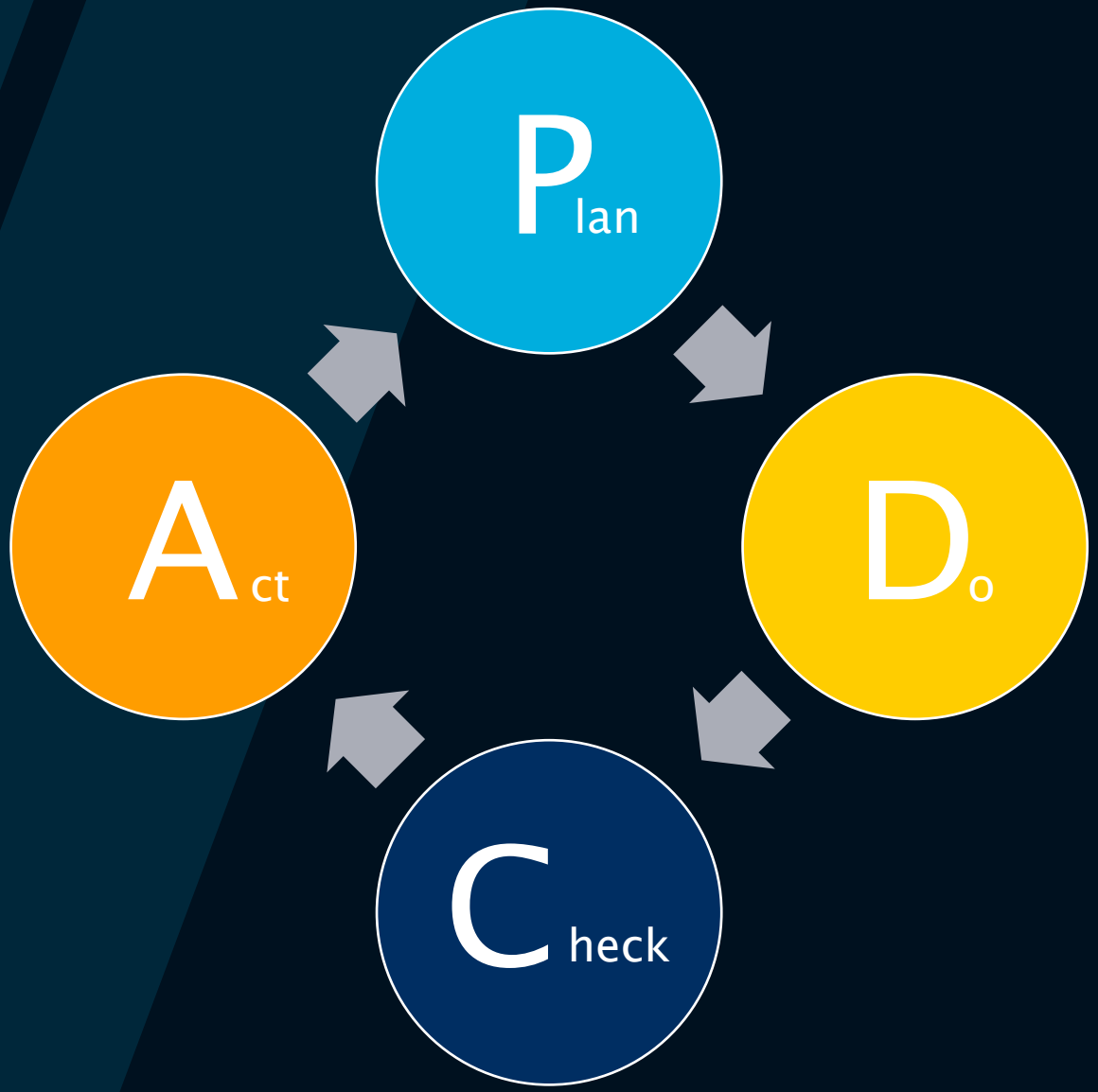
- Regelwerk, das dazu dient, alle Assets einer Organisation mit Hilfe von IT-Sicherheitsmaßnahmen angemessen zu schützen

- Ziele:
  - Compliance
  - Zertifizierungen
  - Identifikation & Behandlung bestehender Risiken

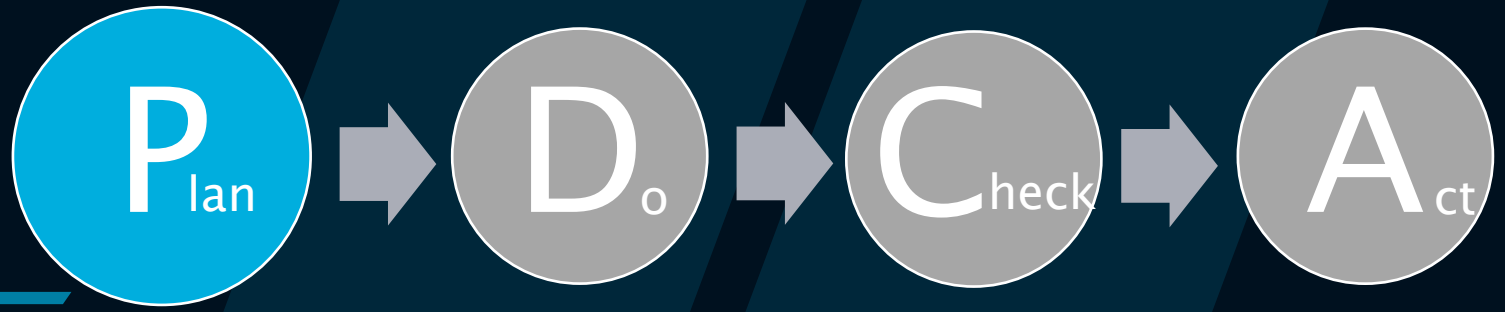
Im Vorfeld

0. Wahl eines geeigneten Sicherheitsmanagementstandards
1. Rechtzeitige Information
2. Aufklärung aller MA

PDCA-Zyklus



Plan-Phase



Was soll das ISMS leisten und welche Werte/Informationen sind zu schützen?

Tasks

- Definition des Anwendungsbereiches
- Asset-Management (Bestandsaufnahme)
- Risikoanalyse
- Business Impact Analyse (BIA)

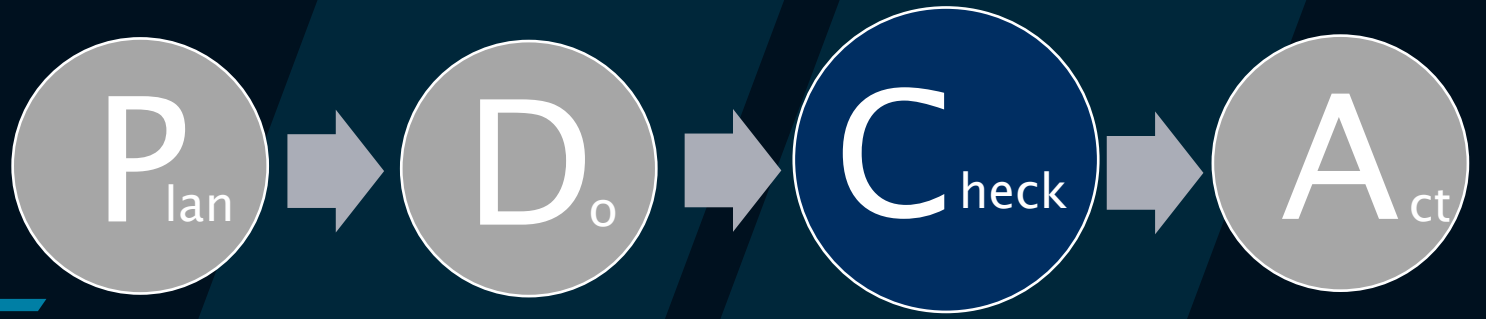
Do-Phase

Ziele, Maßnahmen und Prozesse werden getestet, umgesetzt und eingeführt

Tasks

- Maßnahmen werden erstmal nur im kleinen Rahmen getestet
- Kommunikation des Umsetzungsplans an alle Beteiligten
- Zuweisung von Budget
- MA-Awareness

Check-Phase

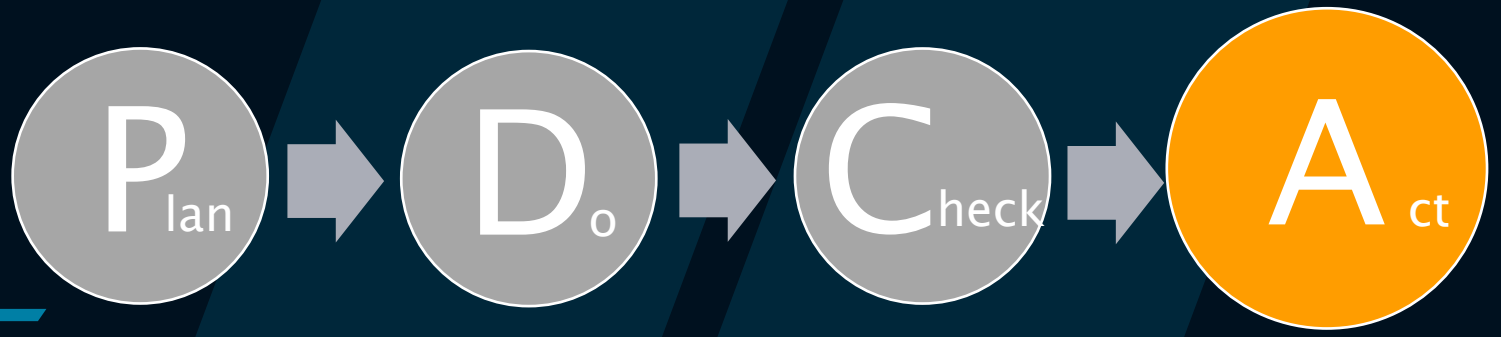


Überwachung, Analyse, Kontrolle und Bewertung der neu eingeführten Maßnahmen und Prozesse

Tasks

- Ehrliche Analyse der gewonnenen Ergebnisse
  - Bei nicht-Übereinstimmung mit Planung -> Gegensteuern
- Beurteilung der aktuellen Gefahrenlage
- Präsentation der Ergebnisse vor Geschäftsführung
- Dokumentation aller Entscheidungen!

Act-Phase



Optimierung, ggf. Mängelbeseitigung und anschließende Einführung auf allen Unternehmensebenen

Tasks

- Dokumentation aller Umsetzungsschritte
- Erklärung zum verbindlichen Unternehmensstandard
- Zusätzliche Kontrollen, ob sich auch alle an die neuen Vorgaben halten

Kritische Erfolgsfaktoren

- Management-Unterstützung
  - Bereitstellung ausreichender Ressourcen
  - Bewusstsein, was geschützt werden soll
- Frühe Einbeziehung aller Beteiligten
- Angemessene Kommunikation
- Priorisierung notwendig
- Umsetzung muss gemessen und geprüft werden

Fragen?

Quellen

- https://www.scope-and-focus.com/informationssicherheit/isms/
- https://www.tuv.com/germany/de/isms-aufbau-gem%C3%A4%C3%9F-iso-27001.html
- Informationssicherheits-Management – Christoph Wegener · Thomas Milde · Wilhelm Dolle
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_9_Aufrechterhaltung/Lektion_9_node.html
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_9_Aufrechterhaltung/Lektion_9_02/Lektion_9_02_node.html%20
- https://karrierebibel.de/pdca-zyklus/
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/3_BusinessImpactAnalysieren/BIA_node.html
- https://www.projektmagazin.de/glossarterm/risikoanalyse