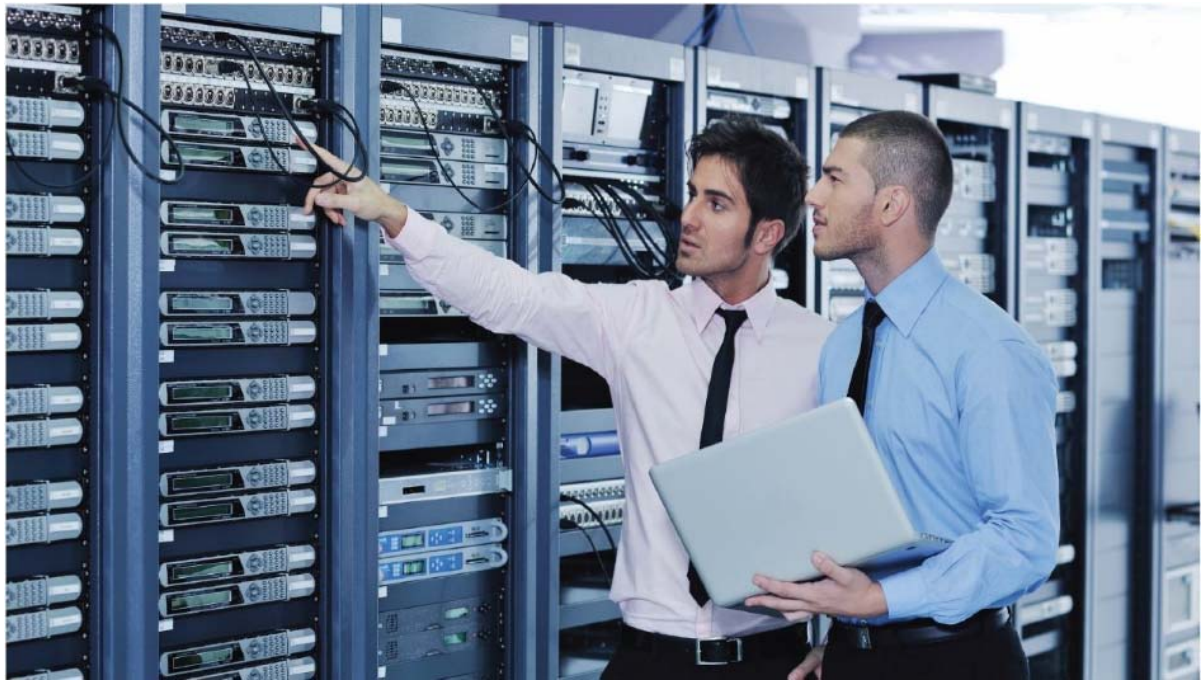
OCG CERTIFICATION
ISO/IEC 27001

ISO/IEC 27001 im Überblick - das Angebot der OCG

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

Akkreditierung Austria
0948
ISO/IEC 17021-1



OCG – der gemeinnützige Verein

Vereinszweck

- umfassende und interdisziplinäre Förderung der Informatik und der Kommunikationstechnologie unter Berücksichtigung ihrer Wechselwirkungen mit Mensch und Gesellschaft.

Arbeitskreise

- IT-Sicherheit
- Forum Privacy

Zertifizierungsstelle f. Managementsysteme (nach ISO/IEC 17021_1)

- Akkreditiert seit Mitte 2013
- Informationssicherheitsmanagementsysteme (ISMS) lt. ISO/IEC 27001:2013
- Derzeit nur ISMS im akkreditierten Scope
- Mögliche kommende Erweiterungen: andere Managementsysteme (z.B. DSMS) oder Personenzertifizierungen nach ISO/IEC 17024

ISO/IEC 27001

ISMS Norm

- (Risikobasiertes) Management Tool um IS-Risiken zu verwalten/behandlen (eine Managementsystem-Norm und keine technische Norm!)
- Strukturierter Ansatz bzw. Herangehensweise
  - Normenpunkte 4-10
  - Normativer Annex A mit 114 Kontrollen in 14 Abschnitten (A5-A18)
- Ständiger Verbesserungsprozess wird institutionalisiert um Herausforderungen sich ändernder Bedrohungen gerecht zu werden (Kapitel 10)
- Rahmen für Audits und Zertifizierung eines ISMS durch Dritte
  - ISMS eingeführt
  - adäquat für Branche, Größe, Stand der Technik und gegenüber Kunden und Shareholdern
  - Beweis dass Governance und Risk Management effektiv sind
  - ISMS im täglichen Betrieb gelebt wird und ständig verbessert (PDCA-Zyklus)

Managementsystemnormen und die ISO/IEC 27000er Gruppe

Managementsysteme

Entsprechen inzwischen alle der HLS nach AnnexSL der ISO (Kapitel 4-10 + Annexe)

- ISO/IEC 9001 (QSMS)
- ISO/IEC 14000 (Umwelt)
- ISO/IEC 20000 (Service Management)
- ISO/IEC 27000 (Informationssicherheit)
- Datenschutzmanagementsysteme (DSMS dz. noch keine ISO-Norm)

Trend zu integrierten Managementsystemen!

ISO/IEC 27000er Gruppe

- 27000 Begriffsdefinitionen
- 27001 Anforderungen an ISMS
- 27002 Umsetzungsrichtlinien (früher ISO 17799 bzw. BS 7799-1)
- 27009 Anforderungen an Sektor spezifische IS-Normen
- 27011 Telekommunikationssektor
- 27015 Finanzsektor
- 27017 Cloud Services
- 27018 Personenbezogene Daten in Cloud
- TR 27019 Energiesektor
- 27799 Gesundheitssektor
- Im Entstehen: 27552

AuditorInnen und Beratung

Objektivität und Unabhängigkeit

- Zertifizierungsstelle darf nicht beraten oder einzelne BeraterInnen oder Beratungsdienstleistungsunternehmen empfehlen!
- Keine engen finanziellen oder personellen Verbindungen zum Kunden
- Präaudits (Feststellung der Zertifizierungsreife/Gap-Analyse) sind erlaubt
- AuditorInnen müssen
  - Kompetenzen und Audit-Erfahrung haben
  - Keine Beratungsleistungen in den letzten 3 Jahren
  - Keine persönlichen Verbindungen
- Überwachung durch Unabhängigkeitskomitee
- Jährliche Officeaudits durch die Akkreditierungsstelle (Akkreditierung Austria im BMDW)

Scope und Auditaufwand

Systemgrenzen des ISMS (Kap. 4.3)

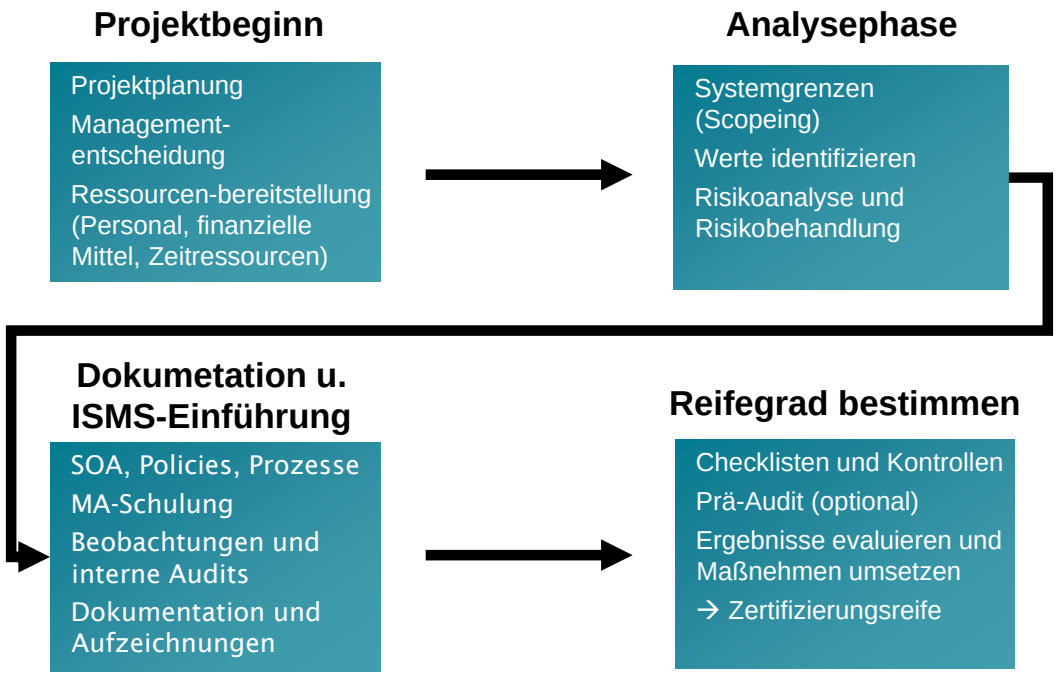
- Gesamtes Unternehmen oder nur abgegrenzter Teilbereich (für DSGVO nicht zu empfehlen)
- Auditaufwand im Zertifizierungszyklus (über 3 Jahre)
  - Vor allem: Zahl der MitarbeiterInnen im Unternehmen (bzw. innerhalb des Scopes)
  - Branche, Komplexität, Standorte

Folgende Tabelle ergibt eine Richtzeit für die Ermittlung des Auditaufwands:

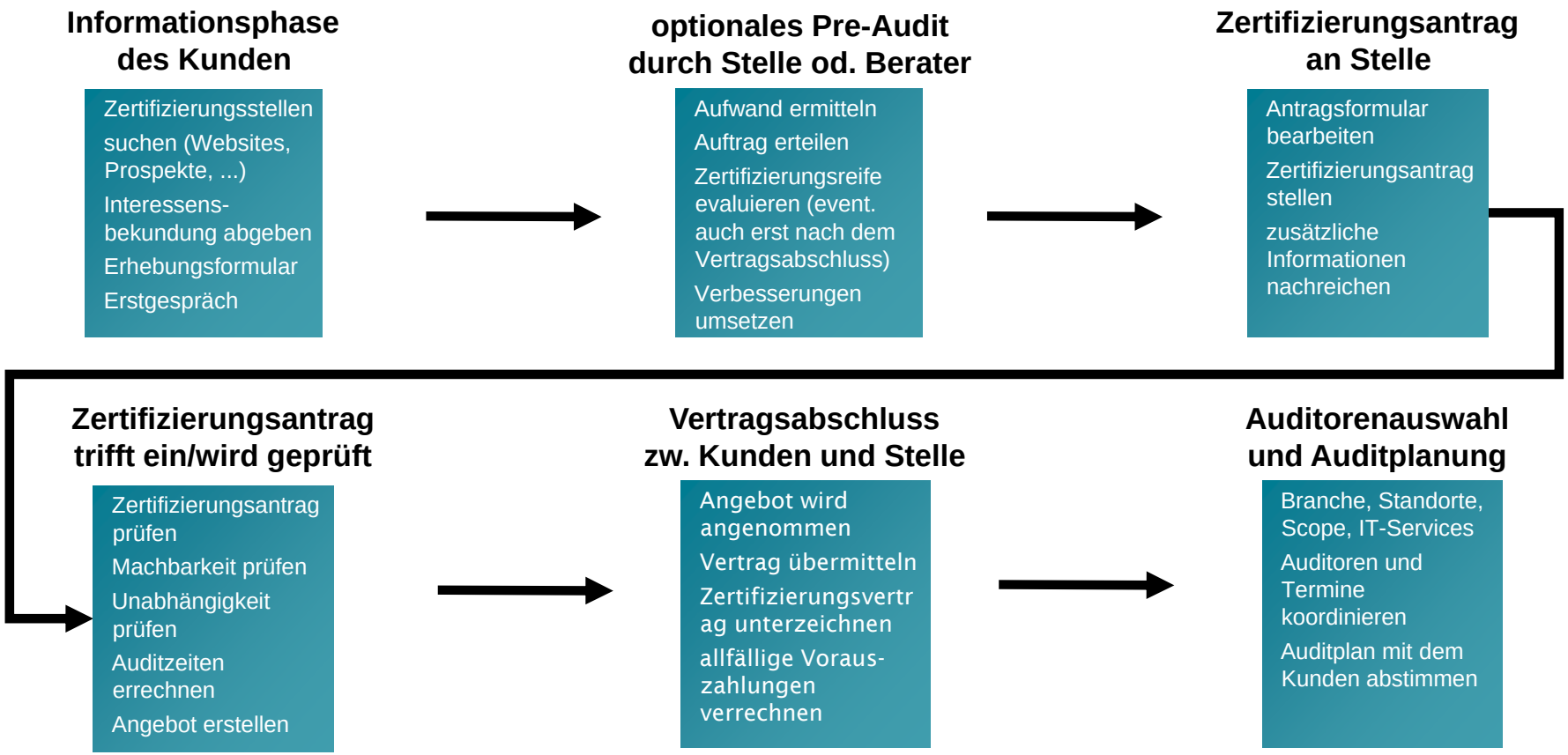
Mitarbeiterzahl innerhalb des Scopes	Audit-Aufwand für Zertifizierungsaudit (Rezertifizierungsaudit ca. -33%)	Auditor-Aufwand für Überwachungsaudit
1-10	5 Tage	1,5 Tage
11-25	7 Tage	2 Tage
26-45	8,5 Tage	3 Tage
46-65	10 Tage	3,5 Tage
66-85	11 Tage	4 Tage
86-125	12 Tage	4 Tage

Zertifizierungsprojekte

Üblicher Ablauf eines Zertifizierungsprojektes

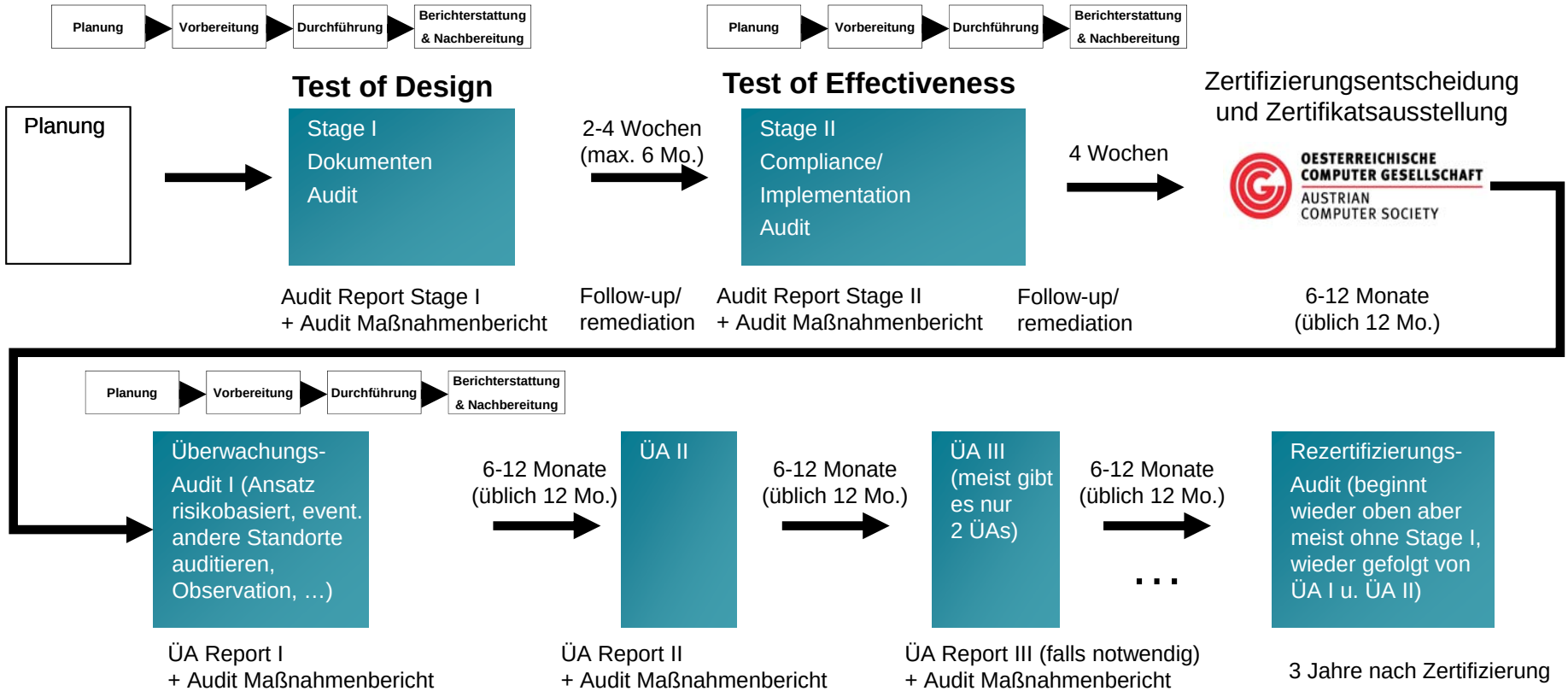


Prozesse vor dem Auditbeginn



Überblick Zertifizierungszyklus

ISO 27001-Zertifizierung im Überblick (über 3 Jahre)



Exkurs DSGVO und Datenschutz

mögliche (bestehende) Erweiterungen Datenschutzaspekte

- ISO/IEC 27001:2013
  - Allgemeiner Pkt. A18 Compliance
    - insbes. A 18.1.4 (Privatsphäre und Schutz von personenbezogener Information)
- Branchenerweiterungen nach ISO/IEC 27009:
  - ISO/IEC 27018 (zum Schutz von personenbezogener Daten in Cloud)
  - ISO/IEC 27017 für den Betrieb von Cloud Services
- Britische Norm BS 10012:2017 (DSMS-Norm, berücksichtigt schon DSGVO, aber BREXIT!!)
- ISO/IEC 29151 (Umsetzungsrichtlinien f. personenbezogene Daten)

Ausblick DS-Zertifizierungen

Kommende nationale/internationale Normen u. Zertifizierungen

- NEUE Arbeitsgruppe bei Austrian Standards: ASI AG 001-18 (Datenschutz)
  - Normprojekt für ÖNORM zu DSMS lt. DSGVO (HLS lt. AnnexSL für Kombiaudits)
  - Anforderungen an DS-Beauftragte (Grundlage für Presonenzertifizierung)
- Branchenerweiterung ISO/IEC 27552 (2.Draft): ist Branchenerweiterung lt. ISO/IEC 27009 und referenziert auf die ISO/IEC 27002 und ISO/IEC 27001
- Mögliche Normen/Zertifizierungen lt. Art. 42 DSGVO
  - datenschutzspezifische Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen (Berücksichtigung KMUs) um Konformität mit der DSGVO zu bestätigen
  - Eventuell Europäischen Datenschutzsiegel (Art. 42 Abs.6)
  - Akkreditierungsstelle für Zertifizierungsstellen ist in Österreich die Datenschutzbehörde (nicht wie bei Managementsystemen die Akkreditierung Austria)!

Kontakt

Wolfgang Resch
Österreichische Computer Gesellschaft (OCG)
Wollzeile 1, 1010 Wien

T: +43 1 5120235 13
M: +43 664 886 74 866
resch@ocg.at
www.ocg.at bzw. www.ocgcert.com