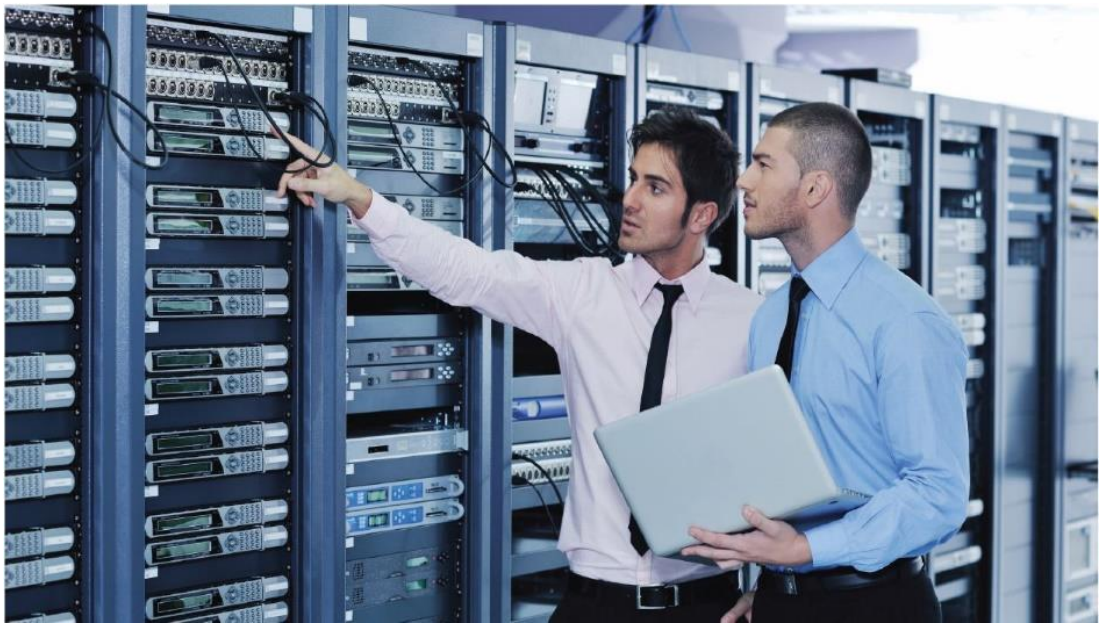
ISO/IEC 27001 Zertifizierung

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

Akkreditierung Austria
A
0948
ISO/IEC 17021-1



Über die

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

OCG CERTIFICATION ISO/IEC 27001

Gemeinnütziger Verein zur Förderung der IT in Österreich
(Slogan: IT-Kompetenzen fördern und zertifizieren!)

- OCG-Gründung: 1975 (u.a. Prof. Zemanek)
- Arbeitskreis IT-Sicherheit: seit 1993
- weitere Aks z.B.: IT-Governance, Forum Privacy, Forum e|Government, Forum eBusiness
- Veranstaltungen: OCG Horizonte, OCG Impulse, Talk am Campus, IT-Konferenzen und Workshops
- Personenzertifizierungen: ECDL (seit 1997 >600.000 Teilnehmer) seit 2012 neues Modul ECDL IT-Security
- dz. ca. 20 MA

OCG MS-Zertifizierungsstelle

Akkreditierung nach ISO/IEC 17021-1:2015 und ISO/IEC 27006:2015 als Zertifizierungsstelle für ISO/IEC 27001 Managementsystem-Zertifizierungen:

- Erster Akkreditierungsbescheid des BMWFJ: 5.7.2013
- aktuelles Zertifikat v. 10.7.2017

- Zertifizierungszeichen:

OCG CERTIFICATION
ISO/IEC 27001

Akkreditierung Austria
A
0948
ISO/IEC 17021-1

Objektivität und Unparteilichkeit

Das Unabhängigkeitskomitee

Die OCG verpflichtet sich als Zertifizierungsstelle der Objektivität und Unparteilichkeit. Zu diesem Zweck wurde das Unabhängigkeitskomitee eingerichtet, das sich mit folgenden Themen befasst:

- Bewertung der Unabhängigkeit von möglichen Kunden der OCG vor der Angebotserstellung und auch der Abläufe innerhalb der Zertifizierungsstelle
- Bewertung der Unabhängigkeit aller im Zertifizierungsprozess involvierter Personen (vor allem Auditoren)
- Behandlung von Beschwerden Dritter über Kunden oder die Zertifizierungsstelle selbst
- Einsprüche von Kunden gegen Entscheidungen des Zertifizierungskomitees

ISO/IEC 27001

Eine etablierte ISMS Norm

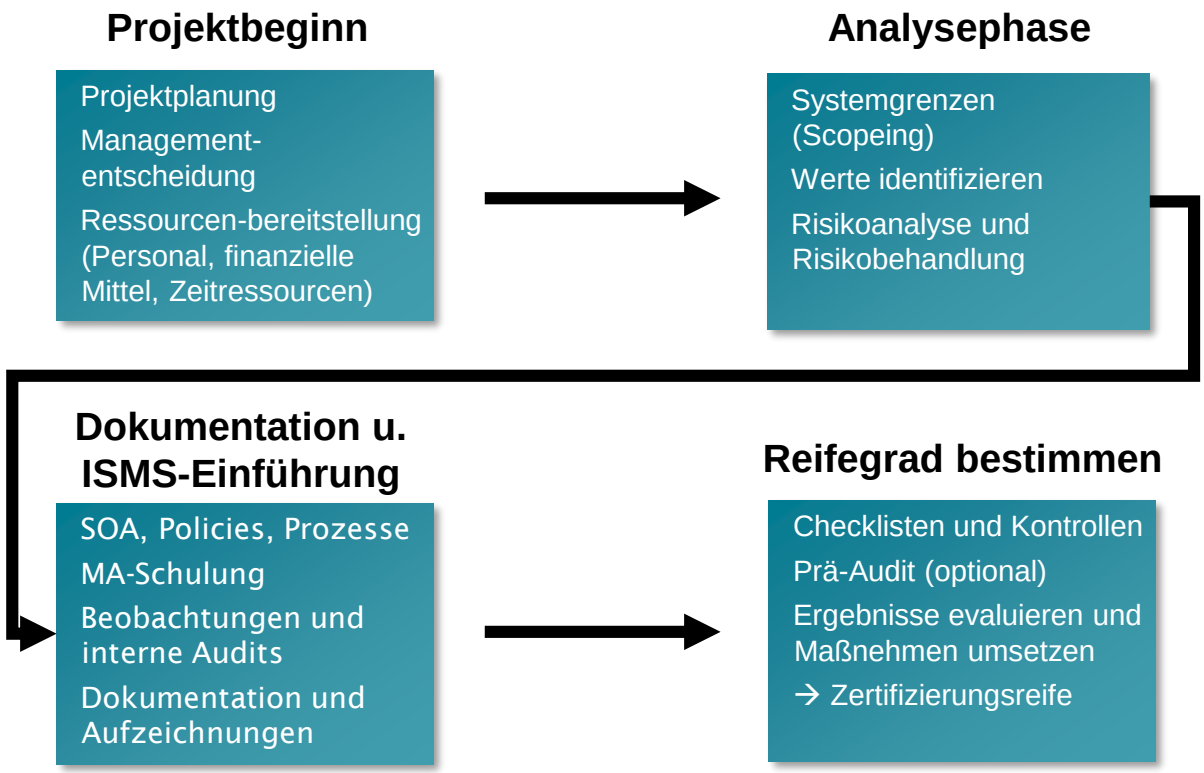
- (Risikobasiertes) Management Tool um IS-Risiken zu verwalten/behandeln (das ist eine Managementsystem-Norm und keine rein technische Norm!)
- Strukturierter Ansatz bzw. Herangehensweise
- Ständiger Verbesserungsprozess institutionalisiert um Herausforderungen sich ändernder Bedrohungen gerecht zu werden
- 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

Aktuelle Version 27001:2013

- Harmonisierung mit Anhang SL der ISO/IEC Direktiven (Vergleichbarkeit von Managementnormen durch die selbe high-level Struktur)
- Begriffsdefinitionen → ISO/IEC 27000
- Anpassungen an neue technische Entwicklungen: 6.1 Maßnahmen zum Umgang mit Risiken und Chancen
- Pkt. 4-10 in der Norm
- Annex A: bleibt normativ (Abschnitte A5-A18)
- 114 Kontrollen
- Kapitel 10: Nichtkonformitäten und Korrekturmaßnahmen bzw. Fortlaufende Verbesserung

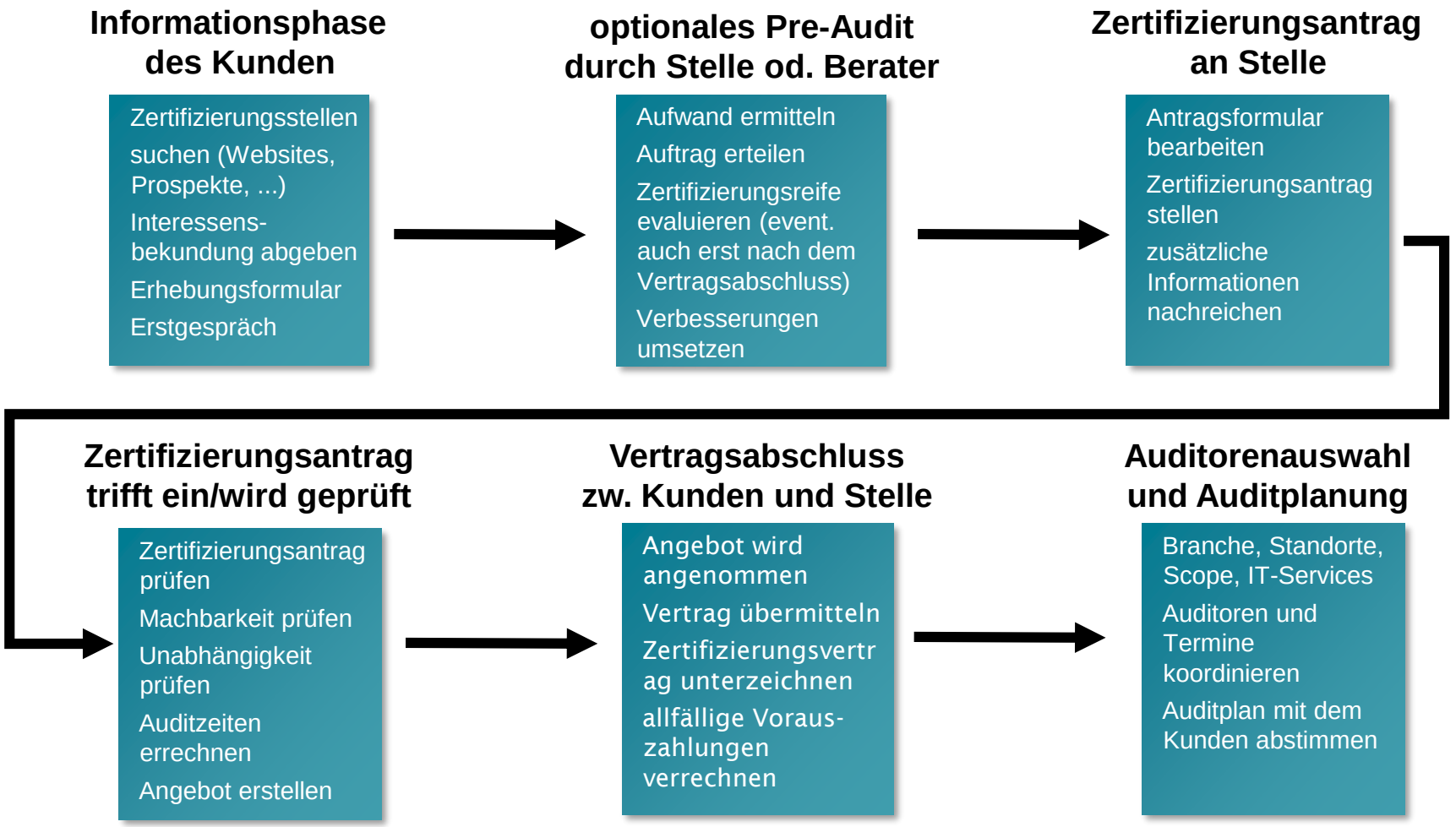
Zertifizierungsprojekte

Üblicher/möglicher Ablauf eines Zertifizierungsprojektes bei Kunden:



Prozesse vor dem Audit

Formale Prozesse zw. Kunden und Zertifizierungsstelle vor dem 1. Audit:



Scope und Auditaufwand

Systemgrenzen des ISMS (Kap. 4.3)

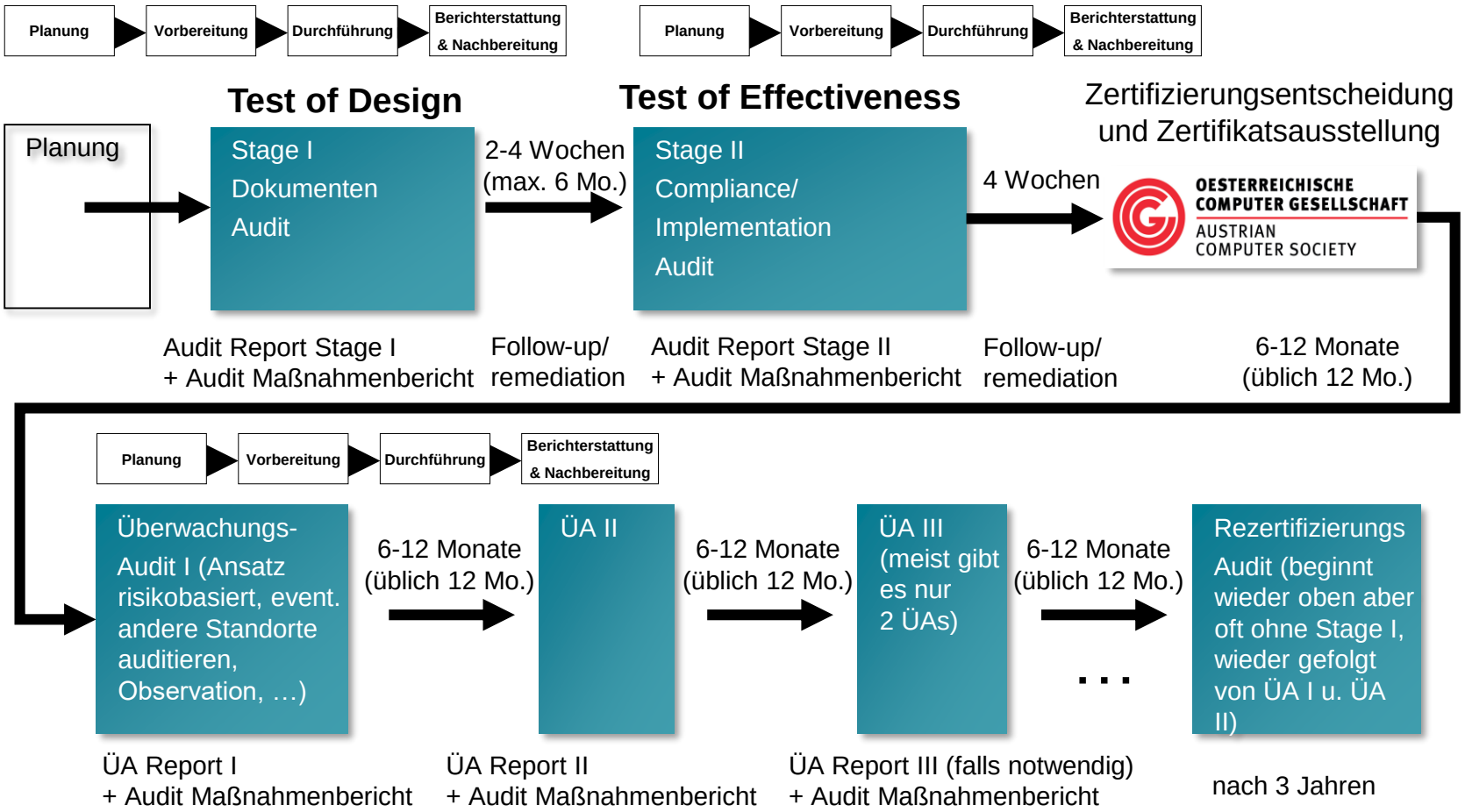
- Gesamtes Unternehmen?
- Auditaufwand im Zertifizierungszyklus (über 3 Jahre)
  - Zahl der Personen im Unternehmen
  - Erhöhende/reduzierende Faktoren
  - Audittage Stage1 Audit
  - Stage 2
  - Ü1 bzw. Ü2
  - Danach: Rezertifizierungsangebot für nächsten 3 Jahre (stage1 entfällt, Rezert ca. 66% des Erstaudits)

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

Überblick Zertifizierungszyklus

Der Zertifizierungszyklus im Überblick (über 3 Jahre)



Auditphase und Reporting

Die Zertifizierungsstelle entsendet Auditoren und ggf. zusätzliche Experten und Übersetzer/Dolmetscher um beim Kunden vor Ort die Wirksamkeit des ISMS sicherzustellen.

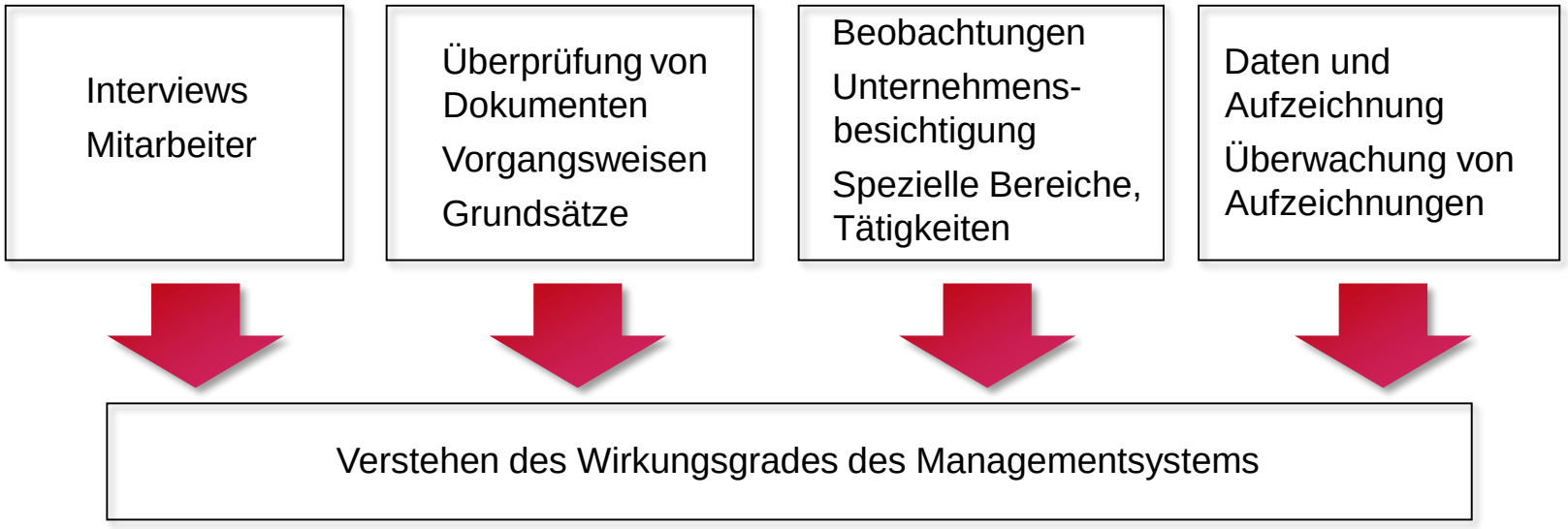
- Dokumentenaudit (bei Rezertifizierung verkürzt)
  - Dokumentation des ISMS prüfen
  - Umfang/Standorte/Systeme kennenlernen
  - Vollständigkeit und Compliace
  - Auditbericht
  - Planung Umsetzungsaudit
- Umsetzungsaudit
  - Überprüfung der Umsetzung vor Ort
  - Abweichungen dokumentieren
  - Maßnahmen und Termine abnehmen
  - Auditbericht verfassen
  - Empfehlung zur Zertifizierung
- Überwachungsaudit (fallweise auch außerplanmäßige Audits aus besonderen Anlass)
  - Überprüfung von Observations und Feststellungen früherer Audits sowie Überwachung des zertifizierten ISMS
  - Auditbericht
  - Maßnahmenumsetzungen gemäß vereinbarter Fristen überprüfen

Methodik

2-teiliges Audit:

- Stage 1: Dokumentenaudit (Test of Design)
- Stage 2: Implementierungsaudit - Interviews und Besichtigung (Test of Effectiveness)

Ergebnisse aus Stage 1 Audit als Basis f. Auditplanung Stage II

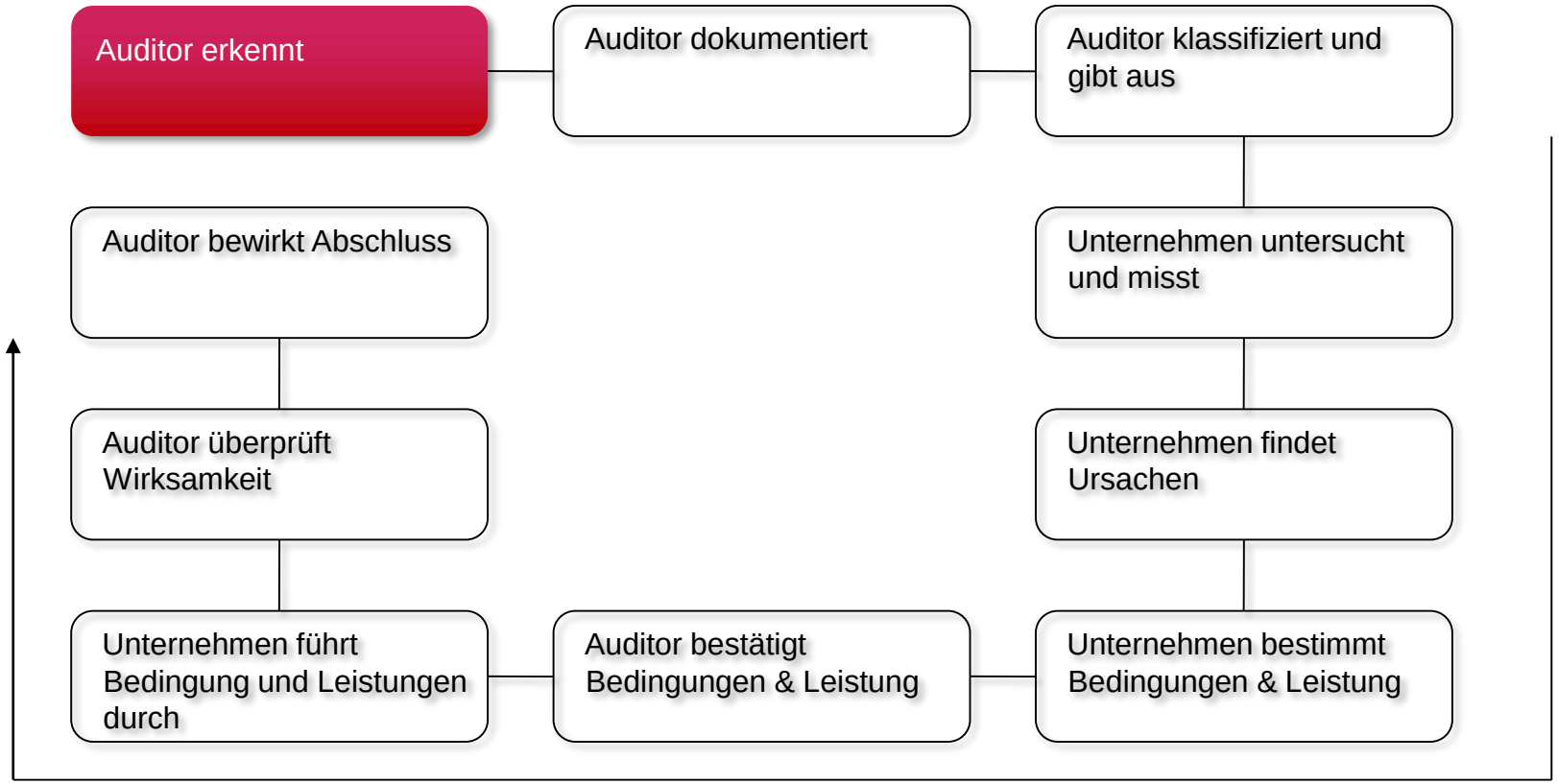


Abweichungen/Feststellungen

Die im Audit durch den Auditor identifizierten Abweichungen (auch als „Feststellung“ bezeichnet), sind wie folgt vom auditierten Unternehmen zu behandeln:

- Beobachtungen
  - Dient nur zur Dokumentation von Tatsachen und Ereignissen, die eine Auswirkung auf das ISMS haben könnten
  - Hilft dem Auditor beim nächsten Audit den Sachverhalt zu beachten
- Geringfügige Abweichung
  - Abweichung von der Norm, die vom Kunden lt. 10.1 behandelt werden muss
  - Oft gegen eine od. mehrere Kontrollen im Annex A
  - Der Kunde schlägt Korrekturmaßnahmen vor
  - Der Auditor beurteilt die Zweckmäßigkeit und kontrolliert die Umsetzung binnen der vereinbarten Fristen
- Wesentliche Abweichung
  - Nur zu Punkten 4.-10. der Norm
  - Erfolgreiche Zertifizierung erst nach Behebung möglich
  - Folgen: Entzug, Aussetzung bzw. Nicht-Erteilung der Zertifizierung

Behandlung von Abweichungen



2-4 Wochen bis max. 6 Monate

Zertifizierungsentscheidung

Die Zertifizierungsstelle erhält von den Auditoren den/die Auditbericht/e

Zertifizierungsentscheidungen:

- Erteilung/Erweiterung/Einschränkung/Aussetzung/Aberkennung des Zertifikats u.a. wegen
  - Änderungen im Scope
  - mehr/weniger Standorte
  - schwerwiegende Mängel im ISMS
  - Übernahmen, Wechsel des Geschäftsfeldern
- Entscheidungsgrundlagen dazu:
  - Auditberichte (von planmäßigen und außerordentlichen Audits)
  - Beobachtungen, Beschwerden
  - Einsprüche des Kunden
  - Input des Unabhängigkeitskomitee

Überwachungsaufgaben

Nach erfolgreicher Zertifizierung bzw. bei allen bestehenden aufrechten Zertifizierungen:

Überwachungsaufgaben der Zertifizierungsstelle

- Überwachung der aktuell zertifizierten Kunden (öffentlicher Auftritt, Dokumente, Beobachtungen und Beschwerden)
- bei Änderungen: event. Überwachungsaudit od. Rezertifizierungsaudit notwendig
- bei Zweifel an Effektivität des ISMS: event. außerordentliches Audit
- mögliche Folgen:
  - Einschränkung/Aussetzung/Aberkennung des Zertifikats bzw.
  - Neuausstellung/Entzug des Zertifikates
  - und ggf. Änderung in der Liste der zertifizierten Kunden

Änderungen der Zertifizierung

- Änderungen im Scope (Erweiterungen oder Einschränkungen)
  - neue bzw. zusätzliche/weniger Standorte
  - zusätzliche/weniger Prozesse/Services innerhalb des Scopes
  - mehr/weniger Personen/gruppen innerhalb des Scopes
  - Folgen daraus: event. Erweiterungsaudit durchführen und dann Zertifikat anpassen
  - Einschränkung bzw. Erweiterung des Zertifikates
- Änderungen im Firmen/Organisationswortlaut bzw. Gesellschaftsform
  - Neuausstellung des Zertifikats
    (falls sich sonst substanziell nichts am Scope geändert hat)
  - Änderungen im Verzeichnis darstellen (Website)
- Neue Normversionen (wie z.B. von 27001:2005 → 27001:2013)
  - Information von Bestandskunden und Planung des Übergangs (bei Überwachungsaudit oder nächster Rezertifizierung)
  - Neuausstellung des Zertifikats

Mögliche Problem

- mögliche sonstige Probleme
  - Beschwerden gegen Zertifikatsinhaber durch Dritte
  - Zweifel an Wirksamkeit des Managementsystems durch Überwachungsergebnisse
  - vorzeitige Vertragsauflösung (Insolvenzverfahren, Kündigung, etc.)
  - sonstige Probleme (z.B.: Gerichtsverfahren, Zahlungsverzug, Interessenskonflikte, Machbarkeitshindernisse)
- mögliche Folgen
  - Nachforschungen beim Kunden, event. Auflagen und/oder Nachaudit zur Überprüfung vereinbarter Auflagen bzw. Umsetzung von Maßnahmen
  - Einschränkung, Aussetzung, Aberkennung des Zertifikates
  - Einspruch des Kunden gegen Entscheidungen der Zertifizierungsstelle
  - Schlichtungsverfahren bzw. Eskalation an Unabhängigkeitsausschuss od. Akkreditierungsstelle (Akkreditierung Austria im BMDW)

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

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY