ABGLEICH ISO 27001 ZU FINANZRELEVANTEN GITC

Reto S. Bürgi

AGENDA

19. Juni 2020

Grundlagen

- Ausgangslage
- Zertifikat - Prüfbericht
- Fragen?

Workshop Kontrollabdeckung

- Zugriffssicherheit
- Änderungswesen
- IT-Betrieb

AUSGANGSLAGE

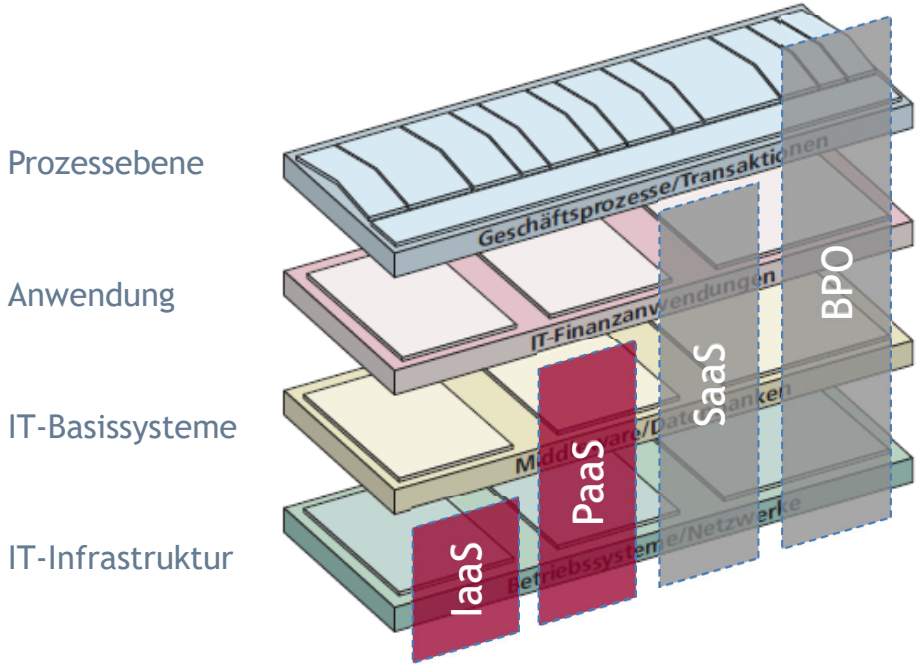
Outsourcing

Outsourcing Situationen
- Business Process Outsourcing (BPO)
- Software as a Service (SaaS)
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

Anwendungskontrollen
- Vollständigkeit
- Gültigkeit
- Berechtigungen
- Funktionentrennung
- etc.

Generelle IT-Kontrollen
- Änderungswesen
- Logischer Zugriff
- Physische Sicherheit
- IT-Betrieb

An den Dienstleister ausgelagerte Geschäftsbereiche:



AUSGANGSLAGE

Beim auslagernden Unternehmen erwartete Kontrollen (Beispiele)

Kontrollen im Bereich des Zugriffsschutzes

- Vergabe, Änderung und Inaktivierung von User-Accounts
- Vergabe, Änderung und Inaktivierung von Rollen / Berechtigungen im Rahmen von formalen Prozessen
- Periodische Kontrolle der User-Accounts einschliesslich deren Rollen / Berechtigungen
- Bestimmung und periodische Kontrolle der Berechtigten für Vergabe der User-Accounts einschliesslich deren Rollen / Berechtigungen
- Meldung von sicherheitsrelevanten Vorfällen an den Provider zur weiteren Abklärung und geeigneten Reaktion

Kontrollen bei der Änderung von IT-Anwendungen

- Spezifikation der Anforderungen an neue oder zu ändernde IT-Anwendungen und IT-Basissysteme
- Angemessene Tests und formelle Freigabe von neuen oder geänderten IT-Anwendungen und IT-Basissystemen

Kontrollen beim Betrieb der IT-Basissysteme

- Kontrolle und Überwachung der Verarbeitungsprozesse bei der Übergabe der in den vorgelagerten Anwendungen erfassten Transaktionen an die Meldungsaustausch-Plattform
- Kontrolle und Überwachung der Verarbeitungsprozesse bei der Übergabe der Leistungen von der Meldungsaustausch-Plattform an die nachgelagerten administrativen Anwendungen
- Kontrolle und Überwachung der Verarbeitungsprozesse bei der Übergabe von aufzubewahrenden resp. aufbewahrungspflichtigen Unterlagen an das elektronische Archiv

Kontrollen beim Betrieb der IT-Anwendungen

- Abstimmung der in den vorgelagerten Anwendungen erfassten Daten
- Abstimmung des im ERP aufbereiteten Buchungsstoffes mit den im Finanz-Management verbuchten Daten
- Abstimmung des im Material-Management aufbereiteten Buchungsstoffes mit den im Finanz-Management verbuchten Daten

PRÜFBERICHT ODER ZERTIFIZIERUNG

Eine Gegenüberstellung

Zertifikat

- 3 Parteien: Auditierter, Auditor, Zertifizierungsstelle
- Bestätigung der Umsetzung eines Standards
- Wirksamkeit der Massnahmen wird nicht in der Vergangenheit überprüft
- Andere Prüfer können sich bei ihrer Arbeit nicht auf ein Zertifikat abstützen
- i.d.R. 3 Jahre gültig, jährliche Teil-Audits

Prüfbericht

- 2 Parteien: Auditierter (Dienstleister), Auditor
- Auditor arbeitet nach anerkannten Prüfstandards
- Bestätigt Umsetzung der dokumentierten Kontrollen (IKS)
- Andere Prüfer können sich auf Testate abstützen. Der Rückgriff auf Testate ist geregelt im schweizerischen Prüfungsstandard 402 von EXPERTsuisse
- Unbedingt empfohlen für Anbieter von rechnungsrelevanten Geschäftsprozessen oder IT-Dienstleistungen
- i.d.R. ist Prüfperiode 1 Jahr, jährliche Prüfung

ISO 27001 ist eine *Innensicht* auf die Prozesse, Kontrollen eines Informationssicherheits-Managementsystem einer Organisation

ISAE 3402 ist eine *Aussensicht* auf das dienstleistungsbezogene finanzrelevante IKS einer Organisation

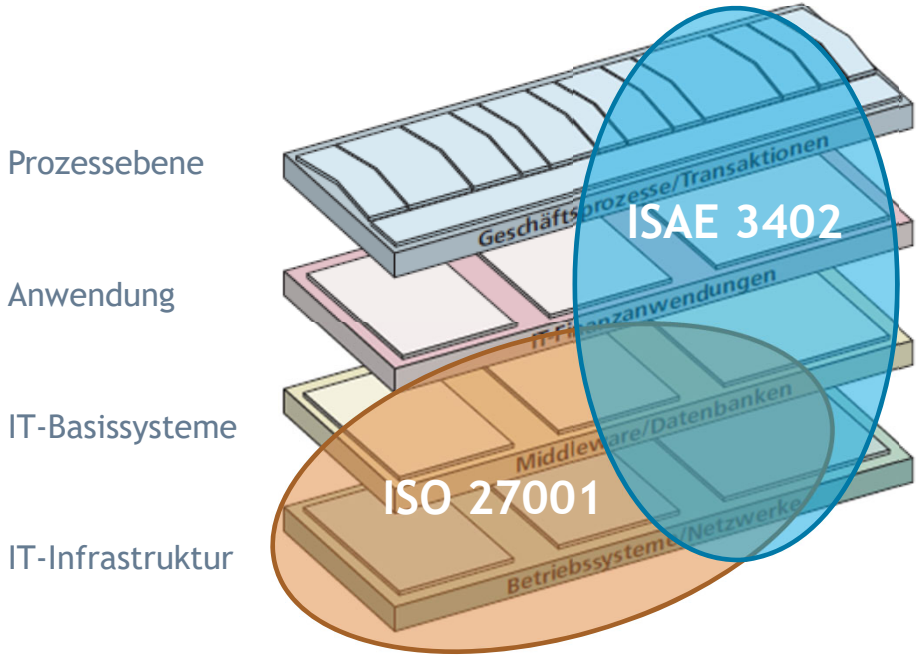
ZIELE

Ausgehend von ISAE 3402:

1. **Abdeckung ISAE 3402 ITGC durch ISO 27001**

2. **Aufzeigen der Lücke von ISO 27001 zu ISAE 3402**

An den Dienstleister ausgelagerte Geschäftsbereiche:



ISAE 3402

Zugriffssicherheit

Logischer Zugriff

- Benutzerauthentifizierung
- Autorisierung von Benutzerberechtigungen
- Entzug von Benutzerberechtigungen
- Einschränkung privilegierter Berechtigungen auf angemessene Personen
- Einschränkung des Zugangs zu Systemressourcen/Utilities
- Überprüfung der Benutzerberechtigungen

Physische Sicherheit

- Zutritt zu Datenverarbeitung (RZ)

ISAE 3402

Änderungswesen

- Autorisierung der Änderung
- Testen der Änderung
- Abnahme der Änderung
- Produktivsetzung der Änderung

ISAE 3402

IT-Betrieb

Datensicherung

- Backupdurchführung und Überwachung
- Auslagerung
- Wiederherstellungstest

Automatische Verarbeitung (Batch Jobs, Schnittstellen)

- Planung
- Überwachung