



RISK ADVISORY SERVICES

Archivierung in der Cloud

Revisions sichere Aufbewahrung/Archivierung

INFORMATION RISK MANAGEMENT

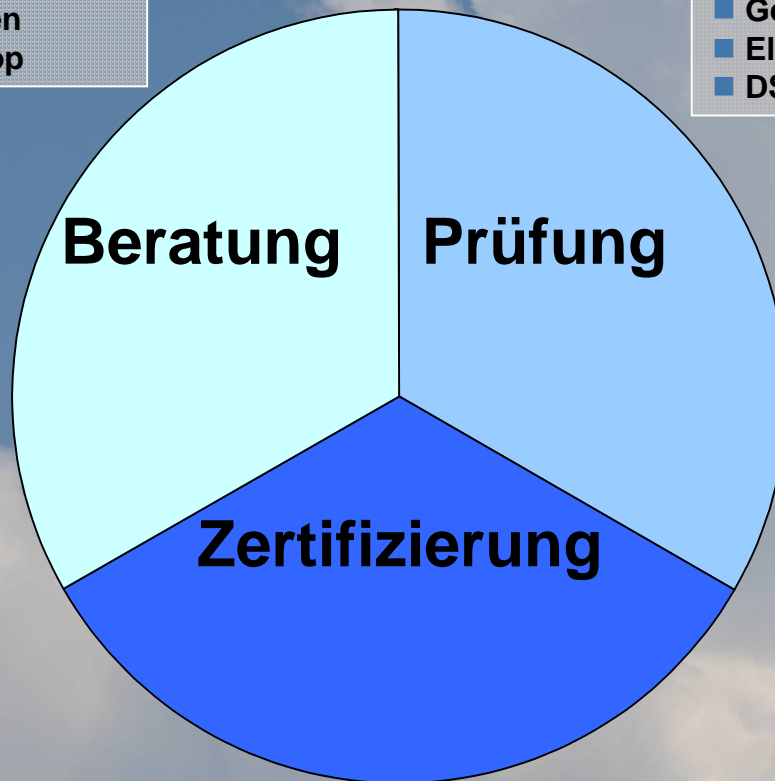
Agenda

- Überblick
- Anforderungen an die Aufbewahrung und Archivierung
- Systematik der Archivierung
- Archivierung in der Cloud, was ist anders?
- GeBüV versus Cloud
- Problemstellungen des Cloud Service Providers (CSP)
- Sicht des Revisors und Fazit

KPMG Archivierungs- und Recordsmanagement Wolke

- ISO 17799
- ISO 15489-2
- Phasen Konzept
- Auditierungs Methoden
- Workshop

- Health check
- Audit Review Programm
- OR 927ff, OR 728a (IKS)
- GeBüV
- EIDI-V
- DSGVO



- ISO 15489-1
- ISO 27001
- Zertifizierungs-Auditprogramm

Interdisziplinäre Teams aus:

- Information Risk Management
- Legal
- Tax
- Audit
- Forensic

Motivationen die eigene Archivierungssituation zu überdenken

- **Externer Druck:** Einhaltung der für Archivierung anwendbaren Schweizer und ausländischen Gesetze
- **Interner Druck:** Einhaltung von Geschäftsanforderungen (z.B. aus möglichen Garantieforderungen)
- Lösen der **Altdaten-Problematik** bei Migrationen von Systemen oder Unternehmensfusionen
- Einführung **neuer Techniken** und Dokumententypen (Email, Auslagerung in die **Cloud**)
- **Technische Archivierung** in Datenbanken und ERP Systemen

Gesetzliche Anforderungen und technische Umsetzung

Archivierungsrelevante gesetzliche Bestimmungen in der Schweiz

- Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: **Obligationenrecht [OR]**)
Artikel 957 - 963
- Verordnung vom 24. April 2002 über die Führung und **Aufbewahrung der Geschäftsbücher (GeBüV)**
Artikel 3 - 10
- Verordnung des EFD über **elektronisch übermittelte Daten und Informationen (EIDI-V)** vom 30. Januar 2002
Artikel 10 – 12
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)

Archivierungsrelevante weitere Bestimmungen und Gesetze

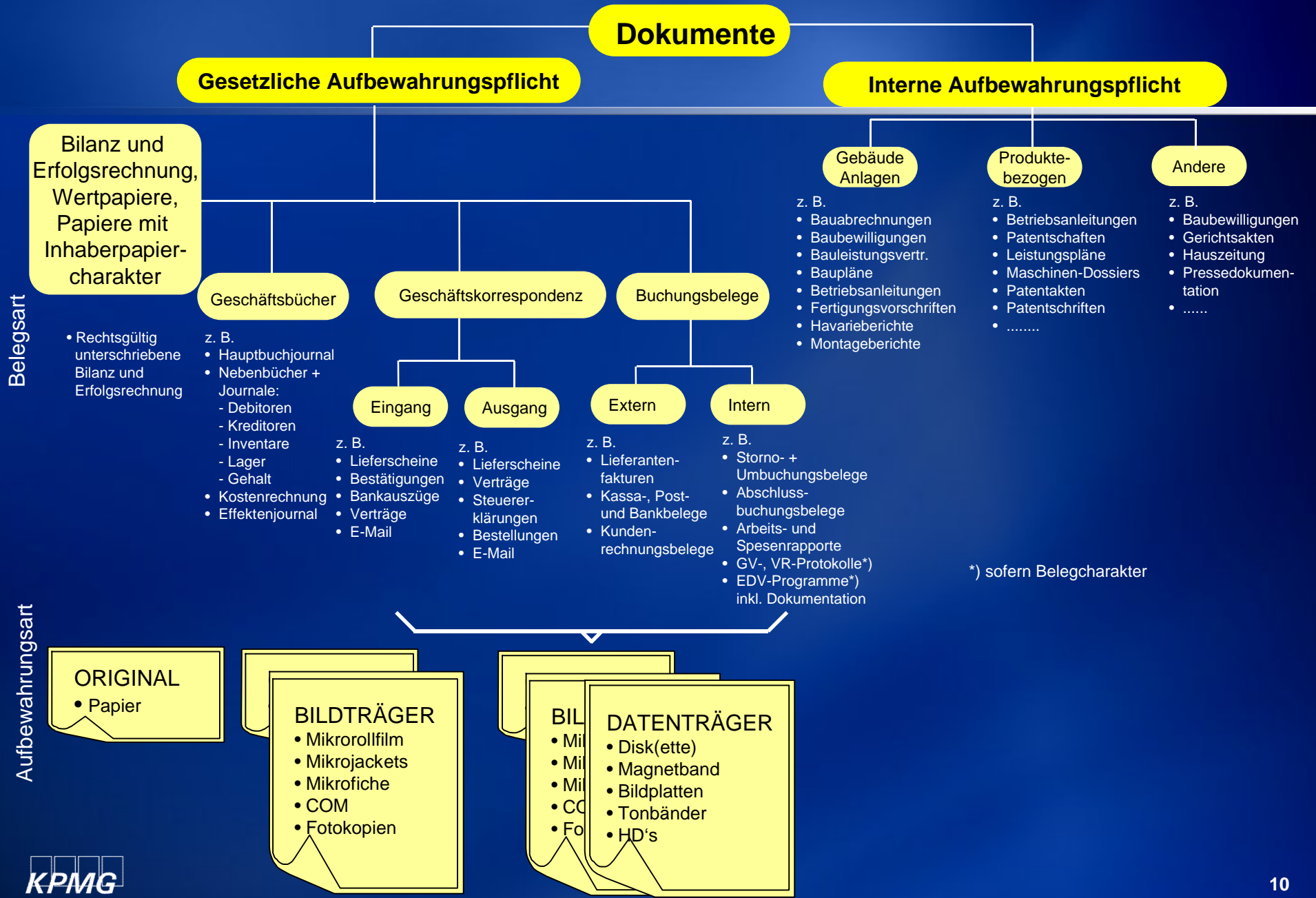
- ISO 15489-1 Schriftgutverwaltung Teil-1: Allgemeines (Records Management)
- Branchenspezifische Spezialerlasse wie Steuergesetze, Bankengesetz, FINMA Outsourcing Rundschreiben 08/7 oder Geldwäschereigesetz
- Verbandserlasse wie die Richtlinien der Schweizerischen Bankiervereinigung
- IKS Thematik, Auslagerung von Kontrollen an CSP und deren Überwachung im nationalen wie auch internationalen Verhältnis
- Erhöhte Komplexität durch länderübergreifende Services, nicht alles ist in jedem Land möglich (z.B. MWST relevante Aufbewahrung D<->CH)

Risiken bei Nichtbeachtung der Aufbewahrungsvorschriften

- **Strafgesetzbuch Art. 325** : Strafe für Verletzung der Pflichten zur ordnungsmässigen Führung der Geschäftsbücher und zur Aufbewahrung der Geschäftsbücher und -korrespondenz
- **Mehrwertsteuer**: Verlust von ausgewiesenen Vorsteuern. Kann der Ausfuhrnachweis nicht erbracht werden: Nachsteuer bis zum Maximalsatz.
- **Datenschutzgesetz Art. 6**: Transfer von Datensammlungen ins Ausland: Haft oder Busse (Art. 34)
- **Geldwäschereigesetz Art. 7**: Sanktionen der SRO / Kontrollstelle für die Bekämpfung der Geldwäscherei
- **Bankengesetz**: Verschärftes Strafmass (Busse oder Gefängnis)

Was muss aufbewahrt werden?

Übersicht Aufbewahrung

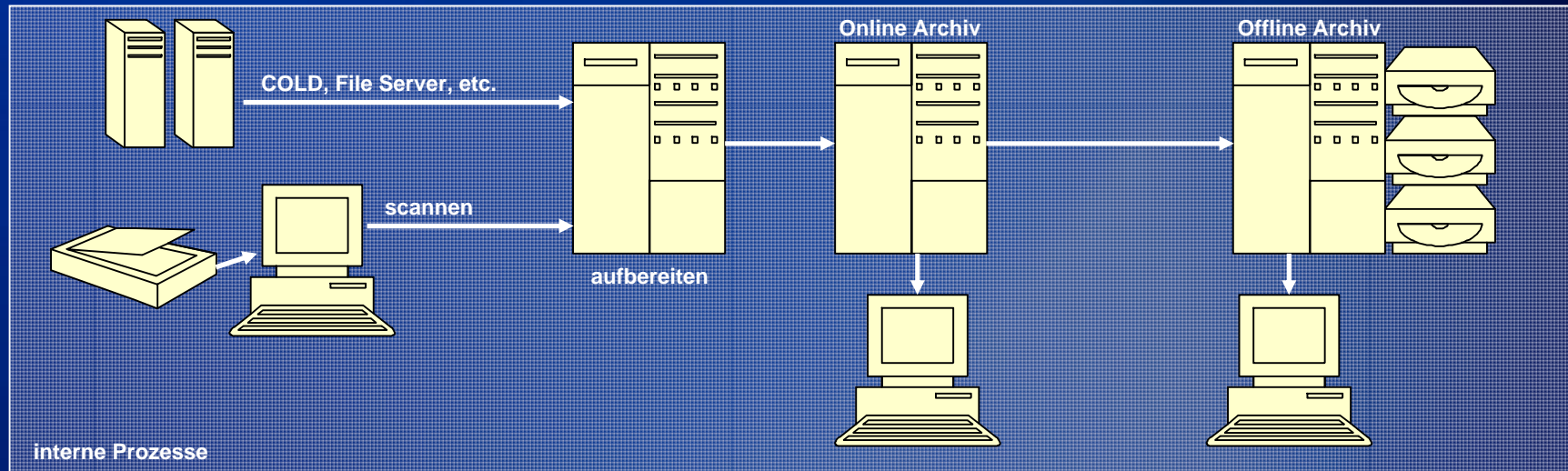


*) sofern Belegcharakter

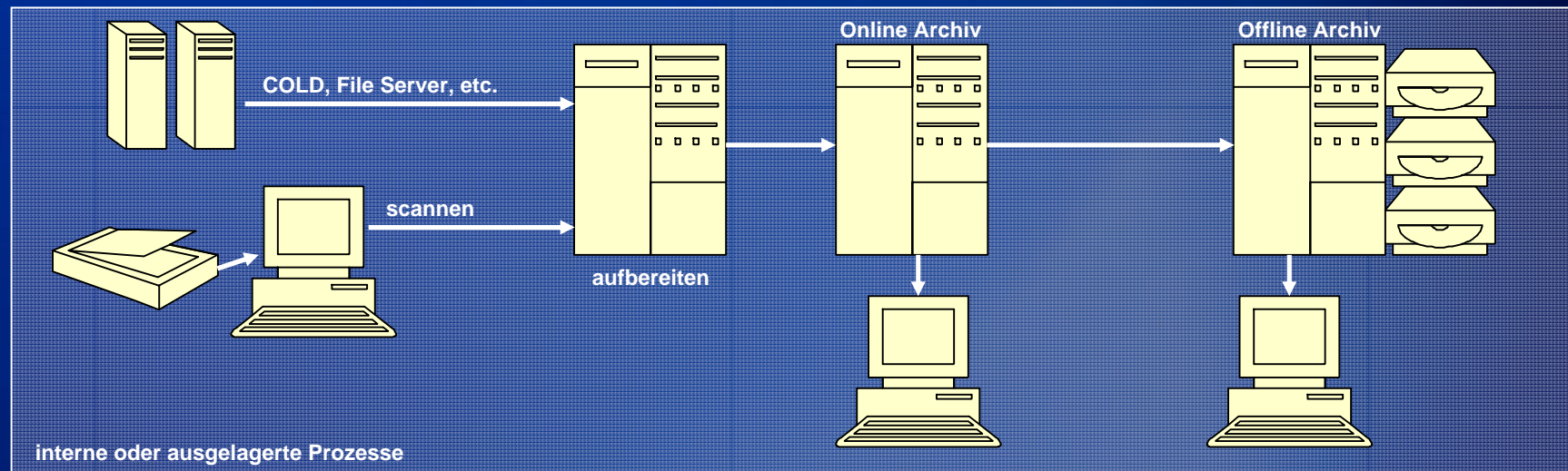
Minimale Kategorien für Dokumenten- und Archivplan

- Dokumentennummer / Systematik
- Bezeichnung des Dokuments
- Gesetz oder Standard pro Dokumententyp (sollte von Rechtsabteilung und GL genehmigt sein)
- Aufbewahrungsdauer
- Aufbewahrungsmedium
- Aufbewahrungsort (**Cloud?**)
- Verantwortliche
- falls vorhanden Klassifizierung (z.B. public, confidential, secret → hat Einfluss auf Schutz der Archive und Anforderungen an CSP)

Vereinfachter Archivierungsprozess



Archivierungsprozess und Cloud



Was kann davon an einen CSP ausgelagert werden?

- **Infrastruktur:** Server, Rechenzentren, Storage mit Variationen von un/managed hosting, System Management etc.
- **Plattform:** z.B. Applikation Server, File Sharing, etc.
- **Applikation:** Software Angebote, Application Program Interfaces (API) zur Erstellung neuer Services etc.
- **Service:** z.B. Business Processes, Scanning Services

Zusätzliche Aufwände und Risiken durch die Auslagerung in die Cloud (1/2)

■ Externe Datenaufbewahrung

- Schwache Kontrolle über die Daten (Mängel in Backup & Recovery)
- Rechtliche Komplikationen (Datenschutz, widersprüchliche Regulationen)
- Lebensfähigkeit CSP (keine/unklare Garantien für Kontinuität/Verfügbarkeit)

■ Mandantentrennung

- Ungenügende Segregation der Daten (Zugriff, Technische Lösung)
- Schlechtes Identity und Access Management
- Ungenügende Überwachung und Logging
- Ausschlaggebend ist das Schwächste Glied der Kette (z.B. Virtualisierung, Shared Databases, etc.)

Zusätzliche Aufwände und Risiken durch die Auslagerung in die Cloud (2/2)

■ Benutzung öffentliches Internet

- Vage und/oder nicht existierende Rechenschaft und Ownership
- Verlust, Missbrauch und Diebstahl von Daten
- Kein Zugriff auf Daten und/oder Services

■ Integration mit der internen IT Umgebung

- Unklare Perimeter und Abgrenzungen
- Keine Verbindung und/oder Abgleich mit der Internen Sicherheit
- Komplexität der Integration

Wichtigste Aspekte der GeBüV

- **Echtheit und Unverfälschbarkeit**
- **Dokumentation von Organisation, Zuständigkeiten, Prozessen und Technik**
- **Verfügbarkeit:**
 - „angemessene Frist“
 - Hilfsmittel
- **Verantwortung regeln**
- **Schutz des Archivs**
- **Integritätsprüfung**
- **Migration**

Zulässige Informationsträger

■ Unveränderbare:

- Papier
- Bildträger (z.B. Mikrofilme)
- unveränderbare Datenträger (z.B. CD, DVD)

■ Veränderbare - gespeicherte Informationen können ohne Nachweis auf dem Datenträger geändert oder gelöscht werden:

- Magnetbänder
- Disk-Systeme
- Solid State Speicher (z.B. SSD)

Zu beachten bei veränderbaren Informationsträgern

- Technische Verfahren zur Gewährleistung der Integrität:
 - Hashwerte
 - digitale Signaturverfahren
 - Zeitstempel
- Allfällige weitere Vorschriften aufgrund der eingesetzten Verfahren
- Abläufe und Verfahren müssen festgelegt, dokumentiert und mit Hilfsinformationen aufbewahrt werden
- Woher kommt die WORM Qualität eines Mediums?

Überprüfung und Datenmigration

- Regelmässig Integrität und Lesbarkeit prüfen.
- Bei Datenmigration sicherstellen:
 - a. Vollständigkeit und Richtigkeit;
 - b. die Verfügbarkeit und die Lesbarkeit muss den gesetzlichen Anforderungen weiterhin genügen.
- Die Übertragung von Daten von einem Informationsträger auf einen anderen ist zu protokollieren.
- Das Protokoll ist zusammen mit den Informationen aufzubewahren.
- Outsourcing Problematiken beachten

Problemstellung des CSP

- **Der CSP muss die verschiedensten Anforderungen und Standards erfüllen:**
 - IKS, SOX, interne/externe Audits,
 - PCI, Datenschutz, Systrust,
 - ISO Zertifikationen, Security Prüfungen, etc.
- **Meist hat der CSP noch keine Integrierten Ansätze um alle Anforderungen abzudecken**
- **Fehlendes Verständniss für Prüfanforderungen bei Design und Effektivität der Kontrollen oder Prüfzeitraum („Schnitt in der Zeit“ versus Abdeckung einer ganzen Periode)**

Prüfberichte und Prüfungen beim CSP

Ansatz	Zweck	Anwendbarkeit
SAS 70 (bis 2011) ISAE 3402 (ab 2011)	Ausgelegt als Tool zur Unterstützung für finanzrelevante Audits von Kunden, welche Service Organisationen benutzen (u.a. relevant bei IKS, SOX, Aufbewahrung nach OR/GeBüV etc.). Kann Archivierungsfragen abdecken.	Meist dort anzutreffen, wo CSP wichtige Rolle in Transaktionsverarbeitung oder Finanzberichterstattung des Kunden spielt, deckt bestimmte Periode ab. Deckt Themen wie Datenschutz und Business Continuity nicht ab.
ISO 27001	V.a. dort wo der (zukünftige) Kunde eine Bestätigung des allgemeinen Sicherheitsprogrammes des CSP benötigt. Kann Archivierungsfragen nur teilweise abdecken.	Vielfältige Anwendbarkeit. Zu beachten: Periode und Scope der Prüfung decken oft die Bedürfnisse des Finanzprüfers nicht ab.
Trust Services (SysTrust and WebTrust)	Ausgelegt für die Bedürfnisse von Online und anderen ausgelagerten Systemen (nicht/ finanzrelevant). Kann Archivierungsfragen nur teilweise abdecken.	Meist dort anzutreffen, wo der CSP belegen will, dass seine spezifischen Sicherheits-, Verfügbarkeits-, Vertraulichkeits-, Verarbeitungsintegritäts- und Datenschutzkontrollen über eine bestimmte Zeitperiode effektiv sind.
Durch die Anwendung eines vereinheitlichten Compliance Ansatzes (aufbau eines Kontrollrahmenwerkes, dass alle wichtigen Anforderungen umfasst, zentrale Prüfung) kann der CSP Risiken effektiv reduzieren, die Sicherheit und Compliance erhöhen und die Effektivität der Kontrollen gegenüber seinen Kunden belegen.		

Fazit aus Sicht des Revisors

- Archivierung in der Cloud ist machbar
- Taxonomie/Archivplan als Basis
- Risiken aber auch Nutzen evaluieren
- Technische Umsetzung unter Einhaltung der nationalen und internationalen Anforderungen
- Wo sinnvoll: Externe Prüfung der Einhaltung und Einverlangen relevanter Prüfungsberichte von CSP's

Fragen/Diskussion



Kontakt:

Christoph Protz
Senior Manager

Master of Law UZH / CISA

KPMG AG

Badenerstrasse 172

Postfach

8026 Zürich

Telefon +41 44 249 21 99

Natel +41 79 754 58 03

Fax +41 44 249 30 17

cprotz@kpmg.com