HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Cloud-Angebote und IT-Compliance

Jan Philipp Timme
November 4, 2016

Begriff: Compliance

- Begriff aus betriebswirtschaftlicher Fachsprache
- engl.: „Compliance“ → dt.: Einhaltung, Befolgung, Regelkonformität
- Siehe auch „to comply“ → einwilligen, nachgeben, den Auflagen entsprechen
- → **Einhaltung von Gesetzen und Vorschriften**
- z.B.: BGB, HGB, AO, GmbHG, JArbSchG, BDSG, Normen, EU-Richtlinien, internationale Konventionen, ...

Einstieg in Compliance

- Menge zu berücksichtigender Regeln von Unternehmen abhängig
- Ab gewissem Umfang ist juristische Unterstützung notwendig
- Mögliche Optionen:
  - Juristische Beratung einkaufen
  - Mitarbeiter für juristische Fragen einstellen
  - Eine eigene Rechtsabteilung aufbauen
- $\rightarrow$ Erste Kosten entstehen

Compliance sicherstellen

- Compliance Management System (CMS)
- Beinhaltet Maßnahmen und Prozesse zur Sicherstellung von Regelkonformität
- $\rightarrow$ Integriert sich tief in das Unternehmen
- Ziele:
  - **Risiken** für Regelverstöße rechtzeitig **erkennen, analysieren und verhindern**
  - Angemessene Reaktionen, falls Regelverstoß dennoch eingetreten ist
- Zusätzlicher Aufwand $\rightarrow$ mehr Mitarbeiter $\rightarrow$ mehr Kosten
- Aber: Vermeidet langfristig Kosten! (wie eine Versicherung)

Begriff: IT-Compliance

- Compliance im IT-Bereich
- $\rightarrow$ Betrifft IT-Systeme des Unternehmens
- Kern-Anforderungen der IT-Compliance sollen gewährleistet werden:
  - Informationssicherheit
  - Verfügbarkeit
  - Datenaufbewahrung
  - Datenschutz
- Laut einer Studie von CSC fließen ca. $2/3$ des IT-Budgets einer Bank in IT-Compliance und Instandhaltung von Systemen.

IT-Compliance: Nichts als teurer Unfug?

- Einhaltung von Gesetzen oder Vorschriften wird nicht belohnt
- Aber: Strafen bei Verstoß gegen Gesetz oder Vorschrift!
  - Bußgelder, Gewinnabschöpfung, Verfall von Gewinn
  - **Haftstrafen** für Vorstand einer AG, Geschäftsführer einer GmbH, ...
- Und: Zusätzliche Kosten durch Folgeschäden:
  - Verfahrenskosten
  - Schadenersatzansprüche
  - Rückabwicklungen
  - Imageverlust / Vertrauensverlust, ...
- $\rightarrow$ (IT-)Compliance ist grundlegendes Unternehmensziel

Vorteile von IT-Compliance

- Unternehmensintern:
  - Frühzeitige Betrachtung von relevanten Gesetzen, Risiken, ...
  - „Volles Risikobewusstsein“ anstatt „Blindflug“
  - $\rightarrow$ (Daten-)Sicherheit durch strukturiertes Vorgehen
- Extern:
  - Schafft Vertrauen, demonstriert Stabilität und Robustheit
  - Ermöglicht Aussprechen von Garantien bezüglich (Daten-)Sicherheit
  - Erfüllt Anforderungen von Kunden und Vertragspartnern
- „... aber wie kann ich jemandem meine (IT-)Compliance nachweisen?“

Begriff: Cloud-Angebote

- Virtuelle Maschinen, Speicher, Anwendungen und Plattformen „on demand“
- Dynamisch anpassbare Dienstleistungen, dynamische Tarife
- Infrastruktur auf Rechenzentren in mehreren Ländern weltweit
- $\rightarrow$ Global vernetzte Infrastruktur
- $\rightarrow$ Daten werden oft weltweit verteilt gespeichert
- Je nach Standort andere Rechtslage

Cloud-Angebote aus Sicht der Kunden

- Eigene IT kostet zu viel, es soll gespart werden
- $\rightarrow$ Outsourcen mit speziellen Anforderungen an Datensicherheit
- Beispiel: Deutsche Versicherung möchte Kundendaten in die Cloud verschieben
  - Bundesdatenschutzgesetz muss eingehalten werden
  - Kundendaten sind vertraulich $\rightarrow$ müssen vertraulich bleiben!
  - Die Daten sollen jederzeit verfügbar sein
  - Die Daten sollen Deutschland nicht verlassen
- Kunde sucht international günstigen Anbieter, der diese Anforderungen belegbar erfüllen kann

Cloud-Angebote aus Sicht der Anbieter

- Pro Standort unterschiedliche Gesetze und Vorschriften zu erfüllen
- Je mehr Standorte in unterschiedlichen Ländern, desto mehr Gesetze finden Anwendung
- $\rightarrow$ (IT-)Compliance sichert eigene Existenz
- Kunden haben je nach Land unterschiedliche Rechte
- $\rightarrow$ Angebote müssen entsprechend konform gehen
- Kunden haben Anforderungen an die Datensicherheit
- $\rightarrow$ Anbieter muss Einhaltung dieser Bedingungen belegen können
- Und: Der Anbieter will dazu **weltweit** in der Lage sein

Steckbrief: ISO 27001

- **Internationaler Standard** aus dem Jahr 2005 (überholt in 2013)
- Gehört zur Familie der ISO 2700X
- Anforderungen an ein Information Security Management System (ISMS)
  - Ähnlicher Ansatz zu Compliance Management System
  - Fokus auf Datensicherheit
  - $\rightarrow$ Bewahren der Vertraulichkeit, Integrität und Verfügbarkeit von Daten
  - Anwendung von Risikomanagementprozessen
- Struktur und Aufbau abhängig von Unternehmensstruktur und Bedarf
- Bonus: Man kann sich nach ISO 27001 zertifizieren lassen!

Inhalte der Ziele ISO 27001

- Enthält Anforderungen an ein ISMS + passende Kontrollen
- Top-Down Ansatz („Top management shall ensure that . . . “)
- Anwendungsgebiete: (Auszug)
  - Managen von **Sicherheitsrisiken**
  - Sicherstellung der Einhaltung von Gesetzen und Vorschriften
  - Definition von Managementprozessen zum Managen von Informationssicherheit
  - Nutzung durch Auditoren als „Checkliste“
- Erzeugung und kontinuierliche Pflege einer Datensicherheitsrichtlinie

Auswirkungen der ISO 27001

- Entwurf neuer Prozesse, Informationssysteme oder Kontrollen berücksichtigt Datensicherheit von Beginn an
- Verursachte Kosten:
  - Interne Kosten verursacht durch ISMS und zugehöriger Dokumentation
  - Externe Kosten durch Beauftragung von Beratungsunternehmen
  - Audit Kosten durch Zertifizierungsunternehmen
- Konformität nach ISO 27001 zeigen?
  - Selbst Konformität verkünden
  - Kunden/Vertragspartner bitten, die Konformität zu bestätigen
  - Verifikation der Konformität durch externen Auditor ($\rightarrow$ Zertifizierung)

Nutzen der ISO 27001

- Langfristige Kostensenkung durch strukturierte Prozesse
- Risikominimierung
  - $\rightarrow$ Geringere Haftungs- und Geschäftsrisiken
  - $\rightarrow$ Geringere Versicherungsbeiträge
  - $\rightarrow$ Verbesserte Kreditwürdigkeit bei Banken/Investoren
- Höhere Wettbewerbsfähigkeit durch belegbare Datensicherheit
- $\rightarrow$ Imageverbesserung

Relevanz der ISO 27001 für Cloud-Angebote

- Internationaler Standard, weltweit anerkannt
- → Cloud-Anbieter können Konformität belegen
- Starker Fokus auf Datensicherheit und Datenvertraulichkeit
- → Mehr Vertrauen bei den Kunden, Anforderungen werden erfüllt
- Zertifizierung und regelmäßige Audits stellen Konformität sicher
- → Erhöhte Transparenz; Kunden können Daten ohne Sorgen bei Anbieter ablegen

1. Compliance und IT-Compliance
2. Cloud-Angebote
3. ISO 27001
4. Umsetzung von Compliance
   - Einführung von Compliance
   - Fall 1 Umgehung von Compliance
   - Fall 2: Lähmung durch Compliance
5. Fazit

Einführung von Compliance

- Management führt Compliance mit CMS (Compliance Management System) ein
- Prozesse werden komplexer, mehr Kontrollmechanismen, ...
- Mitarbeiter akzeptieren Compliance und tragen ihren Teil dazu bei
- $\rightarrow$ Soweit alles gut ...

Fall 1 Umgehung von Compliance

- IT-Compliance bzw. Compliance allgemein sind für Unternehmen überlebenswichtig
- Warum also sollte man versuchen wollen, Compliance zu umgehen?
- → Management fordert höhere Produktivität
- **Interessenkonflikt**: Compliance gegen Produktivität
- → Compliance wird zu Gunsten von Produktivität umgangen

Fall 2: Lähmung durch Compliance

- Ausgangssituation: Compliance ist im Unternehmen etabliert
- Mitarbeiter verstößt ungewollt gegen Compliance-Vorgaben
  - Reaktion: Management führt Genehmigungsprozesse ein
  - Konsequenz: Produktivität geht runter, Mitarbeiter werden verunsichert und schlimmstenfalls durch Angst „gelähmt“
- Sinnvoller Umgang mit Verstößen gegen Compliance notwendig
- → Mitarbeiter „abholen“ anstatt Kontrolle!
- → Kommunikation vom Management ist wichtig!

Abschließendes Fazit

- Kunden wollen stabile und reife Unternehmen als Vertragspartner
- (IT-)Compliance minimiert Risiken, bringt Robustheit und Stabilität
- ISO 27001 schafft Transparenz und Vertrauen durch belegbare Datensicherheit
- $\rightarrow$ Unternehmen steht besser dar (Image, Kredite, Wettbewerb)
- Compliance ist überlebenswichtige Versicherung für Unternehmen
- Compliance muss vom Management richtig kommuniziert werden