Rechtliche und organisatorische Anforderungen für den regelkonformen Einsatz von IT
- Ein Überblick -

Forum **7-it**

RA Rainer Friedl

München, 20. Januar 2014

Einführung: Begriffe

- **IT-Governance**: Lenkung/Steuerung, Organisation und Prozesse der gesamten IT-Infrastruktur zur Unterstützung der Erfüllung geschäftlicher Vorgaben (Unternehmensziele, -Strategie).

- **IT-Compliance**: IT-Infrastruktur, IT-Systeme und Prozesse müssen die regulatorischen Vorgaben einhalten und erfüllen können (Regelkonformität: Einhaltung geltender Gesetze, Richtlinien und anderen Verhaltensmaßregeln).

- **Informationssicherheit**: Sicherstellung der Schutzziele

  Verfügbarkeit – Integrität – Vertraulichkeit

  durch die Abwehr von Gefahren und Bedrohungen für Informationen (Risikominimierung, Schadensvermeidung).

Einführung: Einordnung und Bedeutung der IT-Compliance

- IT-Compliance ist Teil der IT-Governance. Abhängigkeiten und Anforderungen an andere Bereiche wie Monitoring, Service-Management, Risikomanagement und Sourcing.

- Aufgrund der heutigen Unternehmensstrukturen sind nahezu alle Prozesse IT-basiert.

- Zunehmende Bedeutung durch zunehmende regulatorische Vorgaben (vertraglich, gesetzlich).

Verpflichtung zur IT-Compliance: Haftung des Vorstands/Geschäftsführer für IT-Risiken

- Vorstandspflicht bei AGs (§ 93, Abs.1 AktG)
  - „… Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden …“
  - Beweislastumkehr aus § 93, Abs. 2, Satz 2 AktG): Exkulpation obliegt dem Vorstand und ist nur bei ordnungsgemäßer Protokollierung möglich
  - Gesetzliche Pflicht zum Risikomanagement § 91, Abs. 2.

    „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

- **Ausstrahlungswirkung auf Geschäftsführer anderer Gesellschaftsformen:** je nach Größe, Komplexität und Struktur eines Unternehmens sind die Geschäftsführer durch analoge Anwendung ebenso verpflichtet/betroffen (vgl. § 43 GmbHG).

Auswahl wichtiger Regelungen mit IT-Compliance-Relevanz

- Vielzahl von allgemeinen Gesetzen und Reglementierungen (Auswahl)
  - Wirtschafts- und Gesellschaftsrecht: HGB, BGB, GmbHG, AktG
  - Steuergesetze und Regelungen (EkStG, KStG, AO, GoBs, GDPdU, Basel II/III, etc.
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)
  - Datenschutzrecht: insbes. BDSG, Europäische Datenschutzrichtlinie (Richtlinie 951461EG), Ggf. Landesdatenschutzgesetze (LDSG)
  - Urheberrecht, Wettbewerbsrecht
  - Arbeitsrecht
  - Jugendschutzgesetz (JuSchG), Sozialgesetzbuch (SGB)
  - Allgemeine und besondere Strafgesetze
- Zusätzliche Vorschriften und Regelungen für bestimmte Branchen und Tätigkeiten (Gesundheitswesen, Banken, Medizintechnik)
- Vertragliche Verpflichtungen (NDA, LoI, SLAs, Auftragsdatenverarbeitung)

Und das heißt …

konkret?

Einzelne wichtige IT-Compliance Anforderungen: Datenschutz

- Datenschutz: Gesetzliche Verpflichtung zum Schutz personenbezogener Daten

- Angehen wesentlicher Compliance-Anforderungen durch die Umsetzung und Weiterentwicklung des Datenschutzes und damit verbundenen Informationssicherheits-Maßnahmen:
  - Klassische Informationssicherheitsgebote werden angegangen
  - Umsetzung technischer- und organisatorischer Maßnahmen
  - Prozessüberblick durch Verfahrensverzeichnis
  - Kontrolle externe Dienstleister durch Auftragsdatenverarbeitung

- Bevorstehende Datenschutz-EU-Verordnung?

- Viele ungelöste Herausforderungen (z.B. GPS-Track, Datenbrillen, …)

Einzelne wichtige IT-Compliance Anforderungen: E-Mail und E-Mail-Archivierung

- Pflichtangaben auf Grund Gleichstellung mit Papierkorrespondenz (§ 37a HGB; §§ 125a; 177a HGB; § 35a GmbHG; § 80 AktG)
- Anti-Spam § 6 TMG, Opt-In aus § 7, Abs.3 UWG
- Kontrolle und Verhinderung rechtswidriger Nutzung (Risiko wegen teilweise verschuldensunabhängiger Störerhaftung)
- Archivierung notwendig aufgrund Eigenschaft von E-Mails als Geschäftsunterlagen und/oder ggf. steuerlicher Steuerunterlagen (§ 257 HGB; § 147 AO; GDPdU; GoBS). (Achtung: unsichere prozessuale Beweiskraft!)

Einzelne wichtige IT-Compliance Anforderungen: Dokumentenmanagement

» Digitale Dokumente sind Geschäftsunterlagen.

» Anforderung aus dem HGB zur Archivierung:
  – Unveränderte (originäre) und unveränderbare Speicherung.
  – Möglichkeit der Anzeige und Ausdrucks wie im Original.
  – Filtermöglichkeiten zur zeitnahen Suche von Dokumenten (Indizierung, Tagging).
  – Migrationen auf neue Plattformen, Medien etc. müssen ohne inhaltliche Informationsverluste erfolgen.
  – Protokollierung aller Aktionen im Archiv zur Nachvollziehbarkeit.

» Eingescannte Rechnungen und anschließende Vernichtung? Sicherstellung der Originalität?

Einzelne wichtige IT-Compliance Anforderungen: Lizenz-Management

- Ermittlung und Überwachung der installierten/genutzten Software.

- Inventur der lizensierten Software und deren Zuweisung:
  - Lizenzart (Einzellizenz, Mehrfachlizenz, Volumenlizenz, etc.).
  - Lizenzklasse (Vollversion, Upgrade, Miete).
  - Lizenzmetrik („Zählmethode“: Anzahl, Zugriffslizenz, Concurrent/Zugewiesen, Volumen, Prozessorzahl).

- Lizenzrechtliche Fragen:
  - Open Source Software kostenlos?
  - Free-Use Software auch für Unternehmen?
  - Gebraucht Software legal?

Einzelne wichtige IT-Compliance Anforderungen: Private Nutzung der IT-Infrastruktur (E-Mail und/oder Internet)

- Private Nutzung der Unternehmens IT generiert Regelungsbedarf:
  - Arbeitgeber als TK-Anbieter (Provider) nach § 3 Nr. 5 TKG.
  - Einschränkung der Kontrollmöglichkeiten (Spam-Abwehr, Malware-Abwehr, Kontrolle/Erstellung von Logs).
  - Zugriff auf E-Mail-Account.
  - Fernmeldegeheimnis (§ 88 TKG).
  - Betriebliche Übung durch Duldung.

- Ist Nutzung erlaubt (z.B. auch durch Duldung/betriebliche Übung) ist eine Einwilligungserklärung des Beschäftigten mit einer Nutzungsvereinbarung (ggf. durch Betriebsvereinbarung) unerlässlich:
  - Einzelgesprächsnachweise.
  - Zentraler Spam-Filter, Blacklisting.
  - URL-Filter.
  - E-Mail Archivierung.
  - Löschung/Nutzung von E-Mail-Accounts (bei Ausscheiden).

- Einwilligung von Beschäftigten ist arbeitsrechtlich hinsichtlich der Freiwilligkeit problematisch und jederzeit widerrufbar; Einwilligung durch Betriebsvereinbarung nicht möglich.

Einzelne wichtige IT-Compliance Anforderungen: Nutzung privater IT-Geräte (BYOD)

- BYOD ist nur mit erheblichem Aufwand umsetzbar:
  - Konzepterstellung.
  - Schaffung technischer Voraussetzung (Sandbox, MDM).
  - Rechtliche Aspekte, die zu lösen sind:
    - Vermischung privater und geschäftlicher Daten.
    - Eigentum am Gerät <-> Verfügungsrecht der Daten.
    - Haftung für Sicherheitslücken.
    - Umsetzung von Compliance-Anforderungen (z.B. handels- und steuerrechtliche Aufbewahrungspflicht, Adressbuchvermischung).
    - Lizenzrechtliche Probleme (Dienste/Apps/Software teilweise nur privat kostenlos).

- Überdenken der Unternehmensstrategie bei BYOD:
  - Sind Vorteile durch Effizienz, Kosteneinsparung, Mitarbeitergewinnung tatsächlich gegeben.
  - Überwiegen die Vorteile die Nachteile (Dezentrales Sicherheitssystem, Sicherheitskonzept, Regelungs- und Kotrollaufwand).

Einzelne wichtige IT-Compliance Anforderungen: Social Media und Apps

- Nutzung von Social Media hat u.U. Vorteile für das Unternehmen
- Richtlinie zur Nutzung von Social Media ist erforderlich
- Regelung über „Eigentum“ des genutzten Accounts
- Wettbewerbsrechtliche Stolpersteine (Äußerungen Angestellter, Impressum)

Informationssicherheit: Überblick die wichtigsten operativen Maßnahmen zur Informationssicherheit

- Malware Protection (2-Lines of Defense Konzept)
- Rechtekonzept und technische Datenabschottung (z.B. HR-Abteilung eigenes Netzwerk/eigenen Server)
- Backup und Desaster-Recovery Konzept
- Restriktive Konfiguration
- Regelmäßige Softwareupdates sowie Ausmusterung veralteter Software (Windows XP)
- Zeitgemäße Firewall
- Sandbox Verfahren (z.B. bei BYOD)
- Datenverschlüsselung bei Kommunikation oder Speicherung sensibler Daten
- Verwendung von Protokollierungen
- Abschottung von Entwicklungs-, Test und Produktivumgebungen

Informationssicherheit: Überblick die wichtigsten organisatorischen Maßnahmen zur Informationssicherheit

- Sicherheits-Policy für das Unternehmen als oberste Direktive und Zieldefinition.
- Informationssicherheits-Richtlinie.
- Mitarbeiter Kompetenzen und Sensibilisierung vorantreiben (Schulungen).

Problem: Wie bekommt man das alles in den Griff?

- Viele Anforderungen, die teilweise auch im Unternehmen nicht identifiziert sind
- Anforderungen ändern sich oder kommen neue hinzu
- „Wald-Bäume“-Problem: Wo fange ich an und wo soll das enden?

IT-Compliance durch Einführung eines Information Security Management System (ISMS)

- Ziele eines ISMS:
  - Definition der Anforderungen an die Informationssicherheit
  - Steuerung und Kontrolle Informationssicherheit
  - Aufrechterhalten der Informationssicherheit
  - Ständige Verbesserung der Informationssicherheit

- Durch Einführung eines ISMS werden die IT-Compliance Anforderungen definiert, identifiziert und gesteuert

- Implementierung und Führung durch einen Informationssicherheitsbeauftragten (ISM; CISO)

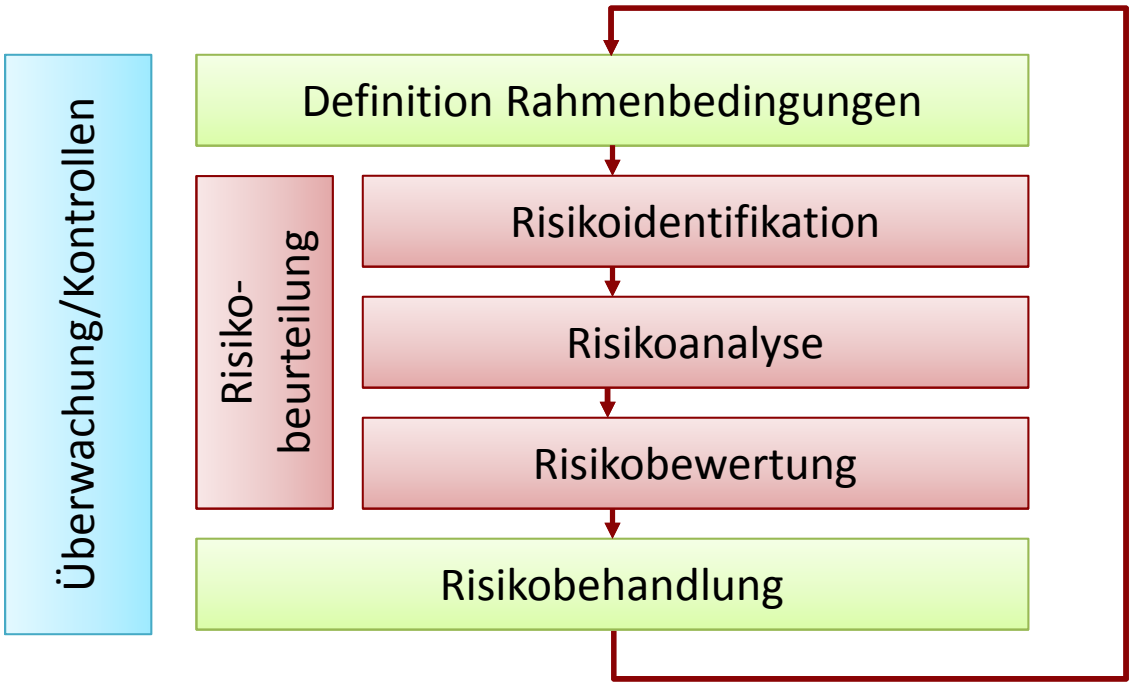
Implementierung eines ISMS: Überblick

- Management Rückhalt sicherstellen
- Erstellen einer ISMS-Policy als oberste Direktive
- Erstellung eines Risikomanagement-Systems (RMS), insbesondere:
  - Definition einer Risikopolitik-Strategie basierend auf der ISMS-Policy
  - Organisationsdefinition des RMS
  - Identifizierung der Unternehmenswerte (Assets)
  - Prozessfestlegung: Identifizierung, Bewertung, Steuerung und Überwachung der Risiken
- Umsetzung und Implementierung (Plan Do Check Act)

Die Implementierung ist ein Projekt

ISMS ist ein Prozess

Implementierung eines ISMS: Der Risikomanagement Prozess



Risikomanagement: Risikobehandlung

Risikovermeidung	Unterbindung eines Risikoeintritts durch Verzicht auf die risikobehaftete Handlung. Aber Chancen gehen auch verloren (Abwägung).
Risikominderung	Herabsetzung des möglichen eintretenden Schadens und/oder Verringerung der Eintrittswahrscheinlichkeit bis zur Risikoakzeptanz.
Risikotransfer (Überwälzung)	Dritter übernimmt die Schadenauswirkungen bei Eintreten eines Risikos (Versicherung, Outsourcing durch Vertrag mit Risikoübernahme. Kosten-/Nutzenabwägung insbesondere bei Inanspruchnahme von Dritten.)
Risikoakzeptanz	Vertretbares Restrisiko ist/wird erreicht (z.B. durch Minderung, niedrigen Schäden oder Eintrittswahrscheinlichkeiten, aber auch Begründung einer höhere Risikobereitschaft)

ABER IMMER: Risiken behandeln. Ignorieren ist keine zulässige Risikobehandlung

Wem die Haftungsreduzierung nicht ausreicht …
Nutzen durch IT-Compliance und ISMS

- Bessere Prozesseffizienz durch regelmäßige Prüfung führt zu Wettbewerbsvorteilen
- Verhinderung negativer Unternehmenswahrnehmung
- Nachweis der Compliance als Voraussetzung für Aufträge
- Sicherheit von Daten als Marketingkriterium in der Unternehmens-Kommunikation
- Transparenz
- Nachhaltiges Unternehmens-Management
- Bessere Einschätzung von Risiken für das Unternehmen
- Kosteneinsparungen (z.B. Lizenzmanagement)

Vielen Dank …

… für Ihre Aufmerksamkeit!

Noch Fragen?