Luther

Rechtsanwaltsgesellschaft mbH

Rechtliche Aspekte von IT-Compliance

Dr. Michael Rath

Agenda

I. Compliance: Überblick

- ➔ Was ist Compliance?
- ➔ Wo ist Compliance geregelt?
- ➔ Wen betrifft Compliance?
- ➔ Welche Konsequenzen drohen bei Nichteinhaltung?

II. Compliance-Anforderungen in der IT

- ➔ Status Quo von IT-Compliance am Beispiel IT-Security
- ➔ Gesetzliche Anforderungen und sonstige Richtlinien
- ➔ IT-Standards

III. Praktische Umsetzung von IT-Compliance

IV. Fazit und Diskussion

I. Compliance – Überblick

"*Der Beitrag rührt mal ordentlich die Compliance-Soße durch und sorgt dafür, dass die Reste an den Rändern kleben bleiben.*"

Compliance – Überblick (1)

Was ist Compliance?

- **Wikipedia:** ”Die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien”
- Versuch einer Definition: „*Compliance ist die Gesamtheit aller organisatorischen Aufsichts-, Schulungs- und Kontrollmaßnahmen der Geschäftsleitung, einschließlich der Einrichtung eines Berichts- und Dokumentationswesens, welche einen Verstoß des Unternehmens gegen gesetzliche Pflichten verhindern sollen*.“
- Compliance als Bestandteil der „Corporate Governance“ („verantwortungsvolle Unternehmenssteuerung durch die Geschäftsführung“)

Compliance – Überblick (2)

Was ist Compliance?

- Befolgung und Einhaltung von „**Spielregeln**“, also Gesetze, Richtlinien, Verordnungen, aber auch Branchen-Standards und Beachtung von Anforderungen des Qualitätsmanagements
- Regelverstoß kann „bestraft“ werden: Risiken für das Unternehmen und die Geschäftsführung
- proaktive Vermeidung von Regelverstößen durch Sicherheits- und Risikomanagement: Risiken erkennen und bewerten
- **Risikomanagement heißt Risiken beherrschen / reduzieren, nicht zwingend Risiken vermeiden.**

Compliance – Überblick (3)

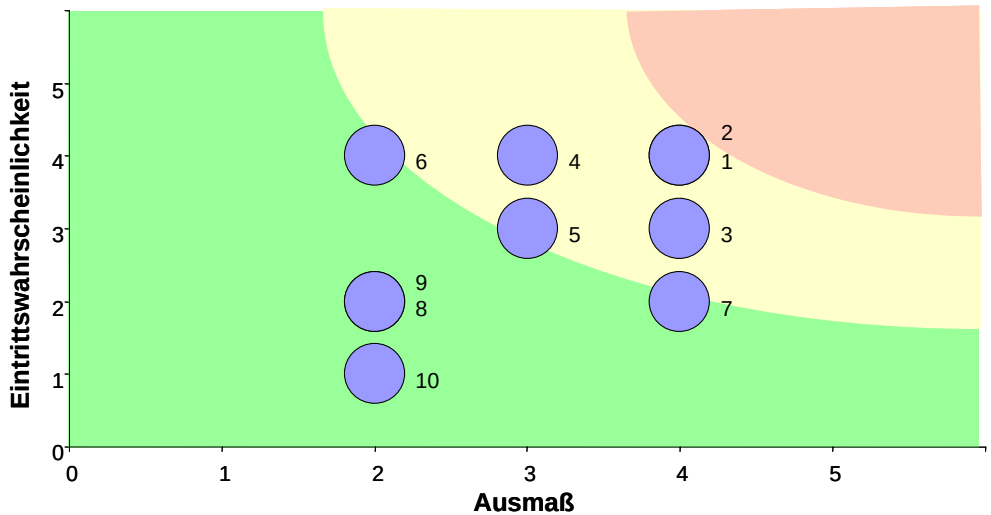
Was ist Compliance?

- ➔ Risk Assessment auf für die IT: neu ist das nicht!
- ➔ Risikoanalyse umfasst:
  - Risikoidentifikation
  - Risikoanalyse
  - Risikobewertung
  - Risikosteuerung
- ➔ Risikosteuerung ist Versuch der Schadensminderung und - vermeidung (immaterielle Schäden: Imageverlust, negatives Rating, Folgeschäden: entgangene Aufträge)

Luther

Compliance – Überblick (4) „Risk Log“

Eintrittswahr-scheinlichkeit	Beschreibung (1-5)	Schadens-höhe	Beschreibung (1-5)
1	Sehr unwahrscheinlich	1	Unbedeutend Risiken, die den Unternehmenserfolg nicht spürbar beeinflussen
2	Unwahrscheinlich	2	Mittel Risiken, die eine spürbare Beeinträchtigung des Unternehmenserfolgs bewirken
3	Möglich	3	Bedeutend Risiken, die den Unternehmenserfolg stark beeinträchtigen
4	Wahrscheinlich	4	Schwerwiegend Risiken, die den Unternehmenserfolg erheblich beeinträchtigen
5	Sehr wahrscheinlich	5	Bestandsgefährdend Risiken, die den Fortbestand des Unternehmens gefährden



Compliance – Überblick (5)

Wo ist (IT-) Compliance geregelt?

- Unternehmensorganisationsregeln (KonTraG, UMAG, HBG, Basel II, etc.)
- Arbeitsrecht (BetrVG)
- Steuerrecht (AO, UStG)
- Buchhaltung, Rechnungslegung, Prüfung (HGB, GoB, GoBS, GDPdU; IFRS, SOX 404)
- Datenschutz / Datensicherheit (IT-Security)
- EU-Vorgaben
- Sektorspezifische Vorgaben

Luther

Corporate Governance (einschl. Deutscher Corporate Governance Kodex)

IT-Compliance

IT-Governance

Gesetzliche / Behördliche Anforderungen

Selbstregulierung

Sektorspezifische Anforderungen

	Steuer-recht	Daten-schutz	Anleger-schutz	Sonstige Gesetze und Verordnungen	Experten	Industrie	Finanzdienst-leister	Medizin	u.w.m.
D	- UStG / SigG, SigV - AO BaFin: - GDPdU - GOB - GoBS	- BDSG - TMG - TKG - UrhG (GoBS/ GDPdU) - ZKDSG	- HGB - KonTraG - AktG - UMAG - IFRS	- BetrVG - BildSch ArbVO - UWG - SGB - SRVwV - BGB - VwVfG - StGB - ElektroG	- IDW FAIT - BSI - AWV	- ITIL - HBVI - ISO	BaFin: - RS 11/2001 Outsourcing - RS 18/2005 MaRisk - KWG - WpHG Umsetzung Basel-II	- MPG	- PCI DSS - AIS - CISP - SDP
EU / Intern. (USA)	EU-Richtlinie Vorratsdaten-speicherung - Tread Act - DoD 5015.2 - NERC - Whistleblowing	- Gramm-Leach-Bliley Act (GLBA)	- IASB - IAS - IFRS - IFRIC - SOX - EU-Anti-Terror-VO -US Patriot Act -- Security Breach Information Act			-COSO - CobiT	- Basel II - Solvency II - Banken-RiLi - Kapital-adäquanz-RiLi - FISMA - GLBA	- HIPAA - FDA	

Compliance – Überblick (6)

Was droht bei Verstößen gegen Compliance-Anforderungen?

- Haft, Geldbußen, Hausdurchsuchungen, negative Presseberichterstattung
- Bußgeldverfahren wegen Aufsichtspflichtverletzung gegen geschäftsführende Organmitglieder
- Zivilrechtliche Ansprüche gegen Organe der Gesellschaft (§§ 91, 93, 116 AktG)
- Abschöpfung des „gesamten wirtschaftlichen Wertes“ durch Verfall (§§ 73 StGB, 29 a OWiG)
- Schadensersatzansprüche von Wettbewerbern (§ 33 GWB)
- Steuerliche negative Folgen (Abzugsverbot, Schätzung, Mitteilungspflicht an StA), gewerberechtliche Unzuverlässigkeit
- Negative Folgen für das Rating des Unternehmens (Basel II)
- Nationale Sperre des Unternehmens von öffentlichen Aufträgen (Einhaltung von Compliance als Wettbewerbsfaktor)
- Internationale Sperre (Blacklist der Weltbank und anderer Institute)

Compliance – Überblick (7)

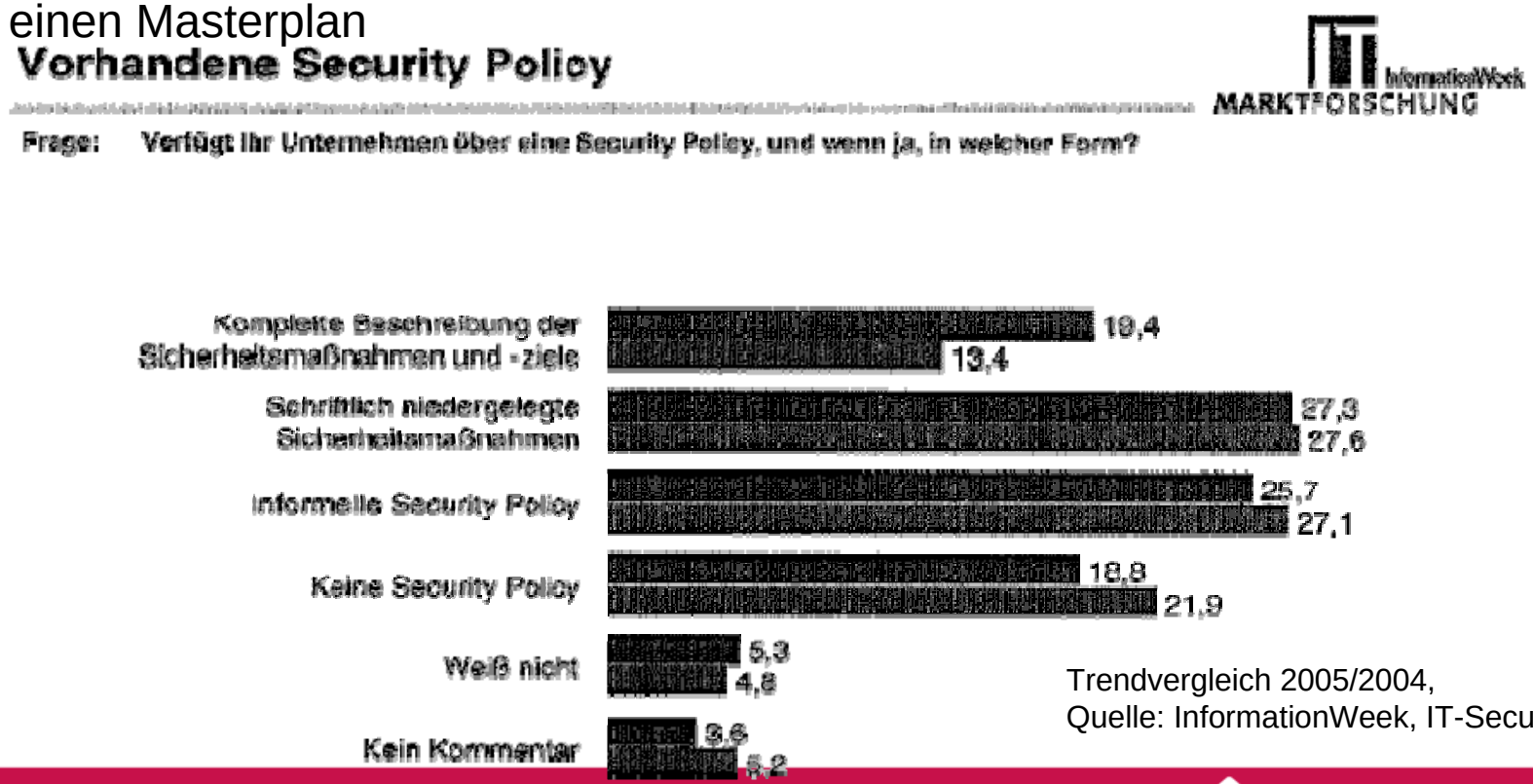
Wen betrifft IT-Compliance?

- Primärer Adressatenkreis von Compliance: Unternehmensleitung, also Vorstand, Aufsichtsrat, Geschäftsführer –> ungenügende Beachtung der §§ 91 Abs. 2 AktG, 43 Abs. 1 GmbHG = Pflichtverletzung der Unternehmensleitung
- Nicht vollständig delegierbare Aufgabe der Unternehmensleitung, auch wenn die konkrete Umsetzung der Compliance-Anforderungen durch Mitarbeiter oder Dritte erfolgt
- Leitende Mitarbeiter des Unternehmens haften auch dann, wenn IT-Compliance zum Bestandteil arbeitsvertraglicher Pflichten gemacht wird (IT-Administrator, Datenschutz-beauftragter, CIO, etc.)
- Aufsichtsbehörden übernehmen Kontrolle der Einhaltung öffentlicher Vorschriften (BaFin, Datenschutzbehörde, Gewerbeamt etc.)
- Auch externe (IT-) Dienstleister müssen vertraglich zur Einhaltung von IT-Compliance verpflichtet werden; Unternehmen behält weiterhin Auswahl- und Überwachungspflichten (vgl. etwa § 11 BDSG, BaFin RS/2001)

II. Compliance in der IT

IT-Compliance – Der Status Quo (1)

- Status Quo von IT-Compliance am Beispiel IT-Security: Lediglich 63 % der mittelständischen Unternehmen haben für Datenverlust nach Systemabsturz einen Masterplan

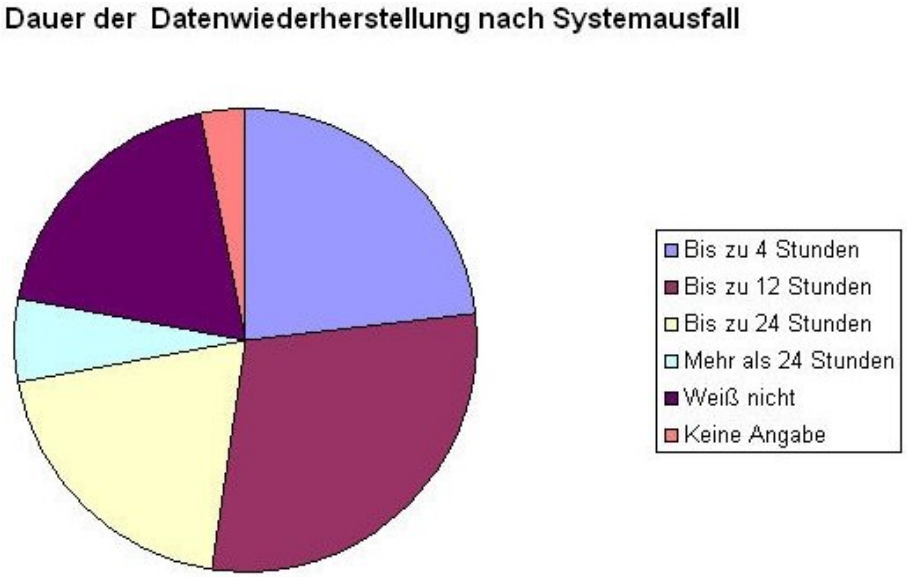


Trendvergleich 2005/2004,
Quelle: InformationWeek, IT-Security 2005

IT-Compliance – Der Status Quo (2)

Frage: Funktioniert Ihr Sicherheitskonzept noch?

- Nur 43 % mittelständischer Unternehmen testen ihre Sicherheitskonzepte regelmäßig
- 20% der Unternehmen brauchen bis zu 24 Stunden zur Datenwiederherstellung



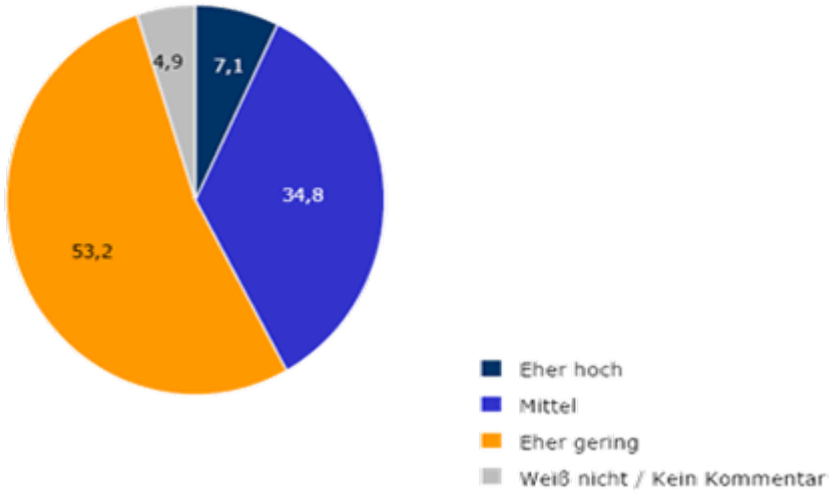
Quelle: Smart Research: IT-Storage im Mittelstand 2006

IT-Compliance – Der Status Quo (3)

- Dennoch fühlt sich die Mehrheit der Unternehmen sicher

Einschätzung des Sicherheitsrisikos

Frage: Wie schätzen Sie das derzeitige Sicherheitsrisiko in Ihrem Unternehmen ein?



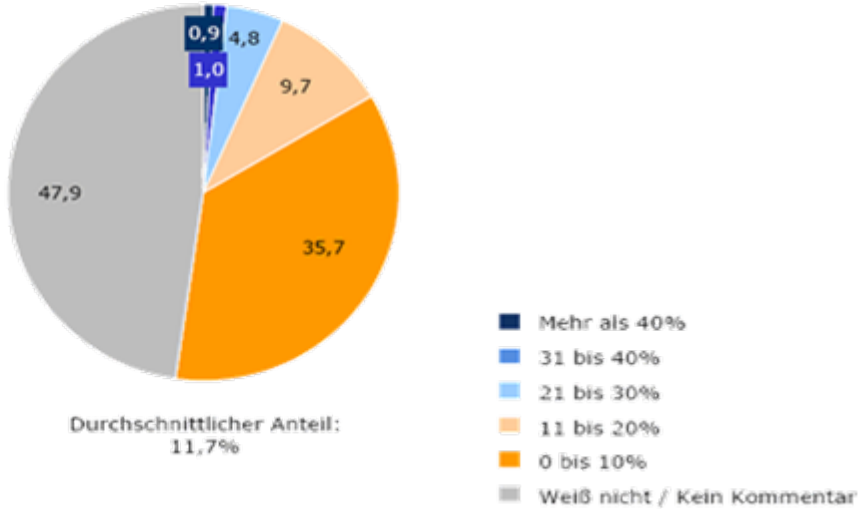
Quelle: Informationweek, IT-Security 2006

IT-Compliance – Der Status Quo (4)

- … und investiert nur durchschnittlich 11,7 % des IT-Budgets in IT-Security

Prozentualer Anteil des IT-Security-Budgets am IT-Budget

Frage: Welcher Prozentsatz des gesamten IT-Budgets Ihres Unternehmens ist für die Informationssicherheit vorgesehen?



Quelle: Informationweek, IT-Security 2006

IT-Compliance – Der Status Quo (5)

- Dabei ist den meisten bewusst, dass der Schutz privater Daten und auch IT-Compliance wesentliche Unternehmensprioritäten darstellen (können)

Quelle: Informationweek Outlook 2007, Jan. 2007

IT-Compliance – Argumente dafür (1)

- IT als zentrales und zugleich anfälliges Nervensystem des Unternehmens
- IT-Risiken: Beurteilung von Eintrittswahrscheinlichkeit und Schadensrisiko (Risk Assessment und Risikomanagement)
- Potentieller Schaden: IT-Systemausfälle können Unternehmen vollständig lahm legen
  - keine Auftragsannahme
  - Ausfall der Produktionssteuerung
  - keine Rechnungsstellung
  - keine Verbuchung eingehender Zahlungen
  - Folgeschäden durch verspätete eigene Zahlungen
- Kunden „bestrafen“ Unternehmen, die fahrlässig mit ihren persönlichen Daten umgehen
  - ca. 20 % der betroffenen Kunden brechen die Geschäftsbeziehung sofort ab
  - ca. 40 % stellen entsprechende Überlegungen an
    (Quelle: PGP Cooperation, Lost Customer Information Study, 2005)

IT-Compliance – Argumente dafür (2)

- Im Unternehmen kann IT-Compliance (neben Einhaltung von Gesetzen) zu Prozessoptimierung und Kosteneinsparung führen, wenn die IT-Architektur die Unternehmensprozesse nachbildet
  - Analyse ist optimale Basis für nachfolgende Optimierung zu effizientem Prozessmanagement
  - Kann Basis für die Einführung einer SOA („Service orientierte Architektur“) sein
  - redundante Datenbevorratung wird aufgedeckt, nicht genutzte Überlizenzierungen werden identifiziert
  - Budgetierung der Wartungsverträge wird erleichtert
  - Asset-Management und Lizenzmanagement
- IT-Compliance bedeutet auch Nutzung rechtskonformer IT-Systeme (Lizenzmanagement)

IT-Compliance – Anforderungen (1)

Gesetzliche Anforderungen mit völlig unterschiedlichen Zielrichtungen:

- Unternehmensorganisation (KonTraG = § 91 Abs. 2 AktG und UMAG = § 93 Abs. 1 S. 2 AktG): Pflicht zur Einrichtung und Nutzung eines Risikofrüherkennungssystems / IKS
- IT-Security (BDSG, TMG, §§ 91 ff. TKG, 77 ff. SGB X, 2 Abs. 2 BSIG): Datenschutz und Datensicherheit (insbesondere Überwachung von datenverarbeitenden Dienstleistern, Erstellung, Umsetzung und Dokumentation eines Datensicherheitskonzepts)
- Arbeitsrecht: Achtung der Rechte des Betriebsrats (§ 80 BetrVG) und Arbeitsschutzvorschriften (BildschirmarbeitsplatzVO)

IT-Compliance – Anforderungen (2)

- Buchhaltung, Rechnungslegung, Prüfung (§§ 238, 239, 257 HGB; 146, 147 AO, GoB, GoBS, GDPdU, SigG, SigV)
- Berücksichtigung in Lagebericht (§§ 289, 315, 317 Abs. 2 HGB)
- International Financial Reporting Standards (IFRS): IT-Systeme müssen aktuelle und „historische“ Daten, wie Zeitwerte, Leistungen an Arbeitnehmer, Segmentinformationen etc. berücksichtigen
- Sarbanes Oxley Act (SOX), v.a. Section 404: Dokumentation und Bewertung von Kontrollmechanismen in IT-Systemen zur Verarbeitung von Finanzdaten nach COSO-Modell („Committee of the Sponsoring Organizations of the Treadway Commission“) –> Konkretisierung in CobiT; erforderlich ist nach SOX rin „Internal Control Report“ und „Certification“ durch Vorstand

III. Praktische Umsetzung von IT-Compliance

a) Buchführungs- und Aufbewahrungspflichten

IT-Compliance - Buchführung

- Gesetzliche Anforderungen an IT-gestützte Handelsbücher (§§ 238, 239, 257 HGB)
- Beachtung der „Grundsätze ordnungsgemäßer Buchführung (GoB)“ und damit verbundener Sicherheitsanforderungen
- Nachvollziehbarkeit der Verfahren und Geschäftsvorfälle
- Einhaltung von Aufbewahrungsvorschriften
- Konkretisiert durch Stellungnahmen des Instituts der Wirtschaftsprüfer (IDW)

IT-Compliance – Aufbewahrungspflichten

- Steuerrecht enthält umfassende Aufbewahrungspflichten (§ 147 AO), insbesondere für
  - Bücher, Aufzeichnungen, …
  - Jahresabschlüsse, Buchungsbelege, …
  - Bilanzen nebst Arbeitsanweisungen
  - Handels- und Geschäftsbriefe (Postein- und –ausgang)

  ➔ **Problem: Dokumenten- und E-Mail-Management (schätzungsweise 400.000 E-Mails weltweit pro Sekunde)**

- Aufbewahrungsdauer:
  - **10 Jahre** für Buchungsbelege, Bücher, Aufzeichnungen, Bilanzen und Jahresabschlüsse
  - **6 Jahre** für Handels- und Geschäftsbriefe, sonstige Unterlagen, soweit für die Besteuerung wichtig

IT-Compliance – GoB (1)

- **Grundsätze ordnungsgemäßer Buchführung (GoB)**
  - **Übersichtlichkeit:** Sachverständiger Dritter muss sich in angemessener Zeit einen Überblick über Geschäftsvorfälle und Vermögenslage des Unternehmens verschaffen können
  - **Vollständigkeit:** Buchungspflichtige Geschäftsvorfälle sind richtig und vollständig zu erfassen; gilt auch für Vermögens- und Ertragslage
  - **Ordnung:** Richtige Zuordnung von Geschäftsvorfällen
  - **Zeitgerechtheit:** Geschäftsvorfälle sind zeitgerecht zu erfassen
  - **Nachprüfbarkeit:** Nachprüfbarkeit der Buchungen durch Belege (durchnummerierte Rechnungen, Quittungen etc.)
  - **Richtigkeit:** Nachträgliche Veränderungen sind auszuschließen (z. B. Korrektur für Fehlbuchungen)

IT-Compliance – GoB (2)

- GoB gelten nicht nur für Kapitalgesellschaften, sondern für jeden Kaufmann gem. §§ 238 ff. HGB u. §§ 145 ff. AO
- Verstoß gegen Buchführungspflichten kann zudem zu strafrechtlichen Folgen führen, § 283 b StGB:
  - „Mit **Freiheitsstrafe bis zu 2 Jahren** oder mit **Geldstrafe** wird bestraft, wer:
    1. Handelsbücher, zu deren Führung er gesetzlich verpflichtet ist, zu führen unterlässt oder so führt oder verändert, dass die Übersicht über seinen Vermögensstand erschwert wird,
    2. Handelsbücher oder sonstige Unterlagen, zu deren Aufbewahrung er nach Handelsrecht verpflichtet ist, vor Ablauf der gesetzlichen Aufbewahrungsfristen bei Seite schafft, verheimlicht, zerstört oder beschädigt und dadurch die Übersicht über seinen Vermögensstand erschwert….“

IT-Compliance – GoB (3)

- Für IT-Systeme ergeben sich daraus Konsequenzen für:
  - Ausgestaltung des Buchführungsverfahrens
    = Abbildung der Prozesse in der IT
  - Richtigkeit der rechnungslegungsrelevanten Programmabläufe und Verarbeitungsregelungen
    = Korrektheit und Fehlerfreiheit der IT-Anwendungen
  - Schutz der IT-Infrastruktur = Systeme und Netze
  - Sicherheit der rechnungslegungsrelevanten Daten

IT-Compliance – GoBS (1)

- **Grundsätze ordnungsmäßiger DV-geschützter Buchführungssysteme**
- GoBS führen GoB im IT-Umfeld weiter, beinhalten konkrete Umsetzungsregelungen mit Blick auf Abgabenordnung
- Wesentliche Grundsätze:
  - Errichtung eines internen Kontrollsystems (IKS)
  - Teil der Pflicht-Dokumentation für DV-Buchführungssystem zu dessen Verständnis
  - Beschreibung der laut Programm zugelassenen Systemänderungen durch Anwender
  - Maschinenlesbare Auswertung muss sichergestellt sein, § 147 AO
  - DV-System muss die Unveränderbarkeit des Datenbestandes gewährleisten

IT-Compliance – GoBS (2)

- Probleme
  - Wechsel des EDV-Systems: Daten müssen auch nach Wechsel des EDV-Systems noch über gesamte Dauer der Aufbewahrungspflicht jederzeit maschinell auslesbar bleiben.
  - Dies kann bei inkompatiblen Systemen bedeuten, dass bereits „ausgemusterte“ EDV-Systeme über die gesamte Dauer aufbewahrt werden müssen
  - „Inhaltliche Datensicherheit“ – Ausschluss von Änderungen an Tabellen und Stammdaten
  - „Tatsächliche Datensicherheit“ - Kein unberechtigter Zugriff auf sensible Unternehmensinformationen, Daten müssen stets auffindbar und sicher vor Vernichtung und Diebstahl sein

b) IT-Security

IT-Compliance – IT-Security (1)

- IT-Security als Teil von IT-Compliance (vgl. § 2 Abs. 2 BSIG: Sicherheit in der Informationstechnik bedeutet die Einhaltung bestimmter Sicherheitsstandards)
- Gesetzliche Forderungen zur IT-Security ergeben sich auch und vor allem aus:
  - Sorgfaltspflichten des Vorstandes gem. §§ 93 Abs. 1 AktG, 43 Abs. 1 GmbHG
  - Buchführungsanforderungen
  - Datenschutz im Sinne von Datensicherheit (§ 9 BDSG i.V.m. Anlage) als auch materieller Datenschutz
  - Vertraglichen Pflichten
  - IT-Security ist Element von Corporate Governance-Strukturen und Bestandteil des gesetzlich geforderten Risikomanagements

Luther

IT-Compliance – IT-Security (2)

- Buchführungspflichten:
  - Jeder Kaufmann muss bei der Führung seiner Handelsbücher und der Aufbewahrung seiner Unterlagen in elektronischer Form die Sicherung der IT-Systeme gewährleisten:
    - § 239 Abs. 4 S. 2 HGB
      „Bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern muss insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist **verfügbar sind** und jederzeit innerhalb **angemessener Frist** lesbar gemacht werden können."
    - § 261 HGB
      „Wer aufzubewahrende Unterlagen nur in Form einer Wiedergabe auf einem Bildträger oder auf einem anderen Datenträger vorlegen kann, ist verpflichtet, auf seine Kosten **diejenigen Hilfsmittel zur Verfügung zu stellen,** die erforderlich sind, um **die Unterlagen lesbar zu machen;** soweit erforderlich hat er die Unterlagen auf seine Kosten auszudrucken oder ohne Hilfsmittel **lesbare Reproduktionen beizubringen.**"

IT-Compliance – IT-Security (3)

- Datenschutz als Teil von IT-Security:
  - „Materieller“ Datenschutz verlangt eine ausreichende Sicherung personenbezogener Daten vor unbefugtem Zugriff und Weitergabe
  - Datensicherheit: Personenbezogene Daten und Sozialdaten sind durch „angemessene“ **technische und organisatorische Maßnahmen** zu schützen (§§ 9 BDSG, 78 a SGB X): Kontrolle des Zutritts, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag, Verfügbarkeit, Datentrennung
  - Anbieter von Telekommunikations- und Telediensten müssen durch entsprechende **technische und organisatorische Vorkehrungen** die von ihnen und den Nutzern verwendeten Daten schützen
    ➔ Betrifft auch Angebot von Internetzugang und Internetdiensten z. B. betriebsintern für Mitarbeiter (Brennpunkt: Vorratsdatenspeicherung)
  - § 9 a BDSG: Freiwilliges Datenschutz-Audit möglich
  - Whistleblowing: „Petze“ über Hotline – Art. 29-Gruppe

IT-Compliance – IT-Security (4)

- Bedeutung von IT-Compliance und IT-Security für Jahresabschlussprüfung:
  - Bei börsennotierter AG ist der Wirtschaftsprüfer gesetzlich zur Kontrolle der Risikofrüherkennungssysteme (also auch der IT-Security-Systeme) verpflichtet, vgl. § 91 Abs. 2 AktG, § 317 Abs. 4 HGB
  - Auch bei allen anderen Gesellschaften sind Systeme, welche die Risiken künftiger Entwicklungen berühren, für den Lagebericht zu prüfen (§§ 289, 315, 317 Abs. 2 HGB)
  - Bei Versicherungsunternehmen ist die IT-Systemprüfung zwingender Bestandteil der Jahresabschlussprüfung (siehe auch IDW PS 260, PS 330)
  - Auswirkungen auf Rating durch Basel II

IT-Compliance – IT-Security (5)

- IT-Standards füllen unbestimmte Rechtsbegriffe aus
  ➔ BSI Grundschutzkataloge (ehemals Grundschutzhandbuch) vs. andere IT-Standards (ITIL, CobiT, COSO, etc.)
- Standards legen Methoden zur Ermittlung des aktuellen Stands der Technik für IT-Sicherheitsmaßnahmen fest
- Empfehlungen in den IT-Grundschutzkatalogen für Standard-Sicherheitsmaßnahmen bei typischen IT-Systemen
- Ziel: Geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen, um ein angemessenes und ausreichendes Sicherheitsniveau für IT-Systeme zu erreichen

c) GDPdU

IT-Compliance – GDPdU (1)

- **Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen,** Seit 2002 darf die Finanzbehörde die DV-geführte Buchführung des Steuerpflichtigen durch Datenzugriff prüfen, § 147 Abs. 6 AO
- Gegenstand der Prüfung sind alle nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen
- Finanzbehörde bekommt Zugriff auf **steuerlich relevante Daten**
  - ➔ insbesondere alle Daten der **Finanzbuchhaltung,** der **Anlagenbuchhaltung** und der **Lohnbuchhaltung**, die für die Besteuerung von Bedeutung sind
  - ➔ Unternehmer muss/kann selbst entscheiden, was steuerlich von Bedeutung ist
  - ➔ Datenschutz und berufsspezifische Verschwiegenheitsregeln sind zu beachten
  - ➔ Für versehentlich überlassene Daten besteht kein Verwertungsverbot

IT-Compliance – GDPdU (2)

- Digitale Prüfungsmethode tritt **neben** die Möglichkeit der herkömmlichen Prüfung im Rahmen steuerlicher Außenprüfung ➔ Finanzbehörde kann Prüfungsmethode nach verhältnismäßigem Ermessen wählen und ggfls. auch wechseln
- Bei Verstoß gegen GDPdU können im Einzelfall erhebliche „Strafen“ verhängt werden: Bußgeld, Zwangsmittel, Schätzung
- DV-Buchführungssysteme müssen sich nach GDPdU richten ➔ Finanzbehörde vergibt aber keine offizielle Zertifizierung als „GDPdU-konform“
- **Maschinelle Auswertbarkeit:** wahlfreier Zugriff auf alle gespeicherten Daten einschl. Stammdaten und Verknüpfungen mit Sortier- und Filterfunktionen unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit
- Steuerbehörde akzeptiert keine Reports oder Druckdateien, die bereits vorgefilterte Datensätze anstatt der Originaldaten enthalten

IT-Compliance – GDPdU (3)

- Digitalisierte Unterlagen müssen nach den **GoBS** archiviert und digital prüfbar zur Verfügung gestellt werden
  - Originalzustand der Daten muss erkennbar sein: Speicherung auf Datenträger, der Änderungen nicht mehr zulässt (CD-R)
  - Verschlüsselte Daten sind verschlüsselt und entschlüsselt inkl. verwendetem Schlüssel aufzubewahren
  - Bei Konvertierung in unternehmenseigenes Format sind beide Versionen zu archivieren
  - Bei elektronischen Abrechnungen ist die qualifizierte elektronische Signatur als Bestandteil der Rechnung mitzuspeichern

  Sonderfall: Internationale Anerkennung elektronischer Rechnungen
- **Bereits digitalisierte Unterlagen** sind auf maschinell verwertbaren Datenträgern zu archivieren, § 146 Abs. 5 AO
  - Ausschließlich ausgedruckte Form oder Mikrofilm reicht nicht
  - Maschinell nicht auswertbare Formate (z. B. PDF und TIFF) genügen nicht
  - gilt auch für E-Mails
- **Bereits vorhandene Unterlagen in Papierform** (z. B. Eingangsrechnungen) müssen nicht digitalisiert werden

d) IT-Compliance: Standards

IT-Compliance – Standards (1)

Standards beim betrieblichen Einsatz von IT-Systemen:

- BSI Grundschutzkataloge, ITIL (Information Technology Infrastructure Library), DIN, ISO 27000 ff., CobIT (Control Objectives IT), BS 15000 (British Standard 15000), CC (Common Criteria, jetzt: ISO 15408), Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW PS-330), BaFin-Rundschreiben, etc.
- Standards füllen gesetzliche Vorgaben / unbestimmte Rechtsbegriffe aus
- Einhaltung dieser Standards kann zumindest als Auslegungshilfe herangezogen werden und damit Maßstab für Sorgfalts-/ Pflichterfüllung bilden („Sorgfalt eines ordentlichen Kaufmanns“)
- IT-Standards werden häufig zu Vertragsbestandteilen gemacht, bei Nichteinhaltung drohen Vertragsstrafen (Empfehlung SEC: Anwendung der „Statements of Auditing Standards SAS 70 Type II“)

IT-Compliance – Standards (2)

- Die Vielfalt der technischen Möglichkeiten in der IT lassen in der Praxis häufig mehrere gleichwertig nebeneinander stehende Möglichkeiten zur Erreichung desselben Ziels zu
  - ➔ Dadurch wird Ermittlung des aktuellen Standards als Benchmark für ordnungsgemäß organisierte IT schwer ermittelbar
- In der Praxis haben sich mehrere technische Standards als „branchenüblich“ herausgebildet, anhand derer sich die Qualität der IT-Organisation messen lassen kann
- **Beispiele:**
  - ITIL / BSI-Standards
  - ISO 17799 / ISO 27000 ff
  - CobIT (Kontrollmodell in Anlehnung an COSO-Report)
  - BS 15000 / ISO 20000
  - Audit-Standards SAS 70 Reports Type I / II für SOX-Compliance

IT-Compliance – Standards (3)

- **ITIL = Information Technology Infrastructure Library**
  - von britischen Regierungsbehörden entwickelt und in Büchern definiert, die vom Office of Gouvernement Commerce seit 1989 herausgegeben werden
    - 1. Version der Library 1995 abgeschlossen; Version 2 wurde 1999 bis 2003 herausgegeben, aktuelle Version 3 soll 2007 veröffentlicht werden
  - Beschrieben werden Modelle und Organisationsformen für IT-Servicemanagement nach „Best-Practice“ Ansätzen
    - In 7 Büchern (+1 Ergänzungsbuch) werden Aufgabenstellungen definiert, die beim Betrieb der IT-Infrastruktur anfallen
      ➔ ITIL beschreibt nicht, **wie** etwas getan werden muss, sondern nur **was** getan werden sollte
  - keine Zertifizierung als „ITIL konform“ möglich
    - aber Zertifizierung nach zugehöriger Norm ISO 20000

IT-Compliance – Standards (4)

- **ISO 27000 ff. (Vorläufer: ISO 17799:2005)**
- Internationaler Standard, der Kontrollmechanismen für die Informationssicherheit beinhaltet
  - entstanden aus britischen Standards der neunziger Jahre, erstmals veröffentlicht im Jahr 2000 als ISO Standard
- beschreibt in 11 verschiedenen Überwachungsbereichen 39 sogenannte Kontrollziele
  - ➔ 130 beschriebene Sicherheitsmaßnahmen sollen helfen, die Kontrollziele zu erreichen
- basiert wie ITIL auf Erfahrungen und Methoden aus der Praxis nach Best-Practice Ansatz
- Wird seit 2005 stufenweise in die verbindlichen Normenreihe ISO 27000 ff. überführt - > jetzt auch Zertifizierung möglich
- Spezial-ISO: etwa ISO 27799 für „Health Informatics“

IT-Compliance – Standards (5)

- **CObIT = Control Objectives for Information and related Technologies**
- Regelwerk für die Beschreibung und Kontrolle von Geschäftsprozessen durch IT
  - 1993 vom internationalen Verband der IT-Prüfer und Auditoren ISACA entwickelt seit 2000 unter Verantwortung des IT-Governance Institute, Schwesterorganisation der ISACA
- CObIT definiert 34 Prozesse zur Verarbeitung von Informationen, Planung von IT-Ressourcen und Erbringung von Services
- In jedem Prozess wird mit beschrieben, wie mit Hilfe von Control Objectives (Steuerungsvorgaben) zuvor definierte Prozessziele erreicht werden können

IT-Compliance – Standards (6)

- **BS 15000 / ISO 20000**
- BS 15000 = British Standard 15000: In UK entwickelter Standard, der Anforderungen für ein professionelles IT-Servicemanagement dokumentiert
- Beschreibt die notwendigen Prozesse („Objectives and Controls“) die notwendig sind um IT-Services in definierter Qualität bereit zu stellen und zu managen
- orientiert sich an den ITIL-Prozessbeschreibungen und ergänzt diese komplementär
- Seit 15. Dezember 2005 in ISO 20000 überführt
  - ➔ Damit besteht erstmals die Möglichkeit, die erfolgreiche Implementierung eines IT-Servicemanagements objektiv zu messen und zu zertifizieren

IT-Compliance – Standards (7)

- Sektorspezifische Vorgaben, etwa für Finanzdienstleister
- IT-Standards durch Rückgriff auf bankenspezifische Vorgaben der §§ 35 a KWG, 33 Abs. 2 WpHG
- Konkretisierung durch Rundschreiben der BaFin
  - RS 11/2001 (IT-Outsourcing)
  - RS 18/2005 (MaRisk – Mindestanforderungen Risikomanagement)
  - Einhaltung BSI-Standards Grundschutz
- Damit können diese Vorgaben ggfls. auch als „Best Practice“ für Unternehmen außerhalb des Finanzdienstleistungssektors Anwendung finden

e) IT-Compliance: Interne Kontrolle

IT-Compliance – Interne Kontrolle

- Gesetzesentwurf zur Änderung des Computerstrafrechtes für Hacking & Co.
- Aber: 80 % der Angriffe erfolgen von innen
- Mögliche Aufklärungsmaßnahmen des Arbeitsgebers
  - Protokollierung von Nutzungen
  - „Scanning“ von Mailboxen oder Festplatten
  - Auswertung von „Log-Files“ etc.
  - Sichtung von Mails, Dokumenten und Dateien
- Differenzierung aus rechtlicher Sicht: der Arbeitgeber als Telekommunikationsanbieter
  - Protokollierung / Auswertung von Nutzungsdaten
  - Kenntnisnahme von Kommunikationsinhalten (Telefonate, E-Mails, Websites, Downloads)

IT-Compliance – Konfliktfelder

- Welcher IT-Standard? BSI vs. ITIL vs. ISO (etc.)
- Komplexität der IT-Standards / teilweise Deckungsgleichheit
- Einhaltung von SOX oder IT-Standards als vertragliche Verpflichtung für Unternehmen, die gar nicht in deren Anwendungsbereich fallen
- Zertifizierung nur für Teilbereiche möglich / Gültigkeitsdauer der Zertifikate (Bsp.: Datenschutz-Gütesiegel, BSI-Aufbaustufen)
- Ständige Änderung von gesetzlichen Anforderungen
- Kosten / Nutzung – Rechnung für Einhaltung von IT-Compliance
- Wo kein Kläger, da kein Richter? 5% der Unternehmen haben bislang Compliance-Projekte umgesetzt ….

IV. Fazit und Diskussion