IT-Compliance – Herausforderung für Unternehmens- und IT-Management

Prof. Dr. Michael Klotz

Information Day
„IT-Compliance“ 16. Juli 2010

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

Gliederung

1. Compliance-Begriff
2. Einordnung in das IT-Management
3. Beispiele von Non-Compliance
4. Risiken
5. Verantwortlichkeiten
6. Managementansatz
7. IT-Compliance-Prozess
8. Angebote des SIMAT

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

Quick-Check:
Müssen Sie wirklich hier sitzen?

fachhochschule stralsund
university of applied sciences
SIMAT STRALSUND INFORMATION MANAGEMENT TEAM

	ja	nein
1. Sie haben Ihre Verträge zur Auftragsdatenverarbeitung entsprechend der BDSG-Novelle überprüft und ggf. anpasst.	☐	☐
2. Sie kennen die neue DL-InfoV und haben sie schon umgesetzt.	☐	☐
3. Sie prüfen die Signaturen der eingehenden elektronischen Rechnungen, dokumentieren die Prüfung und archivieren revisionssicher.	☐	☐
4. Ein Kunde möchte vor Aufnahme der Geschäftsbeziehung die Gliederung Ihres Notfallkonzepts – kein Problem für Sie.	☐	☐
5. Sie sind in der Lage, von außen kommende Angriffe auf Ihre IT zu entdecken.	☐	☐

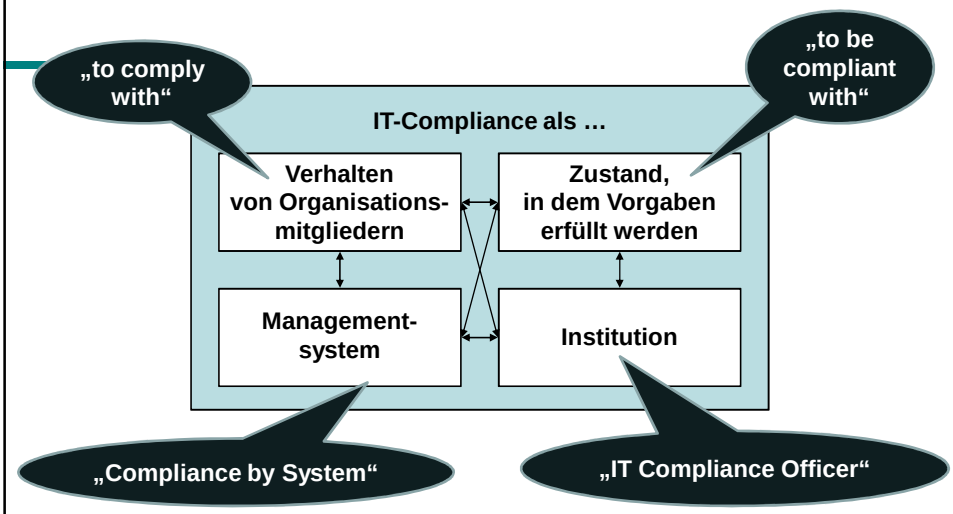
Quick-Check:
Müssen Sie wirklich hier sitzen?

fachhochschule stralsund
university of applied sciences
SIMAT STRALSUND INFORMATION MANAGEMENT TEAM

	ja	nein
7. Ihr Datensicherungskonzept ist aktuell, der gesamten Belegschaft bekannt und seine Einhaltung wird regelmäßig überprüft.	☐	☐
8. Der Betriebsprüfer verlangt Z1-Datenzugriff – für Sie kein Problem.	☐	☐
9. Für das Management Ihrer IT orientieren Sie sich an den führenden Standards, wie ITIL oder Cobit.	☐	☐
10. Sie können zwar 1 bis 9 nicht beantworten, wissen aber, an wen im Unternehmen Sie sich zu wenden haben.	☐	☐

1. Compliance-Begriff
Sichtweisen

fachhochschule stralsund
university of applied sciences



Klotz, Michael: Facetten der IT-Compliance, in: it Service Management, September 2009, Nr. 9, Jg. 4, S. 5

1. Compliance-Begriff

fachhochschule stralsund
university of applied sciences

➔ Compliance ist ein Zustand, der als Ziel nicht erreichbar ist, sondern nur ständig angestrebt werden kann

d. h. Verpflichtung der Vertretungsorgane
➔ Compliance ist Chefsache

Compliance liegt vor, wenn alle für das Unternehmen verbindlich vorgegebenen bzw. als verbindlich akzeptierten Regelwerke nachweislich eingehalten werden.

Welche Regelwerke?

faktische Nachweisbarkeit
➔Bedeutung der Dokumentation

1. IT-Compliance-Begriff

fachhochschule stralsund
university of applied sciences

weite Auffassung

IT-Compliance bezeichnet einen Zustand, in dem alle für die IT des Unternehmens relevanten bzw. als relevant akzeptierten internen und externen Regelwerke nachweislich eingehalten werden.

IT-Compliance bezeichnet einen Zustand, in dem alle für die IT des Unternehmens relevanten, allgemein geltenden rechtlichen Vorgaben nachweislich eingehalten werden („Legal IT compliance“).

enge Auffassung

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

7 / 13

1. Compliance-Begriff
Klassifikation von Regelwerken

fachhochschule stralsund
university of applied sciences

Unternehmensinterne Regelwerke	Rechtliche Vorgaben	Unternehmensexterne Regelwerke
Richtlinien	• Rechtsakte der EU • Internationale Abkommen • Rechtsvorgaben anderer Staaten • Verfassung • Gesetze • Rechtsverordnungen • Erlasse/Satzungen • Verwaltungsvorschriften • In Bezug genommene Regelwerke	Kodizes
Hausstandards		Normen
Verfahrens-anweisungen		Branchen-standards
Service Level Agreements		Verbands-standards
...	Rechtsprechung Verträge	...

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

8 / 13

2. Einordnung in das IT-Management

fachhochschule stralsund
university of applied sciences

- Compliance-Anforderungen betreffen direkt oder indirekt die Unternehmens-IT:

Compliance-Anforderungen stellen sich der IT hinsichtlich …

Schutz	Verfüg-barkeit	Nachvoll-ziehbarkeit	Trans-parenz	Sorg-falt	Organisation

- Compliance-Anforderungen betreffen oft auch das IT-Sicherheits- und das IT-Risikomanagement.

2. Einordnung in das IT-Management
Beispiele

fachhochschule stralsund
university of applied sciences

Schutz	Verfügbarkeit
• Verschiedene Gesetze (**BDSG, TKG**) fordern für personenbezogene Daten Schutz bzgl. Vertraulich-keit und Integrität. • Die **GoBS** fordern u. a. den Schutz von Daten vor nachträglicher Ver-änderung und unbefugter Kenntnisnahme durch Dritte. • …	• Die **GDPdU** verlangen eine revisionssichere Speicherung und Archivierung sowie die Verfügbarkeit der Daten für den sofortigen und unmittelbaren Zugriff durch den Betriebsprüfer. • Die **GoBS** fordern eine steuerlichen Aufbe-wahrungsfristen entsprechende Archivierung. • Im Bereich der **Produkthaftung** sind Auf-bewahrungsfristen für zahlreiche Dokumente, z.B. Konstruktions- und Fertigungsunterlagen, Reklamationsberichte, zu beachten. • …

2. Einordnung in das IT-Management
Beispiele

fachhochschule stralsund
university of applied sciences

Nachvollziehbarkeit	Transparenz
• Das **BDSG** fordert Nachvollziehbarkeit hinsichtlich der Änderung, Löschung und Weitergabe personenbezogener Daten. • Aus **HGB/GoBS** folgt die Notwendigkeit von Verfahrensdokumentationen und Nachvollziehbarkeit durch einen sachverständigen Dritten. • **Basel II** stuft das Unterlassen von Informationspflichten gegenüber Privatkunden als Risiko ein, so dass die erfolgte Information nachvollziehbar dokumentiert werden muss. • …	• Um die Vorgaben von **SOX** Section 404 einhalten zu können, müssen IT-Kontrollen und Dokumentationsstandards eingerichtet/verbessert werden. • **Basell II** stuft das Ausnutzen der eigenen Position als Risiko ein, das durch Transparenz-Maßnahmen, wie z. B. Vier-Augen-Prinzip oder Funktionstrennungen, einzugrenzen ist. • …

2. Einordnung in das IT-Management
Beispiele

fachhochschule stralsund
university of applied sciences

Sorgfalt	Organisation
• Generelle Sorgfaltspflichten für die Unternehmensleitung – und damit auch das für IT verantwortliche Mitglied – resultieren aus dem **AktG** und dem **GmbHG**. Dies betrifft die genannten Strukturen der IT-Governance. • Geschäftsunterbrechungen wegen Ausfall von Hard- und Software ist ein Risiko, das auch existenzbedrohende Auswirkungen haben kann. Derartige Risiken im Rahmen eines Risikomanagements auszuschalten, wir von **Basel II** und **MaRisk** gefordert bzw. ist Gegenstand der Risikofrüherkennung von **KonTraG**. • …	• Das **BDSG** fordert die Einrichtung der Stelle eines Datenschutzbeauftragten. • Um internen Betrug zu verhindern (operatives Risiko nach **Basel II**), sind Funktionstrennungen und Berechtigungskonzepte erforderlich • …

2. Einordnung in das IT-Management

fachhochschule stralsund
university of applied sciences

Anforderungen hinsichtlich	Forderungen an IT
Schutz	Dokumentenmanagement
Verfügbarkeit	Identitymanagement
Nachvollziehbarkeit	Datenklassifizierung
Transparenz	Netzwerksicherheit
Sorgfalt	Zugriffskontrolle
Organisation	Schutz vor Schadsoftware
	Überwachung und Reporting
	…

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

13 / 13

3. Beispiele von Non-Compliance
Einige Verstöße des Jahres 2008

fachhochschule stralsund
university of applied sciences

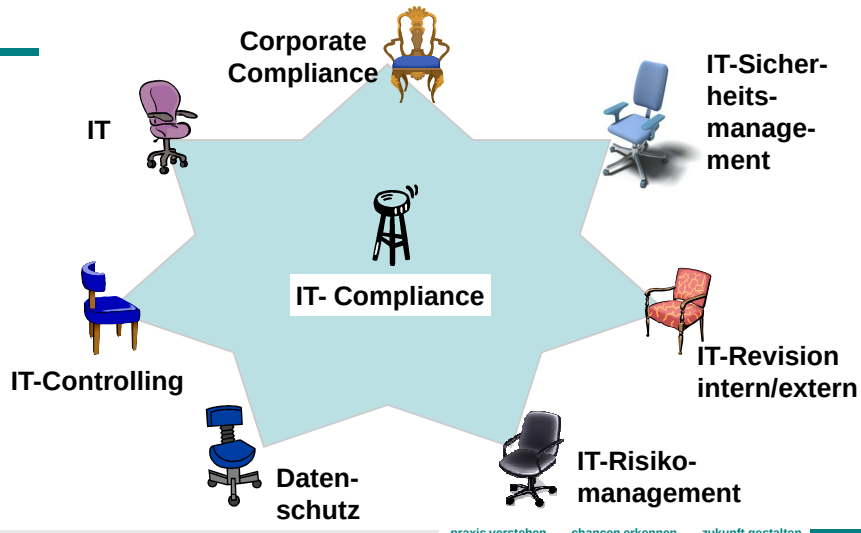
Institution	Fall
Lidl	Überwachung der Mitarbeiter durch Detekteien per Video; Lidl wird zu einer Gesamtstrafe in Höhe von 1,462 Mio. € verurteilt
Deutsche Telekom	Ausspionieren von Journalisten, Telekom-Aufsichtsräten und eigenen Mitarbeitern
KfW	Überweisung von 300 Mio. € aus einem Termingeschäft an die US-Investmentbank Lehman Brothers, die am gleichen Tage einen Insolvenzantrag stellte
Einwohner-meldeämter	Daten von Bürgern aus rund 200 Städten und Gemeinden waren über Jahre hinweg frei im Internet zugänglich
T-Mobile Deutschland	Datendiebstahl von über 17 Mio. Mobilfunkkunden (bereits 2006 erfolgt, aber erst 2008 bekanntgegeben)

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

14 / 13

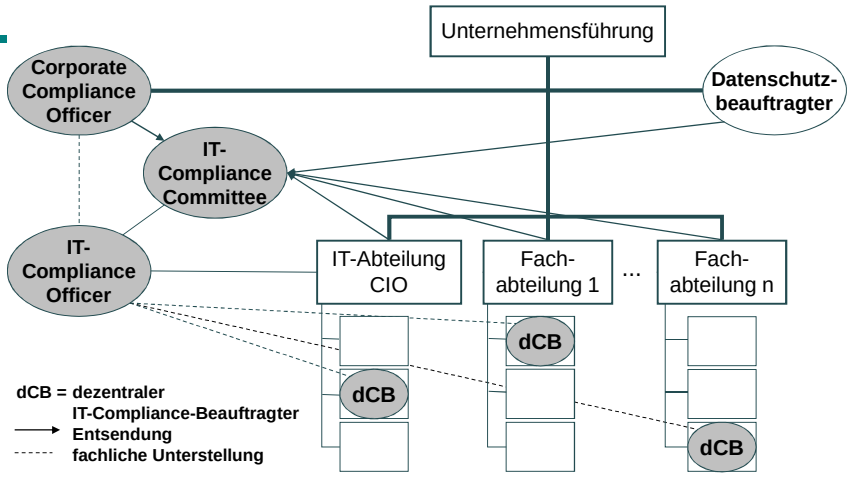
4. Verantwortlichkeiten
Die Situation von IT-Compliance

fachhochschule stralsund
university of applied sciences



4. Verantwortlichkeiten
Exemplarisch IT-Compliance-Organisation

fachhochschule stralsund
university of applied sciences



5. Nutzen von IT-Compliance

fachhochschule stralsund
university of applied sciences

Nutzenkategorien

Ethische Fundierung der Regelwerke:

- Freiheit
- Schutz der Privatsphäre
- Allgemeinwohl
- Gleichbehandlung
- Nachhaltigkeit

Vermeidung von Nachteilen aus Non-Compliance:

- Freiheitsstrafen
- Bußgelder
- Zwangsgelder
- Steuerschätzung
- Vertragsstrafen
- Schadensersatz
- Reputationsschaden

Positive Nebeneffekte:

- Steigerung des Wertbeitrags der IT
- Erhöhung der (IT-)Sicherheit
- Reduzierung von (IT-)Risiken
- Senkung von (IT-)Kosten
- Erhöhung der (IT-)Qualität

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

5. Nutzen von IT-Compliance

fachhochschule stralsund

Positive Nebeneffekte

Erhöhung des Unternehmenswertes

- Überwindung von Markteintrittsbarrieren
- Sicherung von Vermögenswerten
- Vermeidung von Risikoabschlägen
- …

Erhöhung der Qualität

- Reduzierung der IT-Komplexität
- Verbesserung der Auditierbarkeit
- Erhöhung der Transparenz
- …

Erhöhung der (IT-)Sicherheit

- Höhere Verfügbarkeit von Daten und Infrastruktur
- Sicherung von Betriebsgeheimnissen
- Wahrung der Vertraulichkeit
- …

Senkung von (IT-)Kosten

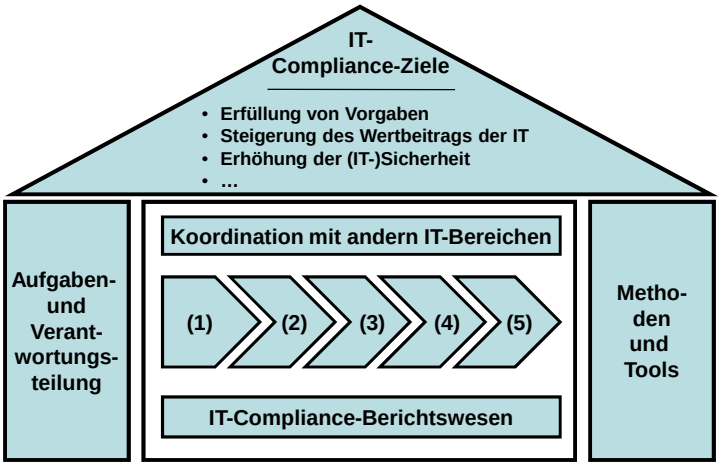
Senkung von
- Überwachungskosten
- Auditierungskosten
- Lizenzkosten
- Ausfallkosten
- Betriebskosten
- …

Reduzierung von (IT-)Risiken

Vermeidung/Reduzierung von
- Geschäftsunterbrechungsrisiken
- Betrugsrisiken
- Reputationsrisiken
- …

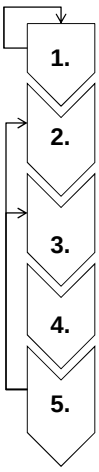
erkennen — zukunft gestalten
understand reality — face challenges — create future

6. Managementansatz



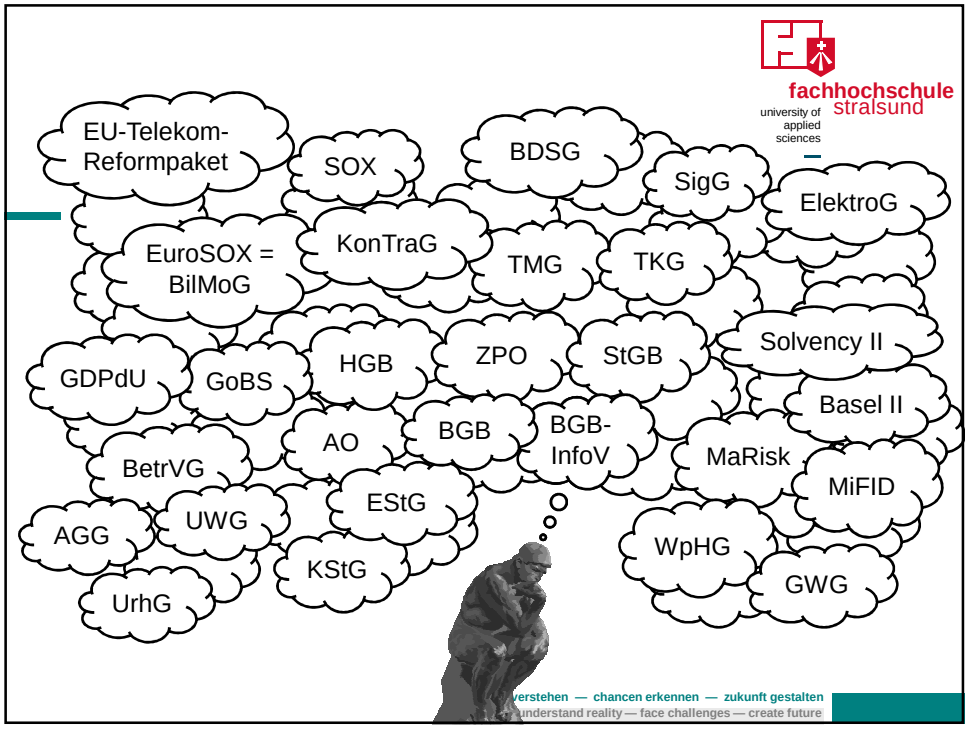
praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
19 / 13

7. IT-Compliance-Prozess

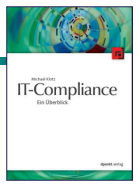


1. Identifizierung von relevanten Regelwerke und Ableitung der Compliance-Anforderungen
2. Gestaltung von Abläufen, Zuständigkeiten, Delegationen und Kontrollen zur Überwachung der Einhaltung aller Compliance-Anforderungen
3. Information aller betroffenen Betriebsangehörigen (und ggf. Dritter) über die einzuhaltenden Regelungen
4. Dokumentation der Gestaltungs- und Informationsmaßnahmen und insbesondere deren Überwachung
5. Reaktion auf Neuerungen/Änderungen von Compliance-Anforderungen, z. B. auf neue Rechtsprechung

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
20 / 13



7. Angebote des SIMAT



- Broschüre „IT-Compliance“ beim dpunkt-Verlag auf Anfrage erhältlich
- Es erscheinen regelmäßig Arbeitspapiere zu IT-Compliance und verwandten Themen; die APs stehen auf der Website http://simat-stralsund.de/ zum Download bereit

- Online-Seminar für Führungskräfte zur „Corporate Governance“ in Kooperation mit PROF. BINNER AKADEMIE (nächster Start 10. September 2010)
- ISACA-Zertifikatskurs „IT-Compliance-Manager“ (nächster Start am 7. Oktober 2010)

- SIMAT-Newsletter informiert auf laufende Arbeiten und Ergebnisse
- Zeitschrift „IT-Governance“

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
22 / 13

Kontakt und Information

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Prof. Dr. Michael Klotz

FH Stralsund, FB Wirtschaft/SIMAT
Zur Schwedenschanze 15, 18435 Stralsund
Fon +49 (0)3831 45-6946
Fax +49 (0)3831 45-6604
eMail michael.klotz@fh-stralsund.de

Competence Center “IT Governance, Riskmanagement & Compliance“

Aktuelle Projekte:

- Datenschutz in GDPdU-Prozessen
- IDEA-Analysen im Vorfeld von Betriebsprüfungen
- Compliance von Projektmanagement-Tools

www.simat-stralsund.de

twitter
@simat_stralsund

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

23 / 13