Zukunft Technik Vorpommern

fachhochschule stralsund
university of applied sciences

Der Wandel des Informationsmanagements

Governance – Riskmanagement - Compliance

Prof. Dr. Michael Klotz

ZTV Fachtagung „Arbeiten in der digitalen Welt“

27. Oktober 2010

SIMAT

STRALSUND INFORMATION MANAGEMENT TEAM

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

Intro: IT GRC in der Fachpresse

fachhochschule stralsund
university of applied sciences
SIMAT

„Klar ist, dass es sich bei **Governance** um Unternehmensführung durch Richtlinien handelt, bei **Risikomanagement** um Strategien zur Minimierung von Risiken sowie Krisenmanagement und bei **Compliance** um das Einhalten interner und externer Normen.“

Quelle: http://www.cio.de/subnet/oracle-finance/2238761/

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

2 / 26

Gliederung

fachhochschule stralsund
university of applied sciences
SIMAT

1. Warum das Ganze?
2. Begriffliche Klärung
3. Die GRC-Trias
4. Auswirkungen im IT-Alltag
5. Handlungsbedarf
6. Kontakt und Information

1. Warum das Ganze?

fachhochschule stralsund
university of applied sciences
SIMAT

- Die FlowTex Technologie GmbH & Co. KG, Ettlingen, handelte mit Horizontalbohrmaschinen zum unterirdischen Verlegen von Leitungen.
- Von 1994 bis 1999 leaste FlowTex nicht vorhandene Maschinen im Sale-Lease-Back-Verfahren. Einnahmen hieraus: 4,2 Mrd. DM. 2,6 Mrd. an Leasingraten wurden zurückgezahlt
  ⇨ betrügerischer „Gewinn“: 1,6 Mrd.
- 2000 wurden bei einer Betriebsprüfung Scheinrechnungen gefunden.
- 2003 wird der Unternehmer Manfred Schmider zu 12 ½ Jahren Haft verurteilt (auch der Hausanwalt wurde zu vier Jahren Haft verurteilt).
- Fazit 2008:
  -127 Ermittlungsverfahren seit 2000
  - 27 Menschen wurden verurteilt:
  9 zu Haftstrafen, 16 zu Bewährungsstrafen und 2 zu Geldstrafen.

1. Warum das Ganze?

fachhochschule stralsund
university of applied sciences
SIMAT

- Die zahlreichen Unternehmensskandale haben ab 2002 die Geschäftswelt nachhaltig verändert.
- Vertrauen von Aktionären und Kreditgebern wurde nachhaltig erschüttert.
- Die Themen Unternehmensüberwachung und Risikomanagement treten noch stärker in den Vordergrund.
- Die Rolle von Wirtschaftsprüfern wird kritisch hinterfragt.
- Die Haftbarkeit von Führungspersonen erscheint nunmehr als real.
- Die Verantwortung und Qualifikation von Aufsichtsräten wird hinterfragt.
- Das persönliche Verhalten von Topmanagern und ihre Vergütung erlangten seitdem starkes öffentliches Interesse.
- Wirtschaftsethische Fragen werden zunehmend diskutiert.
- Die Politik regiert mit gesetzlichen Maßnahmen gerade in Bezug auf Corporate Governance.

1. Warum das Ganze? Corporate Governance als globale Antwort

fachhochschule stralsund
university of applied sciences
SIMAT

Nach **OECD**, 2004:

- Corporate Governance (CG) betrifft das Geflecht der Beziehungen zwischen Management, Aufsichtsorgan, Aktionären und anderen Beteiligten (Stakeholder).
- CG liefert auch den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle.
- CG hängt ferner vom rechtlichen, regulatorischen und institutionellen Umfeld ab.
- CG-Strukturen werden durch die Beziehungen zwischen den an diesem System beteiligten Akteuren geprägt.

Quelle: OECD: OECD-Grundsätze der Corporate Governance, S. 11f, verfügbar unter: http://www.oecd.org/dataoecd/57/19/32159487.pdf (Zugriff am 28.09.2010)

1. Warum das Ganze? Der DCGK als deutsche Antwort

fachhochschule stralsund
university of applied sciences
SIMAT

- Der „**Deutsche Corporate Governance Kodex**“ (DCGK) wurde am 26. Februar 2002 von einer durch das BMJ im September 2001 eingesetzten Regierungskommission verabschiedet.
- Der Kodex soll die in Deutschland geltenden **Regeln für Unternehmensleitung und -überwachung** für nationale wie internationale Investoren transparent machen, um so das Vertrauen in die Unternehmensführung deutscher Gesellschaften zu stärken.
- Der Kodex hat über die Entsprechungserklärung gemäß § 161 AktG eine **gesetzliche Bindungswirkung**.

Quelle: http://www.corporate-governance-code.de/index.html (Zugriff am 28.09.2010)

1. Warum das Ganze? Der DCGK als Antwort

fachhochschule stralsund
university of applied sciences
SIMAT

DCGK fordert hinsichtlich Riskmanagement und Compliance:

3.4 Die ausreichende Informationsversorgung des Aufsichtsrats ist gemeinsame Aufgabe von Vorstand und Aufsichtsrat.

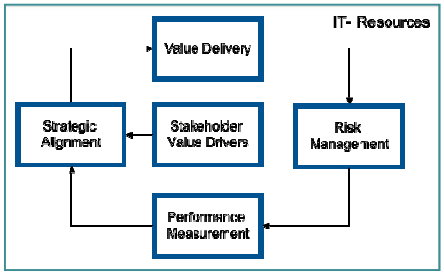
Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein.

4.1.3 Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

4.1.4 Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.

Quelle: http://www.corporate-governance-code.de/index.html (Zugriff am 28.09.2010)

2. Begriffliche Klärung IT-Governance



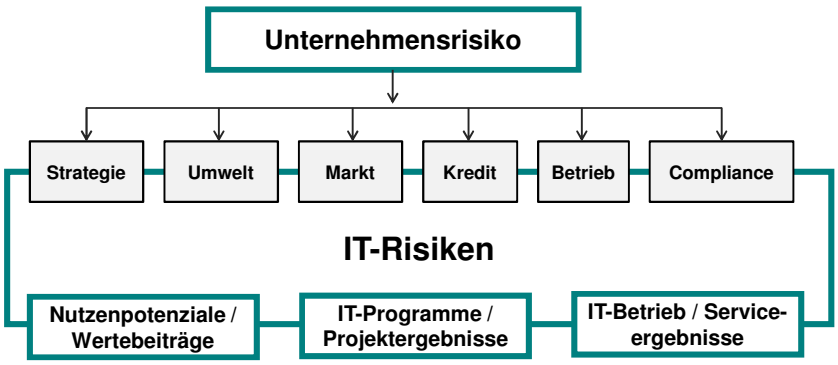
Der IT-Governance-Prozess:

- Erwartungen verschiedener Stakeholder *(Stakeholder Value Drivers)* als Ausgangspunkt
- Abgleich von IT- und Geschäfts-Strategie *(Strategic Alignment)*
- Umsetzung der Strategie führt zu Wertbeiträgen der IT *(Value Delivery)*
- Risiken als zu minimierende „Störgrößen“ *(Risk Management)*
- Die Ergebnismessung *(Performance Measurement)* gibt Aufschluss über die aktuelle Leistungsfähigkeit
- Effizientes Ressourcenmanagement in allen Phasen

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
9 / 26

2. Begriffliche Klärung IT-Riskmanagement

IT-Risiken sind Teil der operativen Unternehmensrisiken.



praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
10 / 26

2. Begriffliche Klärung IT-Compliance

fachhochschule stralsund
university of applied sciences
SIMAT

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

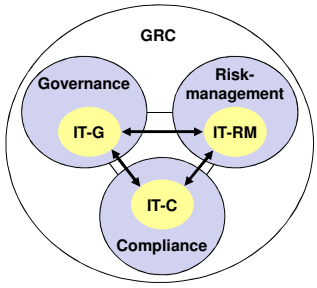
2. Begriffliche Klärung IT-Compliance

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	...

3. Die GRC-Trias

- Inhaltliche, strukturelle und personelle Interdependenzen
- Gleiche oder ähnliche Methoden und Instrumente
- Sachlage erfordert Koordination



praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
13 / 26

Zwischenfazit

- IT-Governance soll ausgehend von Stakeholder-Interessen eine an den Unternehmenszielen orientierte Nutzung von IT sicherstellen.
- IT-Riskmanagement steuert die mit der Nutzung von IT verbundenen IT-Risiken.
- IT-Compliance bewahrt das Unternehmen vor Regelverstößen in Bezug auf die IT.
- IT-GRC ist eine Spezialisierung der Corporate GRC.
- Das G, R und C von IT sind miteinander verbundene Handlungsbereiche, deswegen IT-GRC.

☞ Herausforderung für das Management

☞ Auswirkungen im IT-Alltag

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
14 / 26

4. Auswirkungen im IT-Alltag
Generelles Modell

fachhochschule stralsund
university of applied sciences
SIMAT STRALSUND INFORMATION MANAGEMENT TEAM

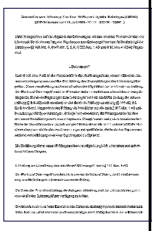
Anlass (Entwicklung, Maßnahme, Neuerung etc. mit IT-Bezug)

IT-Governance	IT-Riskmanagenent	IT-Compliance
• Entscheidung • Aufgaben/ Delegation • Verantwortlich-keiten • Kontrolle	• Risikoart(en) • Risikoumfang • Risikoappetit • Risiko-Eigentümer	• Regelwerke • Betroffene • Information • Dokumentation

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
15 / 26

4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

fachhochschule stralsund
university of applied sciences
SIMAT STRALSUND INFORMATION MANAGEMENT TEAM



- Die **Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen** (**GDPdU**) vom 16.7.2001 sind eine Verwaltungsanweisung des Bundesfinanzministeriums, mit der Regelungen aus der AO und dem UStG zur digitalen Aufbewahrung von steuerlich relevanten Daten/Dokumenten konkretisiert werden.
- Es besteht eine bindende Wirkung nur ggü. den dem BMF nachgeordneten Dienststellen.
- Im Kern enthalten die GDPdU Regelungen zur Aufbewahrung digitaler Unterlagen und zur Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen.
- Für den Datenzugriff kann der Betriebsprüfer zwischen folgenden drei Arten des Datenzugriffs wählen:
  - unmittelbarer Lesezugriff (Z1),
  - mittelbarer Zugriff über Auswertungen (Z2) und
  - Datenträgerüberlassung in verschiedenen Formaten (Z3).

Quelle: http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Aktuelles/BMF__Schreiben/Veroffentlichungen__zu__Steuerarten/abgabenordnung/006,templateId=raw,property=publicationFile.pdf (Zugriff am 12.02.2010)

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future
16 / 26

4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

fachhochschule stralsund
university of applied sciences
SIMAT

Sorgen bereiten kann bei den unterschiedlichen Prüfungsarten:

Datenträgerüberlassung (Z3)	Mittelbarer Datenzugriff (Z2)	Unmittelbarer Datenzugriff (Z1)
• Finanzverwaltung haftet nicht bei Datenverlust	• Eine Person muss zur Unterstützung des Prüfers abgestellt werden (d. h. Zeit und Kosten) • Prüfer prüft vor Ort und erhält Einblick in den laufenden Betrieb	• Bereitstellung eines eigenen Prüfer-PCs • Einrichtung von Zugangsberechtigungen notwendig • Prüfer prüft vor Ort und erhält Einblick in den laufenden Betrieb • Keine Pflicht zur Protokollierung des Datenzugriffs seitens des Prüfers

- Alle drei Zugriffsarten müssen über 10 Jahre gewährleistet sein.
- Anfallende Kosten trägt das Unternehmen.
- Der Prüfer kann die Zugriffsart wählen, ggf. auch alle drei.
- Steuerrelevante Daten sind solche der Finanz-, Anlagen- und Lohnbuchhaltung, aber auch sonstige Daten, z. B. Reisekostendaten, Daten aus der Kostenrechnung oder Office-Systemen (also auch E-Mails) …

4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

fachhochschule stralsund
university of applied sciences
SIMAT

- In den „Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung“ vom 22.1.2009 werden **E-Mails** zu den potenziell **steuerlich relevanten Dokumenten** gezählt.
- Beispiele in Frage/Antwort 9:
  - per E-Mail übermittelte Reisekostenabrechnung in einem Tabellenkalkulationsformat
  - E-Mail, die steuerlich relevante Vertragsgestaltungen enthält.
- Da theoretisch nahezu jeder Mitarbeiter mit einer E-Mail-Adresse in einem Unternehmen solche steuerrelevanten E-Mails empfangen kann, ergibt sich als **Anforderung an die IT**,
  - dass diese Mails als solche **erkannt** und
  - einer geordneten, **revisionssicheren Ablage** zugeführt werden müssen,
  - ggf. unter Aufbewahrung von **Schlüsseln** für Kryptografie/Signatur,
  - wobei der gesamte Lebenszyklus vom Eingang über Verarbeitung bis zur Archivierung zu **protokollieren** ist.

4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

fachhochschule stralsund
university of applied sciences
SIMAT

Anlass

- Außenprüfer wurden seit 2002 systematisch geschult und auch sonst rüsten die Finanzbehörden auf, z. B. Einsatz des Webcrawlers Ypider zum Sammeln von steuerlich relevanten Informationen.
- Bevorstehende Außenprüfung
- Neues IT-System (Mail, Archivierung …)
- Schlechtes Gewissen: „Bisher nichts gemacht“, „ungutes Gefühl im Magen“, …

4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

fachhochschule stralsund
university of applied sciences
SIMAT

IT-Governance

- Entscheidung: Grundsatzentscheidung zu Handlungsbedarf und Einrichtung eines E-Mail-Managements? Komplett- oder Teilarchivierung von E-Mails? Notwendigkeit einer Betriebsvereinbarung? Umsetzung einer E-Mail-Richtlinie?
- Aufgaben/Delegation: E-Mail-Richtlinie bzgl. Nutzung, Aufbewahrung, Suche, Reproduktion inkl. Verfügbarkeit einer technischen Lösung
- Verantwortlichkeiten: IT, Finanzen, Revision, Recht, AN-Vertretung; Zusammenarbeit in initialen Projekten oder kontinuierlichen Prozessen
- Kontrolle: Mitarbeiterführung, interne und externe Revision

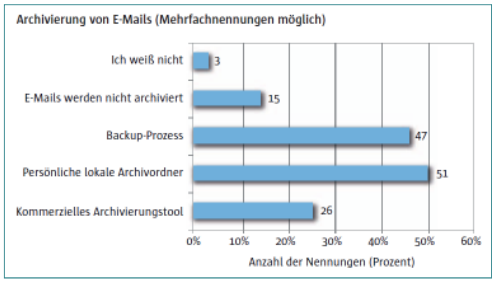
4. Auswirkungen im IT-Alltag
Beispiel 1: GDPdU

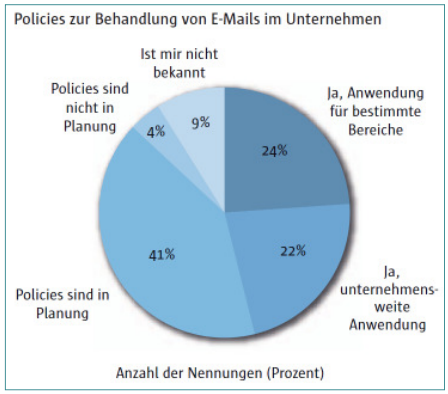
fachhochschule stralsund
university of applied sciences
SIMAT

IT-Riskmanagenent	IT-Compliance
• Risikoart(en): Risiken resultieren aus Rechtsverstößen (Ordnungswidrigkeiten oder Straftaten), • Risikoumfang: Bußgelder, Steuerschätzung (d. h. erhöhte Steuerzahlung), Freiheitsstrafen • Risikoappetit: zu entscheiden • Risiko-Eigentümer: Unternehmen, d. h. handelnde Organe	• Regelwerke: AO, HGB, GDPdU, GOB, GOBS, BDSG, TKG, ProdHaftG … • Betroffene: Unternehmensleitung, Stabstellen, Management, **Mitarbeiter**, AN-Vertretung • Information: Aufklärung/ Sensibilisierung, Schulung • Dokumentation: der Maßnahmen, der E-Mails

5. Handlungsbedarf
Ergebnisse aus einer Studie zum E-Mail-Management von 2008

fachhochschule stralsund
university of applied sciences
SIMAT





Quelle: BearingPoint: Studie – E-Mailmanagement 2008, S. 18f.; verfügbar unter: ftp://public.dhe.ibm.com/software/emea/de/db2/bearingpoint_studie_2008.pdf (Zugriff 26.10.2010)

5. Handlungsbedarf

fachhochschule stralsund
university of applied sciences
SIMAT STRALSUND INFORMATION MANAGEMENT TEAM

- (IT-)GRC in seinen Bestandteilen reflektieren
- Notwendige Verbindungen analysieren und strukturell umsetzen
- Stakeholder identifizieren und Zusammenarbeit organisieren
- Insbesondere Anforderungen Dritter (WP, Finanzbehörde …) beachten
- IT-Lösungen nur auf einer geklärten strukturellen und konzeptionellen Grundlage einführen

6. Kontakt und Information

Prof. Dr. Michael Klotz
Wissenschaftlicher Leiter
☎ +49 3831 45-6946
✉ Michael.Klotz@simat.fh-stralsund.de
✉ michael.klotz@balticmuseums.org

fachhochschule stralsund
university of applied sciences