Themenschwerpunkt Informationsrecht:

Aspekte der **IuK-Compliance und -Governance** *in KMU*

Prof. Dr.-Ing. Uwe Straubel

CETIMA Software & Consulting GmbH
98574 Schmalkalden , Wilhelm-Külz-Str. 58
fon + 49 36 83 / 7 90 20 , fax + 49 36 83 / 79 02 19
www.cetima.de , info@cetima.de

Staatliche Studienakademie Thüringen
Berufsakademie Eisenach, Studienbereich Wirtschaft,
fon +49 3691 629443 / Mail straubel@ba-eisenach.de

CETIMA - Leistungsportfolio

- **Dienstleistung und Lösungen für .. Informationsmanagement und Teamarbeit**

  (CRM-Systeme für Marketing, Vertrieb, Service, elektronische Handbücher, Dokumenten- und Projektmanagement, Kommunikation, ..)

- **.. Integration externer Geschäftsprozesse**

  (Web- und Enterprise-Content-Management, Virtuelle Team-Räume, E-Commerce-Portale, ..)

- **Standardsoftware CETIMA_Suite, Betreuung von Lösungen**
- **Individuelle Softwareentwicklung**
- **Consulting und Training**
- **Administration und Support**

It´s e-time!
Groupware
e-Business
Consulting

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Ziele des Vortrages

„Für die Zukunft ist es unerlässlich, den aktuellen Compliance-Ansatz zu einem strategischen Instrument der Unter-nehmensführung auszubauen.
Isolierte Maßnahmen helfen hier wenig.

Governance, Risikomanagement und Compliance müssen als Gesamtlösung weiterentwickelt werden.“

Marina Walser
Novell Central Europe
(zitiert in Rath / Sponholz, S.117)

- Aktuelle Aspekte aus Praxis aufgreifen,
  keine ganzheitliche und erschöpfende Bearbeitung des Themas und keine „fertigen Lösungen“

- Anregungen, Impulse für
  - praktische Umsetzung,
  - die weitere Profilierung des Dienstleistungsumfeldes sowie
  - ggf. gemeinsame Forschungsthemen

- Fokus: KMU inkl. resultierender Anforderungen an das Dienstleistungsumfeld

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Agenda

1. IuK-Compliance - Grundlagen
2. Quellen und Objekte der IuK-Compliance
3. Probleme von, mit und durch IuK-Compliance
4. Ziele der IuK-Compliance
5. IuK-Compliance-Management (CM)
   - Aufgaben
   - Referenzmodell für KMU
   - Wirkungsintensität von Regelungsmechanismen
   - Organisation inkl. Beispiele
   - Prozess inkl. Beispiele,
     IuK-Compliance-Inventar / -Monitoring
   - IuK-CM im Rahmen der Systementwicklung
   - Werkzeuge inkl. Beispiele,
     IuK-CM im Konzept des „Integrierten Managements“
- Zusammenfassung / Fazit

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Grundlegende Definitionen – Compliance (1)

- „Compliance liegt vor, wenn alle für das Unternehmen verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.“ .. „Als Erweiterung des allgemeinen Compliance-Begriffes bezeichnet IT-Compliance einen Zustand, in dem alle für die IT des Unternehmens relevanten Vorgaben nachweislich eingehalten werden.“ (Klotz 2009, S. 3 u. 6)

- „Compliance ist die Übereinstimmung mit und die Erfüllung von gesetzlichen und regulativen Vorgaben“ (Kampffmeyer 2007, S. 3)

- „IT-Compliance heißt auf ´gut Deutsch´: Einhaltung und Umsetzung von regulatorischen Anforderungen im weitesten Sinne mit dem Ziel eines verantwortungsvollen Umganges mit allen Aspekten der Informationstechnik. Mit der Umsetzung dieser Vorgaben einher geht der Begriff ´IT-Governance´. Darunter sind alle Maßnahmen zur Organisation, Steuerung und Kontrolle der IT-Systeme eines Unternehmens zu verstehen. IT-Governance ist ein wichtiger Bestandteil von Corporate Governance, sprich der verantwortungsvollen Unternehmenssteuerung durch die Geschäftsführung“. (Rath 2007, S. 3)

„Compliance“-Begriff entstammt angel-sächsischer Rechts-terminologie.

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Grundlegende Definitionen – Governance, GRC (2)

***GRC** vereinigt die Disziplinen Corporate Governance, Risikomanagement und Compliance als durchgängiges Vorgehensmodell.*
(IBM / Kampffmeyer 2009)

- Information Management Compliance: Übertragung des Compliance-Begriffes auf die Handhabung von Informationen. Sie spielt eine besondere Bedeutung bei der Nutzung von Informationssystemen, die Compliance-Anforderungen unterliegen. Grundlage sind Regelwerke (Policies), die den Umgang mit Information verbindlich machen.
- Corporate Governance : .. umfasst die rechtlichen und institutionellen Rahmenbedingungen sowie die Entwicklung und Einrichtung von obligatorischen als auch freiwilligen Leitungs- und Kontrollstrukturen auf nationaler und internationaler Ebene, die mittelbar oder unmittelbar Einfluss auf die Führungsentscheidungen eines Unternehmens haben.
- IT-Governance: zielt auf die Transparenz, Beherrschbarkeit und Überprüfbarkeit der eingesetzten IT- und Kommunikationsinfrastruktur, u.a. mittels Verfahrensmodellen und Werkzeuge wie COBIT, ITIL u.a.
- Risikomanagement: Maßnahmen zur systematischen Erfassung, Bewertung und Steuerung der unterschiedlichsten Risiken eines Unternehmens

(vgl. Kampffmeyer 2007, S. 17)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Grundlegende Definitionen – Betroffenheit (3)

- Betroffenheit im Sinne von Auswirkungen regulativer Vorgaben:
  - Direkt: Regelungen müssen in jedem Fall eingehalten werden, lediglich Umfang und Ausprägung sind interpretierbar.
  - Indirekt: Grundlage ist die Ermittlung der für das Unternehmen oder die Organisation zutreffenden Regelungen. Bindungsverpflichtung ist häufig schwierig zu beurteilen und sehr heterogen ausgeprägt („Grauzonen“).

- IuK-orientierte Compliance:
  - IuK als Objekt von Compliance-Anforderungen

- IuK-gestützte Compliance:
  - IuK als Instrument zum Erreichen von Compliance

Die Verantwortung für die Einhaltung von Compliance-Vorgaben liegt bei Vorständen, Aufsichtsräten und Geschäftsführern.
(IBM / Kampffmeyer 2009)

Compliance / Governance und Institutionsbegriff

- Unterscheidung der Institutionen nach:
  - Selbst tragenden Institutionen und
  - überwachungs- und durchsetzungsbedürftigen Institutionen

- These: Compliance muss weitestgehend als selbst tragende Institution funktionieren, um nachhaltig moderne Trends, wie
  - Personen-zentriertes Management,
  - Social Business / Networking und
  - Dezentralisierung / Mobilität der Arbeitswelten
  - Kooperation und Vernetzung der Unternehmen

  Strategie-konform für das Unternehmen zu nutzen.

Institutionen *sind sanktionierbare Vereinbarungen und Erwartungen bezüglich der Handlungs- und Verhaltensweisen eines oder mehrerer Individuen. Sie beschreiben und begrenzen Aktivitäts-räume und stabilisieren bzw. erleichtern somit die Zusammenarbeit.*

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Quellen der IuK-Compliance

- Rechtliche Vorgaben
  - Gesetze und Rechtsverordnungen
  - Rechtssprechung
  - Verwaltungsvorschriften
  - Referenzierte Regelwerke

  Hinweis: als direkt formulierte Pflichtschutzaufgabe oder indirekt ableitbare Betroffenheit mit Interpretationsoptionen und Entscheidungstoleranzen infolge Risikobewertung und -haltung
- Verträge
  - Inkl. IuK-relevanter Vereinbarungen mit Kunden, Lieferanten, ..
- Unternehmensexterne Regelwerke / Regularien
  - Normen, Standards, Kodizes
  - Referenzmodelle, Best-Practice-Modelle
- Unternehmensinterne Regelwerke / Regularien
  - Richtlinien, Verfahrensanweisungen, Vorschriften
- Gesellschaftliche, ethische .. Erwartungen

  (vgl. Klotz 2009, S. 20 ff.; Rath / Sponholz, 2009, S. 119)
- Unternehmens-Ziele und -Strategien (inkl. Elemente der normativen Unternehmensführung)

Bindungsgrad und Risiko nehmen in Richtung der Unter-nehmensinternen Regelwerke ab.

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Objekte der IuK-Compliance

- Unternehmens- / Anweisungsbereiche (Aufbau- / Ablauforganisation), u.a.
  - Rechnungswesen (intern / extern), Steuern, Personalwesen
  - Marketing, Vertrieb, Service und Kundenbetreuung
  - Internet-Dienste
  - Dokumentenmanagement / elektronische Archivierung
  - IT-Beschaffung, -Services
  - Datenschutz
- Geschäftsprozesse (Kern- u. Stützprozesse)
- Management
- IuK-Technologien
- IuK-Infrastruktur, IuK-Anwendungssysteme inkl. Schnittstellen
- Informationen (inkl. Daten, Dokumente, Wissen)
- Stakeholder
- Ressourcen
- Produkte
- Werte
- …

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Probleme von, mit und durch IuK-Compliance

- Mangelnde Kommunikation und Koordinierung zwischen
  - IT-Managern und U.-führung
  - IT-Managern und Compliance-Experten
  - mit externen Aufsichtsbehörden

- Unzureichende Integration der IuK-Compliance-Anweisungssysteme in QM- u. allgemeine Management- und Regelwerke sowie mangelhafte Wirkung als Durchsetzungs-instrumente in täglichen Geschäftsprozessen

- Identifizieren, Bewertung, Beobachtung, Aktualisierung der relevanten IT-Compliance-Elemente (Quellen, Objekte) häufig nur reaktiv und unsystematisch
  - u.a. erschwert durch Vielfalt, Intransparenz, Dynamik und interdisziplinäre Kompetenzerfordernisse

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Beispiel PDA (Smartphone, Tablet) sowie MFG

- Technisch integrierte Funktionen in PDA
  - Audiovisuelle und Schriftliche Kommunikation (asynchron, synchron)
  - Bild- und Ton-Aufnahme / -Dokumentation
  - (Internet-) Informationsrecherche
  - Allgemeine Office-Anwendungen, Adressmanagement, Medienverwaltung
  - Persönliches Termin- und Aufgabenmanagement
  - Unterstützung diverser (insbesondere mobiler) Lebenslagen / Geschäftssituationen sowie der Unterhaltung …
- „Integrierte“ betroffene Management-Bereiche:
  - IuK-Management, Organisation, Personalwesen, Rechnungswesen 7 Kostenrechnung, Vertragswesen, Fachbereiche, …
- Weiteres Beispiel für technische Integration: Multifunktionsgeräte (MFG)
- Technologisches Integrationsniveau divergiert zum bisher nicht erreichten ganzheitlichen und interdisziplinären Vorgehen im Management

Screenshot aus www.apple.com

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Ziele der IuK-Compliance

IuK-Compliance als Erfolgsfaktor und Chance!

- ✓ ***Normieren***
- ✓ ***Handeln***
- ✓ ***Nachweisen***

- Systematische Erfassung und Bewertung der gesetzlichen, vertraglichen und regulativen Anforderungen an das Unternehmen
- Generierung und Umsetzung wirtschaftlicher und effektiver Maßnahmen und Strukturen der Compliance im Unternehmen
- Deutliche Reduktion von Reputationsrisiken
- Reduktion von unternehmerischen Haftungsrisiken und Schadensfällen sowie von persönlichen und individuellen Haftungsrisiken des Managements und der Aufsichtsgremien
- Wirksame Ausübung von obligatorischen Kontroll- und Überwachungsaufgaben
- Erfüllung der Ordnungsmäßigkeit und Wirksamkeit der Nachweisführung gegenüber sachverständigen Dritten
- Vertrauensgewinn bei Kunden, Mitarbeitern, Eigentümern, Investoren und sonstigen relevanten Stakeholdern
- Erkennen von Kompetenz- und Know-how-Defiziten

(vgl. Rath / Sponholz, 2009, S. 119 / TECTEM St. Gallen)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM)

Ganzheitlicher Ansatz (GRC)

- Governance
- Risikomanagement (Risk)
- Compliance

Elemente

- IuK-Compliance-Organisation
- IuK-Compliance-Prozess
- IuK-Compliance-Werkzeuge

(vgl. Rath / Sponholz, 2009, S. 117 ff.)

Säulen der Wirtschaftsinformatik als Orientierungsrahmen

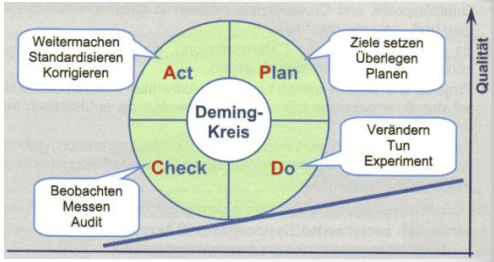
- IuK-Komponenten (Infrastruktur / Hardware / Software),
- Organisation, Prozessmanagement ,
- BWL / Management,
- Personalwesen,
- Recht ….

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Aufgaben

- Schaffung und Aufrechterhaltung von Organisationsstrukturen, Prozessen, Regelwerken, Kontrollsystemen etc. zur Compliance-Überwachung und -Gewährleistung
- Laufende und systematische Identifizierung und Bewertung von IuK-Compliance-Quellen und –Objekten
- Abweichungsanalyse
- Einleitung von Maßnahmen zur Compliance-Erreichung
- Bereitstellung / Verfügbarkeit aller IuK-Compliance-relevanter Inhalte für Stakeholder sowie Nachweisführung / Dokumentation (u.a. erhebliche Bedeutung für Nachweisbarkeit in Zusammenhang mit externen Prüfungen oder mit Streitigkeiten / Rechtsfällen)
- Einrichtung Change-Management (laufende Anpassung und Optimierung entsprechend Entwicklung bei IuK-Compliance-Quellen und -Objekten)

(vgl. Klotz 2009, S. 26 ff.)



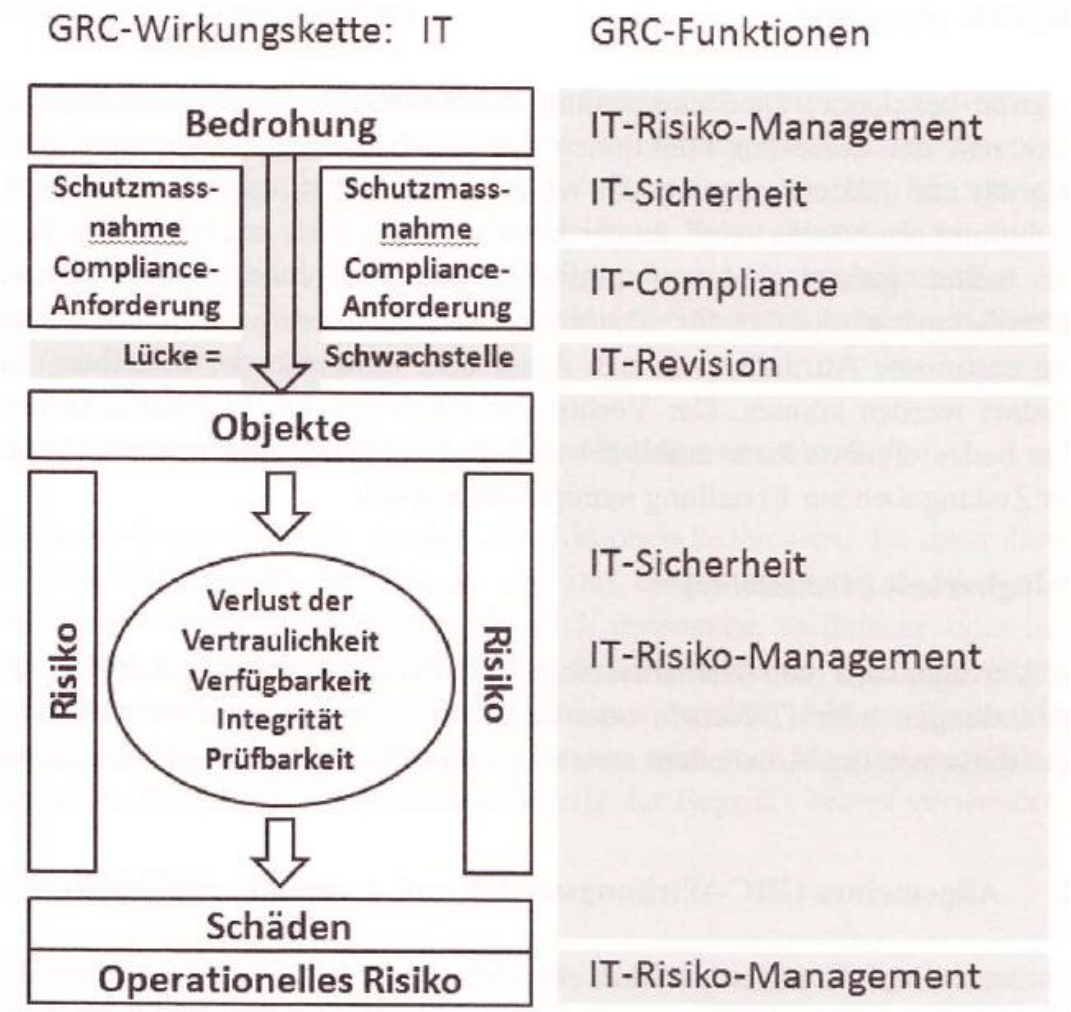
[BENGROH] S. 100: Abb. 3.6

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Allgemeines GRC-Wirkungsmodell zur Informationssicherheit

Prinzipielle Wirkungskette

- ***Gefährdung***
- ***Wert***
- ***Schwachstelle***
- ***Sicherheits-maßnahme***
- ***Risiko***
- ***Vertraulichkeit***
- ***Integrität***
- ***Verfügbarkeit***



Rath / Sponholz, 2009, S. 117

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) mittels vereinfachtem Entwurf eines Referenzmodells für KMU - QOM

Objekte

- Anweisungsbereiche
- Geschäftsprozesse / Management
- IuK-Technologien
- IuK-Infrastruktur / -Systeme, Informationen
- Stakeholder, Ressourcen
- Produkte
- Werte

Quellen

- Rechtliche Vorgaben
- Verträge
- Externe Regularien
- Interne Regularien
- (Gesellschaftliche) Erwartungen
- Unternehmensziele / -strategien

Compliance-Organisation	Compliance-Prozess	Compliance-Werkzeuge
• Organisationsformen • Kommunikation • Kompetenzprofile	• Identifikation / Bewertung • Überwachung, Revision • Nachweis-Dok., Berichtswesen	• Standards / Referenzmodelle • CM-Software • Benchmarking des CM

Management

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) - Wirkungsintensität von Regulierungsmechanismen (u.a.)

Varianten:

AS

- Anweisungssystem, (Organisation)

PU

- Prozess-unter-stützendes System

PI

- Prozess-integriertes automatisiertes System

FQ

- Führung, Qualifizierg., Personalwesen

These: Bevorzugung selbst erhaltender Institutionen“

- **Technisch / organisatorisch**
  - Schriftliche Dokumentation in gesonderten Handbüchern, gekoppelt mit regelmäßigen Belehrungen
    - Ausgeprägt getrennt von den Geschäftsprozessen; parzielle Tätigkeitsunterstützung durch einzelne Vordrucke, Checklisten
    - IuK-CM-Wirkung: schwach
  - Elektronische Dokumentation mittels Intranet / Extranet-Portalen
    - Überwiegend unabhängig von Tätigkeiten bei individuell motivierter Rechercheverfügbarkeit in Prozessen
    - IuK-CM-Wirkung: mittel
  - Integration in IuK-Anwendungssysteme zur (automatisierten) Umsetzung und Kontrolle
    - Typisch für Bereiche der Zugriffs- und Berechtigungssteuerung, Kommunikationsprozesse, Eingabeprüfungen etc. in den klassischen Client-Server-LAN-Umgebungen sowie auch VPN-, SaaS- bzw. Cloud-basierenden Anwendungssystemen
    - IuK-CM-Wirkung: stark
- **Personell / Führung**
  - Persönliches „Complianz“-Verhalten im Rahmen einer gelebten Unternehmenskultur (inkl. Vorbildfunktion der Führungskräfte)
    - IuK-CM-Wirkung: stark

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Wirkungsintensität am Beispiel E-Mail-Management

Schwerpunkt-Bereiche eines E-Mail-Regelwerkes:

1. Private Nutzung von E-Mailadresse / E-Mailkonto des Unternehmens / der Einrichtung
2. Teilnehmer intern / extern
3. E-Mail-Adressen
4. Sicherheit / Zugänge / SPAM- u. Viren-Abwehr in Verbindung mit E-Mailsystem für die Nutzer
5. E-Mail-Erstellung (inkl. Serienmail)
6. E-Mail-Empfang
7. E-Mail-Weiterleitung / -Kopien
8. Bearbeitungsorganisation bei Funktions- / Organisations-Adressen
9. Vertretung und Abwesenheit
10. E-Mail-Speicherung / -Organisationsstruktur / -Löschung
11. Publikation / Schulung des Regelwerkes

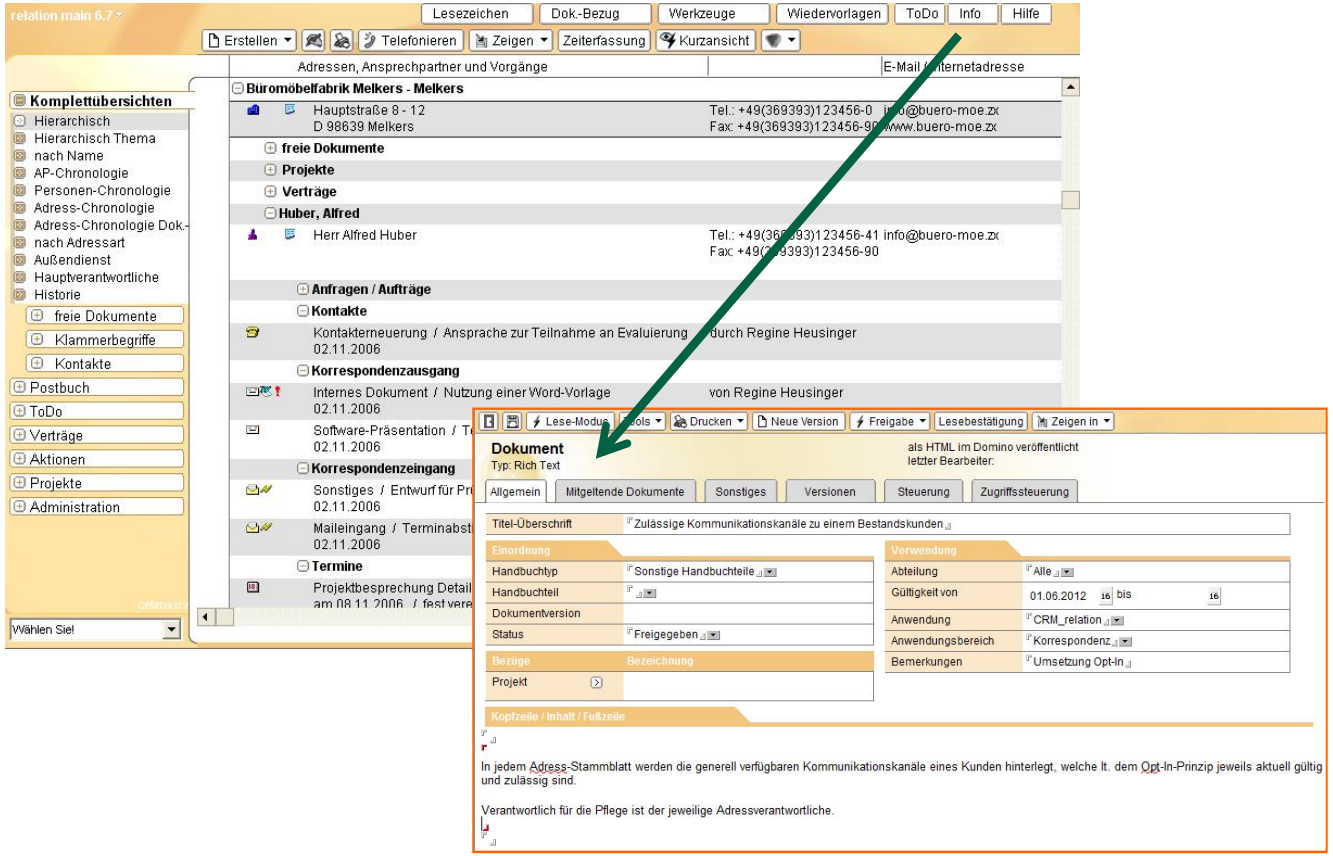
Varianten:

PI PU AS FQ

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Wirkungsintensität am Beispiel Elektronisches Handbuch

Customer-Relationship-Management mit kontextsensitiver Referenzierung auf zugehörige Anweisungen / Regelungen im Elektronischen Management-Handbuch



Varianten:

PU

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Organisation (1)

- Implementierungsformen in KMU
  - Zuweisung Compliance-Aufgaben an Führungskräfte / Fach-Mitarbeiter
  - Auslagerung an externe Kompetenzträger
  - Einrichtung von Stabsstellen oder Vollzeitstellen für Beauftragte
  - Einrichtung von Fachabteilungen
  - Einrichtung eines integrierten Unternehmensbereiches

- Anforderungen an Kompetenzprofile / Qualifizierungen
  - Interdisziplinäres Kompetenzspektrum
  - Führungs- / Sozialkompetenzen
  - GRC-Weiterbildungsangebote

- Modifizierung der Anforderungen an Dienstleister im IuK-Complianz-Umfeld und an moderne Outsourcing-Modelle
  - Beratung „in die Prozesse“ mittels Integration moderner IuK-Technologien
  - Unternehmens-spezifisches aktives Monitoring

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Organisation (2)
Beispiel Social Business / Networking - Thesen

- These 1: Web 2.0 funktioniert nicht ohne „passende“ Unternehmenskultur, welche wiederum durch Web 2.0 einem erheblichen Wandel unterliegt .
  Web 2.0 im Umfeld des Unternehmens findet statt.
  „Monitoring ist Pflicht, aktive Teilnahme die Kür.“[1)]

- These 2: Web 2.0 erfordert neue Qualifizierungsprofile bzw. Fähigkeiten der Mitarbeiter, ergänzt um ein hohes Maß an Eigeninitiative und teilweise Bereitschaft zu persönlicher Transparenz. Zielvorgaben und Verhaltensregelungen sind zwingend erforderlich.

- These 3: Web 2.0 – Dienste und -Technologien sind potenzielle und reale Mittel zur Anbahnung, Durchführung und zum Abschluss von Geschäftsprozessen. Somit ist eine schrittweise Integration in die Compliance-Anforderungen gegeben bzw. zu erwarten.

Varianten:

AS FQ

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Organisation (3)
Beispiel Social Business / Networking - Einsatzpotenziale

Auswahl an Einsatzpotenzialen von Social Media Networking / Web 2.0

- Expertensuche, Expertenrat einholen – XING, Facebook, LinkedIn, Twitter, Chat
- Als Experte profilieren / Kompetenzen persönlich vermitteln – Weblogs, Wikis
- Fachinformationen arbeitsteilig verdichten / klassifizieren – Social Bookmarking
- (Unternehmensübergreifendes) Wissensmanagement – Wikis, ..
- Kooperieren und in Projekten arbeiten – WebConferencing, e-Collaboration, Teamräume
- Dialog (ad-hoc bis systematisch) mit Kunden, Stakeholdern – Facebook, XING, Twitter ..
- Online-Marketing, Public-Relation – alle Formen
- Personen / Unternehmen multimedial vorstellen – YouTube, Podcasting
- Nachrichten bereitstellen (nach Abo-Prinzip) – Newsfeeds
- Kundenbindungsmanagement – Newsfeeds, Weblogs, Twitter, ..
- Mitarbeiter rekrutieren - XING, Facebook
- Kundenmeinungen recherchieren – Communities, Foren, …
- Adressqualifizierung („selbst aktualisierende“ Adress- / Kontaktdaten) – XING, ..

Varianten:

AS FQ

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Organisation (4)
Beispiel Social Business / Networking - Guidelines

Varianten:

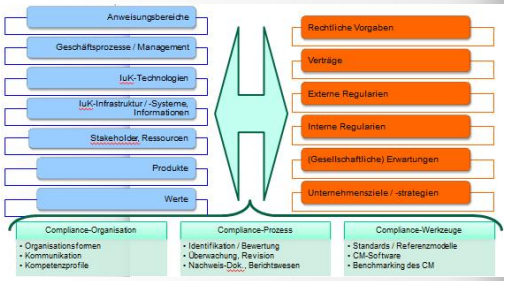
AS FQ

- Dienen der Orientierung und Sensibilisierung für Verhalten in Sozialen Netzwerken, sorgen für einheitliches Auftreten und vermeiden Sanktionen.
- Äußerungs- und Sprachregelungen, Eigenverantwortung
- Geheimhaltungsschutz von Betriebs- und Geschäftsgeheimnissen
- Hinweis auf gesetzliche Bestimmungen (u.a. Urheberrecht, Datenschutz)
- Identität offen legen, Kenntlichmachung von Inhalten als private Meinung, Rahmenrichtlinien für Unternehmensbezogene Angaben in persönlichen Profilen
- Verhalten im Rahmen von Mitarbeiter-Communities innerhalb öffentlicher sozialer Netze
- Optional: Anzeigepflichten von Verstößen
- Sanktionen bei Verletzung der Richtlinien
- Arbeitszeitregelungen, Organisation einer transparenten Zuordnung von Verantwortlichkeiten und Social Media Aktivitäten
  - Unter Verwendung von: Rolf / Riechwald; Social Media Guidelines – Regeln für die betriebliche Praxis; Information Management und Consulting 26(2011)1; S. 39ff.

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Prozess (1) „IuK-Compliance-Inventar“ (QOM)

- IuK-Compliance-Inventar als Aufstellung relevanter IuK-Compliance-Quellen inkl. davon betroffener -Objekte sowie Bewertung und Zuordnung von Maßnahmen
- Struktur-Vorschlag:
  - Name, Art der Regelung (Gesetz, Norm, ..), Quelle, Stabilität
  - Allgemeine Gültigkeit (national/international, Rechtsform, Branche, ..)
  - Bindungsniveau / Verbindlichkeit für eigenes Unternehmen (u.a. zwingend direkt, abgeleitet indirekt, möglicherweise zutreffend, ..)
  - Betroffene IuK-Compliance-Objekte im eigenen Unternehmen (Bereiche, Prozesse, Anwendungssysteme, ..)
  - Handlungsbedarf, Schad- / Nutzen-Wirkungspotenzial
  - (opt.) Einstufung im Chancen- u. Risikomanagement
  - Potenzielle Maßnahmearten (Anweisungen, Verträge, Prüfung, ..)
  - Konkrete Maßnahmen, Verantwortlichkeiten, Fristen / Termine
  - (opt.) Geschätzte Aufwände, Kosten
  - ...
- Gewährleistung der laufenden Aktualisierung und Maßnahme-Zuordnung im Sinne IuK-Compliance-Monitoring



CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Prozess (2)
Bsp. Technologie-Bewertung zu Internet-Umfeld

Privates Portal mit Dominanz-Charakter aufgrund Geschäftshierarchie
www.vwgroupsupply.com

Virtuelle Marktplätze

Horizontaler Marktplatz Konsortienbasierter
www.resale.de, www.mercateo.de

Unabhängiger, vertikaler Marktplatz
www.newtron.net

Sonstige Internetangebote
(Kataloge, Suchmaschinen, Online-Services, Linkverzeichnisse)
www.wer-liefert-was.de

Social-Networks
www.facebook.com ; www.xing.com

Hauptfelder zur Internetnutzung in den Rollen:
Anbieter, Nachfrager, Partner

Collaborationsspezialist

Informationsbroker

Verhandlungs-/Transaktions-spezialist

Spezielle Internetangebote unter eigener Regie

Außenwirksame Operativsysteme

Spezielle Internetangebote in Kooperation mit Partnern

Forschung	Entwicklung	Service	Projekt-management	Qualifizierung	Marketing	Vertrieb	Logistik	...

Intranet/Extranet/Virtuelle Räume (Fabriken)	E-Learning	Shop/Katalog/CMS	Fracht-börsen	...

Quelle: CETIMA / Fachhochschule Schmalkalden

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

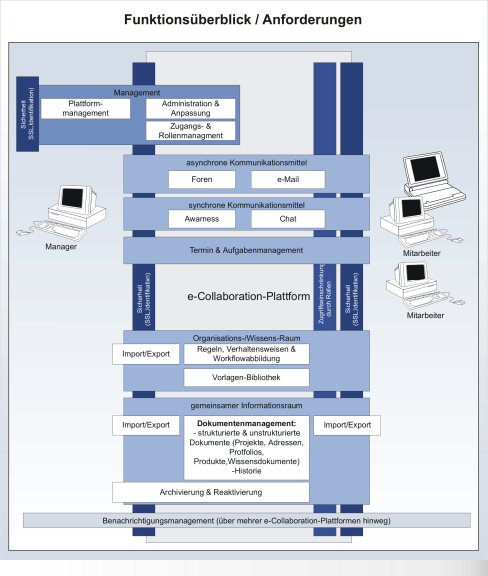
IuK-Compliance-Management (CM) – Prozess (3)
Bsp. Technologie-Bewertung zu Internet-Diensten

- Einzel e-Mail / Serien-Mail (Online-Kampagnen)
- Newsletter
- FTP (Web-basierendes Dateimanagement)
- Electronical Data Interchange
- Feeds (.. Content Syndication)
- Social Bookmarking
- Blogs
- Wikis
- Social Networking
- Chat
- (Web-) Conferencing
- Team Collaboration
- Podcasts
- Twitter
- Second Life
- Rich-Client-Technologien
- …

- URL
- Micro-Sites
- Tag-Clouds
- Mashup
- Keyword-Advertising
- Affiliate-Marketing
- Online-Werbung
- Suchmaschinen-Marketing (SEO)
- Web-Services
- (Vertikale- / horizontale) Online-Marktplätze
- Online-Branchenportale
- Online-Kataloge / -Shops / -Börsen
- Online-Konfiguratoren
- Online-Bezahldienste
- Sicherheits- / Vertrauens-unterstützende Dienste
- ...

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Prozess (4)
Beispiel Virtuelle Teamräume



- Schnelle und einfach handhabbare selbständige Einrichtung inkl. Vorgabe Nutzungs-Policy (dominierendes Selbstorganisations-Konzept)
- Akzeptanz der Aufrechterhaltung von Datenhoheit und IT-Systemen der Partner
- Möglichkeit sowohl zur ad-hoc-Definition und flexibler Anpassung von Struktur und Funktionalität des gemeinsamen Informationsraums als auch zur Verwendung präfixierter Räume; dabei inkl. individueller, geschützter Räume
- Option zum Abruf von verschiedenen Orten und mittels unterschiedlicher Medienkanäle (Erweiterungsfähigkeit bezüglich mobiler Endgeräte)
- Möglichkeiten zur kurzfristigen, einfachen und sicheren Einbeziehung weiterer Partner in den Informationsraum
- Möglichkeit zur Archivierung und Reaktivierung von Projektdaten für Folgevorgänge

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

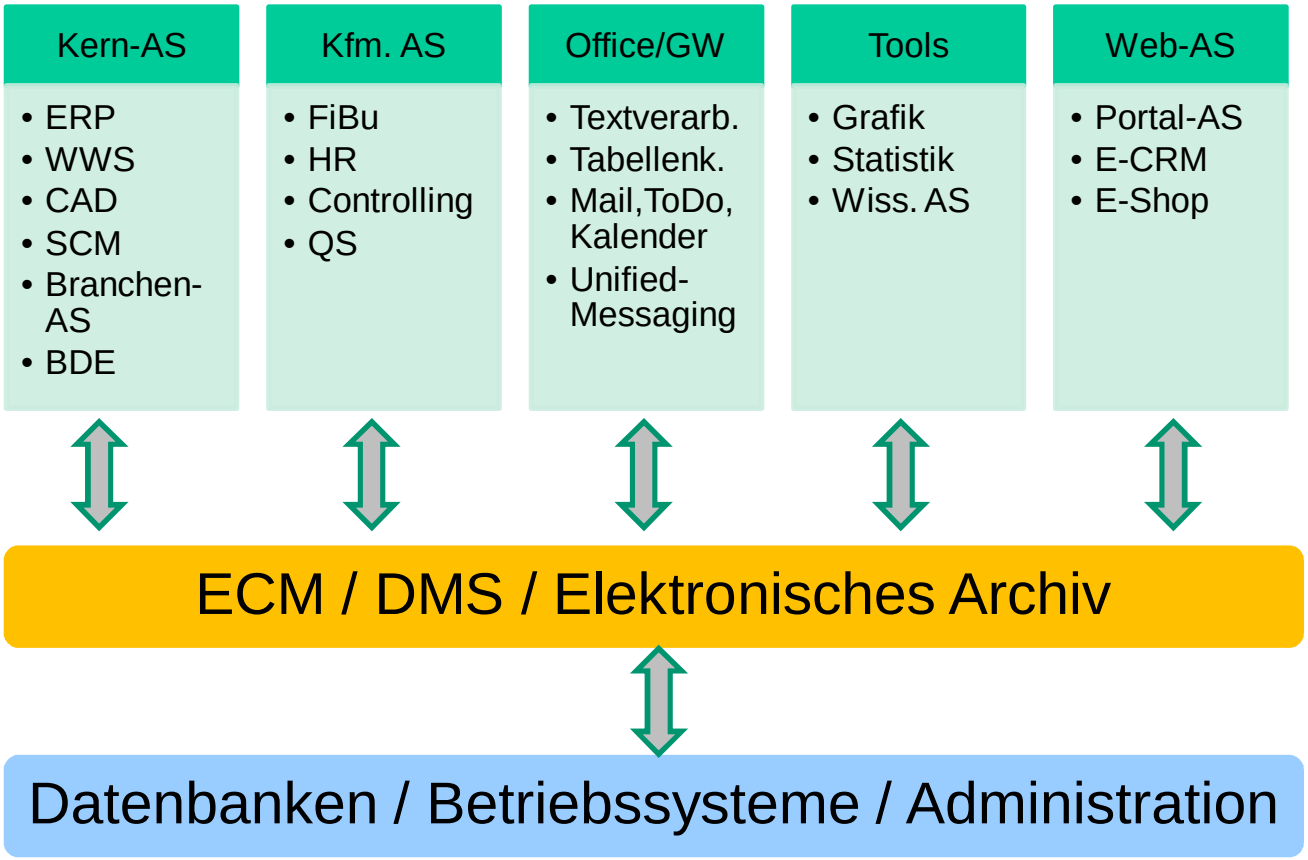
IuK-Compliance-Management (CM) – im Rahmen Systementwicklung am Bsp. ECM / DMS / Elektron. Archiv

Durchgängiges Berechtigungssystem

Fristenüberwachung und -einhaltung

Übergreifende Gewährleistung vollständiger Recherchierbarkeit

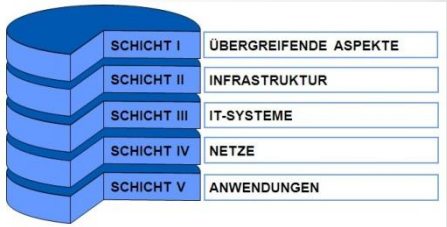
Systematische Berücksichtigung von Compliance-Aspekten bereits bei Konzeption, Entwicklung und Einführung



CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Werkzeuge (1)
Standard-Verfahren und Referenzmodelle (Auswahl)

- COBIT – Control Objectives for Information and Related Technology (generisches und einheitliches Planungs- und Beschreibungsmodell der IT; Grundlage für Prüfungen, Wissensvermittlung zur IT-Revision)
- UCF – Unified Compliance Framework (handlungsorientierte und hierarchisch gegliederte Sammlung von regulatorischen Anforderungen / Auswirkungsbereichen
  - Beschaffung von Technologien und Dienstleistungen, Prüfung und Risikomanagement, Entwicklung / Entwurf und Einführung, Unternehmensführung und -ziele, Management des IT-Personalwesens, Betriebsführung, Überwachen und Messen, Physische Sicherheit, Daten- u. Informationsschutz, Datensicherung, Wiederanlauf, technische Sicherheit, Konfigurationsmanagement
- BSI-Grundschutzhandbuch
  - Schichtenmodell: Übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze, Anwendungen
- Normfamilie ISO 27K (Information technology - Security techniques)
- ITIL – Information Technology Infrastructure Library (Verfahrens-empfehlung für Planung, Betrieb, Überwachung, Steuerung von IT-Services)



CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

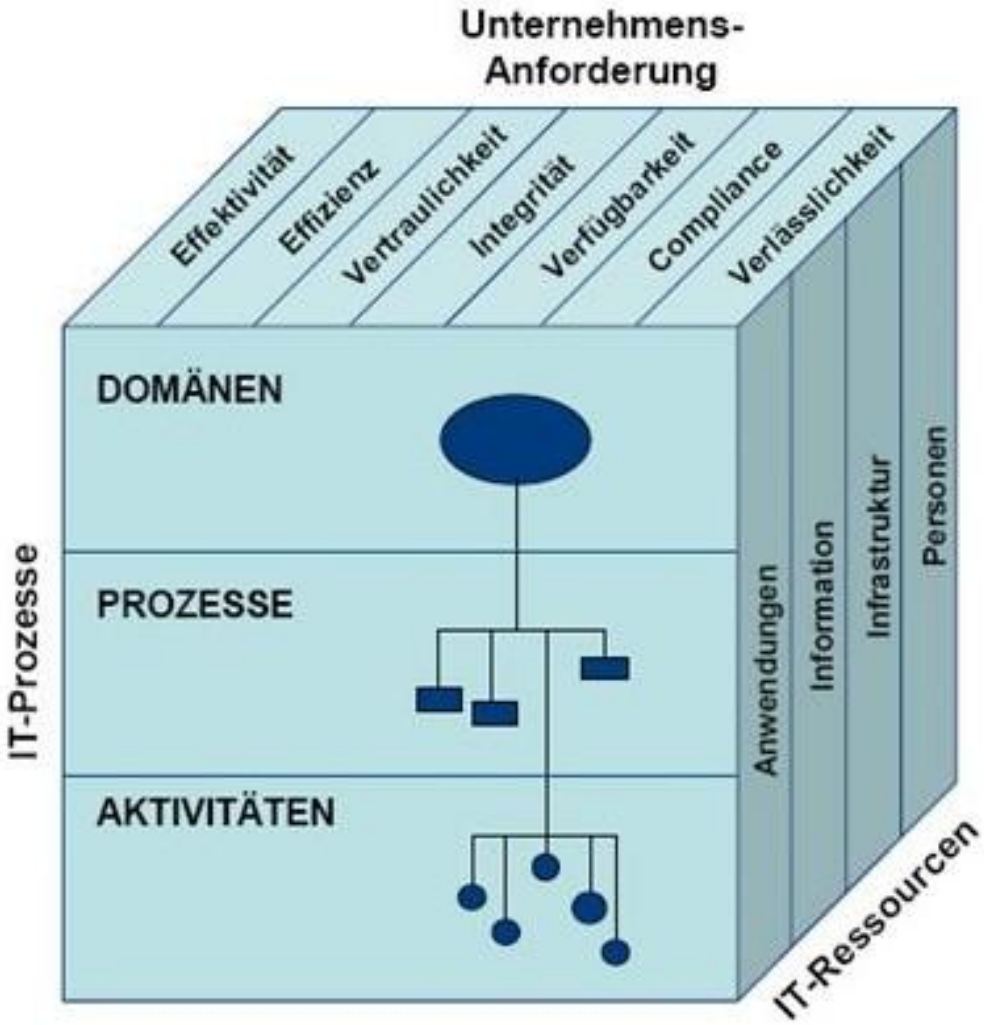
IuK-Compliance-Management (CM) – Werkzeuge (2)
Vorgehensmodell Initialprojekt lt. Bothe (Auswahl)

Haupt-modul	Schritt-Nr.	Schrittbezeichnung
I	1	Compliance-Programm/ -Policy
I	2	Gesetzliche Vorgaben identifizieren
I	3	Aufbauorganisation und Stellenbeschreibungen
I	4	Personalabteilung und Personalakte
I	5	Geschäftsprozessanalyse
I	6	Geschäftsziele definieren
I	7	IT-„Best Practice"-Verfahren identifizieren
I	8	Kompetenzmodell (Rollen und Verantwortlichkeiten)
I	9	Ablauforganisation (IT-Verfahrensanweisungen/ Standard Operating Procedure - SOP)
I	10	IT-Strategie definieren
I	11	Kontinuierlicher Verbesserungsprozess (KVP und PDCA-Zyklus - Plan-Do-Check-Act[186])
II	12	Erfassung von Applikationssystemen (Anwendungen)
II	13	Erfassung von Hardware mit speziellen Compliance-Anforderungen (hier Laborgeräte)
II	14	Erfassung von Hardware (hier IT-Infrastruktur)
II	15	Analyse der Systemkomponenten (HW, SW, Geräte)
II	16	Analyse der Schnittstellensysteme
II	17	Analyse der IT-Compliance-Relevanz für alle Systeme

Rath / Sponholz, 2009, S. 146

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Werkzeuge (3)
CobiT-Würfel als mehrdimensionales System-Modell



CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Werkzeuge (4)
Best Practice in Verbindung mit Compliance-Reifegrad

1. Schutz und Trennung um Zugriff auf sensitive Daten
2. Messbare Kontrollziele
3. Einsatz von Grundsatzrichtlinien (Policies) und Standards (Frameworks)
4. Allgemeingültige IT-Verfahrensrichtlinien
5. Konsistente IT-Konfiguration
6. Vermehrter Einsatz und Automation technischer Kontrollen
7. IT-Change-Management und Verhinderung unautorisierter Änderungen
8. Kontinuierliche Überwachung, Messungen und Berichterstattungen

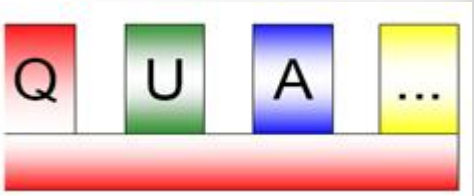
(vgl. IT Policy Compliance Group)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Werkzeuge (5)
Einordnung in Konzept des „Integrierten Managements“

- Integration der IuK-Governance-Inhalte in das übergeordnete System des Integrierten Managements inkl. des Corporate Governance
- Option lt. Forschungsprojekt „The Extended QMS“ der GFE Gesellschaft für Fertigungstechnik und Entwicklung e.V.:
  - Ansatz der partiellen Integration der Teilsysteme Qualitätsmanagement, Arbeitsschutz, Umweltschutz, .., wobei ein Teilsystem-Regelwerk als Basisstruktur verwendet wird; gemeinsame ähnliche Anforderungen werden vereinheitlicht, differenzierte Forderungen werden „angedockt“

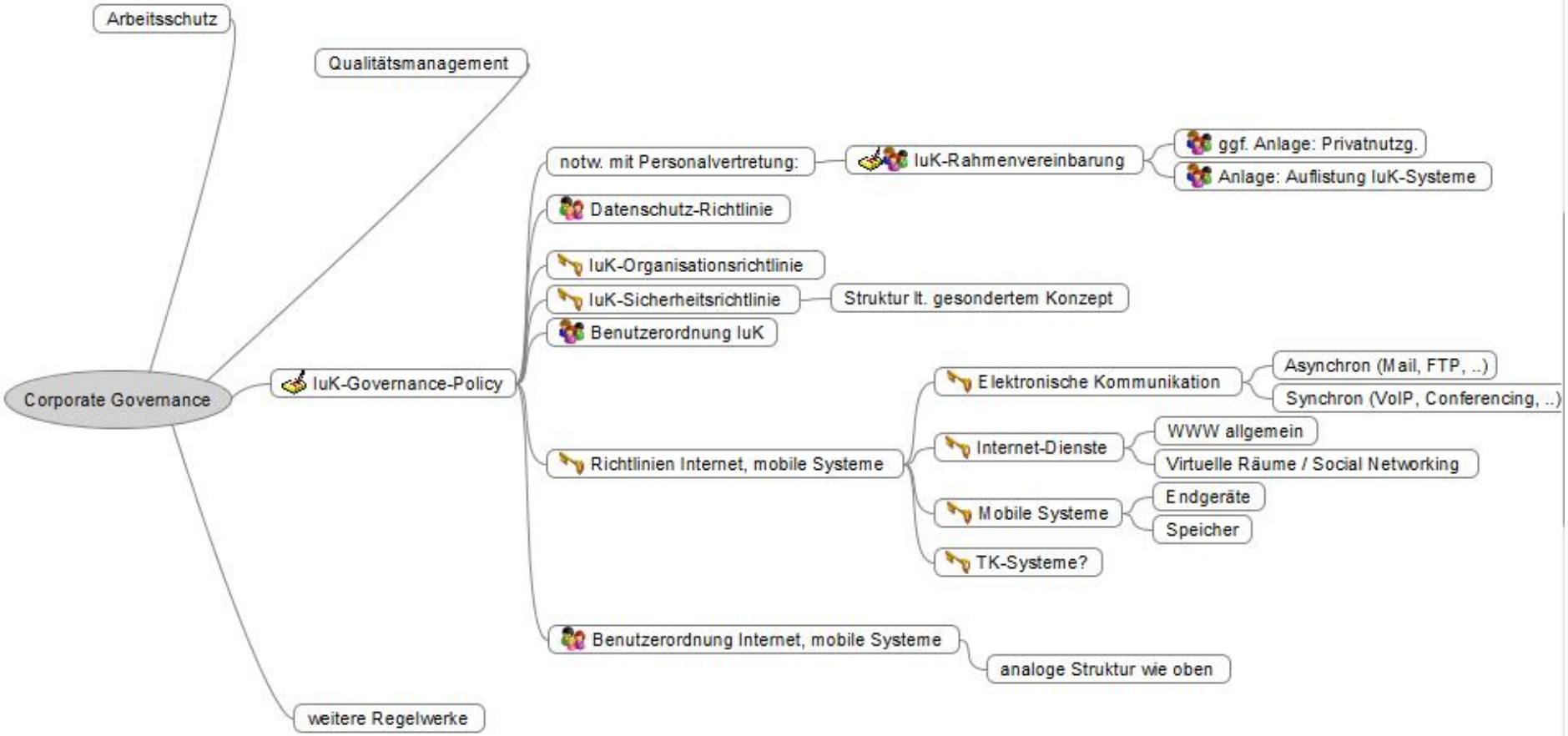
... von Teilsystemen zum integrierten Managementsystem



The Extended QMS
(GFE e.V. Schmalkalden)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Werkzeuge (6)
Einordnung im Kontext Anweisungssystem IuK-Sicherheit



Schwerpunkt:
Handhabung für Pflege, Referenzierbarkeit, Rechercheanforderung

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

IuK-Compliance-Management (CM) – Zusammenfassung wesentlicher Maßnahmebereiche

- Informationsschutz zur Wahrung der Vertraulichkeit
- Gewährleistung der technischen und organisatorischen Verfügbarkeit (Notfallplanung, Wiederanlaufoption durch Redundanz, ..)
- Schutz der Datenintegrität (Virenschutz, ..)
- Prozeßstabilität und –sicherheit der IuK-Prozesse
- Gewährleistung der physischen Sicherheit
- Datenaufbewahrung und –archivierung
- Mitarbeitermanagement mit Hinblick auf IuK-Compliance
- Wirksames IuK-Compliance-Management durch alle Phasen (Plan-Do-Check-Act)
- Kontrolle der ausgelagerten Bereiche

(vgl. Rath / Sponholz, 2009, S. 198 ff.)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Zusammenfassung / Thesen / Empfehlungen (1)

1. Trends, wie Personen-zentriertes Management, Social Business, Mobilität von Arbeitswelten sowie die fortschreitende Multifunktionalität von IT-Komponenten, befördern und benötigen IuK-Compliance-Mechanismen im Sinne selbst tragender Institutionen (Automatisierung und Kompetenz / Compliance-Kultur).

2. Das in Ansätzen vorgestellte und parziell bereits getestete IuK-CM-Referenzmodell mit den Komponenten Quellen-Objekte-Management (QOM) für KMU basiert auf dem Kern-Werkzeug IuK-Compliance-Inventar/-Monitoring bei Berücksichtigung unterschiedlicher Wirkungsintensitäten von Regulierungsmechanismen.

3. IuK-Compliance-Management muss in für KMU praktikable, integrierte Management-Konzepte eingebunden werden (GRC, Extended QM) und so als Markterfolgsfaktor Alleinstellungsmerkmale für ein Unternehmen ermöglichen.

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Zusammenfassung / Thesen / Empfehlungen (2)

4. „IuK-Compliance-Processing“ (im Sinne Aufbereitung / Veredelung): Externe und interdisziplinäre Kompetenz muss „in die Prozesse“. Daraus ergeben sich neue Forderungen und Chancen für ein Dienstleistungs- bzw. Consulting-Umfeld unter Nutzung moderner Technologien, wie SOA oder App-Entwicklung.

5. Nachhaltige IuK-Compliance in KMU verlangt nach spezifischen Werkzeugen und Methoden. Hier kann eine zielgerichtete interdisziplinäre Forschung unter Integration von Fachrichtungen, wie Wirtschaftsrecht, Wirtschaftsinformatik, Betriebswirtschaft aus dem Hochschulbereich in Zusammenarbeit mit Praxispartnern und Anwendern aus meiner Sicht einen wesentlichen und wünschenswerten Beitrag leisten.
   -> Arbeitstitel für erste Interessenten: „IuK-Compliance-Utilities“ ☺

Danke für Ihre Aufmerksamkeit!

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Literaturverzeichnis

- Klotz, Michael: IT-Compliance, 1.Auflage, Heidelberg 2009
- Kampffmeyer, Ulrich: Information Management Compliance, PROJECT CONSULT Whitepaper, Hamburg, September 2007
  (Quelle: http://www.project-consult.de/ecm/wissen/whitepaper, Zugriff 24.06.2012)
- Kampffmeyer, Ulrich: IBM Whitepaper , GRC – Governance, Risk Management & Compliance, Dezember 2009
  (Quelle: http://www.project-consult.de/ecm/wissen/whitepaper, Zugriff 24.06.2012)
- Rath, Michael: Law and Order. Was ist IT-Compliance, in Computerwoche,
  (Quelle: http://www.computerwoche.de/590497 , Zugriff April 2012)
- Rath, Michael / Sponholz, Rainer: IT-Compliance, Berlin 2009

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Man kann den Wind nicht ändern, aber die Segel richtig setzen!

Bildquelle: home.tiscali.de/daabov/

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012

Nutzen- und Wirtschaftlichkeits-Aspekte

- Erfolgs- / Bewertungskriterien zu IuK-CM-Elementen
  - Bindungswirkung

„Das Thema Compliance ist nicht nur aufgrund seiner Komplexität, sondern auch aufgrund der nur schwer ermittelbaren Rentabilität so wenig greifbar. Daher variieren die Meinungen bezüglich des positiven Nutzens von Compliance sehr stark …“

Prof. Michael Amberg, Dekan Friedrich Alexander Universität Erlangen-Nürnberg
(zitiert in Rath / Sponholz, S.97)

CETIMA Software & Consulting GmbH, www.cetima.de; © CETIMA 2012