

**DIENSTORIENTIERTE IT-SYSTEME FÜR  
HOCHFLEXIBLE GESCHÄFTSPROZESSE**

BAMBERG • ERLANGEN-NÜRNBERG • REGENSBURG



**Stephan Weber, Dieter Bartmann**

**IT-Compliance im Kontext von  
hochflexiblen Geschäftsprozessen**

**Herausgeber:**

---

Prof. Dr. Dieter Bartmann  
Prof. Dr. Freimut Bodendorf  
Prof. Dr. Otto K. Ferstl  
Prof. Dr. Elmar J. Sinz

forFLEX ist Mitglied in



---

**Universität Bamberg**

**Universität Regensburg**

**Universität Erlangen-Nürnberg**

---

**Stephan Weber, Dieter Bartmann**

**IT-Compliance im Kontext von  
hochflexiblen Geschäftsprozessen**

**forFLEX-Bericht-Nr.: forFLEX-2011-011**

© Bayerischer Forschungsverbund forFLEX - Dienstorientierte IT-Systeme für hochflexible Geschäftsprozesse

Bamberg, Erlangen-Nürnberg, Regensburg 2011

Alle Rechte vorbehalten. Insbesondere ist die Überführung in maschinenlesbare Form sowie das Speichern in Informationssystemen, auch auszugsweise, nur mit schriftlicher Einwilligung von forFLEX gestattet.

## Zusammenfassung

Die Merkmale von hochflexiblen Geschäftsprozessen (hGP) wie die unbekannte Variantenvielfalt, das Verschwimmen der Grenzen von Planung und Ausführung sowie der Projektcharakter werfen erweiterte Fragestellungen im Bereich IT-Compliance auf. In diesem Arbeitsbericht wird der Frage nachgegangen, wie organisationsübergreifende Geschäftsprozesse in sich ad-hoc bildenden Wertschöpfungsnetzen Compliance-konform gestaltet werden können, d. h. wie das Prozessverhalten so geführt und gleichzeitig beschränkt werden kann, dass keine gesetzlichen und regulatorischen Anforderungen an die IT verletzt werden.

Die Analyse der betreffenden Gesetze und Regularien hat gezeigt, dass inhaltlich überwiegend sehr abstrakte und wenig umsetzungsnahe Vorgaben definiert werden. Deshalb sind zur Transformation in konkrete Anweisungen Standards/IT-Frameworks wie ISO/IEC 27001/2, Control Objectives for Information and Related Technology (CobiT) oder IT Infrastructure Library (ITIL) notwendig, weil diese zum Teil sehr konkrete Handlungsanweisungen beinhalten. Jedoch erfordert netzwerkbezogene Hochflexibilität in einem sich ad-hoc bildenden Instanz übergreifenden Wertschöpfungsnetz zwischen den Instanzen die Transparenz der Qualität der jeweiligen internen IT-Compliance-Regelungen, da nur auf diese Weise sowohl die Bewertung des eigenen Zustands als auch den des jeweiligen potenziellen Kopplungspartners möglich ist. Hierzu ist ein akzeptiertes Reifegradmodell notwendig, um aus organisatorischer Sicht ein einheitliches IT-Compliance-Niveau entlang der entstehenden Prozesskette zu erreichen.

Eine eingehende Untersuchung von ausgewählten Standards/IT-Frameworks hat ergeben, dass CobiT die definierten Anforderungen am besten erfüllt. Zudem wurde die Notwendigkeit der Werkzeug-Unterstützung festgestellt, da gerade die Situationstransparenz auf Knopfdruck über den Umsetzungs- und Qualitätsstand einzelner Aspekte des jeweils verwendeten Standards/IT-Frameworks eine wichtige Grundlage für die (zeitnahe) Entscheidung darstellt, ob die Zusammenarbeit mit einer Instanz unter IT-Compliance-Gesichtspunkten zustande kommt.

Weiterhin muss eine ausreichende Objektivität hinsichtlich des jeweiligen IT-Compliance-Status gewährleistet sein, damit die getätigten Aussagen auch den korrekten Stand im Unternehmen widerspiegeln. Dazu müssen sich gerade in hochflexiblen Geschäftsprozessen die potenziellen Partner gegenseitig vertrauen. Dies kann in Form einer Bestätigung des IT-Compliance-Status durch die Interne Revision oder eine vertrauenswürdige dritte Instanz erreicht werden.

# Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>Abbildungsverzeichnis .....</b>   | <b>iv</b> |
| <b>Abkürzungsverzeichnis .....</b>   | <b>v</b>  |
| <b>1 Problemstellung, Zielsetzung und Aufbau.....</b>  | <b>1</b>  |
| <b>2 Grundlagen der IT-Compliance .....</b>  | <b>2</b>  |
| 2.1 Begriffsbestimmung .....   | 3         |
| 2.2 Ausgewählter Überblick über branchenunspezifische IT-Compliance-<br>Anforderungen.....                 | 5         |
| 2.2.1 Bundesdatenschutzgesetz .....  | 5         |
| 2.2.2 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich.....                                     | 7         |
| 2.2.3 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme.....                                    | 8         |
| 2.2.4 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen .....                           | 9         |
| 2.3 Konsequenzen bei Nichteinhaltung der IT-Compliance .....   | 9         |
| 2.4 Probleme bei der Umsetzung bzw. Einhaltung von IT-Compliance-Anforderungen ..                          | 11        |
| <b>3 Eignung von Standards bzw. IT-Frameworks im Kontext hochflexibler<br/>    Geschäftsprozesse .....</b> | <b>13</b> |
| 3.1 Allgemein .....  | 13        |
| 3.2 Anforderungen.....   | 14        |
| <b>4 Darstellung ausgewählter Standards und IT-Frameworks .....</b>  | <b>15</b> |
| 4.1 IT-Grundschutz.....  | 15        |
| 4.2 ISO/IEC 27002 .....  | 17        |
| 4.3 IT Infrastructure Library.....   | 18        |
| 4.4 Control Objectives for Information and Related Technology .....  | 20        |
| <b>5 Bewertung.....</b>  | <b>22</b> |
| <b>6 Darstellung und Vergleichbarkeit der IT-Compliance-Situation .....</b>                                | <b>24</b> |
| 6.1 Notwendigkeit der Werkzeug-Unterstützung.....  | 24        |
| 6.2 Objektivierung der IT-Compliance-Situation.....  | 25        |
| <b>7 Zusammenfassung .....</b>   | <b>26</b> |
| <b>Literaturverzeichnis .....</b>  | <b>27</b> |

## Abbildungsverzeichnis

|               |   |    |
|---------------|---|----|
| <b>Abb. 1</b> | Zwiebelmodell für Compliance-relevante Regelwerke.....  | 4  |
| <b>Abb. 2</b> | Durchschnittliche Kosten für Einhaltung der Compliance und bei Nichteinhaltung der Compliance ..... | 10 |
| <b>Abb. 3</b> | Anzahl an vorgeschriebenen, separaten gesetzlichen Regulierungen nach Ländern (Mittelwerte) .....   | 11 |
| <b>Abb. 4</b> | An IT-Compliance beteiligte Gruppen und Funktionen.....   | 12 |
| <b>Abb. 5</b> | Aufbau der IT-Grundschutz-Kataloge.....   | 16 |
| <b>Abb. 6</b> | Aufbau des ISO/IEC 27002.....   | 17 |
| <b>Abb. 7</b> | Der ITIL v3 Lebenszyklus.....   | 19 |
| <b>Abb. 8</b> | Der CobiT-Würfel .....  | 21 |
| <b>Abb. 9</b> | Analyse der Standards/IT-Frameworks.....  | 23 |

## Abkürzungsverzeichnis

|         |  |
|---------|--|
| AktG    | Aktiengesetz   |
| AO      | Abgabenordnung   |
| AWV     | Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.             |
| BDSG    | Bundesdatenschutzgesetz  |
| BSI     | Bundesamt für Sicherheit in der Informationstechnik                  |
| CCTA    | Central Computer and Telecommunications Agency                       |
| CMMI    | Capability Maturity Model Integration                                |
| CobiT   | Control Objectives for Information and Related Technology            |
| DIN     | Deutsches Institut für Normung e. V.                                 |
| GDPdU   | Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen |
| GmbHG   | Gesetz betreffend die Gesellschaften mit beschränkter Haftung        |
| GoBIT   | Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz               |
| GoBS    | Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme         |
| HGB     | Handelsgesetzbuch  |
| hGP     | hochflexibler Geschäftsprozess                                       |
| IEC     | International Electrotechnical Commission                            |
| ISACA   | Information Systems Audit and Control Association                    |
| ISO     | International Organization for Standardization                       |
| ITIL    | IT Infrastructure Library  |
| KonTraG | Gesetz zur Kontrolle und Transparenz im Unternehmensbereich          |
| KWG     | Kreditwesengesetz  |
| OGC     | Office of Government Commerce  |
| RACI    | Responsible, Accountable, Consulted, Informed                        |
| SigG    | Signaturgesetz   |
| SLA     | Service Level Agreement  |
| TMG     | Telemediengesetz   |
| UStG    | Umsatzsteuergesetz   |

# 1 Problemstellung, Zielsetzung und Aufbau

Die zunehmende Globalisierung und die damit verbundene steigende Umweltdynamik und -komplexität führen zu erweiterten bzw. veränderten Anforderungen an die Geschäftsprozesse der Unternehmen. Um im Wettbewerb dauerhaft erfolgreich zu bestehen, ist es unabdingbar, auf unvorhersehbare Ereignisse und ad-hoc getroffene Entscheidungen, wie z. B. die rasche Etablierung einer (zeitlich befristeten) Kooperation zwischen Unternehmen, die Erschließung neuer Märkte oder die umgehende Umsetzung von neuen bzw. geänderten Gesetzen und Regularien, flexibel und schnell reagieren zu können. Traditionell weitgehend starre und festverankerte Geschäftsprozesse sowie die unterstützenden IT-Systeme lassen sich jedoch meist nur mit erheblichem zeitlichen und monetären Aufwand entsprechend den jeweiligen aktuell vorherrschenden Anforderungen anpassen.

Die Bewältigung der genannten Beispiele erfordert flexible bzw. hochflexible Geschäftsprozesse (hGP). Diese lassen sich anhand der drei Merkmale (1) Kontextsensitivität, (2) unvollständige Planbarkeit und (3) Überlappung von Planung und Ausführung charakterisieren (Pütz et al. 2009, S. 1). Als Folge daraus müssen auch die unterstützenden IT-Systeme umso flexibler gestaltet sein, je mehr hGP-Merkmale von einem Prozess erfüllt werden (Pütz et al. 2009, S. 2). Denn nur so lassen sich hochflexible Geschäftsprozesse gestalten und realisieren.

Neben der technischen Herausforderung, hochflexible Geschäftsprozesse zu etablieren, muss aber auch zugleich die gesetzeskonforme Ausgestaltung gewährleistet werden. Gerade die Unvorhersehbarkeit als übergreifender Aspekt der aufgeführten Merkmale von hochflexiblen Geschäftsprozessen erschwert die permanente, nachweisbare Einhaltung der geltenden rechtlichen und regulatorischen Anforderungen. Dabei besteht insbesondere die Herausforderung darin, sowohl auf der technischen Ebene (z. B. IT-Systeme) als auch auf der organisatorischen Ebene (z. B. Personal) in einem hochflexiblen Geschäftsprozess zu jeder Zeit die Gesetzes- bzw. Compliance-Konformität zu gewährleisten.

In diesem Zusammenhang kommt erschwerend hinzu, dass sowohl der Gesetzgeber als auch die Aufsichtsorgane zunehmend eine Abkehr von der traditionell regelbasierten Aufsicht hin zu einer prinzipienbasierten Aufsicht vollziehen, d. h. den Unternehmen wird in Form von sehr generalistisch gehaltenen Empfehlungen bzw. Handlungsanweisungen bewusst mehr Gestaltungsspielraum für die Erfüllung der entsprechenden Gesetze und Regularien gegeben (Bretz et al. 2007, S. 3). Damit wird dem Grundsatz der Verhältnismäßigkeit Rechnung getragen. So wird z. B. das Wort „angemessen“ im § 9 BDSG (Bundesdatenschutzgesetz 2009) von Unternehmen unterschiedlicher Größe und Komplexität auch unterschiedlich ausgelegt. Als Konsequenz sind somit auch die jeweiligen unternehmensspezifischen Regelungen und Richtlinien entsprechend mehr oder weniger scharf bzw. restriktiv formuliert. Diese Tatsache ist vor dem Hintergrund organisations- bzw. unternehmensübergreifender Geschäftsprozesse als problematisch zu betrachten, da in diesem Fall Informationen von Unternehmen mit unterschiedlichen Ausprägungen von IT-Compliance-Konformität empfangen, verarbeitet und wei-

tergegeben werden. Damit gilt auch hier der folgende Grundsatz: „Eine Kette ist nur so stark wie ihr schwächstes Glied“.

Eine weitere Herausforderung stellt die Identifizierung und die Vergleichbarkeit der unterschiedlichen Ausprägungen von IT-Compliance-Konformität dar. Voraussetzung hierfür ist die Transparenz über die Qualität der jeweiligen unternehmensspezifischen IT-Compliance-Regelungen.

Die Zielsetzung dieses vorliegenden Berichts besteht im Wesentlichen darin, ausgewählte Standards bzw. IT-Frameworks auf ihre Eignung im Kontext von hGP zu untersuchen. Zu diesem Zweck werden spezifische Anforderungen unter Berücksichtigung der hGP-Eigenschaften definiert, anhand derer im Anschluss die Bewertungen vorgenommen werden. Weiterhin wird der Fragestellung nachgegangen, wie eine ad-hoc Darstellung der jeweiligen IT-Compliance-Situation im Unternehmen ermöglicht werden kann und welche Möglichkeiten bestehen, gerade unter fremden Kopplungspartnern die Korrektheit der gemachten Angaben zu gewährleisten.

Der Aufbau des Berichts gestaltet sich wie folgt: In Kapitel 2 erfolgt zunächst eine kritische Auseinandersetzung mit dem Begriff „IT-Compliance“ und zur inhaltlichen Konkretisierung dieses Begriffs eine Darstellung ausgewählter, branchenunspezifischer IT-Compliance-Anforderungen. Zudem werden allgemeine Konsequenzen bei Verletzung bzw. Nichteinhaltung von IT-Compliance-Vorschriften sowie die Schwierigkeiten bei deren Umsetzung insbesondere im Kontext von hGP aufgezeigt. Kapitel 3 beinhaltet zum einen eine grundlegende Abgrenzung der Begriffe *Standard* und *IT-Framework* und veranschaulicht mögliche Vorteile die eine Anwendung von Standards/IT-Frameworks bietet. Zum anderen werden unter Beachtung der Eigenschaften von hGP entsprechende Anforderungen an Standards/IT-Frameworks definiert. Im nachfolgenden Kapitel 4 erfolgt die wesentliche Darstellung von vier ausgewählten Standards bzw. IT-Frameworks. Im Anschluss daran wird in Kapitel 5 deren Bewertung anhand der in Kapitel 3 aufgestellten Anforderungen durchgeführt. Die Notwendigkeit der Werkzeug-Unterstützung und die Gewährleistung der Korrektheit der gemachten Angaben über den IT-Compliance-Status werden in Kapitel 6 thematisiert. Abschließend liefert Kapitel 7 eine Zusammenfassung über die gewonnenen Erkenntnisse.

## 2 Grundlagen der IT-Compliance

In diesem Kapitel erfolgt zunächst eine kritische Auseinandersetzung mit verschiedenen Definitionen von IT-Compliance. Im Anschluss daran werden einige ausgewählte IT-Compliance-Anforderungen dargestellt und mögliche Auswirkungen aufgrund der Nichteinhaltung von IT-Compliance-Vorschriften sowie Herausforderungen bei deren Umsetzung thematisiert.

## 2.1 Begriffsbestimmung

In der Literatur sind verschiedene Definitionen zu finden, die den Begriff unterschiedlich stark eingrenzen. Im Folgenden werden einige davon aufgezeigt, um diesen Sachverhalt darzustellen.

Der Begriff „Compliance“ stammt aus dem Englischen und ist grundsätzlich in einem englischen Wörterbuch folgendermaßen definiert:

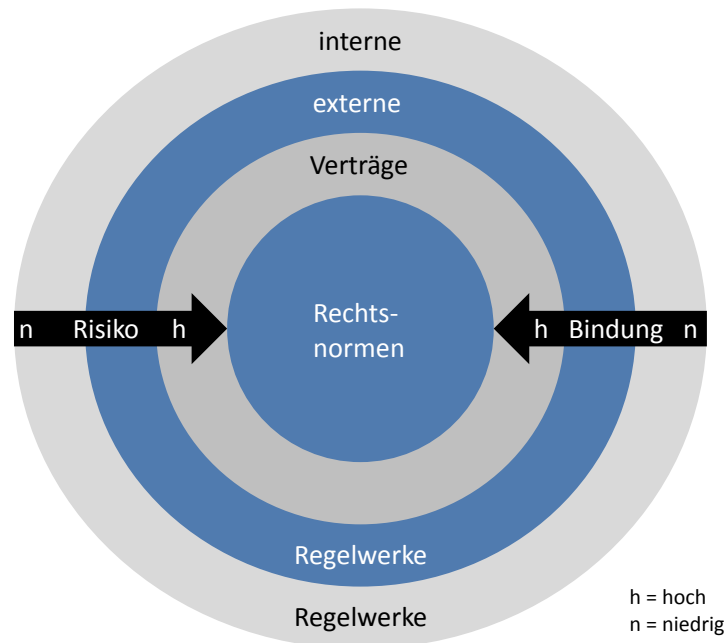
„Compliance /kəmplaɪəns/ noun [U] ~ **(with sth)** the practice of obeying rules or requests made by people in authority: procedures that must be followed to ensure full compliance with the law ◊ Safety measures were carried out in compliance with paragraph 6 of the building regulations. NON-COMPLIANCE – see also COMPLY” (Hornby 2007, S. 309).

Diese Definition ist sehr eng gefasst, denn Compliance bezieht sich hier ausschließlich auf die Befolgung von Regeln bzw. Gesetzen, verfasst von Behörden. Eine ähnlich stark simplifizierte, aber grundlegende Begriffsbestimmung nimmt Hauschka vor. Danach bedeutet Compliance ohne konkreten Bezugsrahmen in etwa „Befolgung, Übereinstimmung, Einhaltung von bestimmten Geboten“, d. h. Unternehmen und Organe müssen sich innerhalb geltender Rechtsnormen und -vorschriften bewegen (Hauschka 2007a, S. 2).

Neben dem allgemeinen Compliance-Begriff, der sich generalistisch auf jeden (Funktions-) Bereich einer Organisation anwenden lässt, hat sich der Ausdruck IT-Compliance speziell für den Bereich der Informationstechnologie etabliert. Dies ist insbesondere auf den enormen Bedeutungszuwachs der IT für Unternehmen in den letzten 10 Jahren und der damit verbundenen Notwendigkeit der Berücksichtigung der IT in Gesetzen und Regularien zurückzuführen.

Klotz bezeichnet IT-Compliance als „einen Zustand, in dem alle für die IT des Unternehmens relevanten Vorgaben nachweislich eingehalten werden“ (Klotz 2009, S. 6). Dabei sind ausdrücklich alle IT-Leistungen, also sowohl unternehmensinterne als auch -externe (z. B. im Rahmen von Outsourcing), zu berücksichtigen (Klotz 2009, S. 6).

Welche Vorgaben als relevant angesehen werden bzw. auf welche Art diese klassifiziert werden können, verdeutlicht nachfolgende Abbildung.



**Abb. 1** Zwiebelmodell für Compliance-relevante Regelwerke  
(Klotz und Dorn 2008, S. 11)

- **Rechtsnormen**

Unter diesen Begriff fallen sowohl nationale Gesetze und Rechtsverordnungen als auch internationale Vorschriften. Exemplarisch für nur in Deutschland geltende Bestimmungen mit starkem Fokus auf die IT lassen sich das Signaturgesetz (SigG), das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG) nennen. Als Beispiel für eine länderübergreifend bindende Verordnung mit Auswirkungen auf die IT kann die 8. EU-Richtlinie (auch Euro-SOX genannt) aufgeführt werden. Diese muss von allen Mitgliedern der Europäischen Union bis zu einem bestimmten Datum in nationales Recht umgesetzt werden. (Klotz und Dorn 2008, S. 11-12; Klotz 2009, S. 21-22)

- **Verträge**

Darunter sind alle Kontrakte und Vereinbarungen zu verstehen, die von einem Unternehmen mit Kunden, Lieferanten und sonstigen Marktteilnehmern abgeschlossen werden und entweder IT-spezifische Leistungen als (Haupt-) Gegenstand wie z. B. Outsourcing eines Rechenzentrums enthalten oder IT-relevante Absprachen (z. B. Verschlüsselung beim Informationsaustausch) als notwendige Ergänzung zum Vertragsgegenstand (z. B. Einkaufskooperation) beinhalten. (Klotz und Dorn 2008, S. 13; Klotz 2009, S. 23)

- **Externe Regelwerke**

Alle unternehmensextern geschaffenen IT-bezogenen Frameworks und (Best Practice) Standards fallen in diese Kategorie. Dazu zählen unter anderem IT-Grundschutz, ISO/IEC 27001/2, IT Infrastructure Library (ITIL) und Control Objectives for Information and related Technology (CobiT). Diese Standards bzw. Frameworks werden von verschiedensten Organisationen wie Behörden (z. B. Bundesamt für Sicherheit in

der Informationstechnik (BSI)), Normierungsinstituten (International Organization for Standardization (ISO)) oder Verbänden (Information Systems Audit and Control Association (ISACA)) herausgegeben. (Klotz und Dorn 2008, S. 13; Klotz 2009, S. 24)

- **Interne Regelwerke**

Dieser Kategorie sind alle unternehmensintern erzeugten Verfahrensanweisungen, Regelungen, Richtlinien und Service Level Agreements (SLAs) zu zuordnen, soweit diese IT-bezogene Inhalte aufweisen. Als Beispiel können hier IT-Sicherheitsvorschriften und Richtlinien zum Umgang mit Passwörtern und E-Mail genannt werden. (Klotz und Dorn 2008, S. 13-14; Klotz 2009, S. 24)

Im Vergleich zu den drei anderen Kategorien ist der Bindungsgrad und das Risiko bei den Rechtsnormen am höchsten, da geltende Gesetze und Rechtsverordnungen ohne Ausnahmen oder Wahlmöglichkeiten von allen, die angesprochen werden, unbedingt einzuhalten sind. Die internen Regelwerke sind hingegen nur für dasjenige Unternehmen relevant, welches diese Richtlinien verfasst hat und freiwillig einhält. Daher weisen unternehmensinterne Regelwerke den niedrigsten Bindungsgrad und das geringste Risiko auf. (Klotz 2009, S. 20)

Gaulke definiert IT-Compliance in einer sehr ähnlichen Art und Weise, da auch hier eine Differenzierung nach relevanten Gesetzen und Rechtsverordnungen, vertraglichen Verpflichtungen sowie externen und internen Richtlinien erfolgt. Jedoch wird in dieser Begriffsbestimmung der Aspekt der nachweislichen Einhaltung noch genauer konkretisiert. So sind von einer Organisation Prozesse einzurichten, welche nicht nur die Einhaltung der relevanten Bestimmungen überwachen, sondern auch Nachweise für diese Konformität gegenüber internen und externen Interessengruppen erbringen. (Gaulke 2010, S. 183)

## **2.2 Ausgewählter Überblick über branchenunspezifische IT-Compliance-Anforderungen**

Auf Basis der Begriffsbestimmung im vorherigen Abschnitt wird in diesem Abschnitt ein Auszug von generellen rechtlichen und regulatorischen Anforderungen an die IT dargestellt, um den Begriff IT-Compliance inhaltlich beispielhaft zu konkretisieren.

### **2.2.1 Bundesdatenschutzgesetz**

Das Bundesdatenschutzgesetz (BDSG) wurde in der ursprünglichen Fassung am 27.01.1977 im Bundesgesetzblatt veröffentlicht und am 01.01.1978 offiziell in Kraft gesetzt, wobei dieses im Laufe der Zeit durch den Gesetzgeber immer wieder an die aktuellen Gegebenheiten angepasst wurde. Das BDSG regelt neben den Datenschutzgesetzen der einzelnen Bundesländer den Umgang (Erhebung, Verarbeitung und Nutzung) mit personenbezogenen Daten, die manuell oder in IT-Systemen verarbeitet werden, denn nach § 1 Abs. 1 BDSG besteht der Zweck

des Gesetzes darin, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (Bundesdatenschutzgesetz 2009).

Die Verdeutlichung der rechtlichen Anforderungen an die IT erfolgt exemplarisch anhand des § 9 Satz 1 BDSG. Dieser Paragraph besagt, dass „öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten“ (Bundesdatenschutzgesetz 2009). Dabei werden in der Anlage zu § 9 Satz 1 BDSG acht Kontrollmaßnahmen aufgeführt, die von Gola und Schomerus mit Beispielen unterlegt werden (Gola und Schomerus, S. 356-358):

- Die **Zutrittskontrolle** soll verhindern, dass Unbefugte physischen Zutritt zu Datenverarbeitungssystemen, die personenbezogene Daten verarbeiten, erlangen. Als Maßnahmen mit IT-Bezug können hier Chipkarten/Transponderkarten, Alarmanlagen und Videotechnik genannt werden.
- Das Ziel der **Zugangskontrolle** ist die Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen, also das unberechtigte Eindringen in ein EDV-System. Die Protokollierung der Passwortnutzung sowie die Passwortvergabe stellen beispielsweise geeignete IT-spezifische Methoden für die Zugangskontrolle dar.
- Mit der **Zugriffskontrolle** soll sichergestellt werden, dass Personen, die zur Nutzung eines Datenverarbeitungssystems autorisiert sind, ausschließlich auf Daten zugreifen können, für die sie zugriffsberechtigt sind. Dies kann unter anderem durch eine automatische Prüfung der Zugriffsberechtigung sowie durch die Protokollierung der Systemnutzung und Protokollauswertung erreicht werden.
- Der Schutz von Datenträgern vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen soll durch die **Weitergabekontrolle** gewährleistet werden. Als beispielhafte Maßnahmen sind die Datenverschlüsselung und die Vollständigkeits- und Richtigkeitsprüfung zu nennen.
- Die nachträgliche Überprüfung und Feststellung wer wann welche personenbezogene Daten in EDV-Systeme eingegeben, verändert, gelöscht oder entfernt hat, soll mit der **Eingabekontrolle** gewährleistet werden. Dies kann mit Hilfe der Protokollierung eingegebener Daten sowie von Verarbeitungsprotokollen realisiert werden.
- Zweck der **Auftragskontrolle** ist die Sicherstellung der korrekten Verarbeitung von personenbezogenen Daten durch den Auftragnehmer entsprechend den Anordnungen des Auftraggebers. Dabei sind unter anderem Maßnahmen hinsichtlich der Aufbewahrung von Datenträgern und bei Verlust von Datenträgern zu konzipieren.
- Das Ziel der **Verfügbarkeitskontrolle** ist der Schutz von personenbezogenen Daten vor zufälliger Zerstörung wie z. B. Brand, Erdbeben oder Blitzschlag. Als geeignete Methoden zum Aufrechterhalten der Verfügbarkeit können die Auslagerung von Siche-

rungskopien sowie das Vorhandensein von Katastrophenplänen (Business Continuity Management) aufgeführt werden.

- Die zweckbestimmte Verarbeitung (auch aus technischer Sicht) von personenbezogenen Daten soll mit Hilfe des **Trennunggebots** gewährleistet werden. Dies kann z. B. durch Zugriffsregelung, Mandantentrennung oder Dateiseparierung bei Datenbankprinzip erreicht werden.

Die Erläuterung der acht Kontrollmaßnahmen sowie die entsprechend dazu aufgeführten Beispiele verdeutlichen, wie stark die IT im Kontext des § 9 BDSG adressiert wird.

## 2.2.2 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Vor dem Hintergrund zahlreicher Unternehmenskrisen, der zunehmenden Globalisierung der Aktionärsstrukturen und der wachsenden Internationalisierung der Kapitalmärkte in Verbindung mit der Forderung der internationalen Vergleichbarkeit trat im Mai 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in Kraft (Schuppener und Tillmann 1999, S. 20). Als Artikelgesetz verändert bzw. ergänzt es bestehende Gesetze wie das Aktiengesetz (AktG) und das Handelsgesetzbuch (HGB). Das KonTraG verfolgt insbesondere zwei Ziele (Speichert 2007, S. 245):

- Korrektur von Verhaltensfehlsteuerungen und Schwächen im deutschen Unternehmenskontrollsystem des Aktienrechts und des Mitbestimmungsrechts
- Berücksichtigung der steigenden Ausrichtung deutscher Publikumsgesellschaften am Informationsbedarf internationaler Investoren

An Hand der folgenden Auszüge aus dem KonTraG lassen sich entsprechende Implikationen für die IT verdeutlichen.

§ 91 AktG wurde um einen neuen Absatz erweitert, der lautet:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Durch diese Erweiterung des § 91 AktG wird ausdrücklich betont, dass der Vorstand verpflichtet ist, ein angemessenes und funktionierendes Risikomanagement zu etablieren. Da mittlerweile nahezu alle Geschäftsprozesse in einem Unternehmen durch IT unterstützt werden, sind mit dem IT-Einsatz auch entsprechende Risiken verbunden, die im Rahmen eines (IT-) Risikomanagements identifiziert, bewertet, gegebenenfalls minimiert und kontrolliert werden müssen. Somit wird deutlich, dass diese gesetzliche Neuregelung auch die IT adressiert.

Das GmbHG wurde nicht explizit um eine solche Bestimmung erweitert, da laut der Gesetzesbegründung davon auszugehen ist, dass die Änderung des Aktiengesetzes auch eine Ausstrahlungswirkung auf GmbHs haben wird, welche in Größe, Komplexität und Struktur mit einer AG vergleichbar sind (Deutscher Bundestag 1998, S. 15).

Bezogen auf § 91 Abs. 2 AktG wurde auch der Prüfungsumfang des Abschlussprüfers dementsprechend angepasst. Dies erfolgte in § 317 Abs. 4 HGB:

„Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Da ein Überwachungssystem (in Form eines Risikomanagements) zum einen heutzutage häufig mit Hilfe von IT realisiert wird und zum anderen die IT als geschäftskritischen Faktor überwacht, sind die Auswirkungen dieser Neuregelung, auch bezogen auf die Interpretation von § 91 Abs. 2 AktG, auf die IT offensichtlich.

Als letzter Auszug werden die Änderungen von § 289 Abs. 1 HGB und § 315 Abs. 1 HGB erläutert. Die beiden Paragraphen wurden jeweils um folgenden Teilsatz erweitert:

„dabei ist auch auf die Risiken der künftigen Entwicklungen einzugehen“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Der Hintergrund dieser gesetzlichen Neuregelung liegt in der Tatsache begründet, dass Unternehmen nicht selten in eine Krise geraten sind oder Insolvenz anmelden mussten, obwohl sie kurz vorher vom Abschlussprüfer eine uneingeschränkte Bestätigung ihres Jahresabschluss- und Lageberichts erhalten hatten, wobei formalrechtlich dem Prüfer kein Vorwurf gemacht werden konnte. Um diesem Umstand zu begegnen ist der Lagebericht um einen Risikobericht zu ergänzen, in welchem die Risiken der künftigen Entwicklung dargestellt werden. Da die mit dem IT-Einsatz verbundenen Risiken durchaus einen bestandsgefährdenden Charakter einnehmen können, sind diese im Risikobericht zu erfassen. (Speichert 2007, S. 245; Bertele und Lehner 2008, S. 11)

### **2.2.3 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme**

Im Jahr 1995 veröffentlichte das Bundesministerium für Finanzen die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) als Verwaltungsanweisung, welche von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV) ausgearbeitet wurden. Die Zielsetzung bestand darin, die allgemeinen Grundsätze ordnungsmäßiger Buchführung (GoB) speziell für den Bereich der DV-gestützten Buchführung zu präzisieren. Ausgangspunkt waren hierbei insbesondere die §§ 238, 239, 257 und 261 HGB sowie die §§ 145-147 AO. (Bundesministerium der Finanzen 1995)

Anhand der nachfolgenden inhaltlichen Auszüge lassen sich die Implikationen für die IT in einem Unternehmen gut verdeutlichen. Gegenstand der GoBS ist unter anderem die Behandlung aufbewahrungspflichtiger Daten und Belege in elektronischen Buchführungssystemen sowie in Dokumentenmanagement- und Archivsystemen. Zudem werden Vorgaben für die Ausgestaltung der Verfahrensdokumentation, welche als Nachweis für den ordnungsgemäßen Betrieb des Systems dient, definiert. Weiterhin erfolgt im Zusammenhang mit DV-Unterstützung unerlässlich eine Erläuterung von Anforderungen an die Datensicherheit. (Henstorf et al. 2002, S. 13-47)

Gegenwärtig ist der Arbeitskreis 3.4<sup>1</sup> der AWW mit der Erstellung der Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT) als Nachfolger der GoBS beschäftigt, um dem aktuellen Stand der IT sowie den rechtlichen und regulatorischen Entwicklungen Rechnung zu tragen.

## **2.2.4 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen**

Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) wurden im Jahr 2001 vom Bundesministerium der Finanzen als Verwaltungsanweisung veröffentlicht und stehen im engen Zusammenhang mit den GoBS. Die Intention bestand darin, die Inhalte der §§ 146 Abs. 5, 147 Abs. 2, 5, 6 und 200 Abs. 1 AO sowie § 14 Abs. 4 UStG zu konkretisieren. Dabei stehen insbesondere Regelungen für den unmittelbaren und mittelbaren Datenzugriff auf relevante digitale Unterlagen sowie für die Datenträgerüberlassung im Rahmen einer steuerlichen Prüfung durch die Finanzbehörde im Vordergrund. Zudem enthalten die GDPdU Anforderungen an den generellen Umgang mit und die Archivierung von digitalen Unterlagen. (Bundesministerium der Finanzen 2001)

Da IT-Systeme zur Erzeugung, Verarbeitung und Archivierung von digitalisierten Unterlagen verwendet werden, hat diese Verwaltungsanweisung Auswirkungen auf die IT in einem Unternehmen unter anderem in Form der Gewährleistung von Integrität und Verfügbarkeit der digitalen Unterlagen sowie der Implementierung einer geeigneten Zugriffs- und Zugangsverwaltung.

## **2.3 Konsequenzen bei Nichteinhaltung der IT-Compliance**

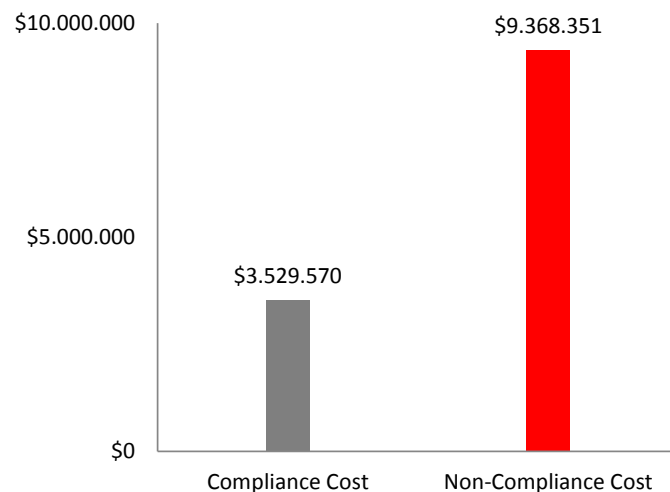
Nach der Begriffsbestimmung und der anschließenden konkreten Darstellung einiger IT-relevanter Compliance-Vorschriften muss der Frage nachgegangen werden, welche Auswirkungen die Nichteinhaltung von Gesetzen und Regularien nach sich ziehen können. Da jedoch eine trennscharfe Unterscheidung zwischen Konsequenzen aus IT-Compliance-

---

<sup>1</sup> Fachausschuss 3: Wirtschaft + Recht, GoBS, [www.awv-net.de](http://www.awv-net.de)

Verstößen und Folgen aufgrund anderweitiger Compliance-Verletzungen nicht sinnvoll bzw. möglich ist, wird an dieser Stelle die Betrachtung auf die ganzheitliche Compliance erweitert.

Die Frage nach möglichen Auswirkungen wird unter anderem in der aktuellen Studie „The True Cost of Compliance“ beantwortet, welche durch das Ponemon Institut in Zusammenarbeit mit dem Unternehmen Tripwire entstand (Ponemon Institute 2011). Dabei wurden 160 Führungsverantwortliche aus 46 multinationalen Unternehmen befragt. Ein wesentliches Ergebnis zeigt auf, dass die durchschnittlichen Kosten für ein Unternehmen für die dauerhafte Einhaltung der geltenden Compliance-Vorschriften bei circa 3,5 Mio. US-Dollar (2,5 Mio. Euro) liegen, wohingegen die Verletzung bzw. die Nichteinhaltung von Compliance-Regelungen (z. B. Gesetze, Regularien, Verträge, Richtlinien) zu durchschnittlichen Kosten in Höhe von etwa 9,4 Mio. US-Dollar (6,7 Mio. Euro) pro Unternehmen führen (siehe Abb. 2). Zusammengefasst lässt sich damit festhalten, dass eine „Vernachlässigung“ des Compliance-Managements inklusive der daraus resultierenden Konsequenzen 2,65-mal höher Kosten verursacht als ein effektives und effizientes Compliance-Management ohne Verstöße. Damit wird auch die Aussage der folgenden aus dem amerikanischen Raum stammenden Redewendung belegt: „If you think compliance is expensive, try non-compliance.“



**Abb. 2** Durchschnittliche Kosten für Einhaltung der Compliance und bei Nichteinhaltung der Compliance (Ponemon Institute 2011, S. 5)

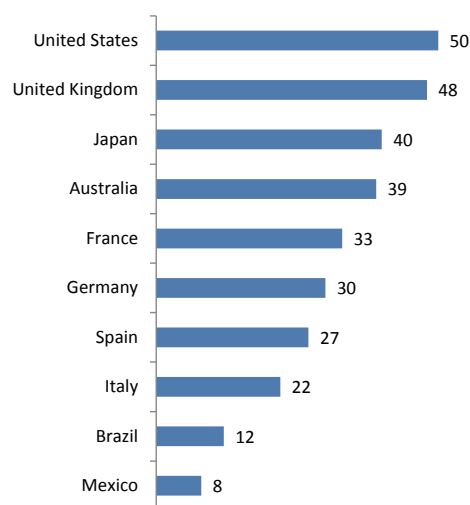
Die nachstehende, keineswegs vollständige Kostenauflistung als mögliche Konsequenzen von Compliance-Verstößen liefert eine plausible Begründung für die deutlich höheren Kosten bei Nichteinhaltung der Compliance-Regelungen (Hauschka 2007b; Ohrtmann 2009, S. 71):

- Direkt anfallende Kosten wie
  - Schadensersatzansprüche von geschädigten Wettbewerbern und Kunden
  - gerichtlich festgelegte Bußgelder und/oder Kartellstrafen
  - Beraterkosten (z. B. Unternehmensberater, Wirtschaftsprüfer, Rechtsanwälte)
  - steuerbehördliche Nachzahlungen
  - Gerichts- und Verfahrenskosten
  - gezahlte Bestechungsgelder

- Weitere Kosten für Gerichtsverfahren wegen
  - Sicherung von Beweismitteln
  - Beschlagnahmung von Vermögenswerten
  - Pfändung von Firmenkonten
  - Verhaftung von Mittelsmännern
- Umsatzmindernde wirtschaftliche Folgen wie
  - Kompensationszahlungen
  - Abfindungen an freigesetzte Mitarbeiter und Manager
  - Ausschluss von öffentlichen Aufträgen
  - Exportbeschränkungen
  - Untersagung des Gewerbes aufgrund von Unzuverlässigkeit

## 2.4 Probleme bei der Umsetzung bzw. Einhaltung von IT-Compliance-Anforderungen

Unternehmen stehen bei der Einhaltung von rechtlichen und regulatorischen IT-Anforderungen vor einigen Herausforderungen, die es zu bewältigen gilt. Zum einen steigt die Anzahl der zu erfüllenden IT-Compliance-Vorschriften kontinuierlich an, was den Unternehmen zunehmend „Kopfzerbrechen“ bereitet. Dies belegt auch eine Studie von GMG Insight, die zu folgendem Schluss gelangt: „The heavy burdens of regulatory compliance is a truly global issue“ (Trub und Olski 2008, S. 5). Alleine für Deutschland wurden 30 IT-Compliance-Anforderungen identifiziert, die für ein Unternehmen relevant sein können (siehe Abb. 3). Vor allem die permanente, nachweisliche Einhaltung ist aufgrund der Menge äußerst schwierig.



**Abb. 3** Anzahl an vorgeschriebenen, separaten gesetzlichen Regulierungen nach Ländern (Mittelwerte)  
(Trub und Olski 2008, S. 5)

Zum anderen ist bezogen auf ein Unternehmen eine Vielzahl an Gruppen und Funktionen an der Herstellung von IT-Compliance-Konformität beteiligt, wie Abb. 4 verdeutlicht. Diese heterogenen Einheiten hinsichtlich der Einhaltung rechtlicher und regulatorischer IT-Anforderungen zu steuern, abzustimmen und zu kontrollieren stellt eine weitere große Herausforderung dar.



**Abb. 4** An IT-Compliance beteiligte Gruppen und Funktionen  
(Klotz 2009, S. 13)

Ein weiteres Problem liegt vermehrt in der eigentlichen Umsetzung der IT-Compliance-Anforderungen, da sowohl der Gesetzgeber als auch die Aufsichtsorgane zunehmend eine Abkehr von der traditionell Regel-basierten Aufsicht hin zu einer Prinzipien-basierten Aufsicht vollziehen, d. h. den Unternehmen wird in Form von sehr generalistisch gehaltenen Empfehlungen bzw. Handlungsanweisungen bewusst mehr Gestaltungsspielraum für die Erfüllung der entsprechenden Gesetze und Regularien gegeben (Bretz et al. 2007, S. 3). Dies sollte eigentlich im Interesse der Unternehmen sein, jedoch herrscht oftmals eine gewisse Unsicherheit vor, ob die entsprechende Anforderung tatsächlich korrekt im Sinne des Verfassers umgesetzt wurde.

Werden diese Probleme zusätzlich im organisationsübergreifenden Kontext gesehen sowie hGP zugrunde gelegt, dann sind die Herausforderungen nicht mehr isoliert auf ein Unternehmen beschränkt, sondern müssen in einer sich dynamisch verändernden Umgebung betrachtet werden. Gerade die unvollständige Planbarkeit sowie die Überlappung von Planung und Ausführung als Eigenschaften von hGP in Verbindung mit einer Vielzahl von Prozessteilnehmern aufgrund von unternehmensübergreifenden Geschäftsprozessen führen zu dem Umstand, dass die zuvor beschriebenen Herausforderungen noch an deutlicher Komplexität und Vielschichtigkeit gewinnen. Insbesondere der Grundsatz „Eine Kette ist nur so stark wie ihr schwächstes Glied“ verdeutlicht die Gesamtproblematik.

## 3 Eignung von Standards bzw. IT-Frameworks im Kontext hochflexibler Geschäftsprozesse

Neben der begrifflichen Abgrenzung von Standard und IT-Framework wird in diesem Kapitel ein Anforderungskatalog definiert, welcher im späteren Verlauf zur Eignungsanalyse auf die in Kapitel 4 dargestellten Standards/IT-Frameworks angewendet wird. In diesem Zusammenhang wird auch deutlich gemacht, welche Kriterien für hGP besonders wichtig sind.

### 3.1 Allgemein

Grundsätzlich lassen sich unter dem Begriff „Standard“ die Ausdrücke „Norm“, „Industrie-Standard“, „De-facto-Standard“ und „herstellerspezifischer Standard“ subsumieren, je nachdem auf welcher Grundlage und auf welchem Entwicklungsprozess der Standard beruht.

Eine Norm ist definiert als „Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“ (DIN Deutsches Institut für Normung e. V. 2007, S. 25). Entscheidet ist hier die Tatsache, dass dieses Dokument in festgelegten Prozessen innerhalb einer Normierungsorganisation wie z. B. DIN oder ISO entstanden ist.

Ein Industrie-Standard bzw. De-facto-Standard ist ein Regelwerk, eine Spezifikation oder eine Verfahrensweise, welche ohne ein Normierungsverfahren entstanden ist, sondern im Laufe der Zeit durch die Praxis in Form von Anwendern und Herstellern für eine bestimmte Problemstellung entwickelt wurde und durch häufigen Gebrauch in der Alltagswelt wie eine echte Norm angesehen werden kann (Schubert 2008, S. 71).

Ein herstellerepezifischer Standard ist dann gegeben, wenn eine Vielzahl von Anwendern aufgrund mehrjähriger Erfahrungen die Erkenntnis gewinnt, dass es vorteilhaft ist, den firmenspezifischen Spezifikationen eines Herstellers zu folgen (Schubert 2008, S. 70-71).

Der Begriff „IT-Framework“ wird weder in der Wissenschaft noch in der Praxis trennscharf verwendet. Ursprünglich kommt die Bezeichnung aus der Softwareentwicklung, diese findet jedoch zunehmend auf Methoden und Vorgehensweisen des IT-Managements Anwendung. Im englischen Sprachgebrauch wird oftmals das Wort „Framework“ als Synonym für Norm, Standard oder Methodik gebraucht. Van Bon und Verheijen bezeichnen beispielsweise ISO/IEC 9000, ISO/IEC 27001, CobiT und ITIL als Frameworks (van Bon und Verheijen 2006). Auch die Autoren von CobiT verwenden den Begriff „IT-Framework“, obwohl in diesem Fall auch die Bezeichnung „De-facto-Standard“ zutreffen würde, da CobiT als das Referenzmodell für IT-Governance angesehen wird.

Wie in Kapitel 2 dargestellt, sind die Umsetzung von IT-Compliance-Anforderungen und deren nachweisliche Einhaltung mit einer Reihe von Problemen bzw. Herausforderungen ver-

bunden. Diesen Schwierigkeiten lässt sich mit der Anwendung von Standards/IT-Frameworks begeben. Jene können in folgenden Fällen besonders hilfreich sein:

- Bei der Konkretisierung von Gesetzen und Regularien hin zu umsetzbaren Anweisungen
- Bei der Erhöhung der Transparenz der Qualität der jeweiligen internen Compliance-Regelungen
- Bei der Setzung von konkreten „Leitplanken“ trotz unvollständiger Planbarkeit als Eigenschaft von hGP

## 3.2 Anforderungen

Die Vielzahl der vorhandenen Standards/IT-Frameworks in Verbindung mit den in Kapitel 1 aufgelisteten Merkmalen von hGP erfordert die Aufstellung eines entsprechenden Anforderungskatalogs, um die Eignung von Standards/IT-Frameworks in dem speziellen Kontext hGP untersuchen zu können. Dabei ist auch deutlich zu machen, welche Kriterien für hGP besonders wichtig sind. Folgende Anforderungen wurden identifiziert:

- Die **Verbreitung** zeigt auf, welche geographische Ausrichtung bei dem entsprechenden Standard/IT-Framework gegeben ist. Bezogen auf hGP ist generell eine eher internationale Orientierung zu bevorzugen, dies ist jedoch insbesondere unter dem Aspekt der Globalisierung zu sehen.
- Die **Vollständigkeit** verdeutlicht, in welchem Ausmaß ein Standard/IT-Framework verschiedene Facetten (z. B. Metriken, Verantwortlichkeiten, Reifegradmodell, etc.) beinhaltet. Für den Kontext hGP ist dieses Kriterium nicht spezifisch, jedoch bietet grundsätzlich eine größere Vielfalt mehr Handlungsspielraum bzw. mehr Variationsmöglichkeiten bei der Ausgestaltung von umsetzbaren Anweisungen.
- Der Aspekt **Transparenz** liefert eine Aussage über den Detailierungsgrad der Inhalte eines Standards/IT-Frameworks sowie über die Klarheit der Formulierungen. Für hGP stellt dies kein spezielles Kriterium dar, jedoch ist grundsätzlich eine hohe Detailtiefe vorteilhaft.
- Unter **Elastizität** ist die Fähigkeit zu verstehen, wie gut einzelne Elemente aus einem Standard/IT-Framework herausgelöst und anschließend separat verwendet werden können. Diese Anforderung ist für hGP besonders wichtig, da je nach vorliegender Situation (welche Daten werden an wen weitergegeben bzw. von wem weiterverarbeitet) ein angemessenes Compliance-Niveau auf unterschiedlich stark bzw. schwach formulierten Regelungen beruht.
- Das Vorhandensein eines **Reifegradmodells** ist ein weiteres Kriterium, welches aufzeigen soll inwiefern ein Standard/IT-Framework die Option enthält, einzelne inhaltliche Anforderungen in unterschiedlich starken bzw. schwachen Auslegungen zur flexiblen Steuerung der Ausprägung von „Compliance-Konformität“ auszugestalten. Im Kontext von

hGP ist dieser Aspekt von besonderer Wichtigkeit, da vor allem im organisationsübergreifenden Zusammenhang Informationen mit unterschiedlichem Schutzbedarf empfangen, verarbeitet und weitergegeben werden. Dabei ist bei der Ausgestaltung der entsprechenden Absicherungsmaßnahmen der Grundsatz der Verhältnismäßigkeit zu beachten.

- Unter **Auditierbarkeit** ist zu verstehen, wie nachvollziehbar und eindeutig die Umsetzung der Inhalte eines Standards/IT-Frameworks überprüfbar ist. Dies ist abhängig davon, wie klar, detailliert und unmissverständlich ein Standard/IT-Framework formuliert ist. Denn je unschärfer und generalistischer die Inhalte verfasst sind, desto mehr Interpretations- und Gestaltungsspielraum ist den Unternehmen bei der Umsetzung gegeben und umso schwieriger gestaltet sich die Überprüfung (z. B. durch interne Revision oder Wirtschaftsprüfungunternehmen), ob die gestellte Anforderung von einem Unternehmen erfüllt wird. Dieses Kriterium ist in Bezug auf hGP von zentraler Bedeutung, da aufgrund der Eigenschaften unvollständige Planbarkeit und Überlappung von Planung und Ausführung möglichst konkrete Handlungs- bzw. Umsetzungsanweisungen vorteilhaft sind.
- Die unvollständige Planbarkeit sowie die Überlappung von Planung und Ausführung als Eigenschaften von hGP erfordern schnelle Aussagen darüber, ob das Unternehmen, welches den nächsten Teilprozess ausführen will und daher entsprechende Informationen vom Vorgänger benötigt, die gestellten IT-Compliance-Anforderungen erfüllt. Diese ad-hoc-Aussagen lassen sich nur mit einer geeigneten **Werkzeug-Unterstützung** z. B. in Form von Software realisieren. Im Kontext von hGP ist diese Anforderung daher von zentraler Bedeutung.

## 4 Darstellung ausgewählter Standards und IT-Frameworks

Im diesem Kapitel erfolgen eine auf das Wesentliche beschränkte Erläuterung von ausgesuchten Standards und IT-Frameworks, welche für hGP in Frage kommen.

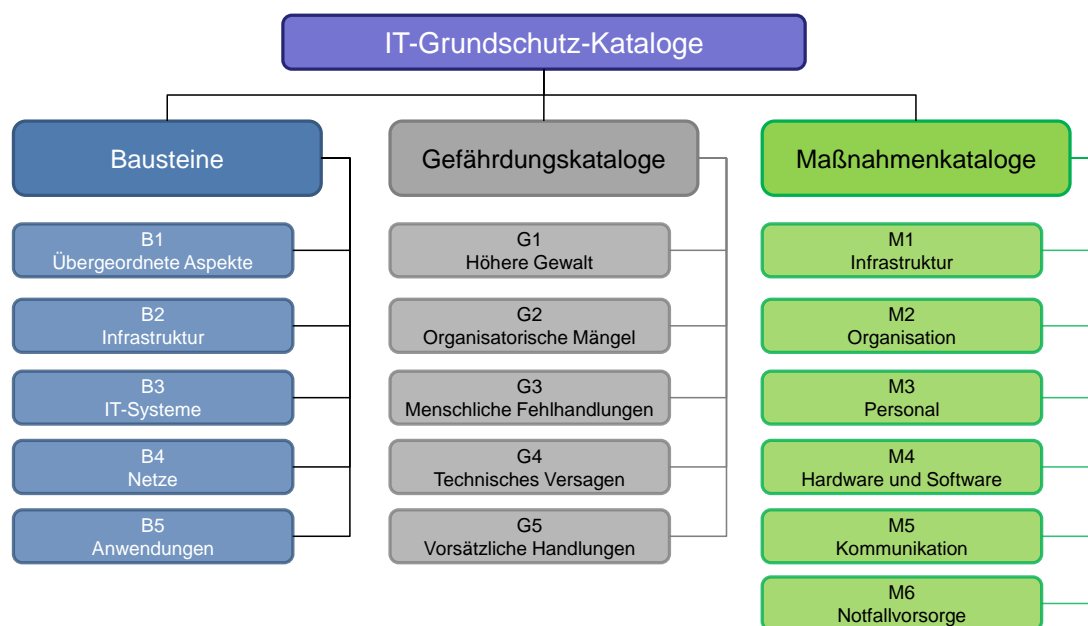
### 4.1 IT-Grundschutz

Der IT-Grundschutz ist eine Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welche eine strukturierte Vorgehensweise für das Management der Informationssicherheit liefert. Es handelt sich dabei um einen ganzheitlichen Sicherheitsansatz, welcher versucht, alle relevanten Bereiche und Aspekte der Informationssicherheit zu berücksichtigen (Speichert 2007, S. 262). Im Jahr 1994 wurde erstmalig diese Methode unter dem Namen „IT-Grundschutzhandbuch“ vom BSI veröffentlicht. Dieses wurde im Laufe der Zeit kontinuierlich in Form von Ergänzungslieferungen aktualisiert. Als Resultat der Neustrukturierung des IT-Grundschutzhandbuchs im Jahr 2005 wurden die IT-Grundschutz-Standards und die IT-Grundschutz-Kataloge geschaffen.

Die IT-Grundschutz-Standards beinhalten Empfehlungen zu Methoden, Prozessen, Verfahren, Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Folgende Standards wurden bis dato vom BSI veröffentlicht:

- **BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)**  
Dieser Standard definiert allgemeine Anforderungen an ein ISMS und ist vollständig kompatibel zu ISO/IEC 27001.
- **BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise**  
Die in diesem Standard beschriebene Methodik baut auf dem BSI-Standard 100-1 auf und erläutert die dort vorgestellte Vorgehensweise des IT-Grundschutzes.
- **BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz**  
In diesem Standard wird eine Vorgehensweise für die Durchführung von IT-Risikoanalysen unter Verwendung der in den IT-Grundschutz-Katalogen aufgeführten Gefährdungen beschrieben.
- **BSI-Standard 100-4: Notfallmanagement**  
Dieser Standard veranschaulicht eine Methodik zur Etablierung und Aufrechterhaltung eines unternehmensweiten internen Notfallmanagements, welche auf der im BSI-Standard 100-2 beschriebenen IT-Grundschutz-Vorgehensweise aufbaut.

Die IT-Grundschutz-Kataloge sind vollständig modular aufgebaut (siehe Abb. 5). Die Bausteine „spiegeln typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes wider“ (Bundesamt für Sicherheit in der Informationstechnik 2009a, S. 17). Für jeden Baustein sind entsprechende Gefährdungen beschrieben, welchen wiederum durch definierte Maßnahmen begegnet werden kann.



**Abb. 5** Aufbau der IT-Grundschutz-Kataloge

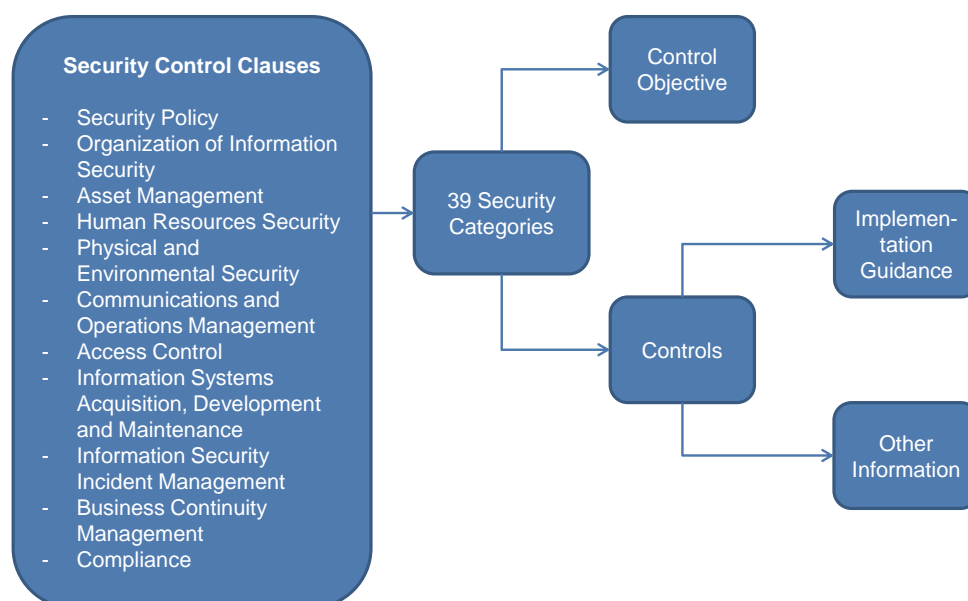
## 4.2 ISO/IEC 27002

Der von der International Organization for Standardization (ISO) herausgegebene Standard (bzw. Norm) ISO/IEC 27002 mit dem Titel „Information technology – Security techniques – Code of practice for information security management“ beinhaltet eine Sammlung von (Best Practice) Maßnahmen, Verfahren und Methoden zur Herstellung bzw. Wahrung der Informationssicherheit.

Der Standard basiert auf dem British Standard BS 7799-1, welcher 1995 erstmalig veröffentlicht wurde. Die ISO übernahm den Standard mit unverändertem Inhalt und publizierte diesen im Jahr 2000 unter der Bezeichnung ISO/IEC 17799. Im Jahr 2005 erfolgte die Umbenennung in ISO/IEC 27002 und die Zuordnung zur Normenreihe ISO/IEC 27000.

Dieser Standard „establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization“ (International Organization for Standardization 2005, S. 1) und stellt somit eine Art Leitfaden für das Management der Informationssicherheit dar. Zudem dient die Norm dem besseren Verständnis der in ISO/IEC 27001 definierten Anforderungen und ist als Ausgangslage zur Entwicklung von unternehmensindividuellen Regelungen und Richtlinien gedacht.

Wie Abb. 6 verdeutlicht, werden im ISO/IEC 27002 11 Bereiche betreffend der Informationssicherheit (Security Control Clauses) adressiert, welche zusammen 39 Sicherheitskategorien (Security Categories) enthalten. Jede dieser Kategorien setzt sich aus einer Zielvorgabe (Control Objective) und einer oder mehrerer Maßnahmen (Controls) zusammen. Eine Maßnahme besteht wiederum aus einem Umsetzungsleitfaden (Implementation Guidance) und optionalen weiteren Informationen (Other Information).



**Abb. 6** Aufbau des ISO/IEC 27002  
in Anlehnung an (International Organization for Standardization 2005)

Zielgruppe des ISO/IEC 27002 ist vorrangig die Management-Ebene, da generell die Inhalte, vor allem die Maßnahmen, sehr generisch gehalten sind und kaum technische Hinweise enthalten (Bundesamt für Sicherheit in der Informationstechnik 2009b, S. 71).

### 4.3 IT Infrastructure Library

Um das Jahr 1990 wurde die IT Infrastructure Library (ITIL) durch die damalige Central Computer and Telecommunications Agency (CCTA) im Auftrag der britischen Regierung entwickelt, mit dem Ziel einen offenen Standard für das IT-Service Management zu entwerfen (Rudd 2006, S. 149). Seit 2001 obliegt die kontinuierliche Weiterentwicklung von ITIL beim Office of Government Commerce (OGC), da das CCTA in das OGC integriert wurde. ITIL ist eine Sammlung von Best Practices und hat sich mittlerweile als De-facto-Standard im IT-Service Management etabliert.

Im Jahr 2007 wurde die bis dato letzte Aktualisierung vorgenommen und ITIL in Version 3 (ITIL v3) veröffentlicht. Kennzeichnend für die neue Fassung ist die viel stärkere Ausrichtung an den Geschäftsanforderungen (IT-Business-Alignment) und die Fokussierung auf einen Service-Lebenszyklus.

ITIL v3 bietet „a unique set of guidelines that creates a view of how mature IT organizations should provide effective business service management (BSM)“ (Shuja 2011, S. 45). Weiter ermöglicht ITIL v3 „IT organizations to plan and implement their transformations and improvements to achieve BSM“ (Shuja 2011, S. 45).

Die Kernpublikation von ITIL v3 besteht aus den folgenden fünf Büchern (Office of Government Commerce 2007b):

- **Service Strategy**

Eine stichhaltige und vernünftige Service-Strategie ist entscheidend für die Schaffung von hochqualitativen IT-Services. Dieses Service-Strategie-Buch ist eine der größten Stärken der neuen ITIL-Version. Es erklärt den Service-Lebenszyklus und seine Zielsetzung und unterstützt die Entwicklung einer Geschäftsperspektive.

- **Service Design**

Gut gestaltete Services spielen eine entscheidende Rolle in der Realisierung einer stichhaltigen Service-Strategie. Effektive Gestaltung trägt zur Lieferung von Qualitätsservices bei, die die Kundenerwartungen erfüllen oder übertreffen. Dieses Buch zeigt, wie nützliche „IT-Service-Assets“ für das Unternehmen geschaffen werden und zwar innerhalb von geschäftlichen Rahmenbedingungen wie Zeit und Geld. Es bietet ein Framework für Service-Design, das aktuelle und zukünftige Kundenanforderungen berücksichtigt, während die Geschäftssicht fest im Blick behalten wird.

- **Service Transition**

Das erfolgreiche Implementieren eines gut gestalteten Services in den Geschäftsbetrieb erfordert eine effiziente Planung. Es ist wichtig, neue oder veränderte Services mit der ent-

sprechenden Geschwindigkeits-, Kosten- und Sicherheitsbalance zu liefern, ohne den laufenden Betrieb gravierend zu beeinträchtigen. Dieses Buch bietet eine Anleitung über das Managen der vielen Aspekte der Serviceveränderungen und über das Verhindern von unerwünschten Konsequenzen trotz der Zulassung von Innovationen.

- **Service Operation**

Sobald die Services erfolgreich in den Geschäftsbetrieb implementiert wurden, müssen sie auf einer täglichen Basis effektiv gemanagt werden. Dieses Buch erklärt und stellt Liefer- und Kontrollaktivitäten vor, die den hochqualitativen Service-Betrieb unterstützen.

- **Continual Service Improvement**

Selbst bei einem erfolgreichen Service-Betrieb ist es erforderlich, Verbesserungen bei jeder Gelegenheit in Betracht zu ziehen. Dadurch wird verhindert, dass Wettbewerbsvorteile verloren gehen, und es wird sichergestellt, dass die bestmöglichen Ergebnisse erreicht werden. Dieses Buch konzentriert sich auf die Prozesselemente, die in der Identifizierung und Einführung eines Kreislaufes von Service-Management-Verbesserungen involviert sind. Es bietet eine Struktur zum Schätzen und Messen von Services und hilft, kurzfristige und vorläufige Lösungen zu Gunsten einer kontinuierlichen Qualitätsverbesserung zu vermeiden.

Jedes dieser Bücher deckt einen Bereich des Service-Lebenszyklus ab (siehe Abb. 7).



**Abb. 7** Der ITIL v3 Lebenszyklus  
(Office of Government Commerce 2007a)

Neben der Kernpublikation gibt es noch ein weiteres Buch mit dem Titel “The Official Introduction to ITIL Service Management”. Hier werden das Grundkonzept von IT-Service-Management und die Einordnung von ITIL erläutert. Zudem erfolgen die Vorstellung des in dieser Version neu eingeführten Lebenszyklusmodells sowie die Erklärung des Hintergrundes der neuen ITIL-Struktur.

## 4.4 Control Objectives for Information and Related Technology

Das IT-Rahmenwerk (engl. IT-Framework) „Control Objectives for Information and Related Technology“ (CobiT) wurde in der ersten Version im Jahr 1996 von der Information Systems Audit and Control Association (ISACA) veröffentlicht. Seit 1998 obliegt die kontinuierliche Weiterentwicklung von CobiT beim IT Governance Institut, welches von der ISACA gegründet wurde. Aktuell liegt das IT-Rahmenwerk in der Version 4.1 vor.

Die allgemeine Intension von CobiT lautet:

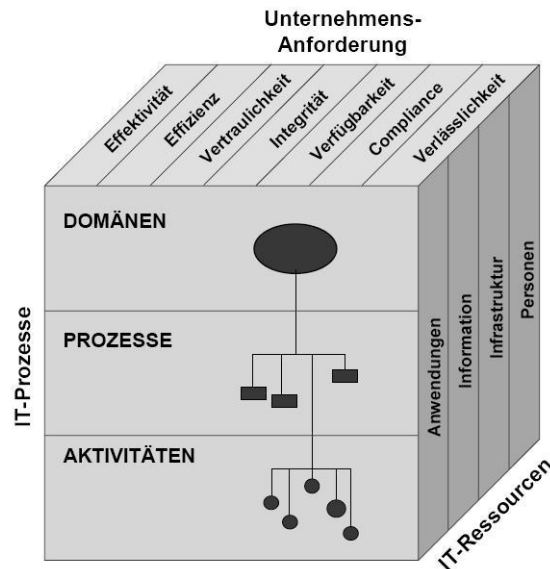
„To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals“ (IT Governance Institute 2007, S. 9).

Durch die Anwendung von CobiT lassen sich folgende konkrete Zielsetzungen erreichen (Johannsen und Goeken 2007, S. 41):

- Ausrichtung der IT-Planungen an den geschäftlichen Anforderungen
- Organisation der IT-Aktivitäten durch allgemein akzeptiertes Modell
- Unterstützung der ökonomischen Verwendung von IT-Ressourcen
- Bereitstellung von IT-relevanten Steuerungs- und Managementinformationen durch Kontrollelemente

CobiT beinhaltet ein Prozessmodell von international akzeptierten IT-prozessbezogenen Kontrollzielen (Control Objectives), welche in einem Unternehmen beachtet und umgesetzt werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten (Sewera 2005, S. 20). Denn erst wenn die Organisation der Informationen, Anwendungen, Infrastruktur und Menschen richtig funktioniert, werden die Geschäftsprozesse die an sie gestellten Anforderungen erfüllen (Gaulke 2010, S. 10).

Anhand des in Abb. 8 dargestellten dreidimensionalen Würfels lässt sich das Grundprinzip von CobiT veranschaulichen. Die Erreichung der vorgegebenen Ziele (Geschäftsanforderungen) wird durch IT-Prozesse unter Einbeziehung von IT-Ressourcen realisiert.



**Abb. 8** Der CobiT-Würfel  
(IT Governance Institute 2006, S. 26)

Die IT-Ressourcen müssen geplant, entwickelt, implementiert, betrieben und überwacht werden. Hierfür sind in CobiT in der aktuellen Fassung insgesamt 34 kritische IT-Prozesse definiert, welche erfolgsbestimmend für das Management der IT sind (Bitterli 2006, S. 18). Jeder dieser IT-Prozesse ist jeweils zu einem der nachfolgend aufgelisteten Bereiche bzw. einer Domäne zugeordnet:

- Planen und Organisieren (Plan and Organise, PO)
- Beschaffen und Implementieren (Acquire and Implement, AI)
- Erbringen und Unterstützen (Deliver and Support, DS)
- Überwachen und Beurteilen (Monitor and Evaluate, ME)

Die Einteilung in diese vier Domänen basiert auf dem Lebenszyklus von IT-Systemen (Design, Build, Run und Monitor) (Johannsen und Goeken 2007, S. 60).

Jeder der 34 IT-Prozesse ist gleich strukturiert. Die Komponenten werden im Folgenden erläutert:

- Die **Prozessbeschreibung** (Process Description) enthält die jeweiligen Prozessziele, die betroffenen IT-Ressourcen, die betroffenen primären und sekundären Informationskriterien sowie in einer wasserfallähnlichen Darstellung die wichtigsten Geschäftsziele für die IT, IT-Ziele, Kontrollen und Metriken.
- Zwischen drei und 15 **Kontrollziele** (Control Objectives) sind für jeden Prozess definiert und konkretisieren die Ziele aus der Prozessbeschreibung.
- Die **Leitlinien für das Management** (Management Guidelines) bestehen aus folgenden drei Elementen:

- Prozesseingangs- und -ausgangswerte (Inputs/Outputs)  
Die jeweiligen Tabellen veranschaulichen, welche Informationen aus anderen CobiT-Prozessen als Input in den jeweiligen CobiT-Prozess eingehen und welche Informationen als Output wiederum in andere CobiT-Prozesse als Input einfließen.
  - Kompetenzmatrix (RACI Chart)  
In dieser Matrix erfolgt eine Zuordnung der Prozessaktivitäten zu verschiedenen Rollen (z. B. CEO, CFO, CIO) im Unternehmen. Zudem werden die entsprechenden Verantwortlichkeiten definiert. Dabei steht das „R“ für Responsible (verantwortlich), das „A“ für Accountable (federführend bzw. rechen-schaftspflichtig), das „C“ für Consulted (beratend) und das „I“ für Informed (zu informieren).
  - Ziele und Metriken (Goals and Metrics)  
Hier erfolgt die Darstellung der Prozess-, IT- und Aktivitätsziele mit den jeweiligen Metriken in Form einer kaskadierten Struktur.
- Das **Reifegradmodell** (Maturity Model) von CobiT basiert auf dem Reifegradmodell des Capability Maturity Model Integration (CMMI)<sup>2</sup> des Software Engineering Institutes. Es beschreibt den Reifegrad für jeden Prozess in sechs Abstufungen (nicht existent, initial, wiederholbar, definiert, gesteuert und überwacht, optimiert).

## 5 Bewertung

Nach der Darstellung von vier ausgewählten Standards bzw. IT-Frameworks erfolgt nun deren Bewertung anhand der in Kapitel 3 spezifizierten Anforderungen. Dabei ist jedoch zu beachten, dass diese Standards/IT-Frameworks teilweise verschiedene Themenbereiche sowie Schwerpunkte adressieren und somit der Umfang der behandelten Aspekte durchaus schwankt (Informationssicherheit beispielsweise wird von allen vier Standards/IT-Frameworks in unterschiedlichen Ausprägungen behandelt). IT-Grundschatz und ISO/IEC 27002 sind Standards für das Management der Informationssicherheit, ITIL stellt eine Best Practice Sammlung für das IT-Service-Management dar und CobiT ist ein Framework für die IT-Governance. Daher wird bei der Bewertung nicht der fachliche Schwerpunkt zugrunde gelegt, sondern der Fokus liegt auf der Struktur und der gesamten Handhabbarkeit, denn nur auf diese Weise ist eine entsprechende Vergleichbarkeit gegeben.

Die nachfolgende Darstellung verdeutlicht das Ergebnis der durchgeführten Bewertung der vier ausgewählten Standards/IT-Frameworks (siehe Abb. 9). Die genaueren Erläuterungen hinsichtlich der einzelnen Bewertungen erfolgen im Anschluss an die kommende Abbildung.

---

<sup>2</sup> siehe: [www.sei.cmu.edu/cmmi](http://www.sei.cmu.edu/cmmi)



ckelt wurde, enthält dieser ebenso entsprechende Prüfungselemente, weshalb auch hier die Analyse zu einem positiven Ergebnis hinsichtlich der Auditierbarkeit führt. Im Gegensatz dazu sind ISO/IEC 27002 und ITIL nicht explizit für Prüfungen/Audits konzipiert worden und daher lassen sich diese nur in eingeschränktem Maße (z. B. als Grundlage für Prüfungspunkte) hierfür verwenden.

Hinsichtlich der **Werkzeug-Unterstützung** insbesondere in Form von Software hat die Analyse gezeigt, dass für IT-Grundschutz, ISO/IEC 27002 und ITIL sehr viele Lösungen auf dem Markt vorhanden sind. Im Vergleich dazu ist bei CobiT das Angebot an Softwareprodukten eher eingeschränkt. Dies könnte vermutlich in der Tatsache begründet sein, dass CobiT sehr komplexe Strukturen und Abhängigkeiten beinhaltet.

Abb. 9 und die anschließenden Erläuterungen zeigen, dass CobiT am besten die gestellten Anforderungen erfüllt. Schwächen sind nur bezüglich der Kriterien Elastizität und Werkzeug-Unterstützung vorhanden. Auf den nächsten Plätzen folgen IT-Grundschutz und ITIL, ISO/IEC 27002 belegt den letzten Rang.

## 6 Darstellung und Vergleichbarkeit der IT-Compliance-Situation

Neben der Anwendung eines für hGP geeigneten Standards/IT-Frameworks (Analyse siehe Kapitel 5) zur Einhaltung von IT-Compliance-Vorschriften sind auch die Situationstransparenz auf Knopfdruck über den Umsetzungs- und Qualitätsstand einzelner Aspekte des verwendeten Standards/IT-Frameworks sowie die objektive Beglaubigung der Korrektheit der gemachten Angaben von fundamentaler Wichtigkeit.

### 6.1 Notwendigkeit der Werkzeug-Unterstützung

Im Kontext von hGP kommt der Darstellung der aktuellen IT-Compliance-Situation eine besondere Bedeutung zuteil, denn netzwerkbezogene Hochflexibilität erfordert in einem sich ad-hoc bildenden Instanz übergreifenden Wertschöpfungsnetz zwischen den Instanzen die Transparenz der Qualität der jeweiligen internen IT-Compliance-Regelungen. Nur auf diese Weise ist sowohl die Bewertung des eigenen Zustandes als auch den des jeweiligen potenziellen Kopplungspartners möglich. Diese Bewertung muss auch insbesondere im Hinblick auf die hGP-Eigenschaft der Überlappung von Planung und Ausführung auf Knopfdruck ersichtlich sein, denn diese ist entscheidend, ob eine Kopplung erfolgt.

Eine in dieser Art geforderte, sofortige Aussage lässt sich nur mit Hilfe einer geeigneten Software-Unterstützung realisieren, denn die bereits heutzutage bestehende und weiter zunehmende IT-Durchdringung im Unternehmen macht eine manuelle und vor allem schnelle Situationsanalyse des IT-Compliance-Status so gut wie unmöglich. Wie die Analyse in Kapi-

tel 4 gezeigt hat, ist das vorhandene Portfolio an Werkzeugen (vor allem Software) für die einzelnen Standards/IT-Frameworks unterschiedlich stark bzw. schwach ausgeprägt. Als Beispiele für IT-Grundschutz und ISO/IEC 27002 lassen sich das GSTOOL<sup>3</sup> und verinice<sup>4</sup> nennen. Das IT-Framework CobiT kann unter anderem mit der GRC-Suite i|RIS<sup>5</sup> unterstützend umgesetzt bzw. implementiert werden. Der HP Service Manager<sup>6</sup>, der Tivoli Service Request Manager<sup>7</sup> oder andere Softwaretools<sup>8</sup> können für die Umsetzung von ITIL verwendet werden.

Die Nennung der Beispiele stellt keine besondere Heraushebung in irgendeiner Art und Weise dar, sondern diese werden in neutraler Absicht, stellvertretend für sämtliche Anbieter in den jeweiligen Bereichen genannt.

## 6.2 Objektivierung der IT-Compliance-Situation

Bei der möglichen ad-hoc Kopplung mit einem unter Umständen zuvor nicht bekannten Partner muss auch gewährleistet sein, dass der jeweilige übermittelte IT-Compliance-Status den korrekten Stand im Unternehmen widerspiegelt, denn auf dessen Basis wird die Entscheidung getroffen, ob eine Kopplung durchgeführt wird. Da sich eine Überprüfung der gemachten Angaben zum einen aufgrund der hGP-Eigenschaften (siehe Pütz et al. 2009, S. 1) und zum anderen aufgrund eines gewissen, vorherrschenden Zeitdrucks (Stopp des Durchlaufs der Wertschöpfungskette!) als äußerst schwierig gestaltet, müssen sich die jeweiligen Partner gegenseitig vertrauen.

Jedoch entsteht das Vertrauen in der Regel erst im Laufe einer länger andauernden Geschäftsbeziehung. Im Kontext von hGP schränkt dieses Vorgehen die Hochflexibilität in erheblichem Maße ein, da der nächste Kopplungspartner gerade aufgrund der unvollständigen Planbarkeit sowie der Überlappung von Planung und Ausführung ein Unternehmen sein kann, mit dem noch niemals zuvor eine Geschäftsbeziehung bestanden hat. Somit ist das Entgegenbringen eines „blinden“ Vertrauens ohne jegliche Grundlage geradezu vermessen und faktisch grob fahrlässig.

Zur Lösung dieser Problemstellung sind folgende zwei Ansätze denkbar:

- Als vertrauensbildende Maßnahme bestätigt die **Interne Revision** eines Unternehmens den ermittelten IT-Compliance-Status. Aufgrund ihrer unabhängigen Stellung in der Organisation und ihres Aufgabenspektrums (spezifiziert unter anderem in § 91 Abs. 2 AktG,

---

<sup>3</sup> [www.bsi.de](http://www.bsi.de)

<sup>4</sup> [www.verinice.org](http://www.verinice.org)

<sup>5</sup> [www.grc-suite.com](http://www.grc-suite.com)

<sup>6</sup> [www.hp.de](http://www.hp.de)

<sup>7</sup> [www.ibm.de](http://www.ibm.de)

<sup>8</sup> [www.ital-officialsite.com/SoftwareScheme/EndorsedSoftwareTools/EndorsedSoftwareTools.aspx](http://www.ital-officialsite.com/SoftwareScheme/EndorsedSoftwareTools/EndorsedSoftwareTools.aspx)

§ 25a Abs. 1 KWG und den Mindestanforderungen an das Risikomanagement), insbesondere der Kontrolle der ordnungsgemäßen Abläufe von Prozessen und der Einhaltung geltender Gesetze und Regularien, liefert die Interne Revision durch die Beglaubigung der zu übermittelnden Angaben damit einen vertrauensfördernden Beitrag, welcher entscheidend für die Kopplung sein kann.

- Falls ein Unternehmen keine Interne Revision besitzt, muss die Bestätigung der jeweiligen IT-Compliance-Situation durch eine vertrauenswürdige **dritte Instanz** (Trusted Third Party) erfolgen.

## 7 Zusammenfassung

Die nachweisliche Einhaltung von IT-Compliance-Vorschriften insbesondere im Kontext von hGP stellt die Unternehmen vor komplexe Herausforderungen. Dies wurde auch durch die Darstellung und Erläuterung einiger ausgewählter IT-spezifischer Gesetze und Regularien veranschaulicht. Die Anwendung von Standards/IT-Frameworks kann bei der Bewältigung der Herausforderungen sehr hilfreich sein, allerdings nur wenn dabei eine Berücksichtigung der hGP-Eigenschaften stattfindet. Um diesem Aspekt Rechnung zu tragen, wurden entsprechende Anforderungen aufgestellt, anhand derer eine Analyse von vier aus-gesuchten Standards/IT-Frameworks erfolgte.

Die durchgeführte Untersuchung hat ergeben, dass CobiT unter den vorgestellten Alternativen am besten die definierten Kriterien erfüllt und damit für den hGP-Kontext ein geeignetes Mittel darstellt. Insbesondere durch das integrierte Reifegradmodell wird zum einen eine hohe Transparenz erzielt und zum anderen eine flexible inhaltliche Ausgestaltung ermöglicht. Nur hinsichtlich der Elastizität und der Werkzeug-Unterstützung sind bei CobiT noch Schwächen vorhanden.

In künftigen Forschungsarbeiten ist die Fragestellung zu beantworten, wie potenzielle Teilnehmer, die nicht CobiT verwenden, trotzdem an dem Wertschöpfungsnetz partizipieren können. Denn die alleinige Fokussierung auf CobiT würde die Flexibilität zu stark einschränken.

## Literaturverzeichnis

Bertele M, Lehner F (2008) IT-Compliance: Rechtliche Aspekte des IT-Managements. Darstellung rechtlicher Aspekte – organisatorische, technische und personelle Maßnahmen – Rahmenkonzepte zur Umsetzung, 1. Aufl. VDM Verlag Dr. Müller, Saarbrücken.

Bitterli PR (2006) Das CobiT-Framework für IT-Governance. In: Bitterli PR (Hrsg.) Praxishandbuch CobiT – IT-Prozesse steuern, bewerten und verbessern, 1. Aufl. Symposion Publishing, Düsseldorf.

Bretz J, Hinssen J, Kolb A, Martin G, Peltier G, Rosenberger P (2007) IT-Sicherheitsmanagement in Banken und Sparkassen: Implementierung, technisch-organisatorische Umsetzung und Überwachung im Lichte gestiegener, gesetzlicher und bankenaufsichtlicher Anforderungen, 1. Aufl. Finanz Colloquium Heidelberg, Heidelberg.

Bundesamt für Sicherheit in der Informationstechnik (2009a) IT-Grundschutz-Kataloge – 11. Ergänzungslieferung, Bonn.

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge\\_2009\\_EL11\\_de.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile). Abruf am 2011-02-04.

Bundesamt für Sicherheit in der Informationstechnik (2009b) Leitfaden Informationssicherheit – IT-Grundschutz kompakt, Bonn.

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden\\_pdf.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile). Abruf am 2011-02-04.

Bundesdatenschutzgesetz (2009) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814).

Bundesministerium der Finanzen (1995) Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS).

[http://www.bundesfinanzministerium.de/nn\\_314/DE/BMF\\_\\_Startseite/Service/Downloads/Abt\\_IV/BMF\\_\\_Schreiben/015,templateId=raw,property=publicationFile.pdf](http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt_IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf). Abruf am 2011-02-04.

Bundesministerium der Finanzen (2001) Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).

[http://www.bundesfinanzministerium.de/DE/Wirtschaft\\_\\_und\\_\\_Verwaltung/Steuern/Veroeffentlichungen\\_\\_zu\\_\\_Steuerarten/Abgabenordnung/Datenzugriff\\_\\_GDPdU/002,templateId=raw,property=publicationFile.pdf](http://www.bundesfinanzministerium.de/DE/Wirtschaft__und__Verwaltung/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/Datenzugriff__GDPdU/002,templateId=raw,property=publicationFile.pdf). Abruf am 2011-02-04.

Deutscher Bundestag (1998) Bundestagsdrucksache 13/9712.

<http://dip21.bundestag.de/dip21/btd/13/097/1309712.pdf>. Abruf am 2011-02-04.

DIN Deutsches Institut für Normung e. V. (2007) DIN EN 45020:2007-03 (D) – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004), 8. Aufl. Beuth Verlag, Berlin.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (1998) in der Fassung der Bekanntmachung vom 27. April 1998 (BGBl. I S. 786-794).

Gaulke M (2010) Praxiswissen COBIT – Val IT – Risk IT. Grundlagen und praktische Anwendung für die IT-Governance, 1. Aufl. dpunkt.verlag, Heidelberg.

Gola P, Schomerus R (2010) BDSG – Bundesdatenschutzgesetz: Kommentar, 10. Aufl. Verlag C. H. Beck, München.

Hauschka CE (2007a) Einführung. In: Hauschka CE (Hrsg.) Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 1. Aufl. Verlag C. H. Beck, München, S. 1-25.

Hauschka CE (2007b) Kosten der Non-Compliance.  
<http://www.compliancemagazin.de/compliancefachbeitraege/kosten/luther060807.html>. Abruf am 2011-02-21.

Henstorf KG, Kampffmeyer U, Prochnow J (2002) Grundsätze der Verfahrensdokumentation nach GoBS – „Code of Practice“ zur revisionssicheren Archivierung. In: VOI Verband Organisations- und Informationssysteme e. V. (Hrsg.) Grundsätze der Verfahrensdokumentation nach GoBS – „Code of Practice“ zur revisionssicheren Archivierung, 1. Aufl. VOI Verband Organisations- und Informationssysteme e. V., Bonn.

Hornby AS (2007) Oxford Advanced Learner's Dictionary, 7. Aufl. Oxford University Press, Oxford.

International Organization for Standardization (2005) ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management, 1. Aufl., Genf.

IT Governance Institute (2006) CobiT 4.0 – deutsche Ausgabe.  
[http://www.isaca.ch/files/DO5\\_COBIT/CobiT%204.0%20Deutsch.pdf](http://www.isaca.ch/files/DO5_COBIT/CobiT%204.0%20Deutsch.pdf). Abruf am 2010-05-12.

IT Governance Institute (2007) CobiT 4.1.  
[http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT\\_4.1.pdf](http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf). Abruf am 2011-01-27.

Johannsen W, Goeken M (2007) Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co, 1. Aufl. dpunkt.verlag, Heidelberg.

Klotz M, Dorn DW (2008) IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD – Praxis der Wirtschaftsinformatik (2008) 263, S. 5-14.

Klotz M (2009) IT-Compliance – Ein Überblick, 1. Aufl. dpunkt.verlag, Heidelberg.

Office of Government Commerce (2007a) ITIL – What is it? / How does it work?  
[http://www.ogc.gov.uk/guidance\\_ityl\\_4671.asp](http://www.ogc.gov.uk/guidance_ityl_4671.asp). Abruf am 2011-02-21.

Office of Government Commerce (2007b) ITIL – Books and resources.  
[http://www.ogc.gov.uk/guidance\\_ityl\\_4899.asp](http://www.ogc.gov.uk/guidance_ityl_4899.asp). Abruf am 2011-02-21.

Ohrtmann N (2009) Compliance – Anforderungen an rechtskonformes Verhalten öffentlicher Unternehmen, 1 Aufl. LinkLuchterhand, Köln.

Ponemon Institute (2011) The True Cost of Compliance – A Benchmark Study of Multinational Organizations. [http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True\\_Cost\\_of\\_Compliance\\_Report.pdf](http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf). Abruf am 2011-02-08.

Pütz C, Wagner D, Ferstl OK, Sinz EJ (2009) Geschäftsprozesse in Medizinischen Versorgungszentren und ihre Flexibilitätsanforderungen – ein fallstudienbasiertes Szenario, forFLEX-Arbeitsbericht, Bamberg.

Rudd C (2006) ITIL – the IT Infrastructure Library. In: van Bon J, Verheijen T (Hrsg.) Frameworks for IT Management, 1. Aufl. Van Haren Publishing, Zaltbommel.

Schubert S (2008) Wettbewerbsvorteile durch Vereinheitlichung am Beispiel der europäischen Schienenfahrzeugindustrie, Dissertation, Juristischen und Wirtschaftswissenschaftlichen Fakultät der Martin-Luther-Universität Halle-Wittenberg. <http://sundoc.bibliothek.uni-halle.de/diss-online/08/08H095/prom.pdf>. Abruf am 2011-02-14.

Schuppener J, Tillmann W (1999) KonTraG: Auswirkungen auf Kreditgeschäft und Bonitätsprüfung. In: Kreditpraxis (1999) 2, S. 20-23.

Sewera S (2005) Referenzmodelle im Rahmen von IT-Governance – CobiT ITIL MOF, Seminararbeit, Wirtschaftsuniversität Wien. <http://www.ai.wu.ac.at/~koch/courses/wuw/archive/inf-sem-ss-05/referenzmodelle.pdf>. Abruf am 2011-01-26.

Shuja AK (2011) ITIL: Service Management Implementation and Operation, 1. Aufl. Auerbach Publications, Boca Raton.

Speichert H (2007) Praxis des IT-Rechts – Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung. In: Fedtke S (Hrsg.) Praxis des IT-Rechts – Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, 2. Aufl. Vieweg Verlag, Wiesbaden.

Trub G, Olski L (2008) Global report on the status of IT compliance processes. <http://ca.com/files/IndustryResearch/gmg-globalcompliancereport.pdf>. Oktober 2008, Version 2. Abruf am 2011-01-26.

van Bon J, Verheijen T (2006) Frameworks for IT Management, 1. Aufl. Van Haren Publishing, Zaltbommel.

**Prof. Dr. Dieter Bartmann**

Universität Regensburg  
Universitätstraße 31  
93053 Regensburg  
Tel.: +49 941/943-1881  
Fax: +49 941/943-1871  
E-Mail: dieter.bartmann@forflex.de

**Prof. Dr. Freimut Bodendorf**

Universität Erlangen-Nürnberg  
Lange Gasse 20  
90403 Nürnberg  
Tel.: +49 911/5302-450  
Fax: +49 911/5302-379  
E-Mail: freimut.bodendorf@forflex.de

**Prof. Dr. Otto K. Ferstl**

Universität Bamberg  
Feldkirchenstraße 21  
96045 Bamberg  
Tel.: +49 951/863-2679  
Fax: +49 951/863-2710  
E-Mail: otto.ferstl@forflex.de

**Prof. Dr. Elmar J. Sinz**

Universität Bamberg  
Feldkirchenstraße 21  
96045 Bamberg  
Tel.: +49 951/863-2512  
Fax: +49 951/863-2513  
E-Mail: elmar.sinz@forflex.de



**Geschäftsführung forFLEX**

Dipl.-Wirtsch.Inf. Corinna Pütz  
Universität Bamberg  
Feldkirchenstraße 21  
96045 Bamberg  
Tel.: +49 951/863-2777  
Fax: +49 951/863-5777  
E-Mail: corinna.puetz@forflex.de  
Internet: <http://www.forflex.de>