

# **COMIDD Expertengipfel IT-Compliance**

**8. September 2009 - Congress Park Hanau**

Statement

Prof. J. Menno Harms

Meine sehr verehrten Damen und Herren,

ich freue mich über das gewachsene Interesse an unserem Thema und begrüße Sie herzlich als Schirmherr der COMMID Initiative. Bevor ich in meinen Impulsbeitrag einsteige, will ich gleich mit der Klärung der Begriffe beginnen. Das hilft bekanntlich immer.

*Compliance*, das ist die zielgerechte Einhaltung vorgegebener Regeln, die z.B. vom Gesetzgeber, vom Unternehmen oder von anderen *stakeholders* vorgegeben werden. Das Konzept *Compliance* wird übrigens in der Medizin seit langem durch Qualitätsvorgaben praktiziert. Im höheren Kontext spricht man von *Governance*, in der Wirtschaft von *Corporate Governance* und versteht darunter die Einhaltung der Regeln zu guter und korrekter Unternehmensführung. Beide Begriffe werden konsequent auch im IT Umfeld eingesetzt. Um Informationen und Diskussionen, vor allem über *IT Compliance* zu fördern und das Verständnis zu erleichtern, gründete HP am 6. April 2009 zusammen mit Optimal Systems, Berlin die Initiative COMIDD, das heisst *Compliance in der Informations- und Datenverarbeitung in Deutschland*. Ziel ist, den Dialog zu diesem Thema unter den Betroffenen zu fördern, also von Soft- und Hardware-Herstellern, Industrie und Politik, Beratern, Rechtsanwälten, Wirtschaftsprüfern, usw. Die Verunsicherung ist ja groß. Die Betroffenen sind grossteils allein gelassen.

Und die Flut immer neuer Regeln und Umsetzungspflichten ist beachtlich. Angesichts massiver Führungsfehler in privaten und öffentlichen Organisationen wurden in den letzten Jahren die bestehenden Regeln wie HGB, AO, Sarban Oxley u.a. durch diverse neue Gesetzeswerke ergänzt, z. B. in Deutschland durch das Gesetz zur Unternehmensintegrität und Modernisierung der Anfechtungsklagen UMAG; das Bilanzrechtsreformgesetz (BilReG), das Bilanzkontrollgesetz (BilKoG), das Bilanzmodernisierungsgesetz (BiLMOG), das Gesetz zur angemessenen Vergütung von Vorständen (VorstAG ) usw. Auch das Bundesdatenschutzgesetz wurde aktualisiert, zuletzt durch Gesetz am 14.8.2009. Zweck dieses Gesetzes ist, den Einzelnen davor zu schützen, dass er durch den Umgang mit personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Alle Gesetze haben deutliche Auswirkungen auf Unternehmensprozesse und -transaktionen und damit auf die *IT Compliance*.

Auch die Anforderungen an die Unternehmensaufsicht steigen, in Aktiengesellschaften wie auch in GmbH's, KG's usw. Die derzeitige Banken- und Finanzkrise führt - durch öffentlichen und politischen Druck - zu einer Ausweitung und Verschärfung der Haftung der Führungskräfte insgesamt. Die resultierende Forderung nach mehr Transparenz bei vielen Geschäftstransaktionen erzwingt den Aufbau und Betrieb manipulationssicherer Kontroll- und Berichtssysteme. Um Manipulationssicherheit zu gewährleisten, wird es verstärkte IT Revisionen geben müssen. Ein treffsicheres Beispiel zu diesem Thema wurde kürzlich in der ComputerWoche dargestellt.<sup>1</sup>

---

<sup>1</sup> Computerwoche 23/09, Seite 42

Die Geschichte ging so: „Bei einer Kreditverlängerungssitzung stellte der Banker einen kleinen Unterschied zwischen der vom Mittelständler ausgeteilten Geschäftszahlentabelle und der Tabelle der letzten Sitzung fest, die eigentlich gleich sein sollten. Er stellte die Frage, ob die Tabellen direkt aus der IT , also dem ERP-Fibu System kommen oder über eine bekannte Tabellenkalkulationssoftware erstellt wurden. Bei der Antwort “ Tabellenkalkulation“ klappte er seine Unterlagen zu und stellte fest, dass man jetzt allen Unterlagen nicht mehr trauen könnte, da Manipulationen leicht möglich seien. Daraufhin beendete er das Gespräch.“

Aufsichtsräte werden manipulationssichere Kontroll- und Berichtssysteme verlangen, um nicht in die Haftung genommen zu werden.

Ein weiteres Beispiel sei zum Thema e-mails gewählt. Haben Sie schon mal erlebt, welche Nervosität sich bei Verantwortlichen zeigt, wenn der Wirtschaftsprüfer nach der zwingenden Vorlage bestimmter e-mails von vor drei Jahren fragt? Die US Börsenaufsicht SEC verdonnerte das Bankhaus Morgan Stanley unlängst zu 15 Mio\$ Schadensersatz, weil es den Vorwurf falscher Investmentinformationen nicht widerlegen konnte. Wichtige Mails waren nicht systematisch archiviert. Auch hierzulande häufen sich die Fälle, in denen Unternehmen aufgrund unzureichender Archivierung und Dokumentation in Schwierigkeiten geraten. Ganz zu schweigen von der immer noch mangelhaften Absicherung von Millionen von e-mails eines Unternehmens und den daraus entstehenden Sicherheitsproblemen. Mittlerweile entstehen ja praktisch alle Dokumente ursprünglich elektronisch, deshalb passen die Gesetzgeber weltweit ihre Vorschriften an.<sup>2</sup> Auch die immer wieder zu beobachtende, fahrlässige Behandlung von Kunden- und Mitarbeiter bezogenen Daten bringt Unternehmen, aber auch den öffentlichen Dienst zunehmend in Zugzwang. Wer weiss schon, welche Pflichten eine Organisation gemäss Bundesdatenschutzgesetz bei Sicherheitsverletzungen hat!

Die allein aus der verschärften weltweiten Gesetzeslage resultierenden Konsequenzen für Vorstände und Geschäftsführung, für persönlich haftende Gesellschafter, für Selbständige und andere sind beachtlich. Das Feld möglicher Fehltritte ist weit gesteckt. Beispiele: Falsche Abbildung betrieblicher Fakten und Prozesse in Bilanzen, G&V's und Steuermeldungen; Eingeschränkte Testate durch Wirtschaftsprüfer; Verletzter Datenschutz der Beschäftigten; Unsystematisches *Records Management* vor allem auch für virtuelle Dokumente; Fehlendes Risiko-Management; Fehlerhaftes Vertragsmanagement; Schlampige Umsatzabgrenzung, Verletzung der Exportkontrollen; Verpasste FDA Prüfungen; Falsche Umsatzsteuerverfahren; und und ... Für Nichtbeachtung und Fehler gibt es Strafen, und zwar nicht nur signifikant materielle sondern eben auch solche durch persönliche Haftung und durch indirekt wirkende Schäden wie Imageverlust, niedergestuftes *rating* usw. Wer das einmal als Verantwortlicher in Vorstand oder Aufsichtsrat mitgemacht hat, vergißt die unerbittlich mahelnden Strafmühlen des öffentlichen Systems oder der öffentlichen Meinung nie mehr....

---

<sup>2</sup> Compliance, in blue line 3/2008 HP Kundenmagazin

Die Verbreitung von IT Systemen und die Vernetzung digitaler Anwendungen und Wertschöpfung haben das Transaktionsvolumen weltweit explodieren lassen. Aber das intelligente Überwachen dieser Transaktionen, das Monitoring – das müssen wir eingestehen - hat nicht mitgehalten! Dadurch haben Transparenz und gesetzeskonforme Umsetzung in vielen Fällen gelitten. Und sie werden es weiter tun, sofern nicht gegengesteuert wird.

IT ist ein kritischer Erfolgsfaktor der Unternehmensführung. Es ist daher kein Wunder, dass die *IT Compliance* ins Blickfeld gerät, also das zielgerechte Einhalten relevanter Gesetze und Vorgaben im IT Umfeld einer Organisation. Und *IT Compliance* ist – wie schon erläutert - mehr als das Beachten bisheriger Regeln z.B. der Grundsätze einer ordnungsgemäßen DV-gestützten Buchführung oder der Grundsätze zum Datenzugriff und Prüfbarkeit digitaler Unterlagen. Compliance Regeln werden oft als Strafkataloge wahrgenommen, die einem effizienten Betrieb im Wege stehen. Sicher, Übertreibungen kommen auch hier vor und sie sind teuer. Mehr Augenmaß wäre sicher vernünftig.

Dem Gesetzgeber ist daher zu empfehlen, sich auf Ziele und nicht auf deren Umsetzung zu konzentrieren. Kaufmännische Ehrbarkeit kann letztlich durch rechtliche Formalien nicht ersetzt werden. Eine saubere und transparente Unternehmensführung muss sich vor allem dann zeigen, wenn keiner zuschauen kann...

Den *Compliance* Lösungsanbietern ist andererseits zu empfehlen, sich mit den jeweils unterschiedlichen Anforderungen ihrer Kunden intensiver auseinanderzusetzen anstatt *one size fits all* zu praktizieren.

Und den Anwendern ist zu empfehlen, sich des Themas *Compliance* bewusster anzunehmen, damit sie betriebsverträgliche Lösungen für die neue Gesetzeslagen bekommen und somit schneller als andere ihren Kunden und Gesellschaftern Transparenz und Vertrauen bieten können.

*Compliance* Themen werden vielschichtiger und komplexer. Es werden Fachleute gebraucht, die dieses Thema verstehen, strukturieren und Projekte anstoßen können. Eine Möglichkeit ist die Ausbildung zum *Compliance-Manager*. Diese Ausbildung wollen wir heute noch genauer vorstellen.

Angesichts vielfältiger Konsequenzen ist der wirtschaftliche Nutzen von *IT Compliance* bedeutend, wenn richtig verstanden und umgesetzt. CIO's tragen auch in dieser Hinsicht eine beachtliche unternehmerische Verantwortung. Allerdings stehen ihnen vielfältige Hilfsmittel zur Verfügung. Doch man muss diese auch kennen und richtig einsetzen. Vor allem muss man die Größe der Herausforderung verstehen. Hier will die Arbeitsplattform COMMID ansetzen, Dialoge ermöglichen, das Thema von allen Seiten beleuchten und Lösungen aufzeigen, neutral und offen. Dazu wünsche ich einen informativen Tag und rufe Ihnen fachgerecht zu: *IT Compliance: Komm Mit....*