

In sechs Schritten zur Compliance-Lösung

EuroSOX, MoReq2, ISO 9000, GDPdU etc.: Die Compliance-Anforderungen an die IT werden immer komplexer. Was müssen wir tun, was lassen wir lieber? So fragt sich manches Unternehmen.

Von **Martin Ortgies***

Verstoßen US-Manager gegen den Sarbanes-Oxley Act (SOX), so müssen sie mit einer Gefängnisstrafe von bis zu 20 Jahren rechnen. Ihre europäischen Kollegen lehnen sich noch gemächlich zurück – mit möglicherweise unangenehmen Folgen: In Europa wurden vergleichbare Vorgaben beschlossen. Die „EuroSOX“-Richtlinie (eigentlich 8. EU-Richtlinie/EU-Abschlussprüfer-Richtlinie) gilt seit Juli 2008. Schon im vergangenen Februar wurde „MoReq2“ veröffentlicht. Dabei handelt es sich um eine Spezifikation für elektronisches Dokumenten- und Records-Management.

Der Vorstand haftet persönlich

Vorstände und Geschäftsführer sind persönlich und gesamtschuldnerisch haftbar für die Einhaltung dieser und vieler weiterer Einzelregelungen, etwa für den Finanzbereich oder die Archivierung von E-Mails. Und es ist damit zu rechnen, dass die Entscheidungsträger künftig noch stärker zur Verantwortung gezogen werden. Sie sind verpflichtet, ein wirksames Risikosystem einzuführen, die Funktionsweise der IT nachvollziehbar zu dokumentieren und für eine angemessene Archivierung digitaler Dokumente zu sorgen.

Können sie dies alles nicht lückenlos nachweisen, drohen Haftungsklagen, Marktzugangsbarrieren und Probleme bei der Kreditaufnahme oder Bilanzprüfung. Legendär ist der Fall aus dem Jahr 2005, als

das Unternehmen Morgan Stanley zur Zahlung von 1,45 Milliarden Dollar verurteilt wurde, weil es bestimmte E-Mails nicht vorlegen konnte.

Große Rechtsunsicherheit

Aktuelle Umfragen anlässlich der EuroSOX-Umsetzung in nationales Recht zeigen, dass die meisten Unternehmen noch nicht auf die Anforderungen der EU-Richtlinie vorbereitet sind. Das große Problem: Nicht alle Gesetze und Normen gelten für alle Unternehmen. Wie Horst Speichert, ein auf IT-Recht spezialisierter Rechtsanwalt in Stuttgart, bestätigt, herrscht derzeit große Rechtsunsicherheit. Für international agierende Unternehmen gelte eine schwer zu

überblickende Vielzahl von Rechtsnormen. „Zudem sind die Anforderungen in einzelnen Branchen sehr unterschiedlich, weil oft Spezialregelungen gelten“, ergänzt der Anwalt. Beispielsweise seien bei der Datenarchivierung neben den allgemeinen IT-Gesetzen auch die branchenspezifischen Regelungen einzuhalten.

Was ist ökonomisch sinnvoll?

Die Folge: Der Unternehmensverantwortliche kann im Regelfall kaum beurteilen, welche Maßnahmen aus der Fülle der Normen er unbedingt umsetzen muss und welche er in der Prioritätenliste nach hinten verschieben oder sogar außen vor lassen kann, kurz: was wirtschaftlich angemessen ist. Er muss sich folgende Fragen stellen:

- Ist unser Unternehmen im juristischen Sinn compliant?
- Wo müssen wir eigentlich compliant sein – hinsichtlich der internen Prozesse und IT-Systeme?
- Wie wahrscheinlich ist ein Schadensfall?
- Welche Auswirkungen hätte er?
- Lohnt es sich nach Maßgabe der Betriebswirtschaft, die dafür notwendigen Vorkehrungen zu treffen?

Das Compliance-Assessment

Renate Mayer, Compliance-Expertin in Diensten des Enterprise-Content-Management-Spezialisten FME AG, Braunschweig, rät, die juristischen, betriebswirtschaft-



lichen und IT-Fragen gleichrangig zu behandeln sowie alle Experten in ein Team zu holen. Der Beratungs- und Implementierungsdienstleister steht hierzu mit einem Experten für IT-Prozesse sowie einer auf IT-Recht spezialisierten Rechtsanwaltskanzlei in Verbindung.

Ein solches „Compliance-Assessment“ dient dazu, Schwachstellen im Unternehmen aufzuzeigen, die notwendigen Änderungen zu definieren und sie betriebswirtschaftlich zu bewerten. Erst auf dieser Grundlage könne ein angemessener Maßnahmenplan erstellt und mögliche Anpassungen der IT-Systeme eingeleitet werden, so FME-Managerin Mayer. Auf der Seite des Servicenehmers soll-

ten neben der Unternehmensleitung das Rechnungswesen, die IT, der Datenschutzbeauftragte und die Revision im Team sein – gegebenenfalls auch der Chief Compliance Officer (CCO), wie ihn große Unternehmen, beispielsweise BASF oder Siemens, bereits haben. Der Ablauf sieht wie folgt aus:

1 Die zutreffenden Gesetze und Normen feststellen

Im ersten Schritt gilt es zu klären, welche Regularien für das Unternehmen relevant sind und welche internen Regelungen sowie Arbeitsanweisungen bereits existieren. Dazu Mayer: „Wir stellen immer wieder fest, dass es angesichts der vielen neuen Regelungen einen erheblichen Nachholbedarf gibt.“ Zum Beispiel werde die Archivierung von E-Mails fälschlicherweise auf die Frage des geeigneten IT-Systems reduziert, so die FME-Managerin. Manchmal würden auch neue Entwicklungen wie die Produkthaftung in der Fertigungsindustrie nicht ernst genug genommen. Zu berücksichtigen sei auch, inwiefern verschiedene Compliance-Felder, beispielsweise die Anforderungen an das Risk-Management (ISO 9000), die Corporate Governance (SOX), spezifische Regularien wie 21CFRPart11 (Pharma) sowie Datenschutz und Telekommunikationsgesetz, Handelsgesetzbuch und Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) einander überlappen.

2 Die betroffenen Prozesse und Systeme definieren (Scoping)

Im zweiten Schritt werden die betroffenen Prozesse und Systeme identifiziert. Dazu gehören unter anderem die installierte Hard- und Software sowie die Zugriffs- und

Ein Assessment für die Compliance

Juristische, betriebswirtschaftliche und IT-Fragen sollten gleichberechtigt sein.



Quelle: FME, Braunschweig

Berechtigungsregelungen. Im Rechnungswesen fallen darunter etwa die Prozesse des Rechnungseingangs und -ausgangs, das ERP-System sowie alle Abläufe bis zum Archivsystem. Die Erfüllung dieser Auflagen muss gut dokumentiert werden. Eine Zulassung kann beispielsweise scheitern, wenn nicht nachweisbar ist, dass die Mitarbeiter alle relevanten Arbeitsanweisungen kennen und das per Unterschrift dokumentiert haben.



Renate Mayer,
FME

„Angesichts der vielen neuen Regelungen gibt es großen Nachholbedarf.“

3 Die nicht erfüllten Regeln (Deficiencies) abgleichen

Lücken und Risiken in der Unternehmenspraxis lassen sich im dritten Schritt entdecken, indem die vorhandenen Systeme und Prozesse mit den geltenden Gesetzen und Regeln abgeglichen werden. Damit zeichnet sich ab, wo Handlungsbedarf besteht. Das kann recht komplex sein, wie am Beispiel der E-Mail-Archivierung deutlich wird: Zum einen müssen alle relevanten E-Mails dem Gewährleistungsrecht entsprechend archi-

viert werden, um die Risiken aus der Produkthaftung abzudecken. Zum anderen ist sicherzustellen, dass bei der Archivierung keine Rechte aus dem Datenschutz verletzt werden, weil auch private E-Mails betroffen sein können.

4 Ursachen und Folgen ermitteln

Werden Regelverstöße festgestellt, müssen zunächst die Ursachen gefunden werden. Vorher ist an Maßnahmen zur Risikominimierung überhaupt nicht zu denken. Allerdings hat nicht jede Verletzung von Regeln und Normen zwangsläufig weitere Maßnahmen zur Folge. Zum Beispiel bedürfen ausgehende elektronische Rech-

nungen eigentlich einer qualifizierten elektronischen Signatur. Ein Unternehmen muss nun abwägen, wie schwer die Nachteile aus der Regelverletzung (Rechnungen ohne Signatur) im Vergleich zum Aufwand wiegen, der nötig ist, um die Regel einzuhalten (Signaturen einführen).

5 Maßnahmen zur Verringerung der Risiken erarbeiten

Sind die Mängel festgestellt und das Risiko bewertet, gilt es im nächsten Schritt, die geeigneten Maßnahmen auszuwählen. Hier sollte das gesamte Team auf der Basis von Best-Practise-Erfahrungen organisatorische Maßnahmen empfehlen, mit denen sich die IT-Systeme verbessern lassen. Zu unterscheiden sind dabei organisatorische und technische Maßnahmen. Reicht die Anpassung der Policy, oder sind Änderungen bei der Technik notwendig? Typische Empfehlungen betreffen die Einrichtung von Frühwarnsystemen, die Entwicklung von Ausfallszenarien oder die Anpassung bestehender Arbeitsprozesse. Das Ziel ist eine möglichst integrierte GRC-Lösung (Governance, Risk and Compliance).

6 Die betrieblichen Prozesse umsetzen und verbessern

Laut FME-Managerin Mayer liegt im notwendigen Übel der Compliance auch eine Chance: „Wir können viel gewinnen, wenn wir das Notwendige mit dem Nützlichen verbinden. Da wir die IT-Systeme oder Abläufe ohnehin anfassen müssen, können wir auch gleichzeitig die Effizienz der Prozesse verbessern.“

(qua) ◀

*Martin Ortgies ist Fachjournalist für IT und Telekommunikation in Königslutter.