IT-Compliance

Ein kompakter Überblick
präsentiert von

bitzer digital-media consulting

Köln 2006

bitzer digital-media consulting
Venloerstr. 13-15
50672 Köln
Tel: 0221-9520554
Mail: fb@bdcon.de
Web: www.bdcon.de

IT-Compliance

oder warum es notwendig ist, gesetzliche Vorgaben zu erfüllen.
Eine Betrachtung von Aufwand und Nutzen

Firmen unterliegen zahlreichen rechtlichen Verpflichtungen, deren Nichteinhaltung zu hohen Strafen führen kann. EU-Richtlinien, internationale Konventionen und Handelsbräuche fügen weitere Regeln hinzu. Da immer mehr Geschäftsprozesse durch EDV und IT abgebildet und unterstützt werden, ist auch die IT-Infrastruktur von diesen Regelungen betroffen.
Bei deren Einhaltung geht es nicht um das „Ob", sondern nur um das „Wie" und „Wann"!

▪ *Was versteht man unter IT- Compliance*

Die IT-Compliance ist ein Teil der Anforderung an die Unternehmensführung. Unter dem Oberbegriff der Unternehmens Governance fasst man eine Sammlung von Gesetzten, Regelwerken und Standards zusammen, welche dazu bestimmt sind, Prozesse, Organisation und Datenhaltung eines Unternehmens nach diesen Regeln zu organisieren, zu dokumentieren und damit nachvollziehbar und transparent zu gestalten. Neben den nationalen Regeln wie [Basel II], [TKG], [BDSG] und [GdpdU] kommen auch europäische Richtlinien und internationale Vorschriften zum Tragen.
Die IT-Compliance fokussiert dabei auf die EDV-, Internet- und TK-Infrastruktur der Firma.

▪ *Warum benötigt man eine IT-Compliance*

Der wichtigste Grund ist die Einhaltung gesetzlicher Vorschriften, bei deren Missachtung zivilrechtliche und auch strafrechtliche Sanktionen drohen. So sieht das Bundesdatenschutzgesetz [BDSG] eine Freiheitsstrafe von bis zu 2 Jahren oder Geldstrafe bei Zuwiderhandlung vor. Werden in einem Unternehmen erforderliche Maßnahmen zur IT-Sicherheit schuldhaft nicht oder nicht hinreichend getroffen, droht Dritten gegenüber ggf. eine Schadensersatzpflicht.
Des Weiteren geht es um das Rating der Firma bei Banken und Versicherungen. Spätestens seit Basel II den Finanzinstitutionen weitgehende Prüfungen vorschreibt, besteht Handlungsbedarf zur Umsetzung der IT-Compliance.

Beispiel 1: Lizenz-Management
Im Rahmen von Unternehmensprüfungen ist nicht selten feststellbar, dass Unternehmen nicht lizenzierte Software einsetzen. Bei einer *Unternehmensbewertung*, z.B. im Rahmen einer *Nachfolgeplanung*, kann dies negative Folgen haben und zu einer Minderbewertung des Unternehmenswertes führen.

Beispiel 2: E-Mail Archiv
Hier besteht ein schmaler Grad zwischen Archivierungspflicht und Schutz der Persönlichkeit. Was sich besonders beim Ausscheiden von Personen aus dem Unternehmen zeigt. Ohne passende Regeln im Vorfeld ist diese Situation kaum befriedigend zu lösen.

- ***Wer benötigt eine IT Compliance***

Diese Frage lässt sich sehr einfach beantwortet: Jedes Unternehmen! Unabhängig von Personalstärke und Umsatz. Sobald ein Computer schlicht für die Kommunikation und – erst recht – für die Abwicklung der geschäftlichen Transaktionen oder der Organisation eingesetzt wird, ist „Compliance" umzusetzen.
Auch internationale Regeln können schnell zum Tragen kommen. Auf einen Maschinenbauer aus dem Oberbergischen, welcher an einen amerikanischen Autokonzern liefert, können indirekt bereits dortige Gesetzgebungen Anwendung finden.

- ***Was kostet Compliance***

Hier lautet die Antwort, wie so oft: "Es kommt darauf an...".
Die Kosten sind abhängig von der Größe des Unternehmens und dessen Verzweigung. Der Umfang reicht von Schulungsaufwand für internes Personal und einigen wenigen Beratertagen bis zu Projekten, die sich über mehrere Monate erstrecken können.
Zusätzlich gilt es über den Einsatz eines geeigneten Software-Werkzeugs zu entscheiden. Hier bieten die großen Softwareanbieter aus dem ERP- Umfeld Produkte an. Für die Dokumentation kann aber auch eine einfache Datenbank Anwendung zum Einsatz kommen.
bitzer digital-media consulting bietet mit dem Produkt "Compliance Check" ein Starter Paket zu einem günstigen Festpreis an, mit dem die grundsätzlichen Felder analysiert werden können.

- ***Wo liegt der weitere Nutzen einer Compliance***

Die Analyse der Schwachstellen eines Unternehmens bringt auch immer ein Potential zur Steigerung der Effizienz, zur Einsparung von Kosten oder zur Ausweitung der Unternehmenstätigkeiten mit sich. Redundanzen lassen sich vermeiden und Medienbrüche eliminieren. Eine höhere Transparenz der Prozesse erlaubt es, diese schneller, effektiver und rationeller zu gestalten. Ein gut organisiertes IT-Service-Management hilft zudem, Kosten zu sparen. Untersuchungen haben gezeigt, das ca. 80% des IT-Budgets in die Pflege und Wartung der Infrastruktur investiert wird. So führt u.a. ungeregeltes individuelles Agieren von Nutzern zu undokumentierten Dateninseln, deren Verwaltung zusätzliche Kosten verusacht. Einige Firmen orientieren bei der Planungen ihrer IT-Services bereits an Standards wie [ISO 17799], [CObIT] oder [ITIL}. Diese definieren ein Rahmenwerk und Beispiele für eine effiziente und an den Kosten orientierte Planung und Betrieb der Unternehmens IT.

Ein Beispiel hierfür ist die Nutzer- und Zugangsverwaltung (Identity Management). Im Rahmen der Compliance spielt die Frage: Wer, wann, was gemacht hat eine wichtige Rolle. Orientiert man sich hier an den obigen Standards und Regeln, so verhindert man zum einen die Kollision mit den Datenschutzgesetzen und kann auf der anderen Seite den Nachweis führen, wer z.B. an Finanzberichten mitgewirkt hat. Last but not least kann die optimierte Verwaltung der Benutzer und deren Zugangsdaten die Kosten für immer wieder vergessene Passworte und deren neue Einrichtung reduzieren.

▪ *Wie erreicht man Compliance*

Compliance muss als dauerhafter Vorgang aufgefasst werden. Mit einen schnellen, aber zeitlich begrenzten Projekt wird man nur kurzen Erfolg erzielen.
Ganz grob kann der Prozess in 5 Schritte aufgeteilt werden:

1. Erste Prüfung und Feststellung des Bedarfs über eine Checkliste
2. Aufsetzten eines Projektes mit entsprechender Ressourcen-Planung.
   Ernennung eines "Compliance Beauftragten". Einschaltung externer Beratung.
3. Analysieren der IT-Infrastruktur und Dokumentieren der Schwachstellen
4. Behebung der Schwachstellen durch organisatorische und technische Maßnahmen
5. Installieren einer laufende Pflege und Kontrolle.

Wichtig ist dabei, in allen betroffenen Unternehmensbereichen ein Bewußtsein für die Notwendigkeit und die Vorteile einer IT-Compliance zu schaffen. Nur die dauerhaft Beschäftigung mit dem Thema sichert den Erfolg.

▪ *Fazit*

Compliance ist keine "Kann" sondern eine "Muss" Aufgabe.
Nutzen Sie die Analyse der Unternehmens IT Architektur als Ausgangspunkt für die Optimierung der Geschäftsprozesse. Verbessern Sie das IT Service Management und sparen Sie Kosten.
Beginnen Sie jetzt mit dem Compliance Check der *bitzer digital-media consulting.*
Sprechen Sie uns an, wir werden Ihnen gerne ein Angebot unterbreiten.

▪ *Glossar*

Gesetzliche Regelungen

- GdpdU = Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

Auf die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) beruft sich ein Finanzbeamter, wenn er bei Betriebsprüfungen auf die Computersysteme von Unternehmen zugreift. Man unterscheidet 3 Arten des Datenzugriffs durch den Betriebsprüfer:

- den unmittelbaren Lesezugriff (Z1),
- den mittelbaren Zugriff über Auswertungen (Z2) und
- die Datenüberlassung in verschiedenen Formaten (Z3).

Für die Datenüberlassung sind verschiedene Formate zugelassen. Mittlerweile gibt es auch eine Empfehlung des Bundesfinanzministeriums für einen entsprechenden Beschreibungsstandard. Die Daten lassen sich dann vom Prüfer in die Prüfersoftware IDEA einlesen.

- Basel II

Regeln für die Analyse und Bewertung des Eigenkapitals und der Risiken bei Unternehmen

- BDSG = Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) regelt zusammen mit den Datenschutzgesetzen der Bundesländer und anderen bereichsspezifischeren Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden.

- SOX = Sarbanes-Oxley Act (of 2002)

Ein US-Gesetz das die Unternehmensberichterstattung beschreibt. Dies wurde in Folge der Bilanzskandale von Unternehmen wie Enron und Worldcom erlassen. Namensgeber sind seine Verfassern (Senator Paul S. Sarbanes), Abgeordneten Michael Oxley). SOX gilt für inländische und ausländische Unternehmen, die an US-Börsen (z.B. der NASDAQ) gelistet sind, sowie für deren Tochterunternehmen. Das Gesetz kann also indirekt auch hier gelten.

Standards

- ITIL = Information Technologie Infrastructure Libraray

Wurde bereits in den späten 80'er Jahren entwickelt und bis heute weiter entwickelt. Zentrales Thema des Rahmenwerks ist der IT Service in Form von Organisation und Software. ITIL beschreibt in 7 Bereichen u.a. Service-Erstellung, Support, Anwendungs-Management und Sicherheit. Es werden jeweils Beispiele und Handlungsanweisungen für zahlreiche Vorgänge gegeben.

- ISO 17799,

Die ISO 17799 ist ein internationaler Standard, der Kontrollmechanismen für die Informationssicherheit beschreibt. Der Standard basiert wie ITIL auf einer Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis.

- CObIT = Controll Objectives for Information and related Technologies.

Ein Regelwerk für die Kontrolle heutiger und zukünftiger Geschäftsprozesse. Hierbei geht es unter anderem um Verfügbarkeit, Vertraulichkeit, Zuverlässigkeit und rechtliche Konformität. Wurde von der Internationalen ISACA Organisation entwickelt. Mehr unter www.isaca.de

- BS 15000 (Britisch Standard 15000)

BS 15000 ist der erste weltweite Standard, der sich speziell auf das IT Service Management bezieht. Dieser Standard beschreibt einen integrierten Satz von Management-Prozessen für die Lieferung von Dienstleistungen. BS 15000 ist ausgerichtet an den Prozessbeschreibungen, und kann damit in Zusammenhang mit ITIL betrachtet werden. Er soll in Zukunft durch den internationalen Standard ISO 20000 abgelöst werden.