Eine Voraussetzung für den Erfolg
White paper

IBM Risk and Compliance

Das IBM Risk and Compliance Framework: Den Compliance-Herausforderungen begegnen

Januar 2005

Kurzübersicht

Unternehmen werden heute mit einer Reihe verschiedener gesetzlicher Bestimmungen konfrontiert, wie Sarbanes-Oxley (SOX), SEC 17a-4, Patriot Act, Basel II und HIPAA, um nur einige zu nennen. Gleichzeitig sind verbesserte Methoden zur Verwaltung der ständig wachsenden Datenmengen gefragt, damit diese kostengünstig erfasst, gespeichert und analysiert werden können.

Das IBM Risk and Compliance Framework veranschaulicht die verfügbare Funktionalität auf Infrastrukturebene, auf die Unternehmen zurückgreifen können, um der Vielfalt der sich heute stellenden Compliance-Anforderungen zu begegnen. Das Tool ermöglicht die flexible Auswahl von Technologien, während frühere Investitionen geschützt und genutzt werden. Mit diesem Framework lassen sich allgemein verfügbare Technologien als Unternehmensstandard etablieren, um so eine Compliance-Architektur zu entwerfen und zu implementieren, die eine effektivere Umsetzung von Compliance-Initiativen ermöglicht.

In diesem Dokument werden die Herausforderungen dargestellt, die bei der Planung und Umsetzung von Lösungen zur Bewältigung von Compliance-Anforderungen im Unternehmen auftreten. Anschließend wird geschildert, welchen Beitrag IBM zur Bewältigung dieser Herausforderungen leisten kann. Das Dokument richtet sich an die Verantwortlichen für die strategische Geschäftsplanung, IT-Strategen sowie Führungskräfte im Bereich Risikomanagement und Geschäftsführung, deren Aufgabe die Planung und Implementierung der Infrastruktur für die Gewährleistung regulatorischer Compliance ist.

Die Compliance-Landschaft

Was ist Compliance? Vereinfacht ausgedrückt beschreibt Compliance den Prozess zur Einhaltung von Richtlinien und Regeln, die von Behörden und Standardisierungsorganisationen oder im Unternehmen vorgegeben werden. Die Einhaltung von Compliance-Anforderungen ist eine Herausforderung, die durch folgende Faktoren gekennzeichnet ist:

- Häufige Einführung neuer Regelungen
- Unklar formulierte Regelungen mit Interpretationsbedarf
- Fehlendes Einvernehmen über die Best-Practices für Compliance
- Überschneidungen zwischen Regelungen, z. B. aus unterschiedlichen Regionen mit abweichenden Anforderungen
- Ständige Änderung der Regelungen
- Regulierungsstellen, die im Allgemeinen keine Produkte oder Services im Bereich der Informationstechnologie genehmigen, empfehlen oder prüfen

Compliance ist daher kein zeitlich begrenztes Projekt, sondern ein fortlaufender Prozess, der solange auf der Tagesordnung der Unternehmen stehen wird, wie diese die unzähligen Vorgaben erfüllen müssen, die für ihre vertikalen Märkte spezifisch sind. Beispiele sind Basel II für das Risikomanagement im Banksektor, SEC 17a-4 für Broker und Händler auf den Finanzmärkten sowie der Healthcare Insurance Portability and Accounting Act (HIPAA) für das Gesundheitswesen.

Einige Unternehmen müssen sich unter Umständen auch mit branchenübergreifenden rechtlichen Bestimmungen wie Sarbanes-Oxley (SOX) und anderen internen Kontrollprozessen wie ISO 9000 oder Six Sigma auseinander setzen. Die Vielfalt und Komplexität dieser Herausforderungen hat in den vergangenen Jahren in vielen Unternehmen punktuelle Lösungen hervorgebracht. Die Möglichkeit, Compliance unter strategischeren Gesichtspunkten anzugehen, könnte Unternehmen von der bloßen Erfüllung einzelner Compliance-Vorgaben bis hin zur Realisierung konkreter Geschäftsvorteile aus der Gesamtheit der Infrastrukturinvestitionen führen.

Das Thema Compliance durchdringt auch andere Aspekte des Unternehmens. Tabelle 1 zeigt einige Faktoren, die ein Unternehmen, das den Rahmen und die Vorgehensweise für seine Compliance-Aktivitäten festlegen will, beachten sollte.

Tabelle 1: Umfang von Compliance-Aktivitäten

Bereich	Überlegung
Strategie	• Die Ermittlung der relevanten Regelungen ist Bestandteil der Strategieentwicklung im Unternehmen. • Die Nachhaltigkeit der Compliance muss ein wesentlicher Bestandteil jeder Compliance-Strategie sein.
Unternehmen	• Die Organisationsstruktur muss so gestaltet werden, dass sie die besonderen Anforderungen (oder die Absicht) aller Regelungen erfüllt (so empfiehlt der Sarbanes-Oxley Act, die Position des Chief Executive Officer und des Geschäftsführers mit zwei verschiedenen Personen zu besetzen).
Prozesse	• Die wichtigsten Prozesse müssen dokumentiert und erprobt werden. • Mit Revisionen oder Prüfungen muss sichergestellt werden, dass die dokumentierten Prozesse effektiv genutzt werden, um die Compliance-Anforderungen sowie die Anforderungen der relevanten Regelungen zu erfüllen.
Anwendungen und Daten	• Auf die Anforderungen der einzelnen Regelungen abgestimmte spezielle Anwendungen müssen entwickelt, implementiert und fortlaufend getestet werden. • Die Daten müssen gemäß den einzelnen Regelungen geschützt und verarbeitet werden.
Technologie	• Entsprechend den Anforderungen der einzelnen Regelungen ist die jeweils erforderliche Technologie einzusetzen (z. B. die gemäß SEC 17a-4 vorgeschriebenen Speichermedien).
Facilities	• Entsprechende Einrichtungen müssen entworfen und bereitgestellt werden, damit die Regelungen eingehalten werden können (einige Regelungen schreiben vor, dass Geschäftsdokumente an einem externen Standort leicht zugänglich und verfügbar sind).

Compliance-Architekturen

In der Vergangenheit wurden häufig punktuelle Anwendungen eingesetzt, wenn kurzfristig taktisch auf gesetzliche Vorschriften reagiert werden musste. Mit der zunehmenden Anzahl und Komplexität der gesetzlichen Vorschriften wurden jedoch nach und nach die Grenzen dieses Ansatzes deutlich. Angesichts des exponentiell wachsenden Datenvolumens sollten Unternehmen auf eine Architektur umsteigen, die nicht nur heute die an sie gestellten Anforderungen erfüllt, sondern flexibel an zukünftige Anforderungen angepasst werden kann.

Die genannten Faktoren stellen auch eine Möglichkeit dar, die aktuelle Infrastruktur- und Geschäftsfunktionalität des Unternehmens zu analysieren. Dabei kann eine IT-Infrastruktur geschaffen werden, die einerseits den geschäftlichen Anforderungen gerecht wird und andererseits Informationen bereitstellt, die u. U. für eine gesetzliche Prüfung benötigt werden. Eine auf diese Weise erstellte Infrastruktur unterstützt nicht nur die Erfüllung von Compliance-Anforderungen, sondern macht das Unternehmen gleichzeitig beweglicher und reaktionsfähiger.

Die Schaffung einer Infrastruktur, die auf der standardmäßigen Nutzung von Compliance-Funktionen und der unternehmensweiten Unterstützung von Technologien basiert, bietet einem Unternehmen die folgenden potenziellen Vorteile:

- **Niedrigere Gesamtbetriebskosten:** Investitionen können für mehrere Regelungen genutzt werden. Beispielsweise werden in vielen Regelungen Anforderungen in Bezug auf die Dokumentaufbewahrung definiert, die durch die einmalige Investition in ein System für Content und Records Management erfüllt werden können.
- **Flexibilität:** Eine der Schwierigkeiten im Zusammenhang mit Compliance besteht darin, dass häufig neue Regelungen erlassen und bestehende Regelungen geändert werden. Eine zentrale Verwaltung der Compliance-Initiativen mittels einer unternehmensweiten Compliance-Architektur erlaubt eine rasche Anpassung des Unternehmens an solche Änderungen.
- **Wettbewerbsvorteil:** Eine Compliance-Architektur macht Geschäftsprozesse im Unternehmen leichter verständlich und kontrollierbar, so dass schneller und präziser auf externe oder interne Notwendigkeiten reagiert werden kann. Bestimmte Regelungen wie Basel II bieten darüber hinaus auf Grund des niedrigeren Mindestkapitalbedarfs konkrete Geschäftsvorteile, die durch eine unternehmensweite Compliance-Architektur realisiert werden könnten.

Die Angebotspalette von IBM umfasst Produkte, Lösungen und Services für die Einhaltung gesetzlicher Bestimmungen, die Unternehmen gleichzeitig die Möglichkeit geben, bewährte Verfahren zu implementieren, ihre Geschäftsabläufe zu ändern und aus ihren Geschäftsinformationen weitergehende Erkenntnisse sowie Vorhersagen abzuleiten. Wichtige betriebswirtschaftliche Faktoren für Investitionen sind z. B. die Fähigkeit, Informationsressourcen besser zu verwalten, die Einhaltung regulatorischer und rechtlicher Vorgaben nachzuweisen, das Risiko von Rechtsstreitigkeiten zu vermindern, die Kosten für Speicherung und Wiederauffinden zu senken und die Verantwortlichkeit des Unternehmens zu demonstrieren.

Auf Grund des breiten Angebotsspektrums von IBM können Risiken und Compliance-Herausforderungen auf vielfältige Weise angegangen werden.

Neben seiner Toolfunktionalität umfasst das Risk and Compliance Framework (siehe Abb. 1) eine Zusammenstellung von Organisationsprinzipien, mit denen Unternehmen, die von mehreren Regelungen betroffen sind, ihre geschäftlichen und technologischen Investitionen verwalten können. Die einheitliche Rahmenstruktur umfasst Risiko- sowie Compliance-Technologien und -Services und kann zur Schaffung einer Compliance-Architektur verwendet werden.

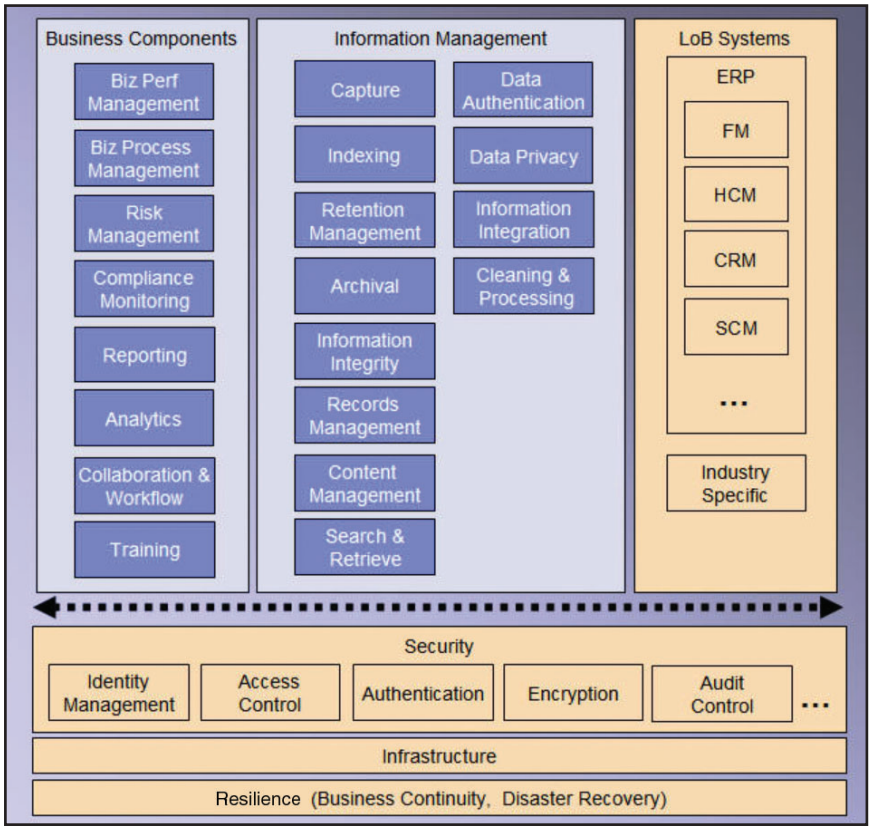

Abb. 1: Das IBM Risk and Compliance Framework.

Die Funktionalität des Frameworks:

- Vermittlung einer ganzheitlichen Sicht der für Compliance wesentlichen Elemente
- Beschreibung der Hauptbestandteile oder potenziellen Bausteine einer durchgängigen Lösung
- Berücksichtigung mehrerer Regelungen unterschiedlicher Branchen und Regionen
- Bereitstellung einer gemeinsamen Sprache (oder gemeinsamer Semantiken), um die Onlinezusammenarbeit zu vereinfachen
- Bereitstellung einer Basis für:
  - die Ermittlung des Umfangs von Projekten
  - die Festlegung einer Roadmap für die Erstellung einer umfassenden Lösung
  - die Ermittlung von Elementen, deren Nichtberücksichtigung das Projektrisiko erhöht
  - Überprüfung der aktuellen Infrastruktur, Tools und Technologien, um Lücken (Gaps) zu ermitteln
- Verkürzung der Realisierungszeit beim Kunden

Das Framework geht auf die Analyse diverser Regelungen und Standards zurück, bei der die Komponenten zur Bewältigung gemeinsamer Anforderungen ermittelt wurden. Bei der Auswahl der Komponenten für das Framework war maßgeblich, ob diese eine Funktionalität aufwiesen, mit der die explizit oder implizit genannten funktionalen Anforderungen einer Regelung erfüllt oder bewährte Praktiken umgesetzt werden konnten.

Das Framework schreibt keine bestimmten Technologien oder Geschäftsprozesse vor. Auch beinhaltet es nicht alle Elemente, die ein IT-System erfordert, da einige Elemente (in Infrastruktur- und Line-of-Business-Systemen(LOB)) von dem Mechanismus (Technologie bzw. manueller Prozess) abhängen, den das Unternehmen auswählt (z. B. Datenbank, Anwendungsserver und Data-Warehouse).

Das Framework macht keine Vorgaben zur Positionierung der von den einzelnen Komponenten repräsentierten Funktionalität innerhalb einer IT-Architektur. Kombinationen dieser Komponenten können u. U. durch ein einzelnes Produkt oder eine einzelne Lösung abgedeckt werden. So können die Komponenten für Erfassung, Indexierung, Aufbewahrung und Records Management möglicherweise in Form einer einzelnen Content-Management-Anwendung bereitgestellt werden.

Im Wesentlichen umfasst das Framework eine Reihe von Schwerpunktbereichen, die bei der Entwicklung von Lösungen für die Compliance-Problematik berücksichtigt werden sollten. Die Komponenten gliedern sich in die drei folgenden Bereiche:

- Geschäftskomponenten (siehe Tabelle 2)
- Informationsmanagementkomponenten (siehe Tabelle 3)
- Regelungsübergreifende Komponenten (siehe Tabelle 4)

Tabelle 2: Geschäftskomponenten

Komponente	Beschreibung	Beispiel
Business Performance Management	Mechanismus zur Optimierung der Unternehmensleistung mittels wichtiger Leistungsindikatoren, mit denen die Effizienz im Vergleich zu den betrieblichen Zielen gemessen werden kann.	• Kombination von Business-Intelligence mit Lösungen für das Business Performance Management, um einen höheren Return-of-Investment in Verbindung mit SOX-Compliance zu erzielen.
Geschäftsprozessmanagement	Verwaltung, Dokumentation und Umsetzung von Geschäftsprozessen.	• Einrichtung und Bewertung einer internen Kontrollstruktur (SOX).
Risikomanagement	Mechanismus für die Definition, Beurteilung und Entwicklung von Strategien für das Risikomanagement.	• Management des Betriebsrisikos (Basel II). • Erforderlicher Prozessbereich auf CMMI-Ebene 3 (Capability Maturity Model Integrated).
Compliance-Überwachung	Mechanismus für die Definition, Verwaltung und Visualisierung von Ereignissen (z. B. im Anzeigefeld) oder Bedingungen im Zusammenhang mit einer Regelung.	• Dauer bis zur Rückgutschrift an den Kunden (Check 21). • Immer das neueste Sicherheitspatch auf den Maschinen (HIPAA). • Volumen des überwachten im Vergleich zum gesamten Nachrichtenvolumen (NASD 3010).
Berichterstellung	Generierung von Ad-hoc- oder regelmäßigen statistischen oder informativen Berichten.	• Finanzberichterstattung und Offenlegung wichtiger Ereignisse (SOX, Basel II) • Frühwarnberichte (TREAD)
Analytik	Sortier- und Bearbeitungsfunktionen für Informationen, z. B.: • Statistische Analyse • Online-Analyseverarbeitung • Textanalyse (z. B. Engines für natürliche Sprachverarbeitung)	• Algorithmen zur Berechnung des Mindestkapitalbedarfs von Banken (Basel II). • Algorithmen zur Auswahl zu überwachender Nachrichten (NASD 3010). • Data-Mining für Erkennung statistischer Muster, Verhaltensvorhersage (z. B. Wahrscheinlichkeit der Nichterfüllung von Basel II) und Ermittlung von Datenanomalien (Anti-Geldwäsche-Bestimmungen des Patriot Act der USA).

Online-zusammen-arbeit und Workflow	Umgebung für die gemeinsame Erstellung und Verwaltung von Informationen. Diese Umgebung muss einen Mechanismus umfassen, um Prozess, Rollen und Ausführung strukturierter Aktivitäten einer bestimmten Aufgabe zu definieren.	• Umgebung für das Dokumentmanagement zur Erstellung von Investitionsforschungsberichten (NASD 2711). • Erstellung von Dokumenten für die Einreichung bei der SEC (SOX).
Schulung	Verteilung von Schulungsmaterialien an die Benutzer und Verfolgung der Lernfortschritte.	• Verantwortlichkeit des Unternehmens für Finanzberichte (SOX 302). • Qualifizierungsprüfung (NASD 2711). • Sicherheitsbewusstsein und -schulung (HIPAA).

Tabelle 3: Informationsmanagementkomponenten

Komponente	Beschreibung	Beispiel
Erfassung	Mechanismus zur Erfassung bestimmter Contentarten in einem Repository, z. B.: • E-Mail-Nachrichten • Sofortnachrichten • Faxe • Dokumente • Sprache • Bilder (z. B. Schecks und Formulare)	• Automatische Erfassung aller E-Mail- und Sofortnachrichten (NASD 3010)
Indexierung	Fähigkeit zur Bewertung von Einheiten sowie zur Erstellung und Verwaltung von Indexierungsbegriffen, die das Auffinden und Abrufen der Einheit vereinfachen.	• Erfordernis der Strukturierung und Indexierung von Informationen (SEC 17a-4)
Retention Management	Mechanismus für Management und Umsetzung einfacher Aufbewahrungsrichtlinien für Daten.	• Korrespondenz muss drei Jahre aufbewahrt werden (SEC 17a-4)

Datenauthentifizierung	Fähigkeit, die Übereinstimmung des Namens einer Einheit mit dem Urheber sicherzustellen und/oder die Fälschung oder Änderung auszuschließen. Wird im Zusammenhang mit Verantwortlichkeit und Unbestreitbarkeit verwendet. Ein Beispiel sind digitale Signaturen.	• Verantwortlichkeit des Unternehmens für Finanzberichte (SOX 302). • Fähigkeit zur Erkennung ungültiger oder geänderter Geschäftsdokumente (21 CFR 11).
Archivierung	Mechanismus für das Management der Datenarchivierung auf Kostenbasis oder für das Disaster-Recovery. Kann auch die Erstellung von Datenkopien umfassen.	• Geschäftsdokumente und Indizes müssen kopiert und von den Originalen getrennt gespeichert werden (SEC 17a-4).
Informationsintegrität	Mechanismus zur Prüfung und Verifizierung der Datenqualität.	• Prüfung der Qualität gescannter Bilder (Check 21). • Verifizierung des Prozesses zur Datenaufzeichnung (SEC 17a-4).
Informationsintegration	Fähigkeit, eine Gesamtsicht mehrerer unterschiedlicher Datenquellen anzubieten.	• Konsolidierung mehrerer Datenjahrgänge für Risikoberechnungen (Basel II)
Records Management	Erstellung und Implementierung systematischer Kontrollen für Informationen von Erstellung bzw. Empfang bis zum Ende des Lebenszyklus.	• Wertpapierbroker und -händler müssen alle Unterlagen nach 17a-3(a)(13) nach Ende ihres Beschäftigungsverhältnisses drei Jahre lang aufbewahren (SEC 17a-4). • Unterlagen zu neuen Indikationen für Arzneimittel müssen ab dem Datum der Einreichung fünf Jahre lang aufbewahrt werden (FDA Good Laboratory Practices).
Datenschutz	Mechanismus zur Definition und Gewährleistung des ordnungsgemäßen Umgangs mit sensiblen Daten (d. h. Verwaltung von persönlichen und Finanzdaten).	• Vorgaben für die Offenlegung persönlicher Daten (GLBA).
Content-Management	Mechanismus für Management (einschließlich Versionssteuerung) und Verteilung von Content aus unterschiedlichen Quellen (d. h. einem Content-Repository).	• System für Management und Verwaltung von Scheckbildern (Check 21). • Repository für Investitionsforschungsberichte (NASD 2711).

Suchen und Abrufen	Zugriff auf Daten über eine Funktion zum Suchen und Abrufen. Deckt auch besondere Anforderungen spezieller Anwendungen z. B. zur Unterstützung bei Rechtsstreitigkeiten ab.	• Jeder Broker bzw. Händler muss nach 17a-3 (SEC 17a-4) unverzüglich Geschäftsdokumente erstellen.
Bereinigung und Verarbeitung	Mechanismus zur Datenbereinigung und -verarbeitung. Unterstützt auch das ETL-Konzept (Extrahieren, Umwandeln und Speichern).	• Beseitigung der Kopien von E-Mail-Nachrichten, die an mehrere Empfänger im selben Unternehmen gesendet wurden (NASD 3010). • Bereinigung und Verarbeitung von Finanzdaten vor dem Speichern in einem Data-Warehouse für Risikoberechnungen (Basel II).

Tabelle 4: Regelungsübergreifende Komponenten

Komponente	Beschreibung	
LOB-Systeme	Allgemeine Bezeichnung für eine Gruppe von Geschäftsanwendungen einschließlich ERP, CRM, Lieferkette usw. Diese Anwendungen sind für ein Gesamtbild des Unternehmens erforderlich.	• ERP-Systeme zur Unterstützung beim Management komplexer Fertigungsumgebungen, um die FDA-Compliance zu gewährleisten.
Sicherheit	Sicherheit ist für alle Elemente des Frameworks relevant. Neben dem Zugriff auf Anwendungen und Daten deckt sie geschäftsregel- und rollenbasierte Datensichten ab. Die Komponente hat technologische, Prozess- und organisatorische Bestandteile.	
Identitäts-management	Mehre Komponenten zur Identifizierung und Verwaltung von Personen in einem System sowie für Verwaltungsaufgaben (z. B. Kennwortmanagement).	• Nutzung eines LDAP-Verzeichnisservers für die Identifizierung von Mitarbeitern.
Zugriffs-steuerung	Mechanismus zur Definition und Durchsetzung der für Personen oder Anwendungen geltenden Beschränkungen und Rechte. Beinhaltet die rollenbasierte Zugriffssteuerung.	• Gewährleistung, dass Patientendaten nur für berechtigte Dienstleister im Gesundheitswesen zugänglich sind (HIPAA).

Authentifizierung	Im Rahmen des Authentifizierungsprozesses versucht eine Einheit, die Identität einer anderen Einheit zu bestätigen.	• Nutzung eines LDAP-Verzeichnisservers für die Authentifizierung von Mitarbeitern.
Verschlüsselung	Verwendung eines Algorithmus für die Umwandlung von Daten in eine Form, in der sie mit hoher Wahrscheinlichkeit nicht ohne einen geheimen Prozess oder Schlüssel entschlüsselt werden können. In diesem Framework gehört auch die Verschlüsselung von Daten und/oder Datenübertragungen dazu.	• Fähigkeit zur Gewährleistung der Vertraulichkeit (21 CFR 11). • Ausnahme für verschlüsselte Daten (SB 1386).
Revisionskontrolle	Mechanismus zur Verwaltung der Revisionsdaten in einem End-to-End-System.	• Jeder Broker bzw. Händler muss über ein Revisionssystem verfügen, um die Eingabe von Datensätzen nachweisen zu können. Dieses System muss zur Überprüfung bereitstehen (SEC 17a-4).
Infrastruktur	Zur Infrastruktur zählen im Wesentlichen Hardware, Plattformsoftware und Netzkonnektivität sowie alle Systemmanagementkomponenten. Sie wurde der Vollständigkeit halber in dieses Framework aufgenommen.	
Hochverfügbarkeit	Fähigkeit eines Unternehmens, auf interne oder externe widrige, sich schnell ändernde oder unerwartete Bedingungen zu reagieren und den Geschäftsbetrieb ohne nennenswerte Unterbrechung fortzuführen.	• Jede Information und jeder Index muss dupliziert und vom Original getrennt gespeichert werden (SEC 17a-4). • Notfallpläne (HIPAA).

Gemeinsame Komponenten

Auf Grund der heutigen großen Zahl von Regelungen und Standards verwendet IBM eine Systematik (ein Klassifikationssystem), um ähnliche Regelungen zusammenzufassen (siehe Tabelle 5). Beispielsweise unterscheiden sich die Anforderungen an die Aufbewahrung von Geschäftsdokumenten je nach Regelung, die angesprochenen grundlegenden Probleme lassen sich jedoch in einer ILM-Klassifizierung zusammenfassen.

Tabelle 5: Regulatorische Systematik

Klassifizierung	Enthaltene Konzepte	Beispiele
Corporate Governance	• Finanzberichterstattung • Transparenz • Unternehmenskontrollen • Verantwortlichkeit • Unternehmens- und Bilanzdelikte • Offenlegung • Finanztransaktionen • Wichtige Ereignisse • Sicherheitsinformationen und Rückrufe	1. SOX 2. SEC Act 1933,1934 3. TREAD 4. IAS
Business Improvement	• Risikominderung • Gesetzliche Bestimmungen zum Kapital • Konstruktionsmodelle	1. Basel II 2. CMMI 3. ISO 9000
Hochverfügbarkeit von Geschäftsprozessen	• Disaster-Recovery • Verfügbarkeit	1. NFPA1600 2. Check 21
Transaktionsintegrität	• Geldwäschebekämpfung • Terrorismusbekämpfung • Brokerüberwachung • Elektronische Signaturen	1. NASD 3010/3110 2. NASD 2711 3. NYSE472 4. 21CFR11 5. Patriot Act
Datenschutz	• Sicherheit • Schutz personenbezogener Daten	1. HIPAA 2. GLBA 3. SB 1386 4. EU-Datenschutz 5. FOIA 6. ISO17799 7. NERC1200UAS
Verwaltung von Daten über ihre gesamte Lebensdauer (Information Lifecycle Management, ILM)	• Standards für das Informationsmanagement • Aufbewahrungsanforderungen • Standards für die Datenhaltung	1. OMBA-130 2. SOX 3. SEC17a-4 4. DOD 5015.2 5. PRO 2 6. MoREQ 7. VERS 8. DOMEA 9. NOARK

Jede der genannten Komponenten kann einer oder mehreren Klassifikationen zugeordnet werden. Aus Tabelle 6 geht hervor, welche Komponenten für mehrere Arten von Regelungen verwendet werden können und ob die Funktionalität der Komponente in einer bestimmten Klassifizierung von primärer oder sekundärer Bedeutung ist.

Tabelle 6: Zuordnung der Komponenten zu den regulatorischen Klassifikationen

	Corporate Governance	Business Improvement	Business Resilience	Transaction Integrity	Information Protection	Information Lifecycle Mgt
Biz Perf Mgt	2	2				
Biz Process Mgt	2	2		2	2	
Risk Mgt	1	1	2	2	2	
Comp. Monitoring	1	2	1	1	1	2
Reporting	1	1	2	1	1	1
Analytics	1	1	2	2		2
Collab/Workflow	1	2	2	1		2
Training	2			1	1	
Capture	1		2	1	2	1
Indexing	2	2	2	2	2	1
Retention Mgt	1		1	1	2	1
Data Authentication	1		2	1	1	2
Archival	1	2	2	2	1	1
Info Integrity	1		2	2	2	2
Info Integration	2	2		2	2	2
Records Mgt	2		2	2	1	1
Data Privacy	1			2	1	
Content Mgt	2		2	2	2	1
Search/Retrieve	1		2	1	2	1
Clean/Proc		2	2	2		2
LoB Systems	1	1	1	1	1	1
Security	1	1	1	1	1	1
Identity Mgt	1	1	1	1	1	1
Access Control	1	1	1	1	1	1
Authentication	1	1	1	1	1	1
Encryption	2	2	2	2	1	2
Audit Control	1	1	1	1	1	1
Infrastructure	1	1	1	1	1	1
Resiliency	1	1	1	1	1	1

1 – Primary Focus, 2 – Secondary Focus

Risiko und Compliance on demand

Das heutige wettbewerbsorientierte Geschäftsumfeld verlangt, dass Unternehmen ihren Mitarbeitern, Geschäftspartnern und Lieferanten den Zugang zu den Systemen und Informationen ermöglichen, die eine effizientere Geschäftsabwicklung erlauben. Neue Technologien in Verbindung mit einer breiten Implementierung offener Standards haben den Durchbruch gebracht. Heute nutzen die Unternehmen für ihre Geschäftsabwicklung Methoden, die noch vor wenigen Jahren undenkbar waren. IBM bezeichnet diesen Durchbruch als On Demand Business. Zudem macht die heutige komplexe regulatorische Umgebung es notwendig, dass Unternehmen sich wirksam und effizient mit Risiken und Compliance-Fragen auseinander setzen.

Ein On Demand Business ist ein Unternehmen, dessen Geschäftsprozesse unternehmensweit durchgehend integriert sind und auch wichtige Geschäftspartner, Lieferanten und Kunden einschließen. So können diese Geschäftsprozesse schnell auf jede Kundenanforderung, jede Marktchance und jede externe Bedrohung reagieren. Unter Risiko- und Compliance-Gesichtspunkten ist ein On Demand Business ein Unternehmen, dessen Risiko- und Compliance-Initiativen unternehmensweit integriert sind, so dass das Unternehmen schnell auf Forderungen von Regulierungsstellen sowie auf das neue und sich wandelnde regulatorische Umfeld reagieren kann.

Die grundlegende IT-Infrastruktur für ein On Demand Business wird als On Demand Betriebsumgebung bezeichnet. Diese Betriebsumgebung kann mit Hilfe des Risk and Compliance Framework eingerichtet werden, das dafür Sorge trägt, dass die notwendigen Services berücksichtigt werden, um regulatorischen Herausforderungen begegnen zu können. Dieses Framework ermöglicht die Bewertung der IT-Anforderungen sowie der vorhandenen Technologien. So kann ermittelt werden, wie mit der Bereitstellung der grundlegenden Infrastruktur die Voraussetzungen für ein widerstandsfähiges, reaktionsfähiges, fokussiertes und variables Unternehmen geschaffen werden können, das heute und in Zukunft für alle regulatorischen Herausforderungen gewappnet ist.

Nutzung des IBM Risk and Compliance Framework

Mit Hilfe des IBM Risk and Compliance Framework können Unternehmen sich innerhalb des Kontinuums zwischen Compliance und Reife bewegen (siehe Abb. 2). In diesem Kontinuum kann ein Unternehmen zunächst manuelle Prozesse einsetzen oder taktische punktuelle Lösungen implementieren, wenn bis zu einem bestimmten Zeitpunkt Übereinstimmung mit einer Regelung erzielt werden muss, um Sanktionen zu vermeiden. Häufig steigen Unternehmen in diese Phase ein, da sie sich zunächst über die Bedeutung von Compliance in ihrer Umgebung klar werden müssen. Am Anfang steht bei diesem Ansatz das Verständnis, welche Schritte nötig sind, und dann das Verständnis, in welchen Bereichen Optimierungs- und Automatisierungspotenzial besteht. Die Verbesserungsphase ist durch die Implementierung von Anwendungen und Infrastruktur gekennzeichnet, die manuelle Prozesse ersetzen und so eine nachhaltige Compliance möglich machen. In der Umgestaltungsphase können die Unternehmen mit der Nutzung ihrer Compliance-Investitionen beginnen, indem sie die erfassten Informationen zur Wertschöpfung einsetzen, um so einen Wettbewerbsvorteil zu erzielen.

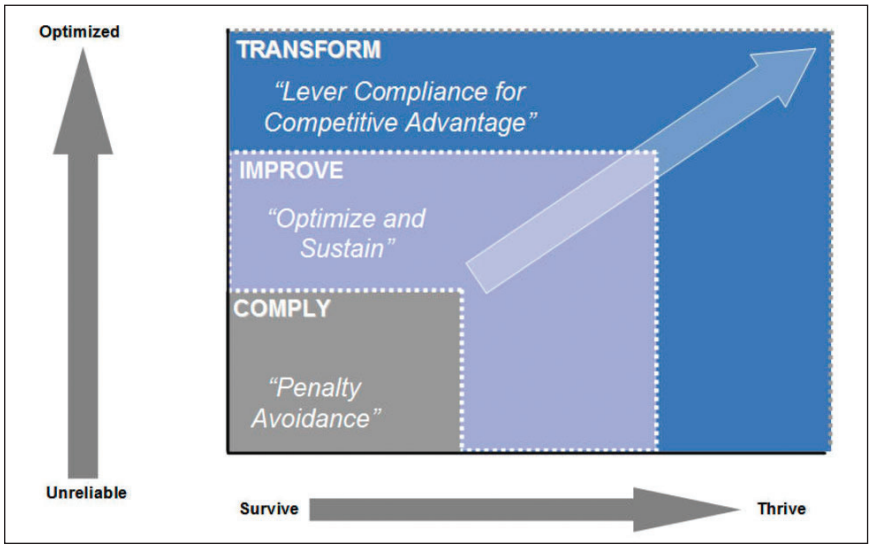

Abb. 2: Kontinuum zwischen Compliance und Reife.

Das Framework kann auf vielfältige Weise eingesetzt werden:

- Als Tool, das Kunden dabei hilft, ihre Ideen zu strukturieren und sinnvolle Verbesserungen ihrer Compliance-Umgebung herauszufiltern.
- Als Tool, mit dem Kunden ihre derzeitige IT-Infrastruktur beurteilen und bewerten können.
- Als Tool, das einen Überblick über die Compliance-Angebote von IBM und IBM Business Partnern bietet.
- Als Input für bestimmte Kontrollziele anderer Frameworks, z. B. CobiT. Eines der Kontrollziele in der CobiT-Domäne „Planung und Organisation" betrifft die Notwendigkeit zur Definition der Informationsarchitektur. Ein Unternehmen, das sich für CobiT als Framework für IT-Governance entschieden hat, kann sich bei der Definition der Kontrollen am IBM Risk and Compliance Framework orientieren.

Die wichtigsten Ziele bei der Nutzung des Frameworks für eine Gap-Prüfung sind:

- Bewertung der Auswirkungen mehrerer Regelungen
- Nutzung der vorhandenen Infrastruktur
- Ermitteln von Möglichkeiten, wie Investitionen für das Business Improvement eingesetzt werden können
- Entwicklung einer umfassenden Roadmap

Beispiel: Verwendung des Frameworks für die Gap-Analyse

Hier werden die Schritte bei der Verwendung des Frameworks für die Gap-Analyse beschrieben. Die wichtigsten Ziele sind nachfolgend zusammengestellt.

Festlegung des Umfangs

1. Der Kunde ermittelt unter Nutzung seiner Beratungs- und Prüfungsressourcen die für das Unternehmen, die Region und/oder den Unternehmensbereich geltenden Regelungen, Verfahren und/oder Vorgaben.
2. Der Kunde ermittelt den Regelungszeitplan sowie bestehende Initiativen.
3. Wahlweise kann sich der Kunde für die Berücksichtigung interner Richtlinien entscheiden, die über die Anforderungen externer Regulierungsstellen (z. B. Interessengruppen) hinausgehen.

Bestimmung der Anforderungen

1. Der Kunde ermittelt unter Nutzung seiner Beratungs- und Prüfungsressourcen die für das Unternehmen, die Region und/oder den Unternehmensbereich geltenden Anforderungen in Bezug auf Regelungen, Verfahren und/oder Vorgaben.
2. Wahlweise kann sich der Kunde für die Berücksichtigung zusätzlicher Anforderungen in Bezug auf interne Richtlinien entscheiden, die über die Anforderungen externer Regulierungsstellen hinausgehen.

Durchführung einer Ist-Analyse

1. Abbildung der vorhandenen Infrastruktur auf die Risiko- und Compliance-Funktionalität:
   a. Ermittlung sämtlicher Anwendungen und Prozesse im Zusammenhang mit der Funktionalität
   b. Komplette Bestandsaufnahme unter Berücksichtigung zentraler und ergänzender Anwendungen
2. Abbildung der bestehenden Anforderungen auf Anwendungen:
   a. Zuordnung von Anforderungen zu Anwendungen
   b. Hervorheben der Bereiche, in denen mehrere Anwendungen ähnliche Anforderungen erfüllen, oder fehlender Anwendungen

Durchführung einer Soll-Analyse

1. Überprüfung und Aktualisierung der Anforderungen:
   a. Zusammenführen der Anforderungen
   b. Aktualisierung auf der Basis neuer Regelungen
2. Durchführung von Visionierungssitzungen:
   a. Vorstellung von Best-Practice-Vorlagen für die Unternehmenspraxis
   b. Erörterung der anvisierten Prozesse

Durchführung der Gap-Analyse

1. Ermittlung von Problemen und Chancen:
   a. Ermittlung von Problemen im Zusammenhang mit bisher eingesetzten Technologien
   b. Ermittlung von Chancen zur Nutzung der vorhandenen Infrastruktur und/oder neuer Produkte und Lösungen
2. Ermittlung von Lösungsalternativen:
   a. Bewertung der vorhandenen Infrastruktur
   b. Ermittlung in Frage kommender Produkte und Lösungen
   c. Aufwands- und Nutzenschätzung

Entwicklung einer Roadmap

1. Bewertung der Alternativen:
   a. Entwicklung einer Bewertungsmatrix
   b. Durchführung einer Bewertungs- und einer Feedbacksitzung
2. Erstellung einer Kosten-Nutzen-Analyse:
   a. Analyse von Wettbewerbsvorteilen
   b. Erstellung einer Empfehlung
3. Erarbeitung/Bestätigung von Arbeitsplänen, Budget und Roadmap:
   a. Vergabe von Prioritäten für Implementierungen
   b. Ausarbeitung einer strategischen Roadmap
   c. Ausarbeitung eines kurzfristigen Arbeitsplans und eines Budgetarbeitsblatts
   d. Verifizierung der Ergebnisse und Empfehlungen mit der Beratungs- und der Rechtsabteilung
   e. Erstellung des Abschlussberichts

Weitere Informationen

Wenn Sie weitere Informationen wünschen, wenden Sie sich an Ihren zuständigen IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie die IBM Webseite Risk & Compliance unter:

ibm.com/software/info/openenvironment/rcf

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Hergestellt in den USA
01-05

G507-1471-00-GE