

## **Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen**



Inhalt
<b>2 Übersicht</b>
<b>3 Zum Verständnis der relevanten Abschnitte des Sarbanes-Oxley-Gesetzes</b>
<b>4 Identifizieren Sie die operativen Schlüsselbereiche, denen Sie sich widmen müssen, um das Sarbanes-Oxley-Gesetz einzuhalten</b>
<b>7 Eine breitere Perspektive durch Enterprise Risk Management</b>
<b>9 Nutzen Sie IBM Lösungen, um SOX im Einklang mit COSO und ERM gerecht zu werden</b>
<b>11 Schlussfolgerung</b>
<b>11 Weitere Informationen</b>

## Übersicht

Das Sarbanes-Oxley-Gesetz von 2002 (SOX) verlangt besonders von Unternehmen in assetintensiven Branchen eine umfassende Analyse der Systeme und Prozesse. Aufgrund der Chancen auf hohe Umsatzzuwächse ergreifen immer mehr Softwarefirmen, Wirtschaftsprüfungsgesellschaften und Unternehmensberater die Gelegenheit, neue Umsatzströme zu erschließen; dies führt zu neuen Produktinvestitionen in Millionenhöhe und zu Tausenden von Arbeitsstunden, die den Vorschriften entsprechen müssen. Die anfänglichen Schätzungen der US-Wertpapieraufsichtsbehörde Securities and Exchange Commission (SEC), dass Aktiengesellschaften weniger als 100.000 US-Dollar für die Dokumentierung interner Kontrollmechanismen aufwenden müssten, wurden durch die nackten Tatsachen widerlegt: „Die tatsächlichen Kosten lagen im Durchschnitt zwanzigmal so hoch“.<sup>1</sup>

Auch nach der Entwicklung und Implementierung von Compliancemaßnahmen erfährt ein Unternehmen erst nach einer Prüfung durch die SEC, ob die beträchtlichen Investitionen zum Erfolg geführt haben. Außerdem herrscht Unklarheit in den Unternehmen, was sie unternehmen und worauf sie ihre Anstrengungen richten sollten. Softwarefirmen sind der Meinung, dass mehr Geld für ihre Produkte oder Lösungen ausgegeben werden sollte. Wirtschaftsprüfungsgesellschaften sagen, es gehe um Finanzprozesse. Unternehmensberater empfehlen, sich die Arbeitsabläufe anzusehen und sie individuell anzupassen.

In Wahrheit benötigen Unternehmen eine Mischung aller drei Konzepte. Die richtige Kombination unterstützt nicht nur die Bemühungen zur Einhaltung der SOX-Vorschriften, sondern kann auch zu Wettbewerbsvorteilen führen. Unternehmen sollten diese Gelegenheit zur Überarbeitung der Geschäftsprozesse nutzen, die Softwarenutzung im gesamten Unternehmen konsolidieren und innerhalb der betrieblichen Abläufe die Bereiche ausfindig machen, in denen die fristgerechte Offenlegung gefährdet ist.

Zu SOX gehören im Wesentlichen fünf Gesetze, die sich auf assetintensive Branchen beziehen: die Abschnitte 301, 302, 401, 404 und 409. In assetintensiven Branchen geht es nicht nur um die Einhaltung der SOX-Vorschriften; es geht auch um eine Verbesserung des gesamten Risikomanagements innerhalb einer Organisation. Das vorliegende Dokument widmet sich vor allem diesen Elementen und schafft eine notwendige Verbindung zwischen einer finanzwirtschaftlich orientierten Compliance-Initiative und einem unternehmensorientierten Compliance-Ansatz.

## Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen

Seite 3

### Zum Verständnis der relevanten Abschnitte des Sarbanes-Oxley-Gesetzes

Aufgrund von Skandalen im Zusammenhang mit bestimmten Unternehmen, deren Aktien an der US-Börse gehandelt wurden, wurden durch das SOX das Abrechnungswesen und der Anlegerschutz reformiert. Generell wurden Prüfpunkte zu Richtlinien und Verfahren definiert, um die Unabhängigkeit von Abschlussprüfern sowie Vorstands- und Aufsichtsratsmitgliedern zu stärken. Außerdem wurde ein neuer Prozess zur Zertifizierung der Unternehmensabschlüsse geschaffen, der CEOs und/oder CFOs für jede falsche Darstellung der Leistungswerte des Unternehmens persönlich haftbar macht.

Die Diskussionen über SOX zeigen, dass im Wesentlichen fünf Abschnitte dieses Gesetzes zu beachten sind (im Abschnitt „Nutzen Sie IBM Lösungen, um SOX im Einklang mit COSO und ERM gerecht zu werden“ im vorliegenden Dokument wird gezeigt, wie die Umsetzung dieser Abschnitte mithilfe von IBM Software unterstützt werden kann):

Abschnitt	Überschrift	Beschreibung
301	Public Company Audit Committees (Prüfungsausschüsse für Aktiengesellschaften)	Definiert Regeln, denen zufolge die Mitglieder des Prüfungsausschusses vom Unternehmen unabhängig sein müssen. Fordert vom Unternehmen die Entwicklung eines Prozesses, der anonyme Beschwerden von Mitarbeitern an den Prüfungsausschuss bearbeitet.
302	Corporate Responsibility for Financial Reports (Zuständigkeit für Finanzberichte)	Definiert Regeln für CEOs und CFOs im Zusammenhang mit der Unterzeichnung von Finanzberichten. Mit der Unterzeichnung solcher Berichte übernehmen sie unter anderem folgende Pflichten: <ul style="list-style-type: none"> <li>• Einrichtung und Aufrechterhaltung interner Kontrollmechanismen</li> <li>• Konzeption von Kontrollen, mit deren Hilfe die Führungskräfte des Unternehmens wesentliche Informationen erhalten</li> <li>• Prüfung der Wirksamkeit der Kontrollen innerhalb von 90 Tagen vor der Berichterstellung</li> </ul>
401	Disclosures in Periodic Reports (Offenlegung in periodischen Berichten)	Legt fest, dass die Finanzberichte in Übereinstimmung mit den in den USA geltenden Grundsätzen ordnungsgemäßer Buchführung und Bilanzierung (Generally Accepted Accounting Principles, GAAP) erarbeitet werden müssen. Die Unternehmen müssen alle bilanzneutralen Transaktionen offenlegen und Pro-forma-Kennziffern mit GAAP-Kennziffern abstimmen.
404	Management Assessment of Internal Controls (Prüfung interner Kontrollen durch das Management)	Überträgt dem Management die Verantwortlichkeit für die Schaffung und Aufrechterhaltung interner Kontrollmechanismen und Verfahren für die Finanzberichterstattung. Das Management muss die Wirksamkeit der internen Kontrollmechanismen bewerten und einen Bericht über die Kontrollen erstellen. Der Prüfer muss einen Bericht über die Bewertung der internen Kontrollmechanismen durch das Management erstellen.
409	Real-Time Issuer Disclosures (Unmittelbare Offenlegung)	Ein Unternehmen muss unverzüglich – der Öffentlichkeit gegenüber auf leicht verständliche Art – berichten, sobald es Kenntnis von wesentlichen Änderungen der finanziellen Situation oder der betrieblichen Abläufe erlangt.

# Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen

Seite 4

## Highlights

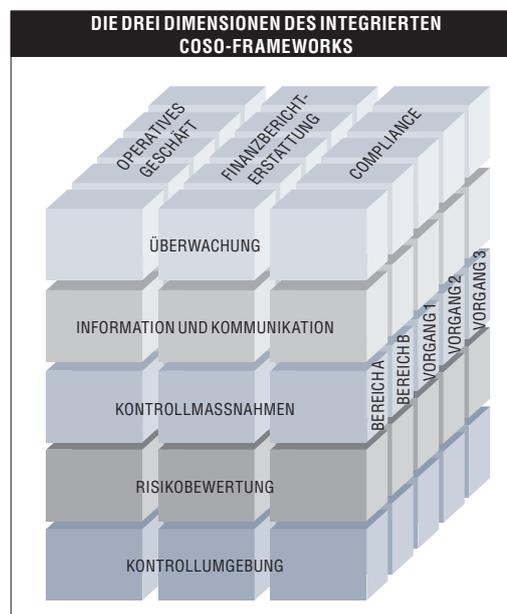
Die meisten Organisationen können für die Implementierung von Compliance-Prozessen vorhandene Systeme nutzen.

Anfänglich könnte eine Analyse dieses Gesetzes einschüchternd wirken; die meisten Organisationen verfügen jedoch bereits über Prozesse, zum Beispiel einen Einkaufsprozess, die zur Unterstützung der Compliance dienen können. Andere Prozesse, etwa ein Verfahren, mit dem Mitarbeiter Beschwerden anonym vorbringen können, müssen in der Regel neu eingerichtet werden. Die gute Nachricht lautet, dass die meisten Organisationen für die Implementierung von Compliance-Prozessen vorhandene Systeme nutzen können.

### Identifizieren Sie die operativen Schlüsselbereiche, denen Sie sich widmen müssen, um das Sarbanes-Oxley-Gesetz einzuhalten

Es gibt viele Möglichkeiten, sich mit den für die Einhaltung der SOX-Vorschriften fehlenden Elementen innerhalb einer Organisation zu befassen, von der Nutzung vorhandener Technologien bis zur Einführung neuer Geschäftsprozesse. Entscheidungen darüber, wie Compliance erreicht werden kann, können auf den bereits vorhandenen Kontrollen und Übereinstimmungen, auf dem erreichten Integrationsgrad der Systeme und auf früheren Finanzberichten des Unternehmens basieren.

Das Framework des Committee of Sponsoring Organizations (COSO) ist das Modell, auf das die meisten Branchenkenner verweisen, wenn es um die in Abschnitt 404 definierten Anforderungen an die Dokumentation und Bewertung der Risiken innerhalb des Unternehmens geht. Dieses Framework dient der Bewertung der Risiken innerhalb der Geschäftsbereiche und/oder Vorgänge innerhalb einer Organisation. Die Bewertung eines Risikos basiert auf einer Übersicht, an welcher Stelle in einem Unternehmen es in Bezug auf Finanzen, Compliance und operatives Geschäft auftreten kann (siehe Abbildung).

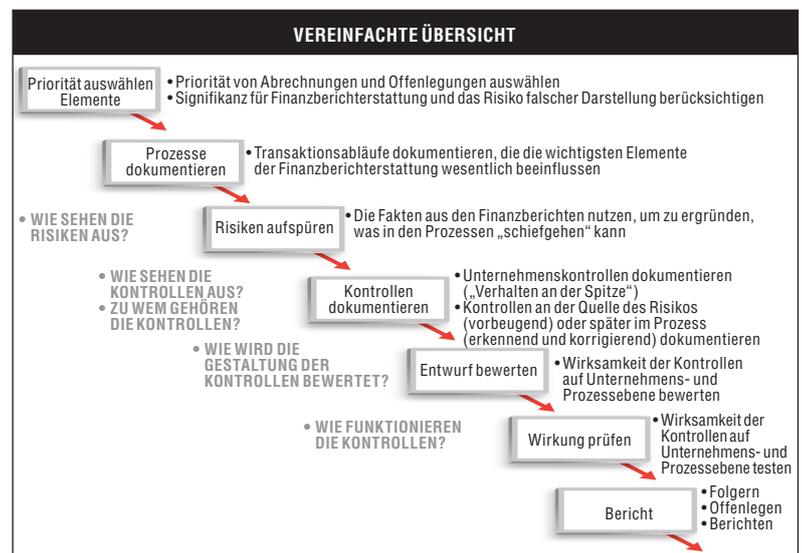


Die drei Dimensionen des integrierten COSO-Frameworks. Quelle: Protiviti, Inc.<sup>2</sup>

# Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen

Seite 5

Wie die folgende Abbildung zeigt, hilft die Dokumentierung – und in einigen Fällen die Einrichtung – von Geschäftsprozessen mit dem COSO-Framework bei der Umsetzung des SOX-Abschnitts 404. Mit Hilfe dieser Maßnahmen kann ein Unternehmen schrittweise ein Konzept erarbeiten, um das Risiko bei jedem einzelnen Vorgang innerhalb eines Geschäftsbereichs zu analysieren. Ein Unternehmen muss dokumentieren, warum es einem Vorgang das jeweilige Risiko zugeordnet hat. Wenn ein Vorgang als sehr riskant eingestuft wurde, muss das Unternehmen den richtigen Workflow implementieren, der bei Auftreten dieses Vorgangs befolgt werden muss.



Einfache Übersicht des COSO-Frameworks. Quelle: Protiviti, Inc.<sup>2</sup>

Ein Beispiel für einen Vorgang, der als sehr riskant eingestuft werden könnte, ist die Verzögerung eines Turnaround-Projekts. Das leitende Management eines Unternehmens könnte zum Beispiel festlegen, dass ein Vorgang, der das Unternehmen 300.000 US-Dollar oder mehr kostet, als wesentliches Ereignis definiert wird. Wenn sich ein Turnaround-Projekt verzögert und die dadurch entstehenden Kosten diesen Schwellenwert erreichen, muss das Unternehmen ein System nutzen können, das eine Sicht auf dieses Asset ermöglicht und einen Workflow einleitet, der die betroffenen Personen und Systeme über das Eintreten des Ereignisses informiert.

### Highlights

Ein Unternehmen kann auf der Grundlage der eigenen Strategie diesen einen Schritt weitergehen und für eine proaktive Benachrichtigung sorgen, sobald die Kosten diesen Schwellenwert zu erreichen drohen. Über eine Statusübersicht für Führungspersonal könnte das Unternehmen einen Blick in dieses Projekt – und auch in vorbeugende Benachrichtigungen – schaffen.

Schließlich könnte das Unternehmen in einem weiteren Schritt die Analyse von „Was wäre, wenn“-Szenarien ermöglichen. Stellen Sie sich beispielsweise ein Öl- und Gasunternehmen vor, das am Quartalsende ankündigt, dass aufgrund von Wirbelstürmen im Abrechnungszeitraum der Gewinn niedriger ausfallen wird als erwartet. Würde dasselbe Ereignis im nächsten Jahr wieder eintreten, dann sollte das Unternehmen auf den Vorwurf der SEC vorbereitet sein, gegen SOX verstoßen zu haben: Die SOX-Regeln über die Informationspflicht in Echtzeit besagen, dass das Unternehmen die Anleger vor dem Quartalsende über die Auswirkungen von Wirbelstürmen auf die Geschäftstätigkeit informieren muss. Die SEC könnte darauf verweisen, dass die vorhandenen Systeme Informationen über die Auswirkungen enthalten und dass das Unternehmen einen dokumentierten Prozess besitzen muss, der die Anleger über die Betriebsbedingungen von Assets informiert.

Nutzen Sie ein assetorientiertes System, das in Echtzeit eine Sicht auf den Status von Assets liefert.

Mithilfe eines assetorientierten Systems, das in Echtzeit eine Sicht auf den Status von Assets – zum Beispiel die Bohrinseln auf dem Weg des Wirbelsturms – liefert, könnte dieses Unternehmen einen Prozess entwickeln, der Benachrichtigungen über den Betriebszustand und die Betriebsbedingungen des Assets verschickt, wenn diese die betrieblichen Abläufe wesentlich beeinträchtigen. Mittels Workflow- oder Systemintegration könnte diese Benachrichtigung an die Finanzabteilung geschickt werden. Außerdem könnte eine Statusübersicht für Führungspersonal eine assetorientierte Sicht auf die Geschäftstätigkeit liefern.

Die Nutzung eines Finanzsystems ist nicht die einzige Antwort zur Einhaltung der SOX-Vorschriften. Das Unternehmen sollte alle Geschäftsbereiche bewerten, von den Regelungen für das Finanz- und Unternehmensmanagement bis zum Asset- und Portfoliomanagement. Ein System allein kann nicht alle Prozesse beherrschen, die mit einem Unternehmen verbunden sind. Würde eine Organisation versuchen, ein solches System zu schaffen, dann würde sie bei kleinen Systemen an der Peripherie (zum Beispiel Microsoft® Access-Datenbanken und Microsoft Excel-Tabellen) landen, die mit branchen- bzw. bereichsspezifischen Anforderungen umgehen müssten.

### Highlights

Betrachten Sie Compliance aus der Sicht eines Unternehmens, um schnell gegenseitige Abhängigkeiten und Beziehungen zwischen Systemen und Unternehmensbereichen zu erkennen.

Die Unternehmen sollten stattdessen Systeme nutzen, die für die operative oder finanzielle Aufgabe geeignet sind. Kritische Systeme sind in assetintensiven Branchen etwa das Enterprise-Resource-Planning, das Projektmanagement, das Asset- und Service-Management und die Produktionsplanung. Ein Unternehmen, das Compliance aus unternehmerischer Sicht betrachtet, erkennt schnell die gegenseitigen Abhängigkeiten und Beziehungen zwischen den Systemen und Geschäftsbereichen, denen es sich widmen muss, um die SOX-Vorschriften einzuhalten. Beispielsweise muss es Systeme im gesamten Unternehmen standardisieren, Sicherheitsperren für Geschäftsprozessabläufe zwischen Systemen und Bereichen einrichten, die Sicherheit der vorhandenen Systeme maximieren und eine Echtzeitansicht des Unternehmens erstellen.

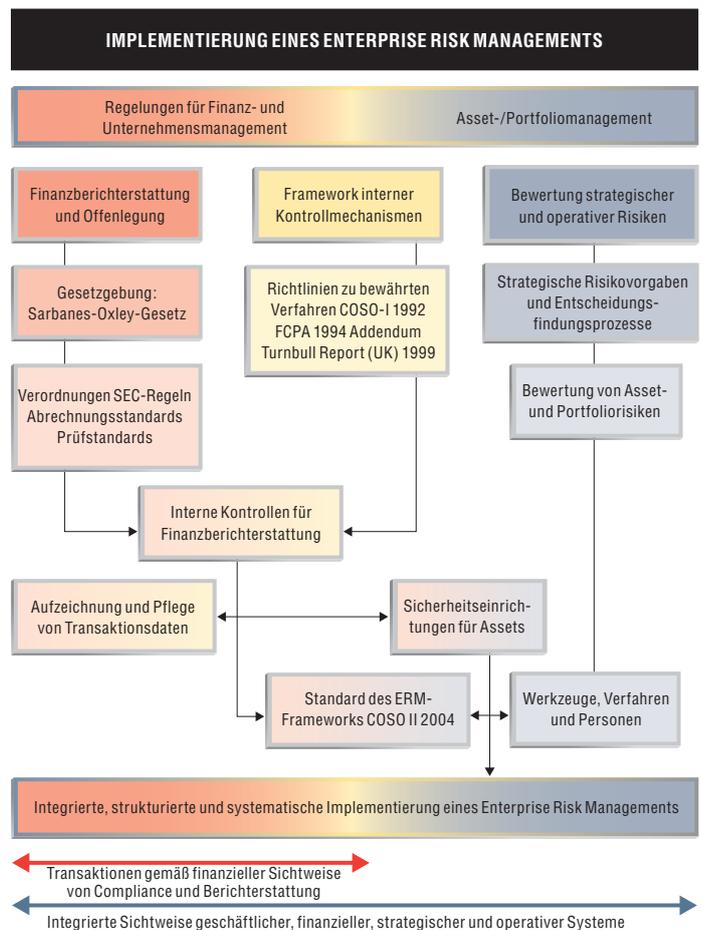
#### **Eine breitere Perspektive durch Enterprise Risk Management**

Unternehmen in assetintensiven Branchen müssen sich nicht nur darum kümmern, wie sie die SOX-Vorschriften einhalten, sondern auch darum, wie die Compliancemaßnahmen mit anderen Aufgaben zusammenhängen, die sich aus staatlichen Verordnungen ergeben.<sup>3</sup> Ein Unternehmen muss weitere strategische oder operative Risiken berücksichtigen und bestimmen, wie sein Asset- und Portfoliorisiko bewertet werden soll. Im Allgemeinen wird dieses übergreifende Konzept als Enterprise Risk Management (ERM) bezeichnet; es stellt eine Weiterentwicklung des COSO-Frameworks dar (häufig als COSO-II Enterprise Risk Framework bezeichnet).

ERM verknüpft die operativen mit den finanziellen Aspekten von Compliancemaßnahmen. Es spiegelt nicht nur die finanzielle Sichtweise von Compliance und Berichterstattung wider, sondern repräsentiert ein integriertes Konzept für geschäftliche, finanzielle, strategische und operative Systeme.

# Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen

Die folgende Abbildung zeigt ein standardisiertes Konzept für die Beziehung zwischen finanziellen und operativen Systemen. Das Committee of Sponsoring Organizations (COSO) entwickelte dieses Framework als typische Basis für ein ERM-Konzept. Das Modell betont die Notwendigkeit, über die internen Finanzkontrollen und die Einhaltung der Prüfungsvorschriften hinauszugehen, um die operativen gegenseitigen Abhängigkeiten zu erkennen und deren Risiken den strategischen Assets einer Organisation zuzuordnen.



### Highlights

Schaffen Sie standardisierte interne Kontrollmechanismen durch Nutzung branchenerfahrener Personen und bewährter Technologien.

Zum Erfolg benötigt das ERM-Framework die Nutzung von System- und Branchen-Know-how. Um standardisierte interne Kontrollmechanismen zu schaffen, müssen Unternehmen mit branchenerfahrenen Personen und bewährten Technologien arbeiten. Wie bereits erwähnt, ist der Versuch, für ein Unternehmen in einer assetintensiven Branche „ein System für alles“ zu schaffen, sehr riskant. Voneinander unabhängige Lösungen an der Peripherie – zum Beispiel Access-Datenbanken und Excel-Tabellen für bereichsspezifische Funktionen und Geschäftsprozesse – führen zu manuellen Eingabeprozessen, bei denen leicht Daten verloren gehen können und die die Fähigkeit eines Unternehmens beeinträchtigen, die Anforderungen an die Berichterstattung einzuhalten, ob es nun um SOX, die Occupational Safety and Health Administration (OSHA) oder die Environmental Protection Agency (EPA) geht.

Im Gegensatz dazu ermöglicht die Nutzung von Systemen, die die operativen Anforderungen erfüllen, einen höheren Verwendungsgrad der Systeme, die Standardisierung der Arbeitsprozesse im gesamten Unternehmen und eine präzisere Datenerfassung. Um das Leistungsvermögen eines Unternehmens ganz auszuschöpfen, sollten die speziell für Projektmanagement, Asset- und Service-Management sowie Finanzmanagement verwendeten Systeme integriert werden.

### **Nutzen Sie IBM Lösungen, um SOX im Einklang mit COSO und ERM gerecht zu werden**

IBM Maximo Asset Management und eine breite Palette branchenspezifischer IBM Maximo-Lösungen, die auf der Basis eines gemeinsamen Frameworks für Asset- und Service-Management entwickelt wurden, bilden ein starkes Fundament für die Bemühungen zur Einhaltung der SOX-Anforderungen. Darüber hinaus unterstützt Maximo-Software die Anstrengungen zur Erstellung eines COSO-Frameworks, das einer Vielzahl gesetzlicher Bestimmungen gerecht wird, und zur Implementierung eines Konzepts für ein Enterprise Risk Management.

Die folgende Tabelle zeigt, wie eine Organisation das Leistungsspektrum von Maximo Asset Management nutzen könnte, um bestimmte Anforderungen im Zusammenhang mit SOX zu erfüllen.

## Nehmen Sie die Herausforderungen an, die durch die Anforderungen von Sarbanes-Oxley an Unternehmen in assetintensiven Branchen entstehen

Seite 10

Abschnitt	Beschreibung	Relevante Leistungsmerkmale der Maximo-Software
301	<p>Definiert Regeln, denen zufolge die Mitglieder des Prüfungsausschusses vom Unternehmen unabhängig sein müssen.</p> <p>Fordert vom Unternehmen die Entwicklung eines Prozesses, der anonyme Beschwerden von Mitarbeitern an den Prüfungsausschuss bearbeitet.</p>	<p><b>Self-Service-Anforderungen</b> – Ermöglicht Endbenutzern die Meldung von Problemen und Beschwerden mithilfe einer intuitiven browserbasierten Schnittstelle. Anonyme Berichte über Probleme und Beschwerden werden mithilfe der Workflowfunktionalität in Maximo Asset Management adäquat weitergeleitet.</p> <p><b>E-Mail-Empfang</b> – Ermöglicht Benutzern ohne das Web das Senden von Problemberichten und Beschwerden über E-Mail-Systeme. Die Workflowfunktionen ermöglichen eine effizientere Verarbeitung eingehender E-Mail-Anforderungen und übertragen diese Anforderungen über den Self-Service-Prozess.</p>
302	<p>Definiert Regeln für CEOs und CFOs im Zusammenhang mit der Unterzeichnung von Finanzberichten. Mit der Unterzeichnung solcher Berichte übernehmen sie unter anderem folgende Pflichten:</p> <ul style="list-style-type: none"> <li>• Einrichtung und Aufrechterhaltung interner Kontrollmechanismen</li> <li>• Konzeption von Kontrollen, mit deren Hilfe die Führungskräfte des Unternehmens wesentliche Informationen erhalten</li> <li>• Prüfung der Wirksamkeit der Kontrollen innerhalb von 90 Tagen vor der Berichterstellung</li> </ul>	<p><b>Wesentliche Leistungsindikatoren (Key Performance Indicators, KPIs)</b> – Stellen besonders relevante Informationen in übersichtlichen Formaten bereit.</p> <p><b>Statusübersicht für Führungspersonal</b> – Ermöglicht einen schnellen Einblick in die Maximo-Software und stellt verlässliche Echtzeitinformationen bereit.</p> <p><b>Workflow</b> – Ermöglicht Unternehmen die Bereitstellung dieser Informationen in regelbasierter Form, sodass alle Geschäftsprozesse nach identischen Verfahren und in derselben automatisierten Form ablaufen können. Die Workflowfunktionen in Maximo bilden ein zuverlässiges und reproduzierbares Verfahren, Maximo-Geschäftsprozesse innerhalb einer Organisation zu definieren und weiterzuleiten. Sie fördern die unternehmensweite Konsistenz und stellen ein umfassendes Prüfprotokoll für alle Geschäftsprozesse bereit, die durch den Workflow von Maximo Asset Management aktiviert wurden.</p>
401	<p>Legt fest, dass die Finanzberichte in Übereinstimmung mit den in den USA geltenden Grundsätzen ordnungsgemäßer Buchführung und Bilanzierung (Generally Accepted Accounting Principles, GAAP) erarbeitet werden müssen.</p> <p>Die Unternehmen müssen alle bilanzneutralen Transaktionen offenlegen und Pro-forma Kennziffern mit GAAP-Kennziffern abstimmen.</p>	<p><b>Produkt zur ERP-Integration</b> – Bietet Integration in führende ERP-Systeme wie SAP und Oracle in einem Paket. Da die Integration in Paketform erfolgt, sind damit weniger Risiken verbunden als in isolierter Form. Die Berührungspunkte und Standards bei der Integration sind mit denen identisch, die für die von ERPs bereitgestellten Bolt-on-Komponenten des Enterprise Asset Managements (EAM) verwendet werden. Durch Nutzung der Integrationspunkte können innerhalb von Auftragsmanagement- und Asset-Management-Systemen wie Maximo erweiterte Wartungsprozesse verwendet werden.</p>
404	<p>Überträgt dem Management die Verantwortlichkeit für die Schaffung und Aufrechterhaltung interner Kontrollmechanismen und Verfahren für die Finanzberichterstattung.</p> <p>Das Management muss die Wirksamkeit der internen Kontrollmechanismen bewerten und einen Bericht über die Kontrollen erstellen.</p> <p>Der Prüfer muss einen Bericht über die Bewertung der internen Kontrollmechanismen durch das Management erstellen.</p>	<p><b>Workflow</b> – Siehe Beschreibung für Abschnitt 302.</p> <p><b>Signatur- und rollenbasierte Sicherheit</b> – Steuert den Zugriff auf bestimmte Maximo-Funktionen und sorgt damit für eine zusätzliche Stufe der Sicherheitssteuerung. Mithilfe der signaturbasierten Sicherheitsfunktion können Organisationen fordern, dass die Person, die einen Datensatz speichert, einen Datensatz ändert oder auf einen bestimmten Menüpunkt zugreift, mit der Person identisch ist, die im System angemeldet ist.</p> <p><b>Datenbanksicherheit</b> – Ermöglicht dem Maximo-Systemadministrator, Gruppen SQL-Berechtigungen (SQL = Structured Query Language) für Maximo-Datenbanktabellen zu erteilen oder zu verweigern. Die Zuweisung dieser Berechtigungen steuert den Zugriff der Benutzer auf die Tabellen über einen SQL-Editor, das Berichtsausgabeprogramm Actuate und weitere Anwendungen außerhalb von Maximo.</p> <p><b>Anmeldungsverfolgung</b> – Ermöglicht Organisationen, die Kontrolle über Anmeldeversuche zu übernehmen, Anmeldeversuche zu verfolgen, Benutzer nach einer festgelegten Anzahl aufeinanderfolgender erfolgloser Anmeldeversuche an der Anmeldung zu hindern und den aktuellen Status von Benutzern anzuzeigen.</p> <p><b>Elektronische Prüfsätze</b> – Erstellen in dem Moment, wenn Benutzer die Datensätze in der Datenbank speichern, eine Kopie von Änderungen an Maximo-Datenbanksätzen. Wird der Datensatz anschließend gelöscht, befindet sich eine Kopie der Änderung immer noch im elektronischen Prüfsatz. Damit entsteht ein überprüfbares Protokoll.</p>
409	<p>Ein Unternehmen muss unverzüglich – der Öffentlichkeit gegenüber auf leicht verständliche Art – berichten, sobald es Kenntnis von wesentlichen Änderungen der finanziellen Situation oder der betrieblichen Abläufe erlangt.</p>	<p><b>Workflow</b> – Siehe Beschreibung für Abschnitt 302.</p>

#### **Schlussfolgerung**

Bei ihrem Versuch, die SOX-Vorschriften einzuhalten, sind die Unternehmen von einer Mischung aus Aufregung, Angst und Unsicherheit umgeben. Es bedarf eines enormen Personalaufwandes, die richtigen Daten zusammenzustellen und die Verfahren zu dokumentieren. Aber mit geeigneten Systemen und Prozessen kann ein Unternehmen Größenvorteile erlangen, was gleichzeitig den Übergang vereinfacht und die Effektivität erhöht.

Obwohl bereits ein ERP-System ein Unternehmen bei seinen Compliancemaßnahmen unterstützt, ermöglichen erst professionelle Systeme für Asset- und Service-Management oder Projektmanagement und weitere Systeme, die in assetintensiven Branchen benötigt werden, den notwendigen Einblick in den Betriebsablauf des Unternehmens. Ein auf dem COSO-Framework basierendes System kann das „fehlende Bindeglied“ sein, das in Echtzeit operative Daten beschafft und Prozesse dokumentiert, die Ihr SOX-Compliance-Programm informieren können.

Dieses Konzept kann auch als Katalysator dienen, der ein ganzes Unternehmen in ein Enterprise Risk Management-Programm hinüberführt. Nach erfolgreicher Implementierung kann ein ERM-Programm Wettbewerbsvorteile generieren und eine Organisation in die Lage versetzen, vorhandene Compliancemaßnahmen besser umzusetzen und neue Maßnahmen einzuführen. In vielen Fällen kann sich dadurch eine Organisation in höherem Tempo und mit geringerem Aufwand zukunftsorientiert verändern.

#### **Weitere Informationen**

Wenn Sie darüber erfahren möchten, wie IBM Maximo Asset Management und branchenspezifische Asset- und Service-Management-Lösungen von IBM Ihnen helfen, heute die SOX-Vorschriften einzuhalten und in Zukunft weitere Anforderungen zu erfüllen, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

[www.mro.com](http://www.mro.com)



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**

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation.

Tivoli ist eine Marke von IBM Corporation in den USA und/oder anderen Ländern

Microsoft ist eine Marke von Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle über Inhalt und Auslegung aller relevanten Gesetze und Bestimmungen beraten zu lassen, die das Unternehmen des Kunden betreffen, sowie über alle Maßnahmen, die der Kunde ergreifen muss, um diese Gesetze einzuhalten. IBM erteilt keine Rechtsberatung und übernimmt keine Gewährleistung, dass seine Produkte oder Services die Einhaltung gesetzlicher Vorschriften sicherstellen.

<sup>1</sup> Helen Shaw. „The Trouble with COSO.“ *CFO Magazine*. 15. März 2006. [www.cfo.com/article.cfm/5598405](http://www.cfo.com/article.cfm/5598405).

<sup>2</sup> Protiviti, Inc. „Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements – Frequently Asked Questions Regarding Section 404.“ 2003. Verfügbar unter [www.protiviti.com/?pgTitle=Sarbanes-Oxley%20Section%20404%20FAQs](http://www.protiviti.com/?pgTitle=Sarbanes-Oxley%20Section%20404%20FAQs).

<sup>3</sup> David Wood und Scott Randall. „Implementing ERM requires integrated approach.“ *Oil & Gas Journal*. 15. November 2004.

© Copyright IBM Corporation 2007  
Alle Rechte vorbehalten.

**TAKE BACK CONTROL WITH** 