Sarbanes-Oxley Act bald auch für Europa relevant

Autoren: Sahin Demir und Kersten Mebus, ORACLE Deutschland GmbH

Finanzskandale in den USA haben die Notwendigkeit international einheitlicher Regelungen (Compliance) bei der Abschlussprüfung deutlich gemacht. Der Sarbanes-Oxley Act (SOX), der nach den Bilanzskandalen verabschiedet wurde, hat nicht nur Auswirkungen auf die Corporate Governance amerikanischer Unternehmen, sondern auch auf ausländische Unternehmen, die an der US-Börse notiert sind.

Inzwischen hat auch die Europäische Union einen SOX-Pendant, die 8. EU-Richtlinie, verabschiedet. Ab Mitte 2008 müssen sich somit auch Unternehmen in Europa mit den SOX-Grundsätzen auseinandersetzen. Eine Auswahl an Methoden zur Einhaltung der Compliance bieten das COSO- und CobiT-Modell, wobei das Oracle Identity- und Access-Managementsystem (IAM) alle definierten Regeln zur Einhaltung regulatorischer Anforderungen überwacht.

Sarbanes-Oxley Act

Der US-Kongress verabschiedete am 30. Juli 2002 den Sarbanes-Oxley Act of 2002, um in Zukunft gegen gefälschte Bilanzen und mangelnde interne Kontrolle stärker vorgehen zu können. Primäres Ziel ist es, die Aufrechterhaltung des regulären Geschäftslebens und den Fortbestand des Unternehmens zu gewährleisten, um Bilanzmanipulationen zu verhindern und somit die Anleger und Investoren zu schützen, indem sie künftig besser über die tatsächliche Unternehmenslage informiert sind. Dabei fordert das Gesetz vor allem eine verbesserte Prüfung der Jahresabschlüsse und der Finanzdaten, die Ausgestaltung der internen Kontrollsysteme und verlangt hierüber eine ausführliche Berichterstattung.

Weiterhin verpflichtet dieses Gesetz CEOs und CFOs, die Richtigkeit der finanziellen Berichterstattung mit ihren Unterschriften eidesstattlich zu beglaubigen. Das Management muss eine Beurteilung der Wirksamkeit der internen Kontrolle über die finanzielle Berichterstattung vornehmen. Da das Management und die Revisionsstelle einen Bericht über die Wirksamkeit des internen Kontrollsystems erstellen müssen, ist dies korrekt zu dokumentieren und für Drittpersonen nachvollziehbar sein. Mit dem Sarbanes-Oxley Act wird im Bericht auf die Schwachstellen der internen Kontrolle öffentlich hingewiesen.

Das interne Kontrollsystem dient zur Verbesserung der internen und externen Unternehmensüberwachung sowie der Erhöhung der Unternehmenspublizität, womit die Unternehmensleitung nun verpflichtet ist, Überwachungs- und Kontrollmaßnahmen einzuführen und für deren Richtigkeit und Ordnungsmäßigkeit verantwortlich ist. Dabei handelt es sich um nicht zu vernachlässigende Herausforderungen. Das interne Kontrollsystem wird immer mehr zu einem wichtigen Bestandteil der Corporate Governance, wobei sie als Führungsinstrument dient, aber auch eine Überwachungsfunktion einnimmt und damit im gesamten Unternehmen verwurzelt ist.

Corporate Governance

Man bezeichnet Corporate Governance als die Organisation der Leitung und der Kontrolle eines Unternehmens, die die Macht- und Einkommensverteilung zwischen den unterschiedlichen Interessengruppen, dem Management eines Unternehmens, Aufsichtsrats- beziehungsweise Verwaltungsratsmitgliedern, Aktionären und anderen Stakeholdern ordnet. Ziel der Corporate Governance ist es, die Interessen der Gruppen zu schützen, die vom Erfolg eines Unternehmens profitieren oder bei Misserfolg Verluste erleiden. Demnach wird Corporate Governance als eine verantwortliche und auf langfristige Wertschöpfung zielende Unternehmensführung sowie Unternehmenskontrolle verstanden. Die erste zentrale Aufgabe der Corporate Governance besteht darin, die wirtschaftliche Effizienz und das Wachstum sowie die Stärkung des Anlegervertrauens sicherzustellen. Die zweite zentrale Aufgabe der Corporate Governance ist es, die Verteilung der Verfügungsrechte auf die verschiedenen Interessengruppen des Unternehmens festzulegen, für eine geeignete Verteilung des Faktoreinkommens und des erwirtschafteten Überschusses auf die Anteilseigner, die Fremdkapitalgeber, die Mitarbeiter und die Manager eines Unternehmens zu sorgen.

Mit dem Sarbanes-Oxley Act und den umfangreichen durch ihn veranlassten Ausführungsbestimmungen der zuständigen Institutionen werden tief greifende Veränderungen im Bereich der Corporate Governance und der Abschlussprüfung sowie der Regulierung des Wirtschaftsprüferberufsstands vorgenommen, die die Anforderungen und die Aufgaben der Wirtschaftsprüfer immens verschärfen.

Neben dieser vermehrten Auseinandersetzung mit der internen Steuerung und Kontrolle als adäquates Mittel gegen Finanzskandale ist der Informationstechnologie ein besonderes Augenmerk zu schenken. Bereits in der Vergangenheit gelang dieser ein Fortschritt nach dem anderen – auch in der Zukunft ist damit sicherlich weiter zu rechnen. Die Informationstechnologie hat sich dadurch längst eine zentrale Stellung in fast jedem Unternehmen erkämpft und ist somit auch in der Umsetzung des internen Kontrollsystems nicht mehr außer Acht zu lassen.

Die Praxis bietet eine Auswahl standardisierter Modelle, die den Aufbau und den Betrieb eines internen Kontrollsystems unterstützen. Die bekanntesten Modelle sind für den IT-spezifischen Ansatz das Control Objektives for Information and related Technology-Framework (CobiT), für den generellen Ansatz das von der amerikanischen Börsenaufsichtsbehörde SEC (Security and Exchange Commission) anerkannte interne Steuerungs- und Kontrollsystem COSO (Committee of Sponsoring Organizations of the Treadway Commission). COSO verfolgt, neben einer zuverlässigen und integren finanziellen Berichterstattung, die Einhaltung der anwendbaren Normen (Compliance) sowie die Effektivität und Effizienz der operativen Tätigkeiten. Das COSO-Rahmenwerk berücksichtigt zwar alle wesentlichen Elemente der internen Kontrolle und wird von der SEC empfohlen, richtet sich aber nicht nach der IT-Governance, sondern nach jener der Corporate Governance. Folglich sollte jedes Unternehmen seine Anforderungen an die interne Kontrolle erörtern und ein geeignetes Rahmenwerk auswählen.

Sarbanes-Oxley Act und die EU

Große amerikanische Konzerne mussten die Section 404 des Sarbanes-Oxley Acts ab dem Geschäftsjahr, das am oder nach dem 15. November 2004 endete, erfüllen. Kleine US-Firmen und ausländische, an US-Börsen notierte Unternehmen müssen die Section 404-Anforderungen erst für jene Geschäftsjahre erfüllen, die am oder nach dem 15. Juli 2006 endeten. Die Implementierung eines internen Kontrollsystems der finanziellen Berichterstattung nach Section 404 des Sarbanes-Oxley Acts stellt in diesem Jahr, insbesondere für nicht US-Unternehmen, eine neue Herausforderung dar, da diese erstmals per 31. Dezember 2006 die Existenz eines internen Kontrollsystems der finanziellen Berichterstattung nach Section 404 des Sarbanes-Oxley Acts vorweisen müssen.

Innerhalb der EU gilt bereits seit dem 24. Oktober 1995 die EU-Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU DPD) als weitere EU-Richtlinie zum Datenschutz im EU-GMP-Leitfaden zur Sicherheit und zum Schutz computergestützter Systeme. Darüber hinaus sind international agierende Unternehmen gezwungen, die Regularien der unterschiedlichen Länder einzuhalten, in denen Sie aktiv sind. Auch mit der 8. EU-Richtlinie steht 2008 ein weiteres Gesetz parat, das im europäischen Raum zu einer Verschärfung der gesetzlichen Anforderungen an Informationssicherheit sowie der Haftungsbedingungen beitragen wird. Abzuwarten bleibt, ob eine ähnlich starke Diskussion, wie sie der Sarbanes-Oxley Act ausgelöst hat, auch hierzulande entstehen wird. Somit ist eine frühzeitige Betrachtung des Themas Compliance für deutsche Unternehmen empfehlenswert.

Compliance

Eine allgemeingültige und einheitliche Definition für Compliance gibt es nicht. Der Begriff Compliance bezeichnet in Zusammenhang mit dem Sarbanes-Oxley Act das Einhalten von gesetzlichen Bestimmungen und Regeln, von denen Organisationsmitglieder, Unternehmen und seine Mitarbeiter betroffen sind. Compliance ermöglicht die Revisionssicherheit, wobei Identity- und Access-Management-Systeme wie zum Beispiel von Oracle als Grundlage für das Auditing von IT-Prozessen dienen – und dadurch den revisionssicheren Nachweis ausreichender Risikovorsorge ermöglichen. Compliance ist ein ständiger Prozess. Diesen gilt es zu organisieren und zu etablieren sowie kontinuierliche Audits durchzuführen, um sicherzustellen, dass ihre Compliance-Maßnahmen wirksam sind und die Auflagen an das Berichtswesen erfüllt werden. So müssen erst einmal relevante Regelungen erkannt und gewichtet, Zuständigkeiten geregelt und Dokumentationsstrukturen gefunden werden.

Das Einhalten von internen Vorgaben, globalen Regeln und Standards etc. ist heute für Unternehmen eine Grundvoraussetzung zur effektiven Risiko-Minimierung, die mit einem Verlust der öffentlichen Wertschätzung des Unternehmens in Verbindung steht. Die Nichteinhaltung dieser Anforderungen ist daher selbst ein Risiko für Unternehmen und betrifft zahlreiche Unternehmensprozesse.

Es geht aber nicht nur um die Befolgung von aktuell geltenden Gesetzen, sondern auch um die bewusste und gewollte Einhaltung von Regeln. Trotz der bestehenden Herausforderungen ist das Identity- und Access-Management die wesentliche Basis für die Compliance. Die automatisierte Administration und der rollenbasierte Zugriff des Identity- und Access-Management-Systems erleichtern die Einhaltung von Regeln. Identity- und Access-Management wird für spezifische Compliance-Anforderungen benötigt und ist ohnehin erforderlich, denn andernfalls sind IT-Umgebungen nicht effizient zu administrieren. Zugleich müssen sie in der Lage sein, jederzeit den Nachweis ausreichender Risikovorsorge sowie rechtzeitiger und richtiger Reaktion auf Unregelmäßigkeiten im System zu führen.

Oracle Identity und Access Management Suite

Die Oracle Identity und Access Management Suite (IAM Suite) bietet eine umfassende Lösung für Compliance-Anforderungen. Sie beinhaltet folgende Komponenten:

- **Oracle Virtual Directory**
  Das Oracle Virtual Directory sorgt für die zuverlässige Kontrolle von Applikationen, Verfahren und Prozessen ohne redundante Haltung von Daten und verbindet Identitätsdaten aus Verzeichnisdiensten, Datenbanken und Web-Services in Echtzeit.
- **Oracle Internet Directory**
  Das Internet Directory ist ein klassischer LDAP v3 Directory Server, der auch als Meta-Directory zur Verfügung stehen kann.
- **Oracle Identity Federation**
  Federated Identity Management beschäftigt sich mit einem unternehmensübergreifenden Single Sign-On und basiert auf geschäftlichen sowie technischen Übereinkünften und Regeln. Technische Voraussetzungen sind Single Sign-On, Zugangskontrolle, Single Sign-Off, eine Identitätsüberprüfung bei den Partnern, der Austausch von Benutzerdaten, ein Identity Lifecycle Management, die Bereitstellung von Anwenderdaten, eine sichere Infrastruktur sowie ein gesicherter Zugriff auf Ressourcen der Geschäftspartner.

- **Oracle Identity Manager**
  Der Oracle Identity Manager (OIM) ermöglicht das unternehmensweite Management von Zugriffserkennungen und Rechten über alle Bereiche des Identity Management hinweg. Er bietet vordefinierte Funktionalitäten zum Administrieren von Benutzern, Gruppen und Organisationseinheiten auf Attributebene an. Der OIM liefert eine delegierte Administration und eine integrierte Workflow-Engine für das Management von Benutzern, Gruppen und Organisationen. Über die anpassbare Workflow-Engine können Benutzer-, Gruppen- oder Organisationsprozesse – automatisiert über Regeln (Policies) und Genehmigungen – ausgeführt werden.
  Weitere Funktionen wie der Identitätsabgleich mit anderen Ressourcen/Systemen (Provisioning/Reconcilation), Auditing, Attestierungsprozesse, Role Based Access Control (RBAC), Passwort-Management und ein dynamisches Gruppenmanagement vervollständigen das Portfolio des Oracle Identity Managementsystems.
- **Oracle Access Manager**
  Die Oracle Access-Management-Lösung ist die führende Lösung für ein zentralisiertes, unternehmensweites Identity-, Zugangs- und Rechte-Management regelt Art und Tiefe des Zugriffs.

Compliance-Anforderungen und die IAM Suite

Über die IAM Suite können Compliance-Anforderungen umgesetzt werden, die in vier Schritten zusammengefasst sind:

1. Definition von Richtlinien und Prozessen zur Einhaltung regulatorischer Anforderungen.
2. Einführung von Vorsorgemaßnahmen bei Regelverstößen, um ein unerwünschtes Verhalten oder Ereignis zu verhindern, zum Beispiel die Zuordnung von zwei Berechtigungen, die sich ausschließen, sodass ein Benutzer nicht gleichzeitig Besteller und Genehmigender sein kann.
3. Einführung einer Regelüberwachung, um Regelverstöße aufzudecken, damit die Mitarbeiter Korrekturmaßnahmen einleiten können, zum Beispiel die automatisierte Eskalation eines verzögerten, internen Audits, das an einen anderen zuständigen Mitarbeiter weitergeleitet wird.
4. Validierung der Kontrollen auf Effektivität der Richtlinien und Maßnahmen.

Die nachfolgende Auflistung beschreibt im Einzelnen die Umsetzungsmöglichkeiten innerhalb der IAM Suite, bezogen auf die genannten vier Schritte.

Richtlinien und Prozess-Definitionen

- *Provisioningregeln*
  Mit der Definition rollenbasierter Regeln/Prozesse wird die Zuordnung von Anwendungen einschließlich deren Zugriffsberechtigungen (entitlements) bestimmt, die ein Benutzer erhält.
- *Ablehnungsregeln*
  Durch diesen Prozess (Teil der Provisioningregeln) wird bestimmt, welche Ressourcen und Anwendungen einem Anwender oder einer Gruppe von Anwendern nicht zugeordnet werden sollen.

- *Zugriffsregeln*
  Rollenbasierte Regeln, die den Zugriff auf Ressourcen festlegen
- *Rollenbasierte Zugriffskontrolle/Role Based Access Control (RBAC)*
  Definition von Provisioning-Berechtigungen und Zugriffsrechten in Form von Rollen und zusätzlichen Gruppenzugehörigkeitsregelungen, die auf Rollen abgebildet werden
- *Regelhistorie*
  Bereitstellung der gesamten Regelhistorie, um es Auditoren und Administratoren zu erleichtern, die Definition der Regeln zu finden, geordnet nach der Tagesvergabe
- *Genehmigungsworkflow*
  Anfrage und Genehmigung der Zugriffe auf Anwendungen oder Berechtigungen
- *Genehmigungsregeln*
  Auflistung der Genehmigenden jeder Ressource einer Provisioning-Anfrage sowie die Verwendung von Rollen innerhalb der Genehmigungsregeln
- *Administrative Regeln*
  Definition rollenbasierter Regeln zur Administration verschiedener Identitätsattribute, zum Beispiel Rollen, Organisation und Ressourcen
- *Segregation of Duty (SoD) Regeln*
  Regel- und rollenbasierte Trennung von Aufgaben zur Vermeidung einer widersprüchlichen Zuordnung von Rollen, Ressourcen oder Berechtigungen innerhalb einer Ressource

Vorsorgemaßnahme für Regelverstöße

- *Authoritative Source (berufene Quelle)*
  Bestimmung einer Menge von Ressourcen oder Anwendungen, die als berufene Quelle für den Provisioning-Prozess definiert ist
- *Authoritative Reconciliation*
  Abgleich der Identitätsdaten mit der Authoritative Source
- *Benutzer "On-Boarding" Workflow*
  Definition automatisierter Workflows (mit oder ohne Genehmigung) für die Einrichtung von Benutzerkonten in den verschiedensten Applikationen auf Basis von Provisioningregeln
- *Benutzer "Transfer" Workflow*
  Definition automatisierter Workflows (mit oder ohne Genehmigung) für die Anpassung von Identitätsdaten in den verschiedenen Applikationen, sofern eine Änderung vorgenommen wurde
- *Benutzer "Termination" Workflow*
  Entzug (Deprovisioning) der Benutzerkonten in Anwendungen bei Beendigung des Beschäftigungsverhältnisses
- *Passwort-Synchronisation*
  Möglichkeit zur Synchronisierung von Benutzerpasswörtern in allen Anwendungen, wodurch weniger, von den Benutzern zu pflegende Passwörter benötigt werden
- *Regelergänzungen*
  Abgleich der Benutzerkonten in verschiedenen Anwendungen bei Änderungen der Bereitstellungsregeln
- *Web Single Sign-On*
- *LDAP Firewall*
  Das IAM-System sollte in der Lage sein, virtuelle Zugriffe auf unterschiedliche Datenquellen einheitlich zu kontrollieren und diese DMZ-fähig zur Verfügung zu stellen
- *Verzeichnis-Aggregation*
  Virtuelle Gesamtsicht auf Identitätsdaten, die in unterschiedlichen Datenspeichern liegen, ohne die Daten redundant abspeichern zu müssen (keine Datenkonsolidierung notwendig)

Regelüberwachung & Korrekturmaßnahmen

- *Fehlererkennung im Reconciliation-Prozess*
  Das IAM-System ist in der Lage, Informationsdaten einer Identität auf Basis fein granulierter Berechtigungen in allen Ressourcen abzugleichen einschließlich einer Generierung von Fehlerreports bei Abweichungen der Regeldefinitionen in den Berechtigungen
- *Verwaiste Kontenerkennung*
  Erkennung speziell eingerichteter Benutzer-Accounts, die gegen die dokumentierten Provisioningregeln verstoßen
- *Berechtigungsfehlererkennung*
  Erkennung von explizit gewährten Berechtigungen in verschiedenen Anwendungen, die gegen die dokumentierten Provisioningregeln verstoßen
- *Fehlertracking*
  Speicherung der Statusänderung von Fehlern sowie deren Zurücksetzung
- *Beglaubigungskonfiguration (Attestierung)*
  Möglichkeit periodischer Attestierung von Benutzerberechtigungen in verschiedenen Anwendungen
- *Beglaubigungsablauf*
  Festlegen der Häufigkeit des Attestierungsprozesses
- *Beglaubigung der fein granulierten Berechtigungen*
  Attestierung der fein granulierten Benutzerberechtigungen (verschiedene Rollen, Verantwortlichkeiten, Profile, Privilegien sowie andere anwendungsfunktionale Sicherheitsaspekte) in allen Ressourcen und Anwendungen
- *Beglaubigungsbereich*
  Bestimmung von Filterkriterien für Benutzer, Ressourcen und Berechtigungen im Attestierungsprozess
- *Beglaubigungsdelegation*
  Die zu beglaubigenden Daten können an andere Benutzer zur Überprüfung weitergereicht werden. Zudem besteht die Möglichkeit, Prüfungsanfragen von nicht berechtigten Prüfern zu löschen und diese ausgewiesenen Prüfern zuzuweisen
- *Historische Momentaufnahme*
  Über Snapshots (Speicherauszug) werden Benutzerattribute, Genehmigungen, Workflows, Regelhistorien sowie prüfungsrelevante Daten für Audit-Zwecke zeitbezogen gespeichert
- *Einstellbare Auditingregeln*
  Zu konfigurierende Regeln, die das Auditing einzelner Ereignisse festlegen, zum Beispiel Identitätsadministration, Provisioning, Genehmigungen, Webzugriff etc.
- *Zentralisiertes Auditing*
  Alle Auditinginformationen für Identitätsadministration, Genehmigungen, Bereitstellung und Web-Zu-

griffsereignisse werden in einem zentralen Datenbank-Repository gespeichert
- *Remediation (Korrektur)*
  Durchführung kontextbezogener Korrekturen aus der Regelüberwachung, zum Beispiel Deprovisioning von Benutzern als Ergebnis des Attestierungsprozesses und Fehlerreports

Validierung der Kontrollen

- *Reporting von Zugriffsrechten*
  Berichterstellung über die derzeitigen (wer hat welche) und historischen (wer hatte welche) Zugriffsrechte. Im Zugriffsfall auf Web-Ressourcen sind Reports unabdingbar, zum Beispiel: Wer hat wann auf welche Ressource zugegriffen beziehungsweise wer hat versucht, auf welche Ressource zuzugreifen
- *Fehler-Reporting*
  Berichterstattung über die derzeitigen und historischen verwaisten Accounts sowie über Verletzungen, die in den Benutzerberechtigungen aufgetreten sind
- *Bereitstellung Kontext-Reporting*
  Berichterstellung über Provisioning von Benutzerberechtigungen, zum Beispiel Provisioningregeln, Regeländerungen, Genehmigungen, Datenabgleiche (Reconciliation) etc.
- *Remediation-Reporting*
  Berichterstellung über aktuelle und historische Korrekturaktivitäten
- *Änderungs-Reporting*
  Berichte über alle Veränderungen der Identitätsdaten einschließlich der Regeldefinition, Benutzereigenschaften, Rollendefinitionen, Rollenzugehörigkeitsregeln, Organisationseigenschaften, übertragene administrative und freigegebene Regeln, Genehmigungsworkflows etc.
- *Dashboard zur Attestierung*
  Anzeige aller historischen und aktuellen Beglaubigungsanfragen sowie deren Ergebnisse in einem Dashboard
- *Compliance-Dashboard*
  Dieses Dashboard gibt einen Einblick über Fehler, Korrekturen und andere relevante Metriken

SOX und IAM Suite

Auf Basis der genannten Umsetzungsmöglichkeiten erfüllt das Oracle Identity und Access Management-Systems die nachfolgenden Compliance-Anforderungen der Section 302 (Beglaubigung der Offenlegung interner Kontrollmaßnahmen) und Section 404 (Einrichtung und Durchführung angemessener Steuerungs- und Kontrollaktivitäten für die Finanzberichterstattung) des Sarbanes-Oxley Acts. In diesen beiden Sektionen sind die relevanten Informationen im Bereich Sicherheitsanforderungen angesiedelt (siehe Tabelle).

SOX Abschnitte	Regeln	Vorsorgemaßnahmen	Regelüberwachung
302	Provisioning-regeln Zugriffs-regeln	Mitarbeiter-neueinstellung (On-Boarding) Benutzer Transfer und Benutzerterminierung Regel-ergänzungen	Attestierungs-historie Regelhistorie Berechtigungs-fehlererkennung Historische Moment-aufnahme Überwachung von Fehler-erkennung und Remediation-Aktivitäten
404	SoD-Regeln		Reports & Dashboards Attestierung Verwaiste Konten-Erkennung

Fazit

Im Kern fordern alle Gesetze die Einführung eines unternehmensweiten Risiko-Managements und eines internen Kontrollsystems. Da heutzutage Informationssysteme fast alle Geschäftsprozesse unterstützen, schließt das Risikomanagement auch die IT und deren Infrastruktur mit ein. Häufig sind Informationen und Daten – im Falle des Sarbanes-Oxley Acts vor allem Finanzdaten – schutzbedürftige Vermögenswerte des Unternehmens und somit in die geforderte Risikoanalyse eingeschlossen. Viele dieser Richtlinien haben auch gemeinsame Komponenten, zum Beispiel der Umgang mit elektronischen Daten, die Pflicht zur Verifizierung der Identität, zentrale Berechtigungskonzepte für den Zugriff auf Informationen oder eindeutige Reports für das Rechnungswesen und unveränderbare Log-Dateien für die Revision sowie die Festlegung ihrer Archivierung. Die nachweisbare Einhaltung der einschlägigen nationalen und internationalen Bestimmungen wird so zum wichtigsten Treiber für Identity- und Access-Management-Systeme. Das Oracle IAM-System ermöglicht den revisionssicheren Nachweis der ausreichenden Risikovorsorge und dient als Grundlage für ein professionelles Auditing von IT-Prozessen. Es stellt somit die Basis für Richtlinien zur Steuerung und für Auditing-Lösungen zur Überwachung des Handelns von Benutzern dar.

Kontakte:
Sahin Demir
info@sahindemir.de
Kersten Mebus
kersten.mebus@oracle.com

Neu:

Weitere Informationen zu den Themen der DOAG *News* finden Sie unter
http://email.doag.org/