

Compliance Monitoring in SAP-Systemen

Neue Regulatoren und Anforderungen unterschiedlicher Anspruchsgruppen haben die Notwendigkeit einer unternehmensweiten Beschäftigung mit den Themen Governance, Risk und Compliance (GRC) erhöht. Um in diesen Bereichen effizient sein zu können, setzen sich Unternehmen vermehrt das Ziel, GRC-Aktivitäten weg von periodisch wiederkehrenden Aufgaben hin zu einem strategisch ausgerichteten kontinuierlichen Management zu überführen. Sie möchten damit eine starke Basis für den Geschäftserfolg legen. Jörg Altmeier



Jörg Altmeier
Diplom-Kaufmann
(Uni Saarbrücken), CISA,
Management Consultant,
Lehrbeauftragter, Autor
zahlreicher Fachpublikationen.
joerg.altmeier@wikima4.com
www.wikima4.com
www.mesaforte.com

Die Implementierung einer GRC-Strategie ist ähnlich wie das Erlernen, ein Fahrzeug zu steuern. Es ist schwierig und nimmt lange Zeit in Anspruch, bevor man die Strasse im Griff hat. Schalten und kuppeln, parkieren, die Bedeutung der Strassenschilder kennen, den Bremsweg beurteilen - die Liste ist lang und man muss jeden dieser Bereiche beherrschen. Aus diesem Grunde würde wohl jeder Fahrschüler eher mit einem kleinen wendigen Auto starten, anstatt mit einem grossen, leistungsstarken und schweren. Auch würde sich ein unerfahrener Fahrer (und vielleicht erfolgreicher zukünftiger Risikomanager) eher ein günstigeres Fahrzeug zulegen, als ein luxuriöses und teures. Erst nachdem er Erfahrung und Vertrauen erlangt hat, wenn er gelernt hat, seine eigenen Fehler zu korrigieren, wird er sich ein grösseres und anspruchsvolleres Fahrzeug leisten. Genauso logisch sollte es sein, wenn ein Unternehmen in die GRC-Welt als Prüfkandidat einsteigen möchte, um den Anforderungen einer "Prüfung" in Governance und Compliance bestehen zu können.

Ausgehend von den tatsächlichen Realitäten und Herausforderungen von GRC ist es nötig, auch für das Umfeld der allgegenwärtigen SAP-Systeme geeignete Tools zu deren Monitoring einsetzen zu können. Basierend auf den drei Achsen System-Konfiguration, Compliance und Incident sollte es möglich sein, automatisierte Kontrollen und Systemprüfungen durchzuführen (siehe Grafik: Security Monitoring am Beispiel des Tools „mesaforte“).

SAP Compliance Monitoring in a Mouse click

Was sollte ein solches Werkzeug zum SAP Compliance Monitoring alles

bieten? Im Idealfall ist es ohne grossen Implementations-Aufwand einsatzfähig. Ein Benutzer kann mit möglichst einem Mausklick eine Überprüfung starten und hat innerhalb weniger Augenblicke eine vollständige Diagnose vor Augen.

Als interne Kontrollen stehen die Bereiche Profil-Parameter, verbotene Passwörter, Gewaltentrennung, Audit Log, Rollen und Benutzern zugeordnete kritische Berechtigungs-

Objekte sowie die Benutzung von Notfall-Usern im Zentrum der Betrachtungen. Dazu wird ein Satz vordefinierter Regeln, die die auf externe Vorgaben abgestimmte gültige Unternehmens-Policy widerspiegeln, mit den

tatsächlich vorgefundenen Werten verglichen. Als Ergebnis erhält der Benutzer eine Auflistung der Abweichungen zwischen erwartetem Soll- und vorgefundenen Istwerten, dargestellt in zielgruppengerecht ausgeprägten Berichten und angereichert mit Empfehlungen, wie bei Abweichungen zu reagieren ist. Eingebundene Incident-Management-Mechanismen erlauben die Zuordnung der erkannten Abweichungen zu verantwortlichen Personen. Ebenfalls wichtig sind Funktionalitäten zur Historisierung und Trendanalyse, mit denen die Entwicklung des Reifegrads eines SAP-Systems verfolgt werden kann sowie die Visualisierung der bestehenden Sicherheitsorganisation des Unternehmens. Dadurch ist gewährleistet, dass im Falle von Fragestellungen oder Eskalationen rasch die richtigen Ansprechpartner gefunden werden.

A fool with a tool remains to be a fool

Unternehmen, die durch eine Implementierung von Monitoring-Werkzeugen einen höheren Level von Compliance und Reife erreichen möchten, sollten beachten, dass die Anschaffung eines solchen Werkzeugs, und sei es noch so kostspielig, nicht bedeutet, de facto

„Ein Benutzer kann mit möglichst einem Mausklick eine Überprüfung starten und hat innerhalb weniger Augenblicke eine vollständige Diagnose.“

compliant zu sein. Es spielt keine Rolle, welches Fahrzeug man sich anschafft – es wird einen nicht an den gewünschten Ort fahren, wenn man nicht weiss, wie es zu benutzen ist und wie man seine Pferdestärken sinnvoll einsetzt. Die den Monitoring-Werkzeugen hinterlegten Regeln sind wichtiger als die Lösung, die ja nur eine automatisierte Abarbeitung derselben darstellt. Regeln müssen auf gültige Gesetze, Branchen, Landes-Spezifika, kulturelle Begebenheiten und allgemein akzeptierte Best Practises abgestimmt sein. Was in einem Land als legal gilt, kann für ein anderes Land vollständig anders sein. In manchen Ländern wird die Einhaltung von Datenschutzgesetzen eine gewichtigere Rolle spielen als in anderen, eben weil ihre Nicht-Einhaltung mit hohen Strafen geahndet wird. In Unternehmen, die an einer US-Börse gelistet sind und damit dem Sarbanes-Oxley-Act unterliegen, wird der primäre Fokus auf der Sicherstellung der Gewaltentrennung liegen. Wieder andere werden Prüfmechanismen implementieren, die die Einhaltung der Vorgaben der US Food and Drug Administration (FDA) sicherstellen.

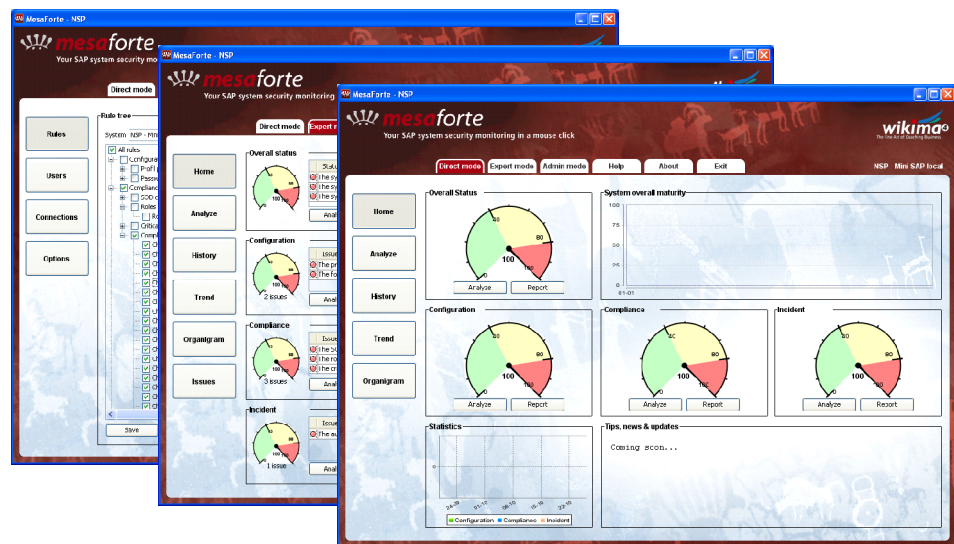
Unternehmen, die die Compliance ihrer SAP-Systeme überwachen möchten, benötigen also einen Satz vordefinierter Best-Practise-Regeln, die an die jeweils besonderen organisatorischen Anforderungen und den angestrebten Reifegrad angepasst werden können. Möglichkeiten, die Kritikalität jeder Regel festzulegen, helfen, den Fokus des Unternehmens auf die wirklich wichtigen Bereiche innerhalb der internen und externen Vorgaben zu richten. Für die Regeln müssen Ausnahmen angegeben werden können, beispielsweise Administratoren, die allumfassende Systemberechtigungen innehaben (was nebenbei gesagt, nicht empfohlen ist) oder Rollen, die

bestimmte kritische Transaktionen vornehmen können sollen. Diese Ausnahmen müssen durch kompensierende Kontrollen, wie sie vom SAP-System oder Werkzeugen zum Compliance Monitoring zu Verfügung gestellt werden, ausgeglichen werden.

Reifegrad Schritt für Schritt erhöhen

Eine Investition in ein mächtiges und bekanntes Compliance-Werkzeug bedeutet noch nicht, dass ein Unternehmen per se compliant ist. Umgekehrt sind kleinere und weniger komplexe Tools nicht minder fähig, einer Compliance-Überprüfung standzuhalten. Es ist vielmehr eine Frage der Durchsetzung von Vorgaben, des bereits

Das Endziel jeder GRC-Implementation sollte es sein, das umfassende Monitoring von Governance, Risk und Compliance des gesamten Unternehmens mit seinen unterschiedlichen Systemen unter einem Dach sicherzustellen. Dies ist erst mit dem Erreichen eines höheren Reifegrads möglich und sollte unter Berücksichtigung von Benchmarks der jeweiligen Branchen durchgeführt werden. Unter diesen Voraussetzungen kann der Reifegrad Schritt für Schritt, System für System und Komponente für Komponente angehoben werden. Dazu sollten die wichtigsten Regeln aus tausenden möglichen ausgewählt, angewandt und die erkannten Verbesserungs-Notwendigkeiten in Abstimmung mit dem Management ausgeführt werden. Erst wenn Systeme bereinigt und alle Überwachungs-Anzeigen auf "grün" stehen, ist ein



erreichten Reifegrads sowie der zugrunde liegenden Prozesse und Dokumentationen. Eine weit verbreitete Methode zur Messung und Beurteilung des Reifegrads von Prozessen oder Systemen in Organisationen ist das Capability Maturity Model (CMM), das eine Bewertung auf einer Skala von 0 bis 5 benutzt. Der Wert 0 wird vergeben, wenn nichts vorhanden ist, der Reifegrad 1 steht für grundlegende erfolgreiche Aktivitäten und kann angehoben werden bis auf Level 5, wenn Aktivitäten kontinuierlich überwacht und statistisch ausgewertet werden. Das vom Software Engineering Institute der Carnegie Mellon University entwickelte CMM-Bewertungsmodell wird heute vielfach zur Bewertung der IT-Governance in Organisationen angewendet.

bestimmter Reifegrad erreicht und das Unternehmen ist bereit für den nächsten Schritt. Weitere Regeln können aktiviert, das System mit diesen zusätzlichen Regeln erneut überprüft und Abweichungen bereinigt werden. Diese Vorgehensweise kann in einem iterativen Prozess solange ausgeführt werden, bis der angestrebte Systemzustand erreicht wurde.

Fazit

Es ist wesentlich, die Umsetzung der Anforderungen aus Governance, Risk und Compliance als einen langfristigen Prozess zu verstehen und den Reifegrad nach und nach zu erhöhen. Daher sollten zuerst die wichtigsten Hundert Probleme gelöst werden, bevor man sich von Hunderttausenden erschlagen lässt. Geduld ist der Partner der Weisheit

Weitere Informationen zu "SAP Compliance Monitoring in a mouse click" unter www.mesaforte.com