

IT-Governance, Risk Management und Compliance mit Microsoft

Automatisierte Prozesse schaffen Sicherheit

Die Regulierung des Geschäftslebens und die Ansprüche an eine transparente Unternehmensführung sind weltweit verschärft worden. Unternehmen betrachten dies meist als Belastung, die Zeit, Geld und Ressourcen kostet. Microsoft bietet jedoch eine durchdachte Produkt- und Lösungsstrategie für IT-Governance, Risk-Management und Compliance (GRC) an. Mit dem System Center Service Manager und dem IT GRC Process Management Pack können Unternehmen ihre GRC-Prozesse effizient verwalten und umfassend kontrollieren.

Geschäftsprozesse müssen nachvollziehbar und transparent sein. Um dies zu gewährleisten, muss die IT-Infrastruktur alle relevanten Daten und Informationen für ein umfassendes Compliance-Management bereitstellen. IT-Verantwortliche stehen dabei vor der Herausforderung, die unterschiedlichen Interessen der verschiedenen Geschäftsbereiche zu bedienen und auch unterschiedliche Fragestellungen zu beantworten, wie beispielsweise: Arbeiten wir gemäß den Datenschutzgesetzen? Erfüllen wir CobiT, ITIL und ISO 27001? Unterstützen wir PCI DSS? Halten wir uns an das US-amerikanische Bundesgesetz SOX? Hinzu kommt heute eine Vielzahl branchenspezifischer Anforderungen und Gesetze, die Unternehmen erfüllen sollen.

Tools für IT-Governance, Risk-Management und Compliance

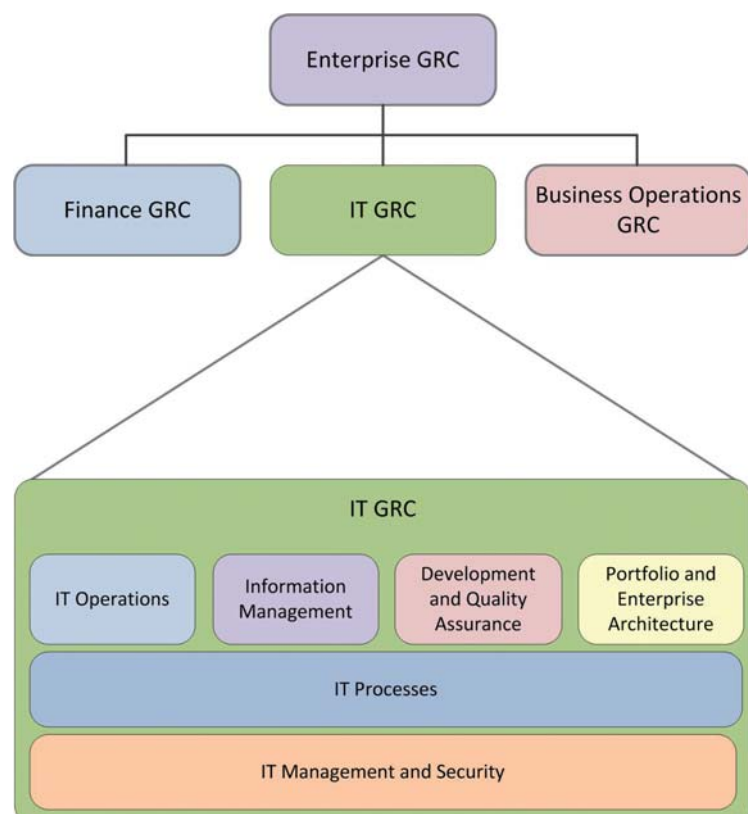
Mit dem System Center bietet Microsoft eine Produktgruppe für das Management der IT-Infrastruktur an, die es ermöglicht, gewachsene und heterogene IT-Umgebungen zentral und professionell zu verwalten. Zum Leistungsumfang des Microsoft System Center gehören unter anderem Softwareverteilung, Inventarisierung, Patch-Management, Monitoring, Datensicherung sowie Service Management und Prozessautomatisierung. Das jüngste Mitglied der Produktgruppe ist der System Center Service Manager. Der System Center Service

Manager ist eine integrierte Plattform zur Automatisierung von Best Practices für das IT-Service-Management und für deren Anpassung an individuelle Unternehmensanforderungen. Die Software stellt Prozesse für das Incident-, Problem-, Change- und Asset-Lifecycle-Management bereit. Für diesen System Center Service Manager bietet Microsoft ein kostenfreies Add-On an: Das Microsoft IT GRC Process Management Pack unterstützt Unternehmen dabei, Governance-, Risk-Management- und Compliance-Prozesse zu verwalten und zu automatisieren. Das IT GRC Process Management Pack umfasst Compliance-Bibliotheken bzw. Frameworks, die internationale Gesetze, Vorgaben, Standards und

Richtlinien beinhalten, beispielsweise für den Sarbanes-Oxley Act (SOX), den Gramm-Leach-Bliley Act (GLBA) oder den Health Insurance Portability and Accountability Act (HIPAA). Auf Basis von definierten Vorlagen können Unternehmen ihre Microsoft-basierende Infrastruktur entsprechend ihren Anforderungen konfigurieren. Diese technischen Konfigurationsvorlagen basieren auf weltweit anerkannten und angewandten Best Practices. Neben der Systemkonfiguration bietet das IT GRC Process Management Pack auch Testverfahren, die prüfen, ob die Standardkonfigurationen korrekt umgesetzt sind und dauerhaft unverändert bleiben. Compliance-Verantwortliche können



Michael Kranawetter
Chief Security Advisor
Microsoft Deutschland GmbH



auf Basis von vordefinierten Berichten prüfen, ob die geltenden Vorschriften eingehalten werden.

Maßnahmen und Aktivitäten verwalten und kontrollieren

Der Compliance-Manager kann unterschiedliche IT-GRC-Programme wie CobiT, ISO 27001, IT-Grundschutz oder auch

selbst gestaltete Programme verwalten. Er kann Risiken, Kontrollziele, Richtlinien und notwendige Kontrollmaßnahmen definieren, administrieren und miteinander verknüpfen. IT-Profis wiederum werden in die Lage versetzt, die technischen Elemente und Aktivitäten für Governance, Risk Management und Compliance systemweit über eine zentrale Benutzeroberfläche zu steuern.

Vorgaben einhalten und überwachen

Das System Center Service Manager und das Microsoft IT GRC Process Management Pack bieten verschiedene Kontrollmechanismen, um sicherzustellen, dass Unternehmen alle regulatorischen und gesetzlichen Vorgaben einhalten können:

- Compliance-Verantwortliche können ihre gewünschten Konfigurationen **automatisch** über das Desired Configuration Management (DCM), den System Center Configuration Manager und die IT CML Configuration Packs setzen, abgleichen und abrufen. Dank dieser Automatisierung reduziert sich der Aufwand, IT-Compliance im Unternehmen beurteilen zu können, drastisch.

- Darüber hinaus können IT-Experten **manuell** bewerten, ob alle geforderten Vorgaben eingehalten werden. Hierfür gibt es drei Möglichkeiten:

Technologie: Dies umfasst alle Konfigurationseinstellungen für IT-Governance, Risk Management und Compliance, die nicht automatisiert erfasst werden.

Menschen: Dies umfasst alle Aspekte, die mit den Mitarbeitern und deren Nutzung der IT zusammenhängen, wie beispielsweise den Zugang der Mitarbeiter zu sensiblen Informationen.

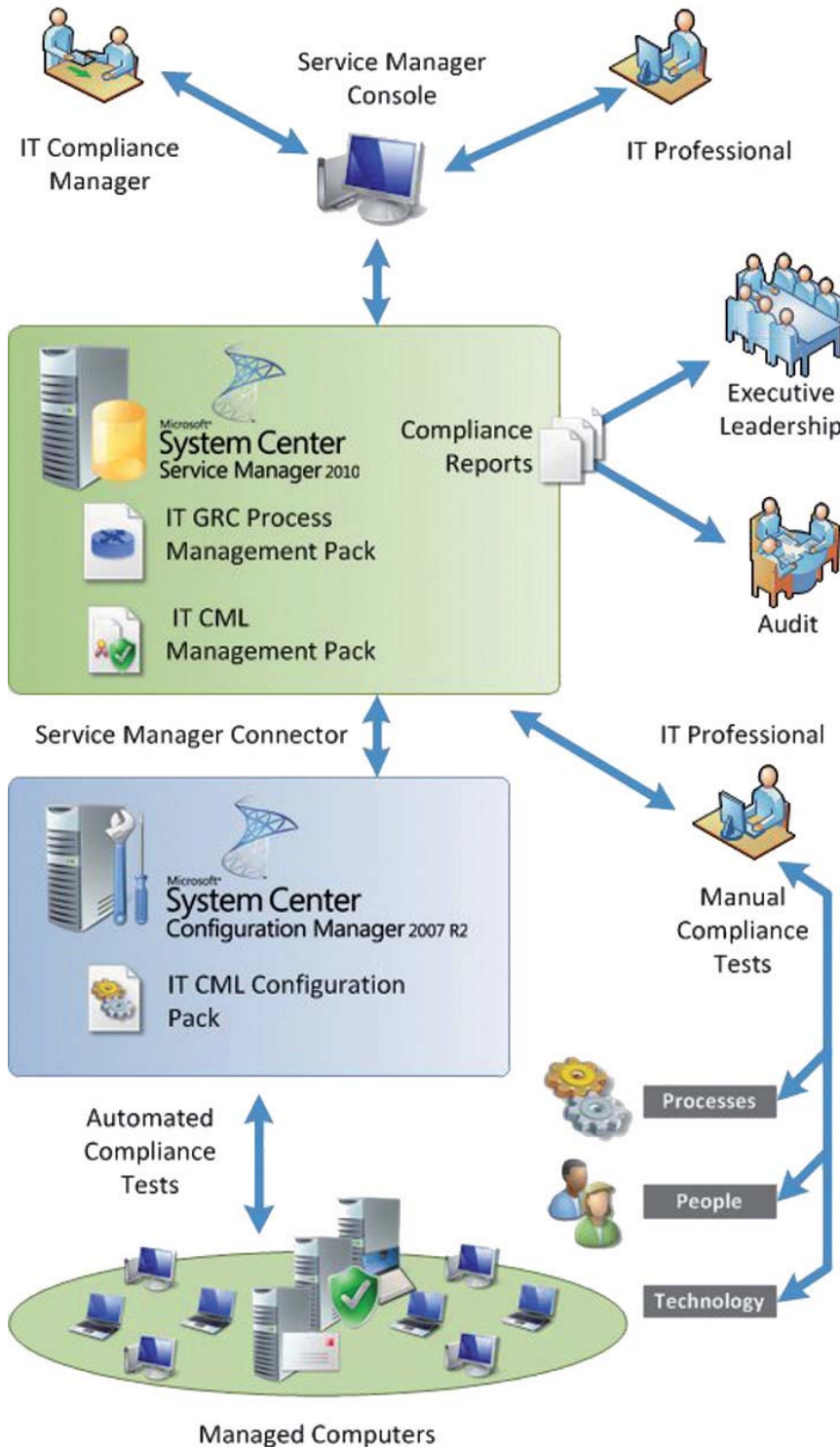
Prozesse: Die Prozesse umfassen alle IT-GRC-Aspekte wie beispielsweise organisatorische Maßnahmen und Aktivitäten. Hierzu zählt zum Beispiel die zuverlässige Löschung von sensiblen Informationen auf Alt-Systemen.

Dank des Zusammenspiels des System Center Service Manager und des System Center Configuration Manager profitieren Unternehmen von den folgenden Funktionen:

- Die Konfigurationselemente (CIs), die in der Configuration Management Database (CMDB) gespeichert sind, können automatisch mit Maßnahmen und Informationen bestückt an den System Center Configuration Manager übergeben werden.

- Compliance-Ergebnisse der automatisierten Maßnahmen-Aktivitäten (CA) lassen sich in der System Center CMDB automatisch aktualisieren.

Unternehmen können darüber hinaus eigene IT-GRC-Konnektoren für den System Center Service Manager entwickeln, um die Einhaltung von regulatorischen und gesetzlichen Vorgaben in anderen Systemen zu prüfen und durchzusetzen.



Microsoft verankert in der Produkt- und Lösungsstrategie alle grundlegenden Funktionen für IT-Governance, Risk Management und Compliance und sorgt dafür, dass Unternehmen die Synergien zwischen regulatorischen Vorgaben und Geschäftszielen optimal nutzen können