

# Governance, Risk and Compliance in SAP-Systemen

Viele Unternehmen stehen vor der Situation, nicht mehr ganz genau zu wissen, wo welche Datenströme fließen oder wie die Systemschnittstellen genau arbeiten. Diese schwere Altlast, gekoppelt mit einer schlechten Systemhygiene, muss adressiert werden *Priska Altorfer*



**Priska Altorfer**  
ist Chairman der Wikima4 AG  
[priska.altorfer@wikima4.com](mailto:priska.altorfer@wikima4.com)

Peter Weill und Jeanne Ross vom Center for Information Systems Research (CISR) der MIT Sloan School of Management in Boston haben IT Governance definiert als eindeutigen Rahmen mit Entscheidungsrechten und Zuständigkeiten, die den unternehmensspezifisch «richtigen» Umgang mit der IT unterstützen. Risk Management bezeichnet das aktive Managen mit dem obersten Ziel der Reduzierung von Risiken. Damit diese Mitigation ermöglicht wird, sind in Unternehmen Controls zu implementieren und deren Einhaltung sicherzustellen (Compliance). In freier Interpretation der altbekannten Formel  $E=mc^2$  können wir es vereinfacht ausdrücken: Governance, Risk and Compliance (GRC) kann gleichgesetzt werden mit Effizienz, Mitigation und Controls. Kontinuität (Continuity) sorgt dafür, dass Erreichtes kritisch hinterfragt wird und Qualitätszyklen angestossen werden.

## Die Anforderungen

SAP-Systeme werden für die Abbildung von geschäftskritischen Geschäftsabläufen verwendet. Die hochflexible Standardsoftware kann durch ihre Konfiguration bestehenden Abläufen angepasst werden, ohne dass die bewährten Prozesse geändert werden müssen.

SAP-Systeme werden von einer Vielzahl von Personen bearbeitet: Entwickler, Basis-Verantwortliche, IT-Architekten, Berechtigungskoordinatoren, businessnahe IT-Mitarbeiter, Systemverantwortliche und externe Berater. Alle haben ihre eigene Betrachtungsweise auf das System.

Entwickler sehen keine Risiken in Eigenentwicklungen – sie arbeiten ja gut. Systemverantwortliche durchschauen die Komplexität nicht mehr und sind auf die Beurteilung ihrer technisch versierten Spezialisten angewiesen. Berechtigungskoordinatoren sitzen zwischen den Stühlen: Die Beteiligten fordern möglichst hohe Rechte und nicht nur

diejenigen, die sie zum Ausführen ihrer Arbeit tatsächlich benötigen. Das Business will möglichst alle Wünsche erfüllt haben mit dem Hinweis, dass sie ja das Budget vergeben. Externe Partner wiederum haben eine nur eingeschränkte Sicht auf die Systeme. Es bestehen also Meinungsdivergenzen über das, was notwendig ist und was nicht. Nur in einem sind sich alle einig: GRC ist ein Reizwort. Denn wer wird schon gern überprüft und legt transparent sein Tätigkeitsgebiet dar?

## Sind die Systeme bereit für ein GRC?

IT Governance, Risikomanagement und Kontrollen müssen sich eingliedern lassen, ohne dass die betroffenen Systeme an Effizienz und Dynamik verlieren. Viele SAP-Systeme laufen gut. Sie funktionieren ohne grosse Einbussen in der Verfügbarkeit. Die meisten von ihnen haben die ausgelieferten Standards individuell auf kundenspezifische Anforderungen «customized».

Dies bringt auf der einen Seite eine höhere Akzeptanz bei den Benutzern, auf der anderen Seite jedoch ein höheres Bedürfnis an Dokumentation und Transparenz in der Systemumgebung. Letztere dürfte dem Kosten- und Zeitdruck zuliebe häufig unvollständig oder gar nicht ausgeführt werden. Viele Unternehmen stehen daher vor der Situation, nicht mehr ganz genau zu wissen, wo welche Datenströme fließen, oder wie die Systemschnittstellen genau arbeiten. Diese schwere Altlast, gekoppelt mit einer schlechten Systemhygiene, lässt sich nicht ohne Aufwand beheben. So verzichten Unternehmen oft auf eine Bereinigung.

Die Auswirkungen dieser mangelnden Visibilität sind für Einführung von IT-Governance-Modellen eine grosse Herausforderung, die es zu meistern gilt. Das Gleiche gilt auch für die Bereiche Risiko- und Compliance-Management.

### Weg von der Black Box

Wir haben es also mit einer Black Box oder besser mit vielen kleinen Black «Böxchen» zu tun. Sie gilt es in einem ersten Schritt zu öffnen. Ohne diese Transparenz kann man GCR nicht sinnvoll implementieren. Die von SAP und anderen Herstellern angebotenen Tools erfüllen ihrerseits erst dann die Anforderungen an die Governance, wenn sie einem bereinigten System aufgesetzt werden.

Dies bedeutet zuerst Knochenarbeit, die – macht man alles auf einmal – selten zum Ziel führt. Erfolg versprechender ist die Vorgehensweise, Mitarbeitende und Systeme in kleinen Schritten von Teilerfolg zu Teilerfolg führen.

Betrachtet man den Sachverhalt aus Sicht der Qualitätsverantwortlichen, ergeben sich zwischen SAP-System und Assembly Lines bei der Automobilproduktion augenfällige Gemeinsamkeiten. Das grosse Rätsel ist, wie es die Automobilindustrie fertig gebracht hat, dass die Autos fehlerfrei und sicher laufen und sich erst noch gewinnbringend verkaufen lassen.

Auf die IT umgemünzt müssen dazu folgende Faktoren berücksichtigt werden:

1. Zuerst ist ein gemeinsames Ziel aufzustellen, das da heisst: «Das SAP-System bildet zuverlässig, effizient und sicher die für das Unternehmen notwendigen Prozesse ab.» Die verarbeiteten Daten erreichen eine hohe Qualität und die Prozesse sind klar und übersichtlich dargestellt. Da in SAP-Systemen Menschen die zentrale Rolle spielen, müssen diese auch besonders beachtet werden. Die meisten Mängel in SAP-Systemen werden schliesslich durch sie verursacht. Die Qualitätsverantwortlichen haben bereits vor über drei Jahrzehnten erkannt, dass jeder einzelne Mitarbeiter persönlich involviert werden muss und Verantwortung für seinen Teilbereich, sein Arbeitsergebnis zu tragen hat. In der Automobilbranche konnte durch eigenverantwortliche teilautonome Arbeitsgruppen die Qualität massiv erhöht werden.
2. Die angestrebte Qualität soll analysiert und Zielwerte der einzelnen Etappen definiert werden. In dieser Projektphase sind Personen der Informatik wie auch des Business vertreten. Alle werden in die Erreichung der Qualitätsziele einbezogen, niemand darf unverhältnismässige Anforderungen stellen.
3. Der Entscheid, wie was und wer überprüft und wie mit den Ergebnissen umgegangen wird, ist ein sehr sensibles Thema. Ganz wichtig für die Erarbeitung der internen

Kontrollen ist die Transparenz. Es muss im Voraus bekannt sein, was passiert, wenn etwas nicht eingehalten wird. Wie alle zu erreichenden Ziele werden auch die Kontrollen in Etappen geplant.

4. Die Überprüfung der gesetzten Ziele soll, wo immer möglich, in einem Exception Reporting erfolgen. Das heisst, erst wenn die Werte nicht mit den Vorgaben übereinstimmen, wird agiert. Dies ist notwendig, da es in SAP-Systemen sehr viele zu überprüfende Werte gibt und das Monitoring immer mit Ressourcenproblemen konfrontiert ist.
5. Die richtige Kommunikation der Themen soll über Abteilungen hinweg gewährleistet werden. Dabei führen die Vergleichsmöglichkeiten, die mit einer Visualisierung der IT erreicht wurden, zu einer höheren Akzeptanz des «Kostenverursachers IT». Lob und Akzeptanz sollen diejenigen erhalten, die die Ziele zuerst besonders gut erreichen oder deren Einsatz besonders hoch ist.
6. Die Erreichung der gesteckten Ziele kann von einer Vielzahl von Werkzeugen und Regelwerken unterstützt werden. Dabei sollen jedoch immer die Vorgaben der IT Governance beachtet werden

### Fazit

Einen GRC-Hut über eine Unternehmens-IT zu stülpen, um so pro forma Resultate zu erhalten, bringt so viel wie ein ISO-Ordner im Bücherregal. Der Qualitätsreifegrad eines SAP-Systems ist ausschlaggebend für eine erfolgreiche Implementierung. Es gilt, in kleinen Schritten komplexe SAP-Systeme mit GRC-Teilen auszustatten, damit valable Resultate bereitgestellt werden können. Die Nachhaltigkeit dieser Vorgehensweise macht sich in jedem Fall bezahlt, denn es ist sicher motivierender, effizient und transparent zu arbeiten.

Was die Anerkennung der Leistungen schwierig macht, ist die Tatsache, dass viele Betreiber wie auch Anwender von SAP-Systemen (noch) nicht bereit sind, für eine höhere Qualität einzustehen. Was die Autos von heute, versehen mit den neusten Technologien, mit aktiven Sicherheitssystemen erreichen, ist Zukunftsmusik für die SAP-Systeme. Manager müssen endlich den Mut aufbringen, auch für Altlasten, die vor ihrer Zeit entstanden, geradezustehen und sich nicht hinter einer Projektflut zu verstecken. Nur so können sie einmal ruhig in ihrem Sessel sitzen und am Dashboard die Geschwindigkeit, Fehlerquote, Compliance-Verstösse etc. online managen. Willkommen in der Zukunft! ■