S@PPORT

Entscheidungsgrundlagen für Auswahl, Installation und Betrieb von SAP*-Lösungen

Sonderdruck aus Heft 5/2012 vom 3. Mai 2012 · www.sap-port.de

GRC: Governance, Risk, Compliance

IT-GRC weist Wertbeitrag der IT nach

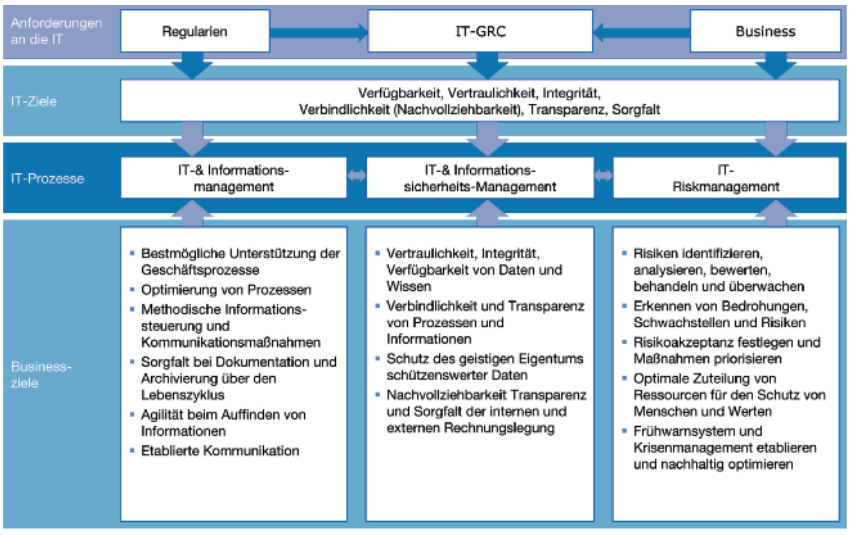
Aus verschiedenen Gründen sind Unternehmen gezwungen, den gültigen gesetzlichen, politischen und kulturellen Anforderungen gerecht zu werden. Die IT als wesentliche Unterstützung für das Business ist ebenfalls an diese Regelungen gebunden. Ihr werden sogar zusätzliche Anforderungen und Pflichten auferlegt. Die Stunde der IT-Governance schlägt.

*Von Dr. Jochen Ruben**

Eine Wahlfreiheit haben Unternehmen hinsichtlich des Erfüllens der Vorgaben nicht. Denn mit der Entscheidung, Märkte zu besetzen, geht auch die Verpflichtung einher, sich deren Regularien zu unterwerfen. Gleichzeitig steigen die Anforderungen und damit auch die Anzahl und der Umfang interner Regelungen aus bestehenden und neuen Geschäftsprozessen.

Regulatorische Anforderungen an Unternehmen sind vielfältig und von unterschiedlichen Randbedingungen abhängig. Hierzu gehören neben Branchen und Gesellschaftsformen auch regionale und kulturelle Gegebenheiten. Daraus ergibt sich zwingend, dass neben nationalen auch internationale Gesetze und Vorgaben zu berücksichtigen sind.

Unternehmen sollten diese Anforderungen aber nicht als Zwang betrachten. Denn viele gesetzliche Anforderungen stehen nicht im Widerspruch, sondern im Einklang mit strategischen Geschäftsinteressen. Ein bekanntes Beispiel ist der Schutz des Persönlichkeitsrechts, das Bundesdatenschutzgesetz (BSDG). Es liegt im Interesse jedes Unternehmens, etwa Kundendaten so gut



Anforderungen an die IT-Compliance aus Geschäftszielen

*Dr. Jochen Ruben ist Senior Consultant bei bridgingIT.

wie möglich vor Missbrauch und unberechtigtem Zugriff zu schützen. So verhält es sich auch mit einigen weiteren Anforderungen wie dem Gesetz für ein Risikomanagementsystem, das in einigen Ländern gefordert wird.
Umgang und Schutz von Informationen organisatorisch, technisch und kulturell in einem Unternehmen auszuprägen, ist entscheidend, um Industriespionage und Betrug vorzubeugen und eine gute Reputation aufzubauen. Nur so können Unternehmen spezifische Werte in Form von Wissen und die darauf aufbauende Innovationskraft schützen, um eine erreichte Branchenposition zu halten und Fortschritt sicherzustellen. Die Anforderungen werden in Prozessen und Führungsstrukturen definiert, in Corporate Governance, Compliance und Risikomanagement integriert und somit Teil der Unternehmensstrategie.

Aufgabe der IT-Governance

Durch die allgegenwärtige und vielschichtige Unterstützung der Geschäftsprozesse durch IT-Services übertragen sich die Compliance- und Business-Anforderungen auf diese Services und somit auf die IT-Organisation. Neben der Aufgabe der IT, dies zu unterstützen, kommen demnach auch direkte businessspezifische und regulatorische Anforderungen hinzu. Diese zu kennen und den Nachweis der entsprechenden IT-Unterstützung zu erbringen, ist eine elementare Aufgabe der IT-Governance.
Die gemeinsamen Anforderungen aus dem Inneren des Unternehmens und den externen Regularien lassen sich in sechs Zielen zusammenfassen, die unternehmensspezifisch ausgeprägt werden müssen:

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Verbindlichkeit (Nachvollziehbarkeit)
- Transparenz
- Sorgfalt

Um diesen Anforderungen an die IT-Unterstützung gerecht zu werden, müssen auf Seiten des IT-Dienstleisters die folgenden Domänen implementiert und auf effiziente Weise miteinander aggregiert werden:

- Informationsmanagement
- Informationssicherheitsmanagement
- Informationsrisikomanagement

Daneben muss die IT sinnvoll durch die Fachabteilungen gesteuert werden. Nur so kann die Abstimmung zwischen Fachabteilung und IT noch stärker ausgeprägt werden. Bei einer sinnvollen und auf das Unternehmen adaptierten Umsetzung lassen sich IT-Governance-, IT-Risk- und IT-Complinance-Prozesse vollständig abbilden. Dann sind die Voraussetzungen zum Erfüllen der internen und externen Anforderungen geschaffen.
Durch die Nachweisbarkeit der Erfüllung regulatorischer und interner Anforderungen – auch von Seiten der Informationsverarbeitung – und die Synchronisation der IT mit den Fachabteilungen, lassen sich IT- und Geschäftsrisiken gemeinsam kalkulieren und behandeln. Insbesondere Schnittstellenprozesse werden optimiert, IT-Architekturen konsolidiert, Investitionen und Werte geschützt und letztendlich die Reputation und das Unternehmensimage gesteigert.

Mehrwert der IT entsteht durch proaktives Handeln

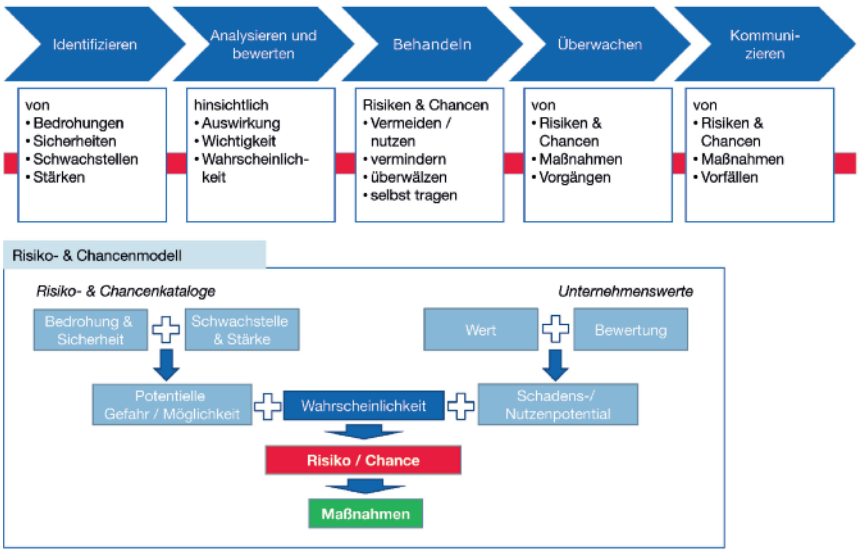
Geschäftsprozesse sind immer stärker von der unternehmensweit genutzten IT abhängig. Das Neugestalten von Geschäftsprozessen ist daher nicht mehr ohne unterstützende IT-Services machbar. Diese Abhängigkeit gilt es grundsätzlich zu beachten.
Jedoch ist die IT nicht gezwungen, ausschließlich auf Änderungen der Geschäftsprozesse zu reagieren. Durch proaktives Handeln generiert sie einen direkten Mehrwert für das Unternehmen. Dabei müssen sich IT-Verantwortliche verschiedene Fragen stellen:

- Welche Informationen und Services werden heute benötigt, um Geschäftsprozesse optimal auszuführen?
- Welche Informationen und Services werden in der Zukunft benötigt?
- Welche Wettbewerbsfaktoren sind für das Unternehmen kritisch und welche können durch die IT positiv beeinflusst werden?

Ziel ist eine enge Zusammenarbeit zwischen Business und IT auf allen Ebenen. Nur so können das Leistungspotenzial des gesamten Unternehmens erhöht und die Unternehmensziele erreicht werden. Dazu kann und muss die IT einen nachweisbaren Mehrwert leisten. Das Informationsmanagement liefert Blaupausen für die mittel- und langfristige Weiterentwicklung der Technik-landschaft, die nicht nur bisherige Anforderungen der Anwender aufgreifen, sondern auch zukünftige Ansprüche berücksichtigen. So können adäquate Zielarchitekturen von Infrastrukturen und Anwenderlandschaften erstellt werden.

Assets und Schutzziele definieren

Essenziell für diese Aufgaben ist, die primären und sekundären Werte (Assets) zu identifizieren und sie hinsichtlich der Schutzziele und der Relevanz für das Unternehmen zu bewerten. Gute Anhaltspunkte bietet die ISO/IEC 27005, die das Management von Informationssicherheitsrisiken im Rahmen der ISO/IEC-27000-Reihe beschreibt. Es werden Vorschläge für die Definition primärer und sekundärer Assets aus Sicht der Informationssicherheit gemacht. Die Bewertung der Werte erfolgt nach dem normativen Teil der ISO/IEC 27001 konform zum IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) in den Schutzzielen „Verfügbarkeit“, „Vertraulichkeit“ und „Integrität“. Diese Schutzziele können



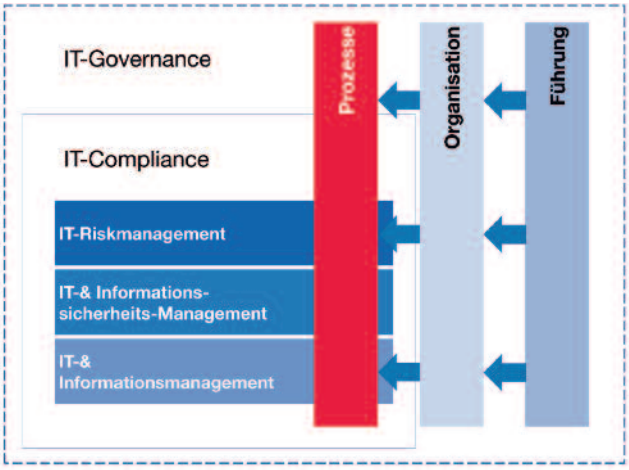
IT-Risk-Management-Prozess – Kenntnis von Risiken ermöglicht Maßnahmen

nach Bedarf ergänzt werden. Als primäre Assets werden vorgeschlagen:

- Geschäftsprozesse und Aktivitäten
- Informationen.

Sie werden durch unterstützende (sekundäre) Werte ergänzt:

- Hardware
- Software
- Netzwerk
- Personal
- Standorte
- Organisationsstruktur



IT-GRC ist untrennbar

Diese Empfehlungen unterstreichen die Tatsache, dass die ISO/IEC-27000-Reihe nicht die IT-Organisation, sondern das gesamte Unternehmen betrachtet. Eine wesentliche Voraussetzung insbesondere zur Definition technischer und organisatorischer Maßnahmen zum bedarfsgerechten Schutz von Informationen ist, die Abhängigkeiten zwischen den primären Assets und der unterstützenden IT greifbar zu machen.

Dazu muss die IT-Architektur unter Einbezug der Geschäftsprozesse und der relevanten Informationen transparent gemacht werden. Dies wird im Wesentlichen in der Domäne „Plan and Organise" des COBIT-Frameworks adressiert und unterstreicht die elementare Wichtigkeit dieser Aufgabe. Zentral ist an dieser Stelle der Gedanke, dass sich die Anforderungen der Schutzziele auf die unterstützenden Assets vererben und durch die jeweiligen Asset-Owner bewertet werden. Nun lässt sich ein bedarfsgerechter Schutz fundiert begründen und umsetzen. Durch diese Vorgehensweise für Business-Impact-Analysen werden die Wichtigkeit und mögliche Wertschöpfungspotenziale des Informationsmanagements transparent. Ein IT-Architekturmodell ist nicht nur Basis für die Informationssicherheit, es ist vielmehr der zentrale Eckpfeiler zum Konsolidieren von IT-Services und kann Einsparpotenziale sichtbar und nachweisbar machen.

Risikomanagement als Basis für bedarfsgerechten Schutz

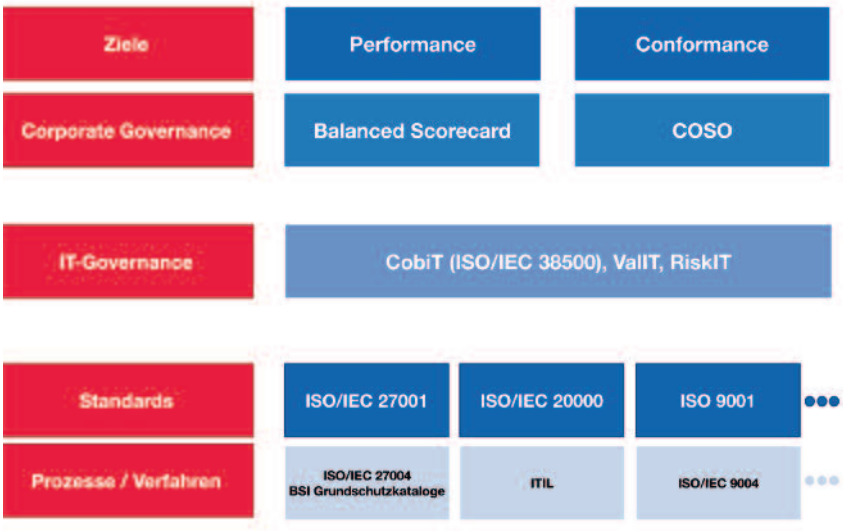
Gerade im Informationsmanagement nehmen Risiken und deren Behandlung eine wichtige Rolle ein. Bedrohungen lassen sich auf höchster Ebene in folgende Kategorien einteilen:

- Höhere Gewalt
- Technisches Versagen
- Organisatorische Mängel
- Menschliches Versagen
- Vorsätzliche Handlungen

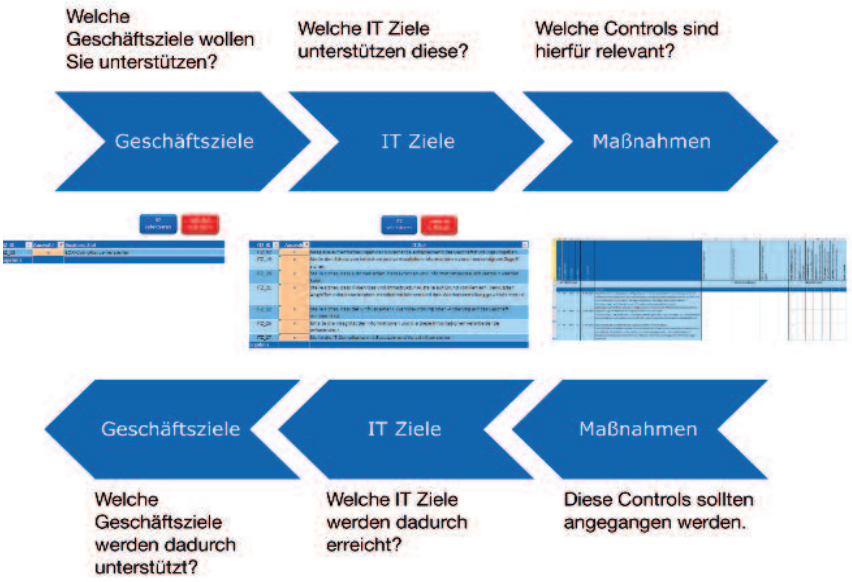
Neben gesetzlichen Regelungen, die sich mit dem Schutz beschäftigen, sind die steigenden Anforderungen an ein adäquates Risikomanagementsystem auch Unternehmenszielen zuzuschreiben. Hier wird wieder die Synergie zwischen Unternehmenszielen und Regularien deutlich. Beim Beachten dieser Synergien bereits in der Konzeptionsphase des Risikomanagementsystems lassen sich deutliche Vorteile erzielen und redundante Sicherheitsmaßnahmen vermeiden. Auch ein proaktives Handeln wirkt sich positiv auf die Wirksamkeit und Effizienz eines Risikomanagementsystems aus. Gemeint ist damit das Umsetzen von künftigen, absehbaren Anforderungen, bevor diese akut werden. Die reine Reaktion auf Anforderung aus Regularien und Geschäftsbetrieb lässt einen gezielten Einsatz der sich ergebenden Synergien kaum zu.

Grundsätzlich unterstützt ein gezieltes Risikomanagement Unternehmen dabei, sich der Gefahren im Zusammenhang mit der IT bewusst zu werden, künftige Anforderungen sinnvoll und rechtzeitig zu integrieren, Chancen zu identifizieren und zu nutzen sowie Handlungsalternativen zu erkennen und zu bewerten. So kann nicht nur im Notfall reagiert, sondern bereits im Vorfeld ein Bündel an Schutzmaßnahmen etabliert werden, die bei Bedarf ergriffen werden können.

Der in den Standards ISO/IEC 31000 und ISO/IEC 27005 beschriebene Prozess zum Management von Risiken beziehungsweise Informationssicherheitsrisiken umfasst im ersten Schritt die Definition des Kontextes. Grundsätzlich ist dies im Rahmen des Prozessdesigns zu berücksichtigen. Allerdings empfiehlt es sich, diesen und alle weiteren Schritte stets und insbesondere bei der Analyse einzelner Risiken einzuhalten. Werden beispielsweise Risiken und Chancen in einem Projekt durch den Projektleiter analysiert und bewertet, so muss dieser zunächst definieren, ob er die Auswirkungen auf das einzelne Projekt betrachtet, oder ob sie im Kontext eines übergeordneten Programms analysiert werden, beziehungsweise ob die Auswirkungen auf das gesamte Unterneh-



Die Zusammenhänge zu den Unternehmenszielen



IT-GRC-Reifegradmodell: Von den Geschäftszielen zu IT-Maßnahmen

men in die Bewertung eingehen. Ein hierarchischer Aufbau des Reportings zur Integration und Aggregation der Risiken und Chancen im Risikomanagement ist möglich, aber nicht erforderlich.

Somit ergeben sich unterschiedlich große und ineinander verzahnte PDCA-Zyklen, deren Konsistenz sichergestellt werden muss. Dies gilt zum einen für eine unternehmensweit konsistente und integrierte Methodik (Top-Down-Ansatz), und zum anderen für die Aggregation (Bottom-Up-Ansatz).

Nicht nur im Sinne der IT-Sicherheitsrisiken ist es von zentraler Bedeutung, die im vorherigen Abschnitt beschriebenen Business-Impact-Analysen als Grundlage zum Beurteilen der Auswirkungen von möglichen Vorfällen zu nutzen. Sind diese Voraussetzungen nicht gegeben, können lediglich Bedrohungen, Schwachstellen und Szenarien bewertet werden. Ein bedarfsgerechter Schutz lässt sich auf diese Weise nicht sicherstellen.

Implementierung in der Organisation

Im nächsten Schritt gilt es, diese Prozesse nachhaltig im Unternehmen zu etablieren und so zu gestalten, dass auf weitere Veränderungen der Vorgaben flexibel reagiert werden kann. Dazu gehört das konsequente Beobachten von Veränderungstendenzen der gesetzlichen Regularien und Anforderungen durch das Unternehmen und die proaktive und reaktive Anpassung von IT-Prozessen. Dies ist Aufgabe der IT-Governance. Ihr obliegt das Gestalten von Führung, Organisation und Prozessen. Ein konsequentes Umsetzen sichert eine hohe Effizienz, Effektivität und Wirksamkeit von organisatorischen und technischen Prozessen. Mitarbeitern werden verbindliche Rahmenbedingungen gegeben, innerhalb derer sie sich bewegen können.

Neben diesen Anforderungen sprechen spezielle Interessen des Vorstands und der Geschäftsführung für eine konsequente IT-Governance. Als Spezifizierung der Corporate Governance für die IT haftet das oberste Management direkt und persönlich für das Einhalten der regulatorischen Anforderungen. Daraus ergeben sich folgende Hauptaufgaben der IT-Governance:

- Strategic Alignement
- Value Delivery
- Resource Management
- Risk Management
- Performance Measurement

Umsetzen lassen sich diese Aufgaben durch den Einsatz entsprechender Frameworks. Neben gängigen Frameworks für das IT-Service. Management, die die IT-Governance unterstützen, gibt es eine Vielzahl spezifischer Frameworks zur Etablierung der IT-Governance im Unternehmen wie COBIT. Mit deren Hilfe lassen sich Führungsstrukturen und Prozesse im Unternehmen etablieren, die aufgrund ihres Charakters als etablierte Rahmenwerke auch direkt Transparenz sicherstellen. Das COBIT-Framework schafft einen vollständigen Rahmen dafür. Sollen jedoch einzelne Ziele erreicht werden, bietet sich die Detaillierung in den einzelnen Domänen, Prozesse und Aktivitäten an. Folgende Methoden sind empfehlenswert: Aufbauend auf einem Qualitätsmanagementsystem sollten ein IT-Service-Management und Managementsystem für Informationssicherheit implementiert werden. Hierfür bieten sich die Standards und Frameworks entlang der ISO/IEC 9000, der ISO/IEC 20000 beziehungsweise ITIL und der ISO/IEC 27000 an.

Durch ein sinnvolles Umsetzen sind diese aufgrund einiger Überschneidungen integrierbar. So lassen sich Synergien nutzen und sowohl derzeitige, als auch künftige Anforderungen transparent darstellen und im Unternehmen berücksichtigen. Damit kann die IT-Governance auch in diesem Punkt einen Wertbeitrag leisten.

Das Unternehmen unterstreicht damit seine Nachhaltigkeit und die Bereitschaft, gesellschaftliche Verantwortung zu übernehmen. Es kann sein Image verbessern und letztlich seine Marktposition ausbauen. Nicht nur die Außenwirkung, auch die internen Abläufe werden durch dieses Verfahren strukturiert und aufeinander abgestimmt. Durch die Transparenz der Prozesse lassen sich Effizienz und Effektivität messen und steuern.

Unterm Strich...

Die Zusammenhänge der IT-Governance, IT-Risk und IT-Compliance bietet also neben vielen Herausforderungen auch enorme Chancen. Neben der ohnehin geforderten Einhaltung von Regelungen können gleichzeitig die Anforderungen des Business erfüllt werden. Dabei liegt der Fokus nicht auf reaktivem, sondern auf proaktivem Handeln. Gerade dies ermöglicht, den oft angemahnten Mehrwert der IT zu schaffen. Dabei dienen die drei Kernbereiche (Informationsmanagement, Informationssicherheitsmanagement und Informationsrisikomanagement) als Basis für ein gemeinsames Verständnis der Notwendigkeit, Motivation und Umsetzung bei Geschäftsführung, Fachbereichen, technischen Entscheidern und IT-Experten.

Diese Herausforderungen lassen sich unter anderem mittels eines Tools ganzheitlich im Unternehmen adressieren und die Umsetzung der Ziele in Prozessen implementieren. Ein Beispiel für ein solches Werkzeug ist das Reifegradmodell von bridgingIT, das gängige und anerkannte Methoden und Standards miteinander verzahnt und somit einen tiefgreifenden Blick in die Prozesswelt des Unternehmens gewährleistet. Gleichzeitig bietet es neben der ganzheitlichen Sicht Einblicke in bestimmte Teilaspekte wie ITIL, ISO/IEC 20001 oder COBIT. *(ur)* @