

Die Unternehmens-IT auf dem Prüfstand

Eine „Gesundheitsvorsorgeuntersuchung“ für Ihre IT im Unternehmen?

Die Krise ist mit mehr oder weniger großen Nachwehen überwunden. Der Wirtschaftsmotor beginnt wieder auf Touren zu kommen. Um die Wirtschaftskraft in den Unternehmen wieder voll entfalten zu können, müssen nach dem teilweisen Zurückfahren und Drosseln der Kapazitäten die einzelnen Aggregate wieder auf Volllast getuned werden. So auch die IT im Unternehmen, die in ihrer Querschnittsfunktion alle Bereiche des Unternehmens unterstützen, beschleunigen und helfen können deren Prozesskosten zu optimieren.

Jedoch wie sieht der Prüfstand aus, der Ihre Unternehmens-IT auf Effizienz und Effektivität überprüfen kann?

Auch, und besonders in Zeiten des wirtschaftlichen Aufschwungs sind Ressourcen knapp und endlich. Dies ist auch in den IT-Abteilungen unseres Landes zu erkennen. Dennoch, die IT aus mangelnden Ressourcen nicht auf den Prüfstand zu stellen und IT-relevante Risiken für die wertschöpfenden Prozesse im Unternehmen nicht zu kennen oder zu ignorieren, kann rasch zum „Stottern“ des eigenen Motors führen, Ihr Unternehmen an die Box zwingen oder zum Hinterherfahren verurteilen.

CRISAM[®] ist der Prüfstand, der Ihre Unternehmens-IT auf Effizienz und Effektivität IT-unterstützter Geschäftsprozesse analysiert, Unter- und Übererfüllung technologischer und organisatorischer Maßnahmen zu vordefinierten Zielen aufzeigt, sowie den monetären Impact IT-relevanter Risiken darstellt.

CRISAM[®] steht für „Corporate Risk Application Method“ und ist eine ganzheitliche Methode zur Implementierung eines IT-Risikomanagement Prozesses.

Die wesentlichen Unterscheidungsmerkmale zu derzeit verfügbaren Methoden, Standards und Best Practices sind:

1. eine nachvollziehbare Quantifizierung von IT-Risiken
2. Berücksichtigung der Ursache-Wirkungsbeziehung einzelner Risiken zueinander (Berechnung des Fehlerbaums)
3. eine Beurteilung der Risiken entsprechend ihrer Auswirkungen auf die unterstützten IT-Prozesse
4. eine monetäre Bewertung der IT-Risiken nach ihren Best-, Worst- und Most Likely Szenarien
5. die Umsetzung in einem kontinuierlichen Verbesserungsprozess (KVP).

Abbildung 1 zeigt das 6-stufige Prozessmodell anhand dessen der Risikomanagement-Prozess implementiert wird. Besonders an den Stufen „Festlegen der Rahmenbedingungen“ und „Analyse des Umfelds“ ist zu erkennen, dass CRISAM[®] neben den IT-Ressourcen auch das IT-Umfeld, den Governance und Compliance Aspekt, sowie den IT-Kunden in die Prüfung einbeziehen. CRISAM[®] legt das Grundprinzip „Risiko ist das Resultat aus Ursache und Wirkung“ zugrunde. Die Ursache eines IT-Vorfalles wurzelt in der IT oder deren unterstützenden Aggregaten (Stromversorgung, Facilities oder Zulieferung von Leistung). Die Wirkung bzw. der aus dem Vorfall resultierende Schaden ist als negativer Impact auf den IT-unterstützten Geschäftsprozess zu messen.

Aufgrund der implementierten Rückkoppelungen wird sichergestellt, dass ein nach der Methode *CRISAM*[®] implementierter Risikomanagement-Prozess, den von normkonformen Managementsystemen geforderten „PLAN-DO-CHECK-ACT“ (PDCA) Prozess entspricht. Dies wird auch dadurch unterstrichen, dass automatisiert die Compliance zu Normen und Standards, beispielsweise ISO 27001, COBIT, BSI Gshb etc. gemessen und in Berichten ggf. auch als Zertifizierungsgrundlage festgehalten wird.

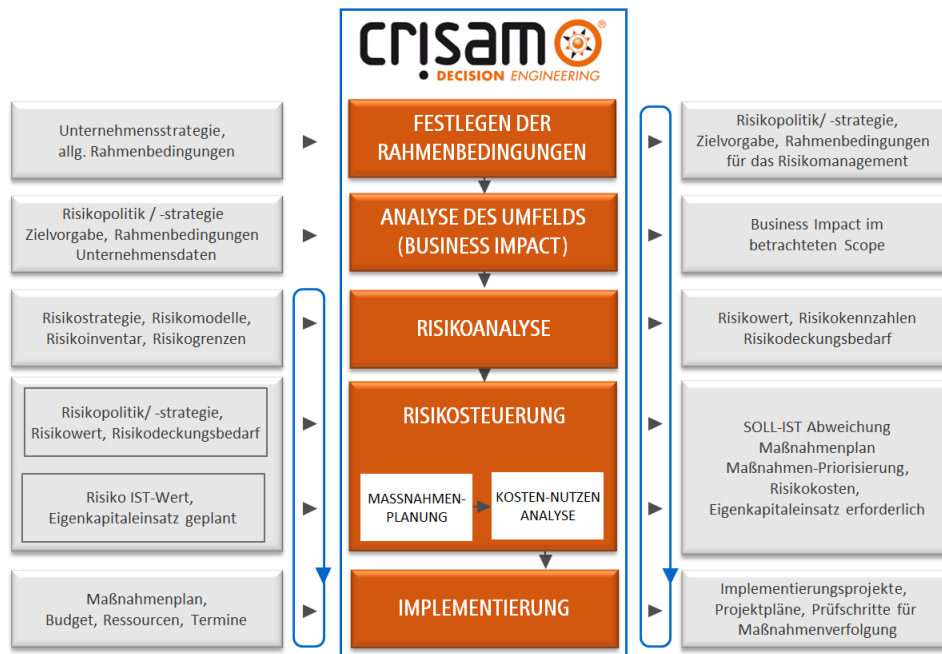


Abbildung 1: CRISAM[®] Vorgehensmodell

Aufgrund der beiden Rückkoppelungen kann der kaskadierte Regelkreis sowohl anlassbezogen auf technologische Veränderungen und auch Veränderungen der Bedrohungsprofile, als auch auf strategische Neupositionierungen des Unternehmens reagieren.

CRISAM[®] versteht sich aufgrund der modellhaften Abbildung der realen IT mit deren „Kundenbeziehungen“ als Zentrale des strategischen IT-Managements, denn:

1. CRISAM[®] stellt eine „Testumgebung“ für „Was wäre Wenn?“ Szenariotests zur Verfügung.
2. CRISAM[®] unterstützt durch die Möglichkeit einer Risikobewertung alternativer Varianten sowohl IT-Änderungen an bestehenden Strukturen, als auch Implementierungen von neuen IT-Projekten vor der Realisierung auf Risiken zu prüfen.
3. CRISAM[®] liefert aufgrund der Kenntnis aller Abhängigkeiten im Fehlerbaum einen wesentlichen Input für eine effiziente Business Continuity Planung.
4. CRISAM[®] unterstützt durch eine serviceorientierte Modellierung des Fehlerbaums und Aggregation von Service-Qualitäten das IT-Service- und Service Level Management.
5. CRISAM[®] liefert mit der monetären Risikoauswertung sowohl dem Entscheidungsträger realistische Werte für die Investitionsplanung, als auch dem unternehmensweiten Risikomanagement Prozess nachvollziehbare Bewertungen des IT-Risikos.

CRISAM[®] ist ein gesamthafter und zeitgemäßer Prüfstand, der eine „Gesundheitsvorsorgeuntersuchung“ Ihrer IT auf Basis anerkannter Normen und Standards durchführt und dem Entscheidungsträger Daten und Fakten für die Unternehmenssteuerung liefert.