

IT Governance

Definition, Standards & Zertifizierung

O. UNIV.-PROF. DR. A MIN TJOA; O. UNIV.-PROF. DR. DIMITRIS KARAGIANNIS

Gesetzliche Regularien wie Sarbanes-Oxley Act, Corporate Governance Kodex und Basel II verlangen von der IT nicht nur aus rechtlicher und betriebswirtschaftlicher, sondern auch aus technischer Sicht Rechenschaftsberichte über die effiziente und effektive Steuerung und Kontrolle. Dabei gilt es, Transparenz für IT-Service-Management zu schaffen und dadurch operationelle Risiken signifikant zu reduzieren. Durch die Etablierung von IT Governance kann dieses Ziel erreicht werden. International anerkannte Frameworks wie ITIL und COBIT bilden hierzu eine optimale Grundlage. Ziel muss es jedoch sein, Elemente dieser Standards in ein unternehmensweites Managementsystem zu integrieren, welches in das operative Geschäft eingebunden werden muss. Durch die Zertifizierung nach BS 15000 kann dieses Ziel erreicht und offiziell beglaubigt werden.

Definition

Allgemein werden unter IT Governance „Grundsätze, Verfahren und Maßnahmen zusammengefasst, die sicherstellen, dass mit Hilfe der eingesetzten IT die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden“ [1]. Gemäß dieser Definition sollte jede Organisation zu einem gewissen Grad über IT Governance-Mechanismen verfügen.

Zur Bestimmung des Reifegrads der IT Governance kann ein Modell herangezogen werden, das sowohl in Industrie als auch in der Wissenschaft als „IT Governance Maturity Assessment“ bekannt ist [2]. Es bewertet die Prozesse der IT Governance auf einer 5-stufigen Skala: initial, wiederholbar, definiert, gelenkt (managed) und optimiert. Im Durchschnitt befinden sich laut Studien die Unternehmen auf Stufe 2 (wiederholbar). 74 % der IT-Operationsbereiche wollen prozessorientiert agieren, 14 % sind bereits prozessorientiert aufgestellt, während 57 % sich in einem frühen Stadium befinden und aktuell ihre Prozessdefinitionen überprüfen.

Als typische Fallen bei der Implementierung von IT Governance werden u. a. die fehlende Fokussierung oder unzureichendes Investment in die Prozessarchitektur

und die Neugestaltung einzelner Prozesse, ohne Berücksichtigung eines Gesamtkonzepts, genannt.

Die Implementierung von IT Governance muss gemäß Forrester Research auf drei wesentlichen Elementen basieren [3]:

- **Struktur:** Wer trifft die Entscheidungen? Welche Organisationsstrukturen müssen geschaffen werden?
- **Prozesse:** Wie werden IT-Entscheidungen getroffen? Wie sind die Entscheidungsprozesse für den Vorschlag, die Bewertung, Durchführung und die Reihung von IT-Investitionen strukturiert?
- **Kommunikation:** Wie werden die Ergebnisse der Prozesse und Entscheidungen überwacht, gemessen und kommuniziert? Welche Mechanismen werden genutzt, um IT-(Investment)-Entscheidungen zu kommunizieren.

Frameworks, wie ITIL und COBIT, beschreiben dabei

nicht die konkrete Umsetzung, sondern definieren den Rahmen, die Anforderungen und die Ergebnisse des IT-Managements. Die Ausformulierung der operativen IT-Prozesse muss für jedes Unternehmen in Einklang mit den branchen- und unternehmensspezifischen Geschäftsprozessen erfolgen.

Standards und Best Practices

Es existiert kein „Off-the-Shelf-Framework“ für die Umsetzung von IT Governance. Allerdings gibt es eine Reihe an Standards und Best Practice-Ansätzen, die die Implementierung unterstützen. Die zwei anerkanntesten Frameworks sind ITIL und COBIT.

ITIL (Information Technology Infrastructure Library) stellt ein Set an Best Practices und Referenzprozessen in Textform zur Verfügung, um IT-Prozesse zu definieren



Abb. 1: IT Governance nach dem ITGI



Abb. 2: ITIL

und deren Betrieb zu sichern. ITIL wurde in den achtziger Jahren von der britischen Regierung entwickelt und beschreibt ein systematisches, professionelles Vorgehen für das Management von IT-Dienstleistungen. Der Standard stellt nachdrücklich die Bedeutung der wirtschaftlichen Erfüllung der Unternehmens-Anforderungen in den Mittelpunkt. Vor allem die Bereiche Service Delivery und Service Support gewinnen immer mehr an Bedeutung.

COBIT (Control Objectives for Information and related Technology) wurde von Revisoren aus der Industrie und der ISACA (Information Systems and Control Association) auf Basis bestehender Revisionsrichtlinien, Kontrollmodellen sowie branchenspezifischen Regularien und Richtlinien entwickelt. Dabei stützt sich das Framework auf die Anforderungen an Informationen aus den definierten Geschäftszielen und den damit einhergehenden, notwendigen IT-Ressourcen und -Prozessen. COBIT liefert 34 kritische IT-Prozesse, strukturiert in die Bereiche Planung und Organisation, Beschaffung und Implementierung, Betrieb und Unterstützung und Überwachung.

Zertifizierung

Den Best Practices von ITIL und COBIT fehlte es bisher an einem international anerkannten Gütesiegel. Eine Bestätigung von Effektivität und Effizienz des IT-Service-Managementsystems von Unternehmen kann neuerdings (seit 2002) durch die Norm BS 15000 attestiert werden.

BS 15000 wurde von der BSI (British Standards Institution), in enger Kooperation mit dem IT Service Management Forum (ITSMF) und zahlreichen Partnern aus Wirtschaft und öffentlicher Verwaltung entwickelt. Die Norm orientiert sich sehr stark an den ITIL Best Practices. Der erfolgsentscheidenden Integrationsmöglichkeit in ein unternehmensweites Managementsystem wurde durch den Abgleich mit existierenden Standards wie ISO 9001:2000 Rechnung getragen.

Dabei erfolgte vor allem die Einbindung eines nachhaltigen Verbesserungsprozesses (Plan-Do-Check-Act, PDCA), um effektive Steuerung und Kontrolle zu erreichen und einen kontinuierlichen Verbesserungsprozess zu garantieren.

BS 15000 unterstützt beim Design und letztendlich bei der kontinuierlichen Evaluierung nach der Einführung, während ITIL und COBIT vor allem bei der Umsetzung und beim laufenden Betrieb eine wesentliche Rolle spielen.

Branchenweit gilt BS 15000 als richtungweisend und gewinnt zunehmend an Bedeutung. Mit der geplanten Norm ISO 20000 wird das Regelwerk in Zukunft international noch mehr an Bedeutung gewinnen.

Neben BS 15000 existiert die auf Personen ausgerichtete ITIL-Zertifizierung mit drei möglichen Stufen (ITIL Foundation, ITIL Service Manager und ITIL Practitioner).

Die Zertifizierung sowohl von Unternehmen als auch von Personen kann ausschließlich durch akkreditierte Zertifizierungsinstitutionen durchgeführt werden. In Österreich wird diese Rolle derzeit von ausländischen Institutionen übernommen. ■



Abb. 3: Das COBIT-Framework

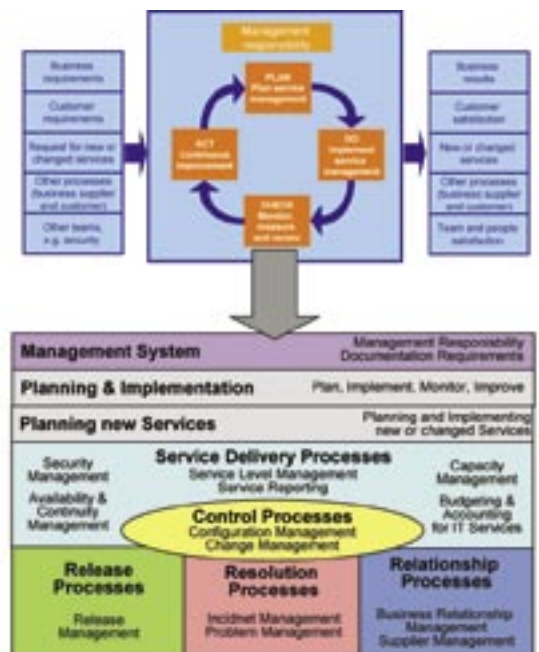


Abb. 4: Integration des PDCA



Abb. 5: Einführung und Zertifizierung

Literatur

- [1] Meyer, M. et al. (2003): IT-Governance: Begriff, Status quo und Bedeutung, Wirtschaftsinformatik, 45, S. 445-448.
- [2] Guldentops, E. et al. (2002): Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool, Information Systems Control Journal, Vol. 6, ISACA.
- [3] Symons, C. (2005): IT Governance Framework, Forrester Best Practices March 29, 2005.
- [4] Office of Government Commerce (OGC): <http://www.ogc.gov.uk>
- [5] IT Governance Institute: <http://www.itgi.org/>
- [6] COBIT - Information Systems Audit and Control Association (ISACA): <http://www.isaca.org/cobit/>
- [7] IT Infrastructure Library: <http://www.itil.org>
- [8] IT Service Management Forum

Kontakt

In der OCG befindet sich derzeit eine Arbeitsgruppe zum Thema IT Governance in Gründung

Leitung:

O. Univ.-Prof. Dr. Dimitris Karagiannis
O. Univ.-Prof. Dr. A Min Tjoa,

Assistenz: Mag. Hans-Georg Fill
Kontakt: dk@ocg.at